A Survey on Security Issues and Solutions at Different Layers of Cloud Computing

Chirag Modi[1], Dhiren Patel[1], Bhavesh Borisaniya[1],

Avi Patel[2], Muttukrishnan Rajarajan[2]

[21]*NIT Surat, India*

[2]*City University London, UK*

Abstract

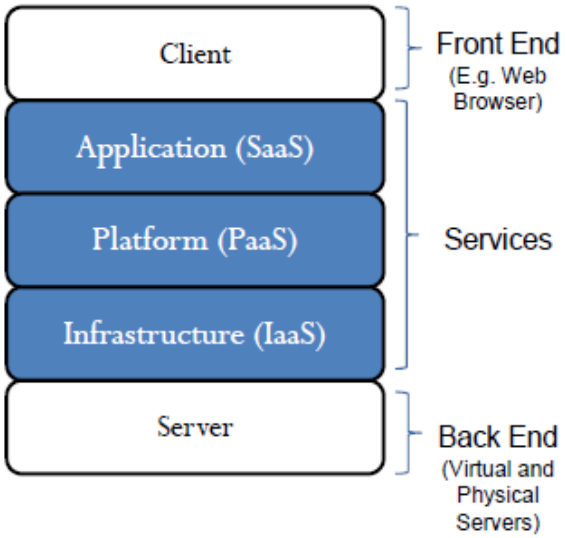
Cloud computing offers scalable on-demand services toconsumers with greater flexibility and lesser infrastructure investment. Since Cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existent in these protocols as well as threats introduced by newer architectures raise many securityand privacy concerns. In this paper, we survey factors affecting Cloud computing adoption, vulnerabilities,and attacks, and identify relevant solution directives to strengthen security and privacyin Cloud environment.

Keywords: Cloud Computing; Virtualization; Security; Privacy; Vulnerabilities

1. Introduction

Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software [1]. NIST defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction" [2]. It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use. It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction and rapid deployment are main factors that drive industries to utilize Cloud servicesand allow them to focus on core business concerns and priorities rather than dealing with technical issues. According to [3], 91% of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment.

As shown in Fig. 1, Cloud services are offered in terms of Infrastructure (IaaS), Platform (PaaS) and Software (SaaS). It follows a bottom up approach wherein at the infrastructure level; machine power is delivered in terms of CPU consumption to memory allocation. On top of it, lies the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level resides the application layer, delivering

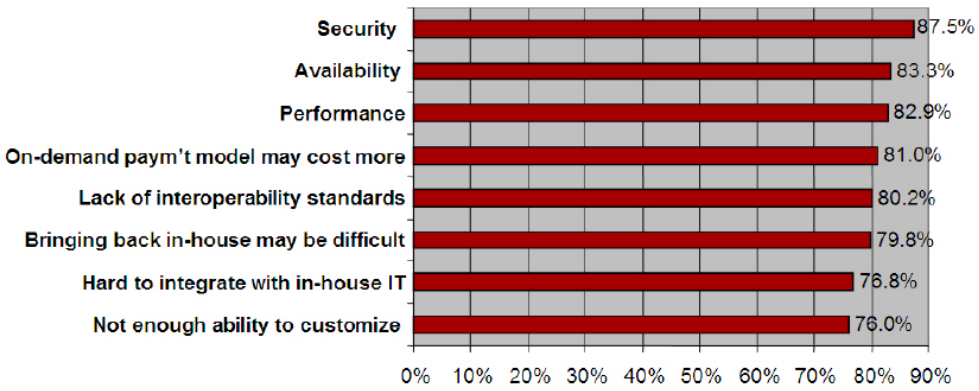


software outsourced through the Internet, eliminating the need for in-house maintenance of sophisticated software[4]. At application layer, the end users can utilize software running at a remote site by Application service providers (ASPs). Here, customers need not to buy and install costly software. They can again pay for only they use and their concerns for maintenanceare cut off. All the software or applications are kept under the control of service provider.

Fig. 1.Cloud service stack.

1.1. Need for Security and Privacy in Cloud Computing

Cloud computing is a merger of several known technologies including grid and distributed computing, utilizing Internet as a service delivery network. Public Cloud environment is extremely complex when compared



to a traditional data center environment [2]. Under the paradigm of Cloud computing, an organization surrenders

direct control over major aspects of security, conferring a substantial level of trust onto the Cloudprovider. A survey regarding use of Cloud services made by IDC says that security is the greatest challenge of the Cloud as shown in Fig. 2 [5].

Fig. 2.Results of IDC ranking security challenges [5].

Virtual environments areused in Cloud to achieve multi-tenancy. Vulnerabilities in virtual machines [6] pose direct threat to the privacy and security of the Cloud services. Factors crippling usage of Cloud services are live migration of data over the Internet, entrusting a provider for data security and privacy, vulnerabilities at browser's API, vulnerabilities in network, export regulations for encryption etc.

Shared and distributed resources in Cloud systems make it difficult to develop security model for ensuring the data security and privacy. Due of transparency issues, no Cloud provider allows its customers to implement intrusion detection or security monitoring system extending into the management services layer behind virtualized Cloud instances. Customers may not be aware of detailed security-incidents, vulnerability, or malware reports. For example, through back channel, attackers may be able to access the content of Cloud instances and fix a kernel level rootkit [7]. Attacks on "physical level" such as reading out the random access memory of the virtualized hosts or subverting the virtualization layer [8], are known to the community. Even the host system providing the data can no longer be fully trusted since Cloud provider owns the physical resources.

Cloud service providers often establish a Service Level Agreement (SLA) to highlight security and privacy of the related service. To an extent, there is a lack of a standard methodology to design a SLA. The authors in [9] presented SLA about provided services and the waivers. These waivers do not really help the customers fulfilling their losses. Cloud providers like Amazon, Google, Salesforce etc. rely on detailed SLAs to guarantee security and other parameters for customers. E.g., Amazon's EC2 provides abstraction of virtual hardware to its users, covering all types of failures including operator node failure and software node failure [10]. In future, SLA based Google App Engine would likely to manage all causes of failures.

Rest of the paper is organized as follows: Section 2 discusses vulnerabilities, threats and attacks relevant to Cloud. A survey on security issues at different levels inCloud and their existing solutions are provided in section 3. Section 4discussesresearch directionswith conclusionsand references at the end.

2. Vulnerabilities, Threats and Attacks to Cloud Computing

In Cloud, existing vulnerabilities, threats and associated attacks raises several security concerns. Vulnerabilities in Cloud can be defined as the loopholes in security architecture of Cloud,which can be exploited by an adversary via sophisticated techniques to gain access of network and other resources. A threat in Cloud is a potential (or actual adverse) event, that may be malicious or incidental (such as the failure of a storage device), compromising Cloud resources [11]. An attack is an action to harm Cloud resources. Exploitation of vulnerabilities would affect the availability and productivity of Cloud computing.

2.1. Vulnerabilities in Cloud Environment

In this section, we discuss major vulnerabilities specific to Cloud, which pose serious threats to Cloud computing.

2.1.1. Vulnerabilities in virtualization/ multi tenancy

Virtualization/ multi-tenancy serves as the basis for Cloud computing architecture. There are mainly three types of virtualization are used: OS level virtualization, application based virtualization, and Hpervisor based virtualization. In OS level virtualization, multiple guest OSs are running on a hosting OS that has visibility and

control on each guest OS. In such type of configuration, attacker can get control on the entire guest OSs by compromising the host OS. In application based virtualization, virtualization is enabled on the top layer of host OS. In this type of configuration, each VM has its guest OS and related applications. Application based virtualization also suffers from same vulnerability as in OS based vulnerabilities. Hypervisor or virtual machine monitor (VMM) that is just like code embedded to host OS. Such code may contain native errors. This code is available at boot time of host OS to control of multiple guest OSs. If hypervisor is compromised, then the entire controlled guest OSs can be compromised. Vulnerabilities in virtualization or hypervisor allows attacker to perform cross-VM side-channel attacks and DoS attacks. For instance, a malformed code in Microsoft's Hyper-V is run by an authenticated user in one of the VM caused a DoS attack [53]. In VMware Workstation, an attacker cause an error to store some malformed data, which enabled a DoS attack on the host OS.

Cloud providers thrive to maintain maximum level of isolation between Virtual machine (VM) instances including isolation between inter user processes. By compromising the lower layer hypervisor, attacker can gain control over installed VMs. BLUEPILL [12], SubVirt [13] and DKSM [14] are attack examples on virtual layer. Through these attacks, hackers can able to modify the installed hypervisor and gain control over the host.

Another incident is vulnerability found in the memory management of Microsoft virtual pc. This has resulted into user programs running in guest Operating system getting read/write access to bypass security mechanisms like Data Execution Prevention (DEP), Safe Structured Error Handling (SafeSEH) and Address Space Layout Randomization (ASLR)[15]. Input validation error in Xencan be exploited by root user of a guest domain to execute arbitrary commands in domain 0 (Host domain).

2.1.2. Vulnerabilities in Internet protocol

Vulnerabilities in Internet protocols may prove to be an implicit way of attacking Cloud system, that include common types of attacks like man-in-the-middle attack, IP spoofing, ARP spoofing, DNS poisoning, RIP attacks and flooding. ARP poisoning is the one of the known vulnerabilities in Internet protocols. Using this vulnerability, malicious VM can redirect all the inbound/outbound traffic of a co-located VM to the malicious VM since ARP does not require Proof-of-Origin. HTTP is a web application protocol that requires session state. Many techniques are used for session handling. However, they are vulnerable to session-riding and session hijacking. These vulnerabilities are certainly relevant to Cloud.TCP/IP has some "unfixable flaws" such as "trusted machine" status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered [16].Such attack scenario becomes critical for public Clouds, as the general backbone for Cloud provision is the Internet.

2.1.3. Unauthorized access to management interface

In Cloud, users have to manage their subscription including Cloud instance, data upload or data computation through a management interface e.g. AWS management console [17]. Unauthorized access to such a management interface may become very critical for a Cloud system. Unlike traditional system, higher number of administrators and users for a Cloud system increases probability for unauthorized access. Advances in crypto analysis breaks security provided by cryptographic algorithms, which may turns strong encryption into weak encryption. Insecure or out dated cryptography vulnerabilities are also relavant to Cloud since it is not thinkable to use Cloud without using cryptography to protect data security and privacy in the cloud. For example, a cryptographic hole discovered in Amazon'sEC2 management interface by performing signature-wrapping and cross site scripting (XSS) attacks, where interfaces used to manage Cloud resources are hijacked. Such attacks allow attackers to create, modify and delete machine images, and change administrative passwords and settings[18].Recent research [19]has shown that, successfully attacking a Cloud control interface can allows an attacker to gain a complete power over an account including all stored data.

