Depleting Clouds

A Survey on Security, Privacy, Accountability and Trust Issues in Cloud Computing

Piyush Yadav, Gaurav Gupta

Indraprastha Institute of Information Technology (IIIT-Delhi), New Delhi ,India

Abstract

Today cloud computing offers highly scalable and dynamic services over internet. It provides services to user with more flexibility and less cost. But there are various security concerns on moving these applications to cloud. Lot of the technical security concerns have been raised in recent years like browser security, cloud malware injection attacks and various integrity and binding issues .Various personal and sensitive information of user is in the cloud which make it vulnerable. Privacy is very important in term of legal framework, data governance and user trust. This paper proposes the various security, privacy and trust issues and what the legal methodologies should be drafted and adopted so that these problems can be overcome.

Keywords: Security Attacks, Trust, Privacy, Act and Laws, Accountability.

1. Introduction

Cloud computing is a hosting service on internet . It can be considered as a super computing model and new trend of delivering computing resources like networks ,servers, data storages and services. Cloud computing is a special form of distributed computing which is been lauded for its agility, flexibility , efficieny and easy set up. Cloud Security Alliance(CSA) defines cloud computing as[45]:

"***Cloud Computing is a model for enabling ubiquitous, convinient , on-demand network access to a shared pool of configurable computing resources***."

The evolution of cloud generated services in not too old. It has also came into existence through evolutionary development.The story of cloud computing started from SALESFORCE.COM in *1999* for delivering enterprise applications through website[1].The cloud technology is generated from grid computing.

GRID COMPUTING- The technological innovations demand for more computing power as problems were becoming more sophisticated and complex. This given rise to grid computing in mid of 1990. Grid computing was derived from the electrical power grid to emphasize its characteristics like pervasiveness, simplicity and reliability (Foster and Kesselman 1999)[43].

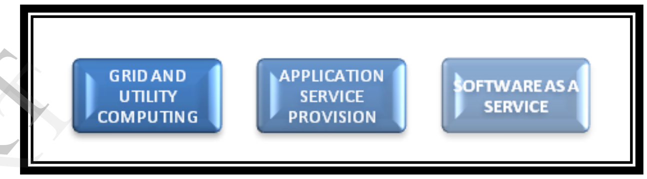


Fig1.1 Evolution of Cloud History

NIST has defined cloud computing model by illustrating five essential charateristics,three cloud service models and four deployment models[45]. These are as follows:

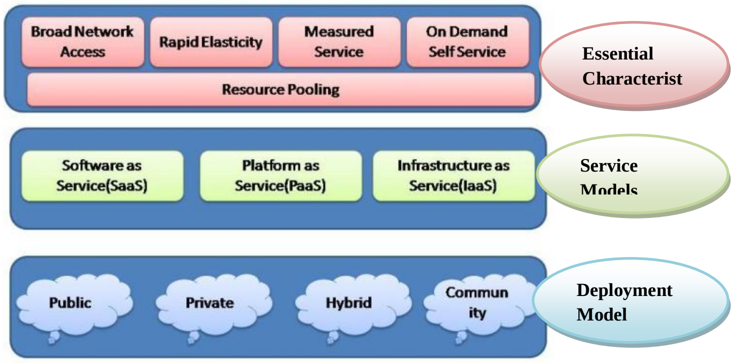


Fig 1.2 NIST Cloud Computing Definition

A recent survey by **Ernst & Young's Global Information Security Survey 2011** shows that there is an increase use of cloud services by the organisations and it seems that it will increase more in next few months[2]. The analysis of survey is depicted below shows comparison between cloud users in year 2010 and 2011 in form of pie chart-

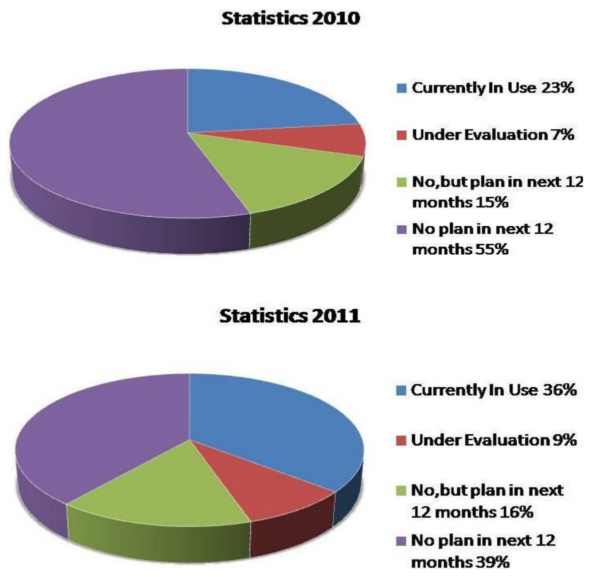


Fig 2.1 Ernst & Young's 2011 Global Information Security Survey

2. Security and Cloud Computing

Cloud computing has provided us a lot of services but with its evolution it possess various security risks. These security issues has created a ruckus in the mind of