2.1.4. Injection vulnerabilities

Vulnerabilities like SQL injection flaw, OS injection flaw and Lightweight Directory Access Protocol (LDAP) injection flaw are used to disclose application components. Such vulnerabilities are outcome of defects in design and architecture of applications. These data may be of organization's applications or private data of other organization's applications residing on same Cloud.

2.1.5. Vulnerabilities in browsers and APIs

Cloud providers expose a set of software interfaces (or APIs)that customer can use to manage and interact with Cloud services. Service provisioning, management, orchestration, and monitoring are performed using these interfaces via client (e.g. Web browser). Security and availability of Cloud services depend on the security of these APIs. Examples of browser based attacks (HTML based services) are- SSL certificate spoofing, attacks on browser caches and phishing attacks on mail clients [20]. APIs should support all key agreement methods specified in WS-Security family of standards, since the resulting keys must be stored directly in the browser. This could be done by enhancing security of APIs, e.g. PKCS#11.

For providing security to Cloud services and resources, these vulnerabilities should be tested (and removed) before delivering Cloud services to user. In Table 1, we summarize vulnerabilities relevant to Cloud and their associated effects.

Table 1.Effects of vulnerabilities in Cloud and consequent effects.

Vulnerability	Consequent effects
Unauthorized Access to Management Interface	An intruder can gain access control and can take advantage of services to harbor attacks. Access to administrative interface can be more critical.
Vulnerabilities in Internet Protocol	Allow network attacks like ARP spoofing, SYN-flood, DoS/DDoS etc.
Injection Vulnerabilities	Unauthorized disclosure of private data behind applications.
Vulnerabilities in Virtualization	Bypassing the security barriers can allow access to underlying hypervisor.
Vulnerabilities in Browsers and APIs	Allow unauthorized service access.

2.2. Threats to Cloud Computing

Cloud security alliance in [20] presented a primary draft for threats relevant to the security architecture of Cloud services. We discuss here some potential threats relevant to Cloud and relevant mitigation directives.

2.2.1. Changes to business model

Cloud computing changes the way of IT services that are delivered. As servers, storage and applications are provided by off-site external service providers, organizations need to evaluate the risks associated with the loss of control over the infrastructure. Data traversing over geographical boundaries are subjected to different federal laws. This is a prime threat which hinders the usage of Cloud computing services. A reliable end-to-end encryption and appropriate trust management scheme can simplify such threat to some extent.

2.2.2. Abusive use of Cloud computing

Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over attackers, malicious users, spammers that can take advantages of trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for strong attacks. Areas of concern include password and key cracking, launching dynamic attack points, DDOS, Captcha solving farms etc. Such threats affect the IaaS and

PaaS service models. For protection, initial registration should be through proper validation/verification and through stronger authentication. User's network traffic should be monitored comprehensively.

2.2.3. Insecure interfaces and API

Cloud provider often exposes a set of APIs to allow its customers to design an interface for interacting with Cloud service. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such interfaces allow vulnerabilities (in the existent API) to move to the Cloud environment. Improper use of such interfaces would often pose threats such as clear-text authentication, transmission of content, improper authorizations etc. Such type of threat may affect the IaaS, PaaS and SaaS service models. This can be avoided by using proper security model for Cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.

2.2.4. Malicious insiders

Most of the organizations hide their own policies regarding the level of access to employees, recruitment procedure for employees. However, using higher level of access, an employee can gain access to confidential data and services. Due to lack of transparency into Cloud provider's process and procedure, insiders often have the privilege. Insider activities are often bypassed by a firewall or Intrusion Detection system (IDS) assuming it to be a legal activity. Trusted insider may turn into an adversary. In such a situation, insiders can cause considerable effect on Cloud service offerings. E.g. malicious insiders can access confidential data and gain control over the Cloud services with no risk of detection [20]. This type of threat may be relevant to SaaS, PaaS and IaaS. To avoid this, more transparency is required into security and management process including compliance reporting and breach notification.

2.2.5. Shared technology/ Multi-tenancy nature

In multi-tenant architecture, virtualization is used to offer shared on-demand services. Same application is shared among different user having VM access. But as presented earlier, vulnerabilities in a hypervisor allow malicious user to gain access and control of legitimate users' VMs. IaaS services are delivered using shared resources, which may not be designed to provide strong isolation for multi-tenant architectures. This may affect the overall architecture of Cloud by allowing one tenant to interfere into the other and affecting its normal operation. This type of threat affects IaaS. Implementation of SLA for patching, strong authentication and access control to administrative tasks are some of the solutions to address this issue.

2.2.6. Data loss and leakage

Data may be compromised in many ways. This may include data compromise, deletion or modification. Due to dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. Examples of such threats are lack of authentication, authorization and audit control, weak encryption algorithms, weak keys, risk of association, unreliable datacenter, and lack of disaster recovery. This threat can be applicable to SaaS, PaaS and IaaS. Solutions include security of API, data integrity, secure storage for used keys, data backup and retention policies etc [20].

2.2.7. Service hijacking

Service hijacking may lead to redirect client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials and passwords may pose service or account hijacking. This threat affects IaaS, PaaS and SaaS. Some of the solutions to address this threat include security policies, strong authentication and activity monitoring.

2.2.8. Risk profiling

Cloud offerings make organizations less involved with ownership and maintenance of H/W and S/W. This offers significant advantages. However, this makes them unaware ofinternal security procedures, security compliance, hardening, patching, auditing and logging process etc and expose organization to greater risk. To avoid it, Cloud provider should disclose partial infrastructure details, logs and data. There should be monitoring and alerting system.

2.2.9. Identity theft

Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator's actions. Relevant security risks include weak password recovery workflows, phishing attacks,key loggers etc. This affects SaaS, PaaS, and IaaS. Solution is to use strong authentication mechanism.

In Table 2, we summarize threats to Cloud and directives to avoid them.

2.3. Attacks on Cloud Computing

By exploiting vulnerabilities in Cloud, adversary can be able to launch the following attacks on Cloud computing.

2.3.1. Zombie attack

Through Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. This type of hosts called *zombies*. In Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. Attacker can flood the large number of requests via *zombies*. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services. Cloud may be overloaded to serve a number of requests and exhausted, which cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker's flooded requests cannot serve valid user's requests. Better authentication/authorization and IDS/IPS can provide protection against such an attack.

In the presence of flooding or *zombie* attack, Cloud provider provides more computational power to serve the huge number of requests (including *zombie* requests). By attacking on a single server, the attacker can cause an unavailability of service. Such an attack is called DoS attack. It may affect other services. If server's resources are completely exhausted by processing the flood requests, other service instances on the same server are no longer able to perform their intended tasks. Finally, whole Cloud system reaches a state of full loss and cannot be able to serve any service request coming from valid users. Such type of distributed attack is called DDoS attack. A denial of service attack against BitBucket.org, a code hosting site, caused an outage of over 19hours of downtime during an apparent denial of service attack on the Amazon Cloud infrastructure [21]. If an attacker cannot be identified, the flooded service raises the user bill for the workload caused by the attacker. To prevent Cloud from such attacks, Intrusion detection System (IDS)/Intrusion Prevention System (IPS) can be used.

Table 2.Summary of threats to Cloud and solution directives.

Threats	Effects	Affected Cloud services	Solution directives
Changes to business model	Loss of control over Cloud infrastructure.	SaaS, PaaS and IaaS.	• Provide control and monitoring system on offered services.
Abusive use of Cloud computing	Allows intruder to launch strongerattacks due to anonymous signup, lack of validation, service fraud, and ad-hoc services.	PaaS and IaaS.	• Stronger registration and authentication. • Comprehensive monitoring of network traffic.
Insecure interfaces and API	Poses threats like clear-text authentication, transmission of content; improper authorizations etc.	SaaS, PaaS and IaaS.	• Ensure strong authentication and access control mechanism with encrypted transmission.
Malicious insiders	Insider malicious activity bypassing firewall and other security model.	SaaS, PaaS and IaaS.	• Provide transparency to security and management process. • Use compliance reporting and breach notification.
Shared technology issues	Allows one user to interfere other users' services by compromising hypervisor.	IaaS.	• Use strong authentication and access control mechanism to administrative task. • Inspect vulnerability and configuration.
Data loss and leakage	Confidential data can be compromised, deleted or modified.	SaaS, PaaS and IaaS.	• Use secure APIs, encryption algorithms and secure keys. • Apply data retention and backup policies.
Service hijacking	User accounts and service instances could in turn make a new base for attackers.	SaaS, PaaS and IaaS.	• Use security policies, strong authentication mechanism and activity monitoring.
Risk profiling	Internal security procedures, security compliance, configuration hardening, patching, auditing and logging may be overlooked.	SaaS, PaaS and IaaS.	• Disclose partial logs, data and infrastructure detail. • Use monitoring and alerting system for data breaches.
Identity theft	Attacker can get valid user's identity to access that user's resources; and obtain credit or other benefits in that user's name.	SaaS, PaaS and IaaS.	• Use strong passwords and authentication mechanism.

2.3.2. Service injection attack

Cloud system is responsible for determining and eventually instantiating a free-to-use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user. An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. Cloud malware affects the Cloud services by changing (or blocking)Cloud functionalities. Consider a case wherein adversary creates his/her malicious services like SaaS,PaaS or IaaS and adds it to the Cloud system. If adversary succeeds to do this, then valid requests are redirected to the malicious services automatically. To defend against this type of attack, service integrity checking module should be implemented. Strong isolation between VMs may disable attacker from injecting malicious code in neighbor's VM.

2.3.3. Attacks on virtualization

There are mainly two types of attacks performed over virtualization: VM Escape and Rootkit in hypervisor.

VM Escape: In this type of attack, an attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows attacker to interact directly with the hypervisor. Therefore, VMEscape from the isolation is provided by the virtual layer. By VM escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

Rootkit in Hypervisor: VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS considers that it is running as the host OS, with the corresponding control over the resources, but it is not there. Hypervisor also creates a cover channel to execute unauthorized code into the system. This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system.

2.3.4. Man-in-the Middle attack

If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, attacker can be able to access the data communication among data centers. Proper SSL configuration and data communication test between authorized parties can be useful to reduce the risk of man-in-the-middle attack.

2.3.5. Metadata spoofing attack

In this attack, an adversary modifies or changes service's WSDL file where descriptions about service instance are stored. If the adversary succeeds to interrupt service invocation code from WSDL file at delivering time, then this attack can be possible. To disable such an attack, information about services and applications should be kept in encrypted form. Strong authentication (and authorization) should be enforcedfor accessing such critical information.

2.3.6. Phishing attack

Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In Cloud, it may possible that an attacker use the use the cloud service to host a phishing attack siteto hijack account and services of other users in cloud.

Wrapping attackIn Cloud, user requests of his/her VM using web browser or a thin client. Web server generates SOAP message (that contains XML based information that will be exchanged between the server and browser) for this request. Before communication between server and browser, such XML based information are signed using signature values. All the information regarding destination are contained in SOAP header. In wrapping attack, an adversary duplicates the body of the message and sends to the server as a legitimate user during the translation of the SOAP message. The signature value in duplicated message and integrity of the message will be valid at server. Finally, an adversary will be able interrupt the Cloud services by running malicious code.

2.3.7. Cross site scripting

In this type of attack, user enters correct URL of a website and attacker on the other site redirect the user to its own website and gets its credentials or sensitive data of the user. This attack allows attacker to perform buffer overflows, DOS attacks and malicious software injection in to the web browsers.

2.3.8. Backdoor channel attack

It is a passive attack, which allows hackers to gain remote access to the compromised system.Using backdoor channels, hackers can be able to control victim's resources and can make it *zombie* for attempting DDoS attack. It can also be used to disclose the confidential data of victim. Better authentication and isolation between VMs can provide protection against such attacks.

\

Table 3 summarizes attacks, their effects and mitigation directivTable 3.Summary of attacks onCloud and its mitigation directives.

Attack type	How? (Attack Surface/Procedure)	Service affected	Effects	Mitigation techniques
Zombie Attack, DoS/DDoS Attack	• By compromising valid user's VMs. • Through direct/indirect flooding to host. • VM level attack/ Hypervisor level attack/ Network level attack. •	SaaS/ PaaS/IaaS	• Affects service availability. • May account for false service usage..	• Better authentication and authorization. • IDS/IPS. •
Service Injection Attack	• Malicious service injected through accessing service identification files. • Application level attack/ VM level attack.	PaaS	• Malicious service provided to user instead of valid service. • Affects service integrity.	• Check service integrity using hash function. • Strong isolation between VMs. • Web service security. • Use secure web browsers and APIs.
Attacks on virtualization VM Escape and attack on hypervisor	• By compromising hypervisor. • By escaping virtualization layer. • VM level attack/ Hypervisor level attack	IaaS	• Allows attacker to gain control over other user's VM.	• Use of secure hypervisor. • Monitor activities at hypervisor. • VM isolation required.
Man-in-the Middle attack	• By accessing data communication between two parties.	SaaS/PaaS/ IaaS	• Affects the data security and privacy.	• Proper configuration of SSL required.
Metadata Spoofing attack	• Modifying web service description file such as WSDL. • Application level attack.	SaaS/PaaS	• Abnormal behavior of deployed services. • Affects service confidentiality.	• Strong isolation between VMs.
Phishing attack	• By allowing users to access fake web link.	SaaS/PaaS/ IaaS	• Affects the privacy of user's sensitive information that should not be revealed.	• Identify the spam mails.
Wrapping attack	• By duplicating body of SOAP header where authentication information are stored.	SaaS	• Allows attacker to intrude Cloud service and run malicious code.	• Use proper signature mechanism. • Use proper configuration of SSL.
Cross site scripting	• By redirecting user from valid URL to attacker's web site.	SaaS	• This allows attacker to perform various attacks like buffer overflow, DoS attack etc.	• Use proper configuration of SSL. • Use anti malware software.

Backdoor channel attacks	• By compromising valid user's VMs. • VM level attack/ Hypervisor level attack.	IaaS	• Provides rights for accessing victim's resources. • Can affect the service availability and data privacy.	• Better authentication and authorization. • Strong isolation between VMs.

3. Security Issues at Different Levels inCloud

Above presented threats/attacks directly or indirectly affect the confidentiality, integrity and availability of Cloud resources as well as services at different layers and raises several security concerns as shown in Fig. 3. In Fig. 3, we explore each layer (as shown in Fig. 1) of Cloud with associated security concerns. Therefore, we classified security concerns based on different levels viz; application level, network level, data storage level, virtualization level, authentication and access control level, trust level, compliance, audit & regulations level. Application level risks directly affect the security of Cloud applications at user layer. Network level threats or intrusions affect the overall security of Cloud services, data as well as physical resources. One can easily gain access of other users resources or services by monitoring network traffic in Cloud. Attacks on data storage directly affects the security of user's data (at rest or in-transit) including application data, sensitive data etc. Virtualization level risks directly affect the data storage level security and application level security. Authentication and access control level risks affects the security of legitimate user's services and resources. Trust level risks directly affect the security of data-in-transit and migrating applications. Auditing, compliance and regulations levels threats directly affect the user's data privacy, confidentiality and integrity.

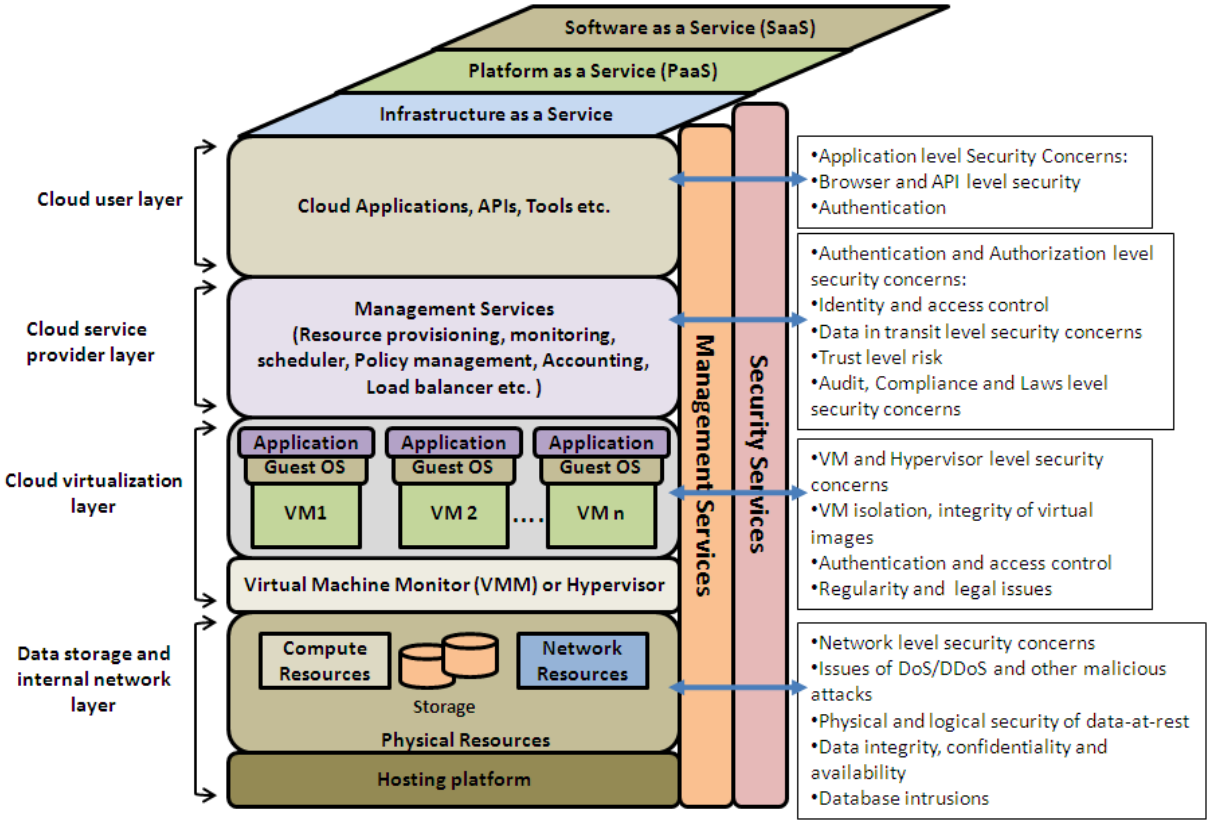


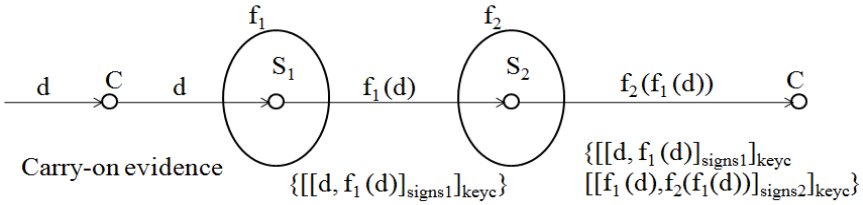
Fig.3.A detailed architecture of Cloud with security concerns at each layer.

3.1. Application Level Security Issues

Application level security refers to the usage of software and hardware resources for providing security to applications such that the attackers are not able to get control over applications and make desirable changes to their format. Since Web applications and SaaS are tightly coupled in providing Cloud services, the security and availability of general cloud services are dependent upon the security of Web browsers, APIs, vulnerability free applications. A Web browser is the platform independent client program that is mostly used to access the cloud services (SaaS), web applications/pages or web 2.0. It uses SSL/TLS protocols for secure transmission and authentication of data. Therefore, attacks on browser based Cloud authentication directly affect the security of Cloud applications. Any attacker can get access of other user's XML tokens (authentication related credentials in browser) and accesses the services of victim. One of the solutions viz; XML signature and XML encryption can be used to enhance browser security. However, XML Signature Wrapping attack enables attacker to change the content of the signed part without invalidating the signature. E.g., Using XML signature wrapping attack (due to exploitation of cross-site XSS scripting vulnerabilities), it is possible to hijack some live Amazon Web Services (AWS) accounts (that uses SOAP and REST interfaces) [54].Therefore XML signature or XML Encryption fails to provide browser level security. To address wrapping attack, authors in [55] recommended the use of a redundant bit (STAMP bit) with the SOAP header. If any adversary infers the message during transmission, the STAMP will be changed. At server side, first STAMP bit is checked and if changed STAMP bit is found, then in the browser, new signature value is generated that sent back to the server to modify the authenticity checking. Using this approach, an adversary cannot interrupt the customer request with a duplication of the SOAP message

because the previous signature value is already altered. For this purpose, only a random signature value generator is needed in the browser end and only the extra message overhead of one bit is required for an authenticity check. However, such approaches are not applied to current Cloud systems and it is still an open challenge to provide a sufficient browser level security.

L. Hu et al. [56] presented an ontology-based Semantic Access Control Policy Language (SACPL) for describing access control policies (ACPs) in cloud computing environment. In this approach, syntax elements of XACML, such as subject, object, action and attribute variables, are annotated with semantic information using the Access Control Oriented Ontology System (ACOOS) and some syntax elements are added such as priority and confidentiality. This approach can solve the problem of semantic interoperability and mutual understanding on the distributed access control policies of resources when cross organizational is involved. However, it is



mentioned that this approach does not provide automatic conflict resolution for rules or policies and semantics-based access control mechanism for variable granularity [56].

M .H. Diallo et al. [57] proposed an approach that extends middleware by incorporating CloudProtect, Cloudprotect stores user's application data in encrypted form. It protects privacy of user's application data. Some application requires access to the data in plain text format. Therefore it is cumbersome to encrypt and decrypt data. CloudProtect maintains the policies defining which data should be in plaintext form and which data should be encrypted on server. The policies are defined based user behavior. It offers key management and secure sharing of data. However, it is mentioned that the feasibility of this approach is not analyzed for Cloud applications.

Otherkey security issues at application level are Service Availability and Integrity of workload state.

3.1.1. Service availability

Temporary or permanent loss of services and DoS/DDoS attacks are main threats affecting availability of Cloud services. For better QoS, services should be available as promised when they are requested. There are few incidents reported in literature. Database cluster failure caused at Salesforce.com [23]. In 2011 (February 27), Gmail goes down for few hours and due to service disruption, 0.29% of Gmail users affected and lost their previous emails and other data [24]. On 28th March 2011, thousands of users registered at Intuit company (which offers financial and tax preparation software and related services) were experienced an outage for 2 to 5 days during change in network configuration and scheduled maintenance. As a result, customers were blocked to access offered services [24].To address such issue, proper configuration of an IDS/IPS can be investigated.

3.1.2. Integrity of workload state

The integrity for state of a workload should be preserved to ensure expected results. Applications involving workflows are required to store temporary results of computation at different levels. There is no standard mechanism used to secure such sensitive files. If these sensitive files are disclosed to attacker, he/she may be able to threaten the expected behavior of application. A provenance based approach [25] can be used for securing application data flow among different sites. This approach provides confidentiality and integrity for data flow processing applications. As shown in Fig. 4 [25], composer (C) encrypts information regarding flow of data. At each hop (S_1) decrypts the next hop's (S_2) information and send data. Here, a single hop cannot see the whole

topology. Malicious hop cannot be able to exploit entire flow of data. This approach can be used to provide a solution for integrity of data flow application delivery in Cloud.

Fig. 4.Dataflow processing in provenance based approach [25].

3.2. Network Level Security Issues

Network is the backbone of Cloud and hence vulnerabilities in network directly affect the security of Cloud. As shown in Fig. 5, security issues at network level should be considered in terms of both external and internal networks. An Adversary outside the Cloud network often performs DoS or DDoS attacks to affect the availability of Cloud services and resources. DoS/DDoS attacks reduce the bandwidth and increases the congestion causing poor service to the users. Due to distributed nature of Cloud, it is hard to prevent DoS/DDoS and Economic Denial of Sustainability (EDoS can be called as HTTP and XML based DDoS) [58] attacks.

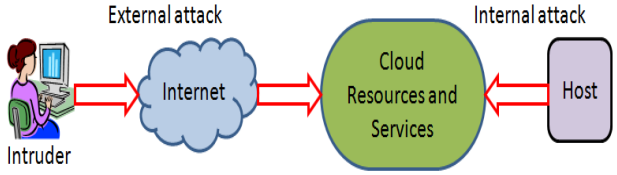


Fig. 5.An abstract view of network layer threat model for Cloud.

Some common attacks at network layer are DNS poisoning attack, Sniffer attack, Port scanning, Cross site scripting, ARP spoofing, IP spoofing and phishing attack, which are executed to gain access of Cloud resources. Internal network attacker (authorized users or users within cloud network) can easily get access to other user's resources without being detected. An insider has higher privileges and knowledge (related to network, security mechanism and resources to attack) than the external attacker. Therefore, it is easy for an insider to penetrate an attack than external attackers. Major security issues at network level include vulnerabilities in Internet protocols, authorization and authentication, intrusions, backdoor attack, session hijacking and clear data transmission. To address some of the issues at network level, major Cloud providers (like Amazon, Window Azure, Rack Space, Eucalyptus etc.)are running their applications behind firewall. However, it only provides security at boundary of network and cannot detect internal attacks. Network based intrusion detection system (NIDS) can be integrated to address some of the security issues. However, an NIDS should be configured for detecting external intrusions as well as internal intrusions. It should be also capable of detecting intrusions from encrypted traffic. In following, we see the existing research efforts to address network security issues in Cloud.

Through experiments and implementation, authors in [26] surveyed about the security solutions that can be applied to detect ARP spoofing attacks. They concluded that XArp 2 [27] tool is an efficient security solution that can accurately detect ARP spoofing attacks.In [59], we discussed existing NIDS approaches to Cloud. For example, C. C. Lo et al. [28] introduced a snort based intrusion detection system framework for Cloud system. As shown in Fig. 6 [28],an IDS module is installed on each region of Cloud environment. If an intrusion is detected at any region, it alerts other regions by using cooperative agent. Other regions cooperatively compute severity of that and then differentiate it as an attack or normal activity based on a threshold.

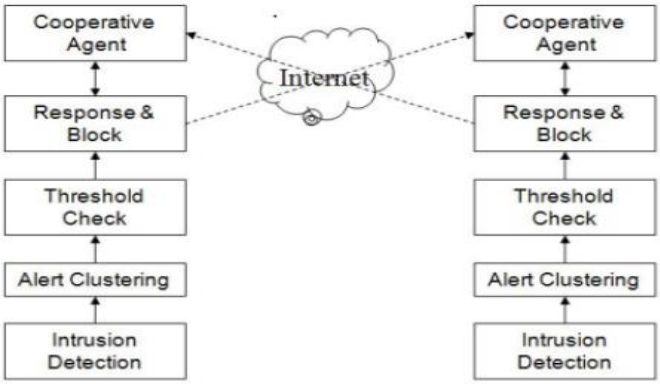


Fig. 6. Block diagram of cooperative agent based approach [28].

This approach is suitable for preventing Cloud system from single point of failure caused by DDoS attack. However, it needs substantial computational effort. A. Bakshi and Yogesh [29] proposed a method to secureVMs in Cloud from DDoS attack using an IDS. In this approach, snort based NIDS tool is installed on VM. If any suspicious activity is detected, it notifies the source IP of that activity and blocks packets coming from that IP. If DDoS attack is found, it transfers the service running on affected VM to another VM and blocks all the packets.

Mazzariello et al. [60] presented Snort based misuse detection in open source Eucalyptus Cloud environment. In this approach, Snort is deployed at a primary controller managing cloud instances called cloud controller as well as on the physical machines (hosting virtual machines) to detect intrusions coming from external networks. This approach solves the problem of deploying multiple instances of IDS. Although it is a fast and cost effective solution, it can only detect known attacks since only Snort is involved.

Sandaret al. [58] introduced a new type of DDoS attack, called Economic Denial of Sustainability (EDoS) in Cloud services and proposed a solution framework for EDoS protection. EDoS attack can be called as HTTP and XML based DDoS attack. EDoSprotection framework uses firewall and puzzle server to detect EDoS attack. A firewall is used to detect EDoS at the entry point of Cloud, whereas the puzzle server is used to authenticate the user. In this work, the authors demonstrated EDoS attack in the Amazon EC2 Cloud. However, it is not an efficient solution since it uses only traditional firewalls. Research is still needed to detect EDoS attacks in the Cloud.

F. Y. Lueet. al [30] integrate an intrusion detection system into a Grid, which uses existing grid resources for detecting strong DDoS attacks. In this approach, traffic from multiple switches is collected by multiple dispatchers and is sent for intrusion detection using scheduler. Scheduler forwards that traffic to intrusion detector, if load on any detector is low. This solution is used to overcome possible performance bottlenecks and deals with the distribution of load which requires several nodes to be utilized.

To overcome limitations existing in above presented approaches, further work related to NIDS is needed to provide fully secure network environment in Cloud. One another challenging problem related to Cloud-NIDS is the monitoring and capturing network traffic. This is due to the multi-tenancy and distributed nature of Cloud computing.

3.3. Data Storage Level Security Issues

Following aspects of data security are still open challenges: Data-in-transit, Data-at-rest, Data Lineage, Data Remanence, Data Provenance, Data Recovery, Data location, Data breaches and investigative support.

In case of data-in-transit, adversary in network affects the confidentiality and integrity of data. The biggest risks for data-in-transit include poor encryption technology and network protocols. Simply going for an encryption technology does not serve the purpose.

Data at rest (stored in Cloud storage) need physical, logical and personnel access control policies. Some examples related to Cloud failures on data security are: Data center of Hosting.com at New jersey went down for few hours due to software bug in a Cisco switch [24] (June 2010). Amazon's EC2 and RDS services have experienced an outage for 4 days (April 2011). Amazon reported that its Elastic Block Store (EBS) volumes are trapped, which affected to EC2 instances trying to use affected volumes [31]. Data at rest (stored in Cloud storage) is generally commingled with other users' data. Even after using techniques to prevent unauthorized access, data at rest can be compromised through exploitation of application vulnerabilities. The main problemwith data-at-rest in thecloud is loss of control, if a non-authorized user accesses the data in a shared environment. Storage devices with in-built encryption techniques failed to prevent unauthorized access since the encryption and decryption keys can be compromised by malicious user. A lockbox approach, wherein the actual keys are stored in a lockbox and there is a separate key to access that lockbox can be used in the above mentioned case. However, again there is a need for security of lockbox key. This poses key management issue.

Data lineage. Tracing the data path is known as data lineage and it is important for auditing purpose in the cloud. It is a challenging task to provide data lineage. Since the data flow is no longer linear in a virtualized environment within the cloud, it complicates the process of mapping the data flow to ensure integrity of the data. Due to shared environment, maintaining the integrity of data is the most challenges task is Cloud.

Data-Remanence refers to the data left out in case of data transferor data removal. It causes minimal security threats viz; disclosure of sensitive information, data sold to others etc.

Data recovery is the one the most challenging problems. Data can be lost due to accidental damage or natural disaster to storage. It poses risk to data availability for users.

Data location. Tracing location of data is difficult in Cloud since user's data are dynamically migrated from one region (or country) to another region (or country). It increases risk of data privacy and security since data owner loses the control over his/her data.

Data breaches and investigative support: It is difficult to investigate inappropriate or illegal activity, because logging and data for multiple customers are co-located and may also be spread across an ever-changing set of hosts and data centers.

D. Lin et al. [32] proposed a data protection framework that is composed of three modules named policy ranking, policy integration and policy enforcement. Policy ranking module is used to find satisfying users' privacy policy requirements. For policy ranking module, there are three models recommended: (i) User-oriented ranking model; (ii) Service-provider-oriented ranking model; and (iii) Broker based ranking model. After finding the best service provider, proposed centralized model (for policy integration module) creates policies to be agreed by involving parties. Finally policy enforcement module (uses either tight coupling or loose coupling) examines whether confidentiality of data and policies are guaranteed at any time and at any location or not.

M. Mowbray et al. [34] proposed a client based privacy manager, incorporated features like obfuscation, preference settings, data access, feedback and personae. Obfuscation is used to modify some data fields of database before sending it to Cloud for processing. So, an attacker using same application would be unable to reveal those data. Only owners of those data can de-obfuscate those data. Using preference settings, set of policy can be incorporated for those data. Policies and data are shared with sender and receiver using cryptographic techniques. Data access will allow users to access personal information for checking accuracy or any violation of privacy. Feedback module monitors personal data transferring from platform and manages feedback including usage of personal data in Cloud. Personae module offers choice for revealing or not revealing different data fields. Data privacy is fully dependent on data owner.

J. Naruchitparames et al. [63] proposed a blind processing service using trusted computing mechanism to provide improved privacy and integrity for user's data. Blind processing is used create a secure channel between dedicated processes that are concealed from the rest of the system including root processes, system administrators, and end-users. This approach provides several layers of abstraction in which a remote system is ensured to have correct hardware, a trusted computing base, correct credentials, and a trustworthy state. However, it requires more hardware for processing. Practical analysis of this approach is not reported.

M. R. Abbasy et al. [64] proposed an approach that hides sensitive data using DNA reference sequences. In this approach, first data are converted from binary to DNA Nucleotides sequences for encrypting data. Then, complementary rules on encrypted data are applied. After that index of each couple of Nucleotides in DNA reference sequence are found. These sequences contain encrypted data. For decrypting these data, same procedure is followed in bottom-up manner. This approach provides security and privacy of user's data in resource sharing environment. However, if DNA sequence is altered or modified, it is difficult to retrieve original data.

S. J. Stolfo et al. [65] proposed an approach that uses user behavior and decoy information to mitigate insider data theft. In this approach, data access patterns are monitored by profiling user behavior. Decoy documents that are stored in the Cloud along with the user's real data act as sensors to detect illegitimate access. When unauthorized access is found, it is verified using challenge questions.

3.4. Virtualization Level Security Issues

In the virtualized (multi-tenant) environment, multiple OSs run concurrently on a host computer using hypervisor. Existing vulnerabilities [6] in VM that are distributed throughout the physical and virtual enterprise resources allow cyber attacker, malware, or other threats to remotely exploit.VMs' collocation also increases the security risk. In general, an attacker exploits these vulnerabilities be able to threaten the security of Cloud.

As the number of Guest operating systems (OSs) running on a hypervisor increase, the security concerns with that newer guest OSs also increase. Because it is not possible to keep track of all guest OSs and hence maintaining the security of those OSs is difficult. It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest OSs. There are risks associated with sharing the same physical infrastructure between a set of multiple users, even one being malicious can cause threats to the others using the same infrastructure.

If a hacker is able to get control over the hypervisor, he can make changes to any of the guest Oss and get control over all the data passing through the hypervisor. Isolation between two VMs is not completely adequate by current virtual machine monitors (VMMs). By compromising the lower layer hypervisor vulnerabilities, attacker can gain control over installed VMs. E.g. Bluepill, SubVirt and DKSM are some well-known attacks on virtual layer. This is still an open problem to prevent such threats.

Virtualization based malware and rootkit: New generation of rootkits that benefit from the processor technology that allows attacker to insert an additional hypervisor between the hardware and the software. The hypervisor takes control of the system and converts the original operating system into a virtual guest on the fly. In contrast to software-based virtualization, this kind of hijacking does not need a restart, and that makes it all the more difficult to detect the intrusion.

Sharing of VM images in Cloud introduces security risks. The owner of an image is concerned about confidentiality (e.g., unauthorized accesses to the image). The user of an image is concerned about safety (e.g., a malicious image that is capable of corrupting or stealing the user's own private data). For example, instances running on Amazon's EC2 platform can be easiliy compromized by performing various attacks like signature-wrapping attack,cross site scripting (XSS) attackDoS attack.This allowsattackers to create, modify and delete VM images, and change administrative passwords and settingsthat are put into instances with EC2 for S3 access.There is a risk of non-compliance (e.g., running unlicensed software or software with expired licenses). The administrator of Cloud is concerned with the security and compliance of the Cloud as a whole and the integrity of images. There is a risk of damages caused by malware contained in any image stored in the repository.

There should be standard mechanism for checking integrity of guest VMsfor successfully executing workload and avoiding interruption of computation, data loss and misuse of resources. As shown in Fig. 7 [36], host based transparentCloud protection system (TCPS) monitors integrity of Cloud components.TCPS is placed between guest'skernel and the virtualization layers, which monitors guest VMs and protects them against intruders and attacks. It also addresses transparency problem in Cloud.

Fig. 7.Architecture of TCPS [36].

Authors in [37] provided solution for securing virtual image repository and access control. As shown in Fig. 8, access control mechanism is used to reduce risk of unauthorized access to publisher's VM images. Image filters are used to remove user's personal information for providing privacy at publishing and retrieving time, where tracking system is used to disable malicious attempts by tracing versions of image and their operations. Also, image repository is maintained by periodically implementing virus scan and fixing vulnerabilities.

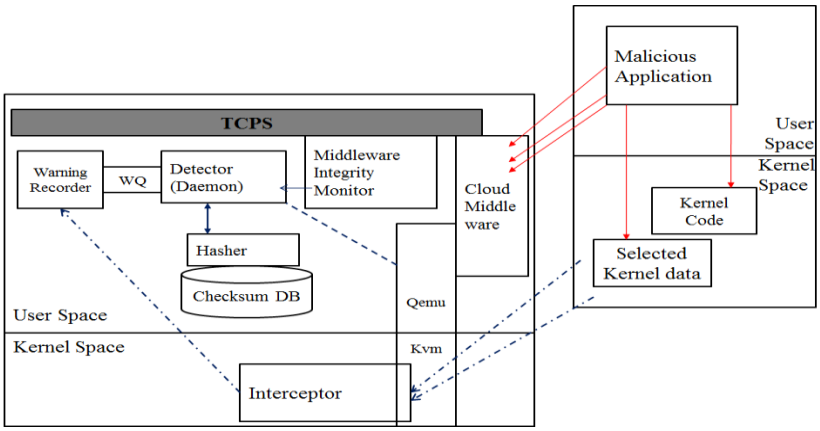
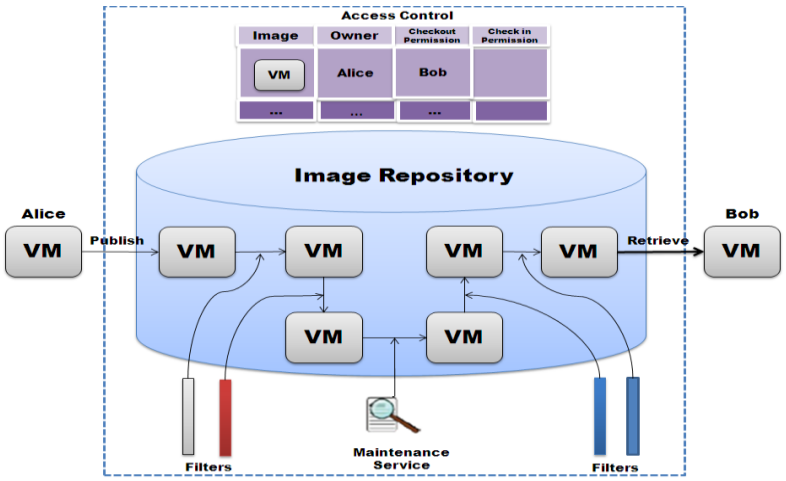


Fig. 8. Securing virtual image repository and access control [37].



A.Volokyta et al. [66] proposed a mechanism of monitoring of virtual machines to increase security of Cloud resources that can be affected by attacks. Using a detector, Host OS is monitored for integrity checking. All the malicious activities are analyzed by this detector and logged into log file. Using periodic checksum verification of executable file and libraries, integrity of Cloud resources are checked by virtual machine monitor (VMM). In this approach, all the monitoring activities are done through VMM. However, if hypervisor (or VMM) is compromised, guest OSs (running on that VMM) can be compromised.

3.5. Authentication and Access Control Level Security Issues

In Cloud computing, the client's information is transmitted over the Internet, which poses data ownership issues [36]. As this information is processed outside the enterprise, it brings inherent level of risk.

This issue is addressed by providing support for security assertion markup language (SAML) federation protocol (which contains authentication credentials in the form of SAML assertions) with their own authentication protocol [38]. SAML is issued to exchange information, such as assertions related to a subject or authentication information between cooperating domains. The request and response messages of it are mapped over Simple Object Access Protocol (SOAP) relying on XML. As discussed in section 3.1, using a Signature Wrapping Attack, it is possible to modify an eavesdropped message despite of it beingdigitally signed. Thus, an attacker may be able to execute arbitrary machine commands on behalf of a legitimate user. To address such issues, data should be transmitted via secured channel, fine-grained authentication and authorization techniques can be used for preventing data from unauthorized access.

L. Yan et al. [67] proposed an authentication approach that uses federated identity management together with hierarchical identity-based cryptography (HIBC). It provides key (public key and private key) distribution along with mutual authentication between parties in Cloud. It allows users to access services from other Cloud with single digital identity. For web services, this approach can be used to distribute public keys, while reducing SOAP header size. It is used to create session between two parties without message exchange. However, it creates trust issues since third party key distribution is involved.

A.Celesti et al. [68] addressed identity management problem in inter cloud. In this approach, third party is used as identity provider (IDP). In order to communicate, each cloud has to create an account using ID provided by IDP. Each cloud performs authentication task on provided ID to establish a trust and gains the access of needed resources. Trust on foreign cloud is accomplished by the IDP. The limitation of this approach is that each Cloud has to trust and rely on identity provider. Experimental evaluations are not reported.

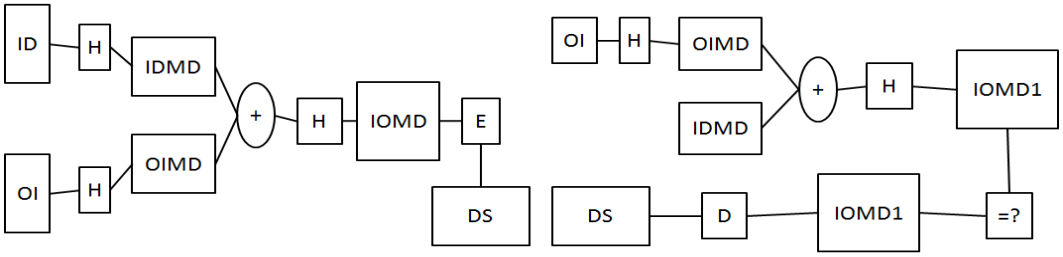
To solve third party problem, R. Ranchal et al. [69] proposed an approach to protect identity information without including trusted third party and using active bundle scheme. In this approach, Samir's multi party secrete sharing scheme is used to encrypt data. In this scheme, encrypted data and keys are shared among multiple hosts. By computing predicate over encrypted data and multiparty computing, active bundle based authentication can be done without decrypting data.

Fine-grained access controls should be available for controlling access to sensitive data or application code. Security group is able to define a setof controls applied to applications depending on the data.

For controlling access to Cloud resources, standards like eXtensible Access Control Markup Language (XACML) expressing access policies can be used. Service providers like Salesforce and Google Apps are using XACML for authorization decision and access control. Authors in [39] presented security model for restricting access to information through covert channels in Cloud. The solution for identity management among Clouds is presented in [40]. According to proposed protocol in [40], Cloud user registers his/her ID with service provider and gets a certificate with public key. Then third party service Cloud and service providers send their certificate to each other. While requesting to third party service Cloud, user can verify its certificate. After that, messages for third party service Cloud and service provider Cloud are produced. In produced messages, service level information is hidden for service provider, whereas ID and privileges (IOMD as shown in Fig.9) are hidden for third party service Cloud. For hiding such information, dual signatures(produced by hash function and encryption using user's private key) are used. Thus, disclosure of user's ID and privileges can be protected from service providers.

Fig. 9.(a)Dual signature procedure (b) Service verification [40].

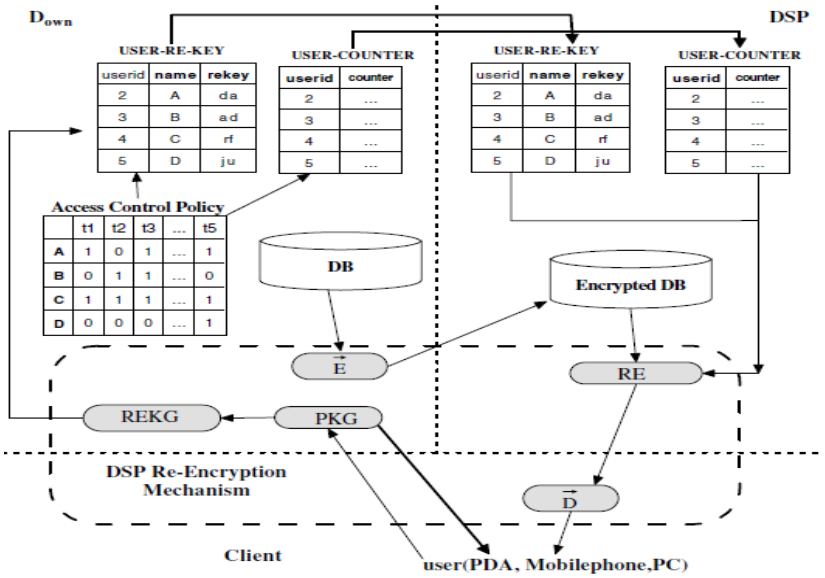
A re-encryption approach (as shown in Fig. 10[41]) provides flexible access control mechanism in Cloud data storage. Here, data owner (D_{own}) (who provides data to service provider) generates private key and public key using private key generator (PKG) for each user of these data. Then re-encryption keys corresponding to private key for each user are generated using key generator (REKG) and stored into authentication table. After that access control policies are stored in access control matrix. Using public key of each user, each tuple of owned database is encrypted. Authorization table is encrypted using public key of database services provider (DSP). Encrypted database and authorization table are transferred to DSP. By using re-encryption keys, DSP re-encrypts



tuples of database. Produced re-cipher text is decrypted only by legal user's private key. Thus, DSP can authorize data users without seeing data.

Fig. 10. Re-encryption based approach [41].

V. Echeverria et al. [70] proposed an idea to control an access of user data in Cloud; that is called Permission as a Service. It separates access control from other services to provide a separate service in the cloud. This allows users to set permissions for all data in a single location. This approach provides confidentiality of user'sby encrypting them using attribute based encryption (ABE) to provide data confidentiality. When any user wants to



access this data, permissions to access this data are managed via decryption keys. However, this approach is applied only for PaaS.

E. E. Mon et al. [71] combined Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC) to provide the privacy and security of sensitive data of cloud users. In this approach, Cloud clients store their data based on privacy laws according to their user levels. With the use of RBAC and ABAC, the privacy manager defines the privacy policies, privacy laws, user levels and security levels to control data access. Using an access control list (ACL), users are granted or denied to access the data. In this approach, security and privacy policies are defined by service providers, which restrict users to store all type of data since service providers are not fully trusted.

D. Slamanig [72] presented a dynamic accumulator based approach for privacy preserving access control to outsourced data. In this approach, the concept of access control lists (ACLs) is used to provide permissions (read, write, delete) to other users who are able to unlinkably and anonymously perform operations on outsourced data items when having these permissions. Using this approach, it can be decided that whether the users are allowed to system or not. Data user can give/get access rights to/from other users, whereas Cloud provider will not be able to identify such users and linked operations done by users. The limitation of this approach is that if data owner want to revoke permission from user, then that user must have to revoke granted permission from other users. This makes computationally difficult to maintain chain of users.

M. Raykova et al. [73] proposed privacy enhanced access control for outsourced data. In this approach, authors combine coarse-grained access control and fine-grained cryptographic access control. Coarse-grained access control offers an affordable communication overhead and provides privacy of information against view of the access rules and the access patterns, whereas fine-grained cryptographic access control is used at the user's side, which provides the desired access control policies. This approach offers read and write access control to user's data.

3.6. Trust Level Security Issues

This is one of the serious problems in Cloud. Since users have lack of control over resources, they have to rely on trust mechanisms and contracts in conjunction with mechanisms that provide a compensation. But trust is a very fuzzy concept and very difficult to calculate in a heterogeneous environment that is assessed by human or social trust. Contractors may be sub-contracting without user's knowledge. That means limiting visibility of network and system monitoring to user poses a trust issue. Contract requirements may not be propagated down the sub contracts. Employees (authorized users) or malicious insiders of organization often perform attacks that affect the confidentiality and privacy of other users' data as well as resources. Lack of public relations poses trust issue. Data Processing outside the organization poses inherent level of risk. There is no direct control on some service components outside the organization. Limiting visibility of network and system monitoring to user may also pose a trust issue. This issue can be addressed by providing adequate means of visibility of monitoring system. There should be mechanism for managing and assessing theinvolved risk. Cross-site scripting, access control weaknesses, insecure storage, and insecure configuration are some of the threat examples. Advanced cryptography techniques and signature technique can be used to address trust issue when outsourcing data. Authors in [42] presented approach for verifying dynamic data and securing data storage against adversary. Using this approach, users can check correctness of their data in Cloud storage with minimum overhead. Also, it protects users' data against any failure and locates data errors.

3.7. Security Issues related to Auditing, Regulatory Compliance and Laws

Audit and compliance to internal processes and external processes must be met with classified requirement and customer agreements, laws and regulations. Therefore, such policies should be monitored. Multi-tenancy nature of Cloud increases the difficulty of monitoring and log process of VM.Due to dynamic nature of Cloud, it is difficult to audit and compliance with coordination of external auditing, regulatory compliance and internal policy compliance. Risks related to compliance are discussed as follows:

Privacy Compliance: Only owners of data are responsible for the security and privacy of their outsourced data even if the data is held by service provider. This is due to the various laws and regulations in different countries. It poses risk of data security, confidentiality and availability. This is an open problem for providing transparency and controlled environment to owners about their data.

Geographic Compliance: If the tenant or cloud customer operates in the United States, Canada or the European Union, they are subject to numerous regulatory requirements. These include Control Objectives for Information and related Technology. These laws might relate to where the data is stored or transferred, as well as how well this data is protected from a confidentiality aspect.

Most of the cloud-based services have lengthy and onerous license agreements that very few businesses and consumers read or understand in their entirety. As a result, cloud services are often controlled by terms and conditions that limit a user's right of control and access or give the cloud service certain rights over the user's own data.

Industry Compliance: Industry compliance considerations are typically seen as an area where many cloud migrations flounder. Typical regulatory requirements can include:Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA),Family Educational Rights and Privacy Act (FERPA), Federal Information Processing Standard (FIPS) 140-2, Trusted Internet Connections (TIC) compliance.

Placing geographical and other restrictions on the collection, processing and transfer of personally identifiable information (PII) and sensitive information limit the usage of Cloud services. Privacy laws in various countries limit organizations to transfer some type of information to other countries. E.g.,UK businesses storing personal data with Cloud provider like Salesforce on the basis of their standard terms and conditions could find themselves in breach ofUK data protection law [43]. In Asia-Pacific (APAC) region, Japan,Australia and many other

countries have implemented data protection laws which require reasonable measures to protect privacy of personal data based on security guidelines of the Organization for Economic Cooperation and Development (OECD) and Asia Pacific Economic Cooperation's (APEC) privacy framework [44]. In Europe, the European Economic Area (EEA) has enacted data protection laws that follow the European data protection directives [44].A set of standards [45] like HIPAA, SOX, FDA, PCI, FISMA, GLBA, OSHA, ISO 27002, Basel II etc. should be implemented in Cloud to address compliance issue. There is a need to frame unified regulatory compliance.

Multi-Tenancy applications often require modifying existing applications and introducing newer modifications in application programs. In [75], the authors proposed a platform running on top of LAMP architecture for increased stability and security. Their platform does not need modification in current application stack.

In [76], the authors proposed an architecture for self-protecting documents by encapsulating security components like access control and usage control for achieving automatic document architecture for enterprise Digital Rights Management [e-DRM].

In [77], the authors proposed an approach to ensure reliability of data using Sobol Sequence and utilizing token pre consumption. Their analysis show that the proposed scheme is more secure against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks than existing systems

S. Bleikertz et al. [74] proposed a way for visualization and automated analysis based on reachability and attack graphs. In this approach, proposed query and policy language is used to analyze security configuration. It can be used to test the correctness of security policies (defined in Cloud) to trace the attack. However, it audits only firewall rules for Cloud to assure users that their environment is protected. It does not provide ability to Cloud users to control their own resources at the Cloud and assure them about the trustworthiness of Cloud environment.

B. Wang et al. [61] proposed an approach called Oruta (One ring to rule them all)), that provides a new privacy-preserving public auditing mechanism for shared data in an untrusted cloud. In this approach, third party auditor is used, that uses ring signatures to build homomorphic authenticators to verify the integrity of the shared data for a static group of users without retrieving the entire data. However, it is not an efficient solution, when user groups are dynamic. Time taken to verify information increases linearly with the number of users increases in a group.

M.T. Khorshed [62] surveyed on the gaps that is slowing down cloud adoption and reviewed challenges on threat remediation. In this work, author investigated and compared performances of several machine learning techniques to monitor insider activities in Cloud and concluded that rule based technique C4.5 (decision tree classifier) is an efficient technique to solve problem of monitoring the insiders' activities having similar patterns as some other cyber attacks.

Table 4 summarizes security issues at different levels in Cloud environment.

Security measures adopted by major Cloud providers are summarized in Table 5 [46][47][48].

4. Future Research Directions

There are upcoming Cloud models that require newer research directives:

4.1. *Mobile Cloud Computing*

Mobile Cloud computing is confined to availability of Cloud computing to mobile ecosystem. These can also be extended to tablets and portable PDAs having limited processing and memory capabilities. Besides uniform network stability and device access, mobile devices raise several security and privacy concerns; an obvious case

is misplacement or loss of a mobile device that can result into major data breach. There is a lack of platform independent languages to develop applications for mobile devices, i.e. consistent case for Android and Apple..

Table 4.Summary of security issues with their mitigation directives.

Issues		Reported approaches	Solution directives
Application level security Issues	Service availability	• A provenance based approach [25]. • DDoS attack detection for securing VM [29]. • Semantic access control [56]. • CloudProtect [57].	• Before deploying applications, they should be tested and made free from vulnerabilities like buffer overflow, SQL injection etc. • Strong authentication and access control. • Provide browser and API level security. • Implement IDS/IPS for service availability. • Implement secure software development life cycle.
	Integrity of workload state		
Network level security issues		• Various IDS/IPS approaches [28] [30]. • EDoS Protection [58].	• Incorporate efficient firewall. • Use Network based IDS/IPS. • Secure SSL trust configuration.
Data storage level security Issues	Data protection	• Anonymity based technique for data privacy [33]. • Client based privacy manager [34]. • Policy ranking based approach [32]. • Data hiding approach [64]. • Fog Computing [65].	• Provide browser and API level security, use SSL encryption for transmission of data. • Use standard SLAs, periodic audits required. • Provide abstract level transparency for migrated data. • Implement database intrusion detection. • Use secure data backups and recovery protocols. • Data isolation required. • Homomorphic encryption technique can be incorporated to provide data privacy.
	Data location		
	Data segregation		
	Data integrity, confidentiality and availability		
	Data breaches		
	Long-term viability		
	Data recovery		
Virtualization level security issues		• Protection against Intra host attacks [36]. • Virtual machine introspection based IDS approach [35]. • Providing privacy for virtual image repository [37]. • Secure virtualization [66].	• Virtual machines should be isolated and any breach in VM's isolation should be alerted. • Ensure integrity and security of virtual machine images. • Virtual machine manager should be free from vulnerabilities. • Use firewall, host based IDS/IPS, network based IDS/IPS, antivirus for virtualized operating system. These measures should be transferred to each guest machine.
Authentication and authorization level security		• Restricting search and Access control [39]. • Identity management based approach [40]. • RE-Encryption based approach [41]. • Permission as a service [70].	• Use standards like SAML, encrypted SSL, XACML etc. • Use proper firewall to control access. • Use public key infrastructure solutions. • Identity based encryption, policy based encryption or attribute based encryption techniques can be used. • Define access control policies and use proper SLAs.
Trust level security issues		• Data storage security [42].	• Provide certain transparency to data owner. • Use strong authentication and access control mechanism. • Provide periodic audits to data owners for their data. • Provide certain visibility of security system to data owners.
Security issues related to Audit, Regulatory compliance and laws		• Available standards: HIPAA, SOX, FDA, PCI, FISMA, GLBA, OSHA, ISO 27002, Basel II [45]. • Security audits for virtual	• Need to frame unified regulatory compliance. • Proper SLA should be built, where privacy laws for data should be considered.

	infrastructure [74]. • Insider activity monitoring [76].	

Table 5.Security measures adopted by major Cloud providers

Cloud Provider	Services offered	Security measures adopted
Amazon AWS	PaaS IaaS	• Amazon EC2 provides web service interface to configure firewall settings, which controls network access between groups of users. • Amazon simple storage service (S3) is accessible via SSL encrypted end points. It is user's responsibility to encrypt data before storing into S3.
Google App Engine	PaaS	• JVM in a secured "sandbox" environment is used for running Java Applications, which isolate applications and security. Any executable Java byte code can be operated within the sandbox controls. • In addition, Python interpreter is running in a secured "sandbox" that isolates applications and security.
Window Azure	PaaS IaaS	• Firewalls, filtering routers, cryptographic protection of messages, software security patch management, central monitoring, correlation and analysis systems, network segmentation, Service administration access and physical security. • Reduces the damage to infrastructure by providing optional and mandatory "sandbox" features. • Customers are provided security options as available in window server. Configuration and updates are controlled by SSL client certificates and protected by 128 bit encryption. • All administrative operations are audited.
Force.com	PaaS	• For authentication, SAML is used on login, session security and auditing. • Security at various levels such as Physical security, logical network security, host security, transmission level security and database security are provided.
Rack Space	IaaS	• Firewalls, antivirus and spam protection provided. • SSL provided as add on service.
Go Grid	IaaS	• ServePath's secure infrastructure and telecom facility provided.
Joyent Inc.	PaaS IaaS	• Spam protection, advanced traffic security, SSL acceleration and Advanced DNS available. • Isolated memory, storage, and network enforced at the virtualization level. • Users have full control (root access) over ports and processes, but not kernel level access to underlying OS.
Layered Technologies Inc. (3-tera Inc.)	IaaS	• Access restrictions are provided through firewalls. Front-end protection against DDoS attack.
Terremark worldwide Inc.	IaaS	• Certified Infrastructure with SAS 70 Type II. • Firewalls and private VLAN architecture for network. • Connections to the management console are secured by SSL.
Xcalibre Communications Ltd.	IaaS	• VLAN for each customer. • Data is stored in a T1 storage back end.
Eucalyptus	IaaS	• WS-security for authentication, public key and private key for users.
Open Nebula	IaaS	• Firewall and virtual private network tunnel used.

Nimbus	IaaS	• PKI credentials are required.

4.2. Encryption and Key management algorithms

Unknown physical location of data in the Cloud and different laws enforced by nations to manage data make encryption and key management complex. If encryption is applied, it needs to be performed at multiple locations. Within the data center, in between the data centers, or between public and private Clouds etc. There is a strong need of improved solution involving the users for controlling the use of their data. In [49], authors propose the use of symmetric key encryption mechanism for data security in Cloud framework. In [50], authors propose the use of Public Key Infrastructure for the Cloud framework. However, these approaches do not provide an efficient solution for key management due to its complexity. Identity Based approach has to overcome the key management limitation. However, there is a need of more robust approach in this context, which could extend traditional approaches like Cipher text Policy Attribute based encryption (CPABE) [51], Key Policy Attribute based encryption (KPABE) etc. to Cloud computing.

4.3. Ad-Hoc Clouds

Current Model of Cloud computing involves a data center approach, whereby clusters of machines are dedicated to running Cloud infrastructure software. However, there may be some resources whose utilization has been limited. A model called 'Ad hoc Cloud' [52] enables infrastructure software to be distributed over resources harvested from machines already in existence within the enterprise. This may in turn yields several benefits such as reduction of need for the specialized infrastructure for resilience. However, this approach would require newer architectural representations, membership control mechanism for set of machines for ad-hoc Clouds and newer model for maintaining scalability. Apart from these, there are moreopen areas for further research andrequire notable attention. These may include delivery of newer services like high performance computing, implementing a secure Virtual Private Network over the Cloud, Security as a Service etc. These concepts are still in their infancy and its adoption and extension to Cloud computing would require considerable research efforts.

5. Conclusions

Cloud computing can bring various business benefits to organizations. However, there are many challengesrelated to security and privacy. Our attempt is to show various vulnerabilities, threats and attacks hindering the adoption of Cloud computing. We surveyed existing solutions to address security issues at different layer of Cloud, while identifying some open problems. It opens up space for future researchto extend existing techniques and to investigate new techniques for security and privacy to mobile Cloud and ad-hoc Cloud. This includes a need for a dynamic security model and better crypto (and key management) algorithms that targets different levels of security and privacy for Cloud computing.

References

[1] What Cloud computing really means, InfoWorld,http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0 (2011).

[2] P. Mell, T. Grance, The nist definition of cloud computing (draft), NIST, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (2011).

[3] Ponemon, Security of cloud computing providers study, CA Technologies, http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf(2011).
[4] Software as a service-wikipedia, Wikipedia, http://en.wikipedia.org/wiki/Software_as_a_service (August 2011).
[5] F. Gens, New idc it cloud services survey: Top benefits and challenges,IDC, http://blogs.idc.com/ie/?p=730 (2009).
[6] National vulnerability database version 2.2, NIST, http://web.nvd.nist.gov/view/vuln/search-results?query=virtual&search_type=all\&cves=on (2011).
[7] D. Durkee, "Why Cloud Computing Will Never Be Free," Comm. ACM, 53 (5), 2010, pp. 62–69.
[8] J. Rutkowska, Security challenges in virtualized enviroments, Bluepill project, http://bluepillproject.org (2007).
[9] K. R. Balachandra, V. P. Ramakrishna, A. Rakshit, Cloud security issues, in: Proceedings of the 2009 IEEE International Conference onServices Computing, SCC '09, 2009, pp. 517-520.
[10] K. Sripanidkulchai, S. Sahu, Y. Ruan, A. Shaikh, C. Dorai, Are cloudsready for large distributed applications, SIGOPS Operating Systems Review 44 (2) (2010) 18-23.
[11] Security Threats, Microsoft, http://technet.microsoft.com/en-us/library/cc723507.aspx
[12] J. Rutkowska, Subverting vistatm kernel for fun and profit, in: BlackHat Conference, 2006.
[13] S. King, P. Chen, Y.-M. Wang, Subvirt: Implementing malware withvirtual machines, in: 2006 IEEE Symposium on Security and Privacy,2006, pp. 314-327.
[14] S. Bahram, X. Jiang, Z. Wang, M. Grace, Dksm: Subverting virtualmachine introspection for fun and profit, in: Proceedings of the 29thIEEE International Symposium on Reliable Distributed Systems, 2010.
[15] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (34), 2011, pp. 1-11.
[16] W. Halton, Security Issues and Solutions in Cloud Computing, http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/ (2010).
[17] Aws management console, Amazon Web Services, http://aws.amazon.com/console/ (2008).
[18] D. Pauli, Amazon's EC2, Eucalyptus vulnerability discovered, website, http://www.crn.com.au/News/278387,amazons-ec2-eucalyptus-vulnerability-discovered.aspx (2011).
[19] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All your clouds are belong to us – security analysis of cloud management interfaces," ACM workshop on Cloud Computing Security, 2011.
[20] Top 7 threats to cloud computing, HELP NET SECURITY, http://www.net-security.org/secworld.php?id=8943 (2010).
[21] C. Metz, Ddos attack rains down on amazon cloud, Theregister, http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/(2009).
[22] M. Jensen, J. O. Schwenk, N. Gruschka, L. L. Iacono, On technicalsecurity issues in cloud computing, in: In IEEE International Conferenceon Cloud Computing, CLOUD-II 2009, 2009, pp. 109-116.
[23] T. Ferguson, Salesforce.com outage hits thousands of businesses,Cnet News, http://www.ludcastle.co.uk/business_resources/Clouded%20in%20uncertainty.pdf (2009).
[24] Sourya, Should You Be Concerned? A List of Recent Cloud Computing Failures – Intuit Goes Down, CloudTweaks, http://www.cloudtweaks.com/2011/06/should-you-be-concerned-a-list-of-recent-cloud-computing-failures (2011).
[25] J. Du, W.Wei, X. Gu, T. Yu, Toward secure dataflow processing in opendistributed systems, in: In Proc. of ACM Scalable Trusted ComputingWorkshop (STC), 2009.
[26] W. Halton, Security Issues and Solutions in Cloud Computing, http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/ (2010).
[27] Xarp 2.2.2, filecluster, http://www.filecluster.com/Network-Tools/Network-Monitoring/Download-XArp.html (2011).
[28] C. C. Lo, C. Huang, J. Ku, A cooperative intrusion detection systemframework for cloud computing networks, in: In: Proceedings of the2010 39th International Conference on Parallel Processing Workshops,ICPPW '10, 2010, pp. 280-284.
[29] A. Bakshi, Y. B. Dujodwala, Securing cloud from ddos attacks usingintrusion detection system in virtual machine, in: In: Proceedings of the 2010 Second International Conference on Communication Softwareand Networks, ICCSN '10, 2010, pp. 260-264.
[30] F. Y. Leu, J.-C. Lin, M.-C. Li, C.-T. Yang, P.-C. Shih, Integratinggrid with intrusion detection, in: Proceedings of the 19th InternationalConference on Advanced Information Networking and Applications, AINA '05 (1), 2005, pp. 304-309.
[31] C. Metz, Amazon outage spans clouds 'insulated' from each other, The Register, http://www.theregister.co.uk/2011/04/21/amazon_web_services_outages_spans_zones/ (2011).
[32] D. Lin, A. Squicciarini, Data protection models for service provisioningin the cloud, in: In : Proceeding of the ACM symposium on Accesscontrol models and technologies, SACMAT '10, 2010.
[33] Y. J.Wang, S. J. Zhao, J. Le, Providing privacy preserving in cloud computing, in: In: International Conference on Test and Measurement,Vol. 2 of ICTM '09, 2009, pp. 213-216.
[34] M. Mowbray, S. Pearson, A client-based privacy manager for cloud computing, in: In Proceedings of the Fourth International ICST Conferenceon Communication System softWAre and middleware, COMSWARE'09, 2009, pp. 1-8.
[35] T. Garnkel, M. Rosenblum, A virtual machine introspection based architecture for intrusion detection, in: In Proc. Net. and Distributed Sys.Sec. Symp., 2003.

[36] F. Lombardi, R. D. Pietro, Transparent security for cloud, in: Proceedings of the 2010 ACM Symposium on Applied Computing, 2010, pp.414-415.
[37] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managing security ofvirtual machine images in a cloud environment, in: Proceedings of the2009 ACM workshop on Cloud computing security, CCSW '09, 2009,pp. 91-96.
[38] R. Chandramouli, P. Mell, State of security readiness, Crossroads, 16 (3), 2010, pp. 23-25.
[39] T. Morizumi, K. Suzuki, H. Kinoshita, Transparent security for cloud system for search, access restriction, and agents in the clouds, in: In:Proceedings of the 2009 Ninth Annual International Symposium on Applications and the Internet, 2009, pp. 201-204.
[40] X. Huang, T. Zhang, Y. Hou, Id management among clouds, in: In:First International Conference on Future Information Networks, ICFIN2009, 2009, pp. 237-241.
[41] X. Tian, X. Wang, A. Zhou, Dsp reencryption: A flexible mechanism for access control enforcement management in daas, in: In Proc.CLOUD'09, SACMAT '10, 2009, pp. 25-32.
[42] Wang, Q. Wang, K. Ren, W. Lou, Ensuring data storage security incloud computing, in: In: Proc. of IWQoS 2009, 2009.
[43] J. Salmon, Clouded in uncertainty - the legal pitfalls of cloudcomputing, Computing, http://www.ludcastle.co.uk/business_resources/Clouded%20in%20uncertainty.pdf(2008).
[44] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (2011).
[45] Compliance home, Website, http://www.compliancehome.com/(2011).
[46] Cloud Computing Comparison Guide, Web hosting unleashed, http://www.webhostingunleashed.com/whitepaper/cloud-computing-comparison/
[47] Comparison Guide: Cloud Computing, Focus Research, http://www.focus.com/research/comparison-guide-cloud-computing/
[48] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in NCM '09: Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC. Washington, DC, USA: IEEE Comp. Society, 2009, pp. 44–51.
[49] W. Wang, Z. Li, R. Owens, B. Bhargava, Secure and efficient access to outsourced data, In ACM Cloud Computing Security Workshop (CCSW), 2007, pp. 63-69.
[50] S. Sanka, C. Hota, M. Rajarajan, Secure data access in cloudcomputing,in: IEEE 4th International Conference on Internet Multimedia ServicesArchitecture and Application(IMSAA), 2010, pp. 1-6.
[51] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-basedencryption, in: Proceedings of the 28th IEEE Symposium on Securityand Privacy, 2007.
[52] G. Kirby, A. Deale, A. Macdonald, A. Fernandes, An approach to adhoc cloud computing, Cornell University Library, http://arxiv.org/abs/1002.4738v1 (2010).
[53] Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894), Microsoft Security Bulletin MS10-010 – Important, website, http://www.microsoft.com/technet/security/bulletin/ms11-047.mspx (2010).
[54] Tibor Jager, Juraj Somorovsky: How To Break XML Encryption - In Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS), 2011.
[55] K. Zunnurhain, S. V. Vrbsky, Security Attacks and Solutions in Clouds, CloudCom2010, http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf(2010).
[56] Hu, Luokai and Ying, Shi and Jia, Xiangyang and Zhao, Kai, Towards an Approach of Semantic Access Control for Cloud Computing, Proceedings of the 1st International Conference on Cloud Computing, pp. 145—156, 2009.
[57] Mamadou H. Diallo, Bijit Hore, Ee-Chien Chang, Sharad Mehrotra, Nalini Venkatasubramanian: CloudProtect: Managing Data Privacy in Cloud Applications. IEEE CLOUD 2012: 303-310, 2012.
[58] S. V. Sandar, S. Shenai, Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks, International Journal of Computer Applications, 41 (20), pp. 11-16 (2012).
[59] C.Modi, D.Patel, B.Borisaniya, H.Patel, A.Patel and M.Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud," Journal of Network and Computer Applications (JNCA), Elsevier, Accepted on (16 May 2012), DOI= http://dx.doi.org/10.1016/j.jnca.2012.05.003.
[60] Mazzariello, C., Bifulco, R., Canonoco, R.: Integrating a network IDS into an Open source Cloud computing, Sixth International conference on Information Assurance and Security (IAS), pp. 265-270 (2010)
[61] B. Wang et al. "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEE Cloud 2012
[62] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasim, "Monitoring Insiders Activities in Cloud Computing Using Rule Based Learning," TrustCom, pp.757-764, 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011.
[63] J. Naruchitparames, M. H. Gunes, EnhancingDataPrivacyandIntegrityintheCloud, SPCLOUD, 2011.
[64] Mohammad Reza Abbasy, Bharanidharan,Shanmugam, Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences,IEEE World Congress on Services (SERVICES), 4-9 July 2011, pp. 385-390.
[65] SalvatoreJ.Stolfo, MalekBenSalem, AngelosD.Keromytis, Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, IEEE Symposium on Security and Privacy Workshops, 2012

[66] Volokyta, A. , Secure virtualization in cloud computing, Modern Problems of Radio Engineering Telecommunications and Computer Science (TCSET), 2012 International Conference on, pp. 395, 2012.
[67] Liang Yan, Chunming Rong, Gansen Zhao: Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. CloudCom 2009: 167-177 2009
[68] Celesti, A. Tusa, F. ; Villari, M. ; Puliafito, A. Security and Cloud Computing: InterCloud Identity Management Infrastructure, Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on, pp. 263 - 265 2010.
[69] Rohit Ranchal, Bharat Bhargava,, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, Mark Linderman, Protection of Identity Information in Cloud Computing without Trusted Third Party, 29th international symposium on reliable distributed systems, 2010.
[70] Echeverria, Victor and Liebrock, Lorie M. and Shin, Dongwan, Permission Management System: Permission as a Service in Cloud Computing, Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, pp. 371—375, 2010.
[71] Ei Ei Mon Thinn Thu Naing The privacy-aware access control system using attribute-and role-based access control in private cloud, Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on, pp. 447 - 451 , 2011.
[72] Slamanig, Daniel, Dynamic Accumulator Based Discretionary Access Control for Outsourced Storage with Unlinkable Access, Financial Cryptography and Data Security, pp. 215-222, 2012.
[73] Mariana Raykova and Hang Zhao and Steven M. Bellovin, Privacy Enhanced Access Control for Outsourced Data Sharing, Financial Cryptography, pp. 223-238, 2012.
[74] Bleikertz, S\"{o}ren and Schunter, Matthias and Probst, Christian W. and Pendarakis, Dimitrios and Eriksson, Konrad, Security audits of multi-tier virtual infrastructures in public infrastructure clouds, Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pp. 93—102, 2010.
[75] B. Siddhisena, L. Warusawithana and M. Mendis, "Next generation multi-tenant virtualization cloud computing platform," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 405-410.
[76] M. Munier, V. Lalanne and M. Ricarde, "Self-protecting documents for cloud storage security," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1231-1238.
[77] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, "Ensuring data storage security in cloud computing using sobol sequence," in *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*, 2010, pp. 217-222.
[78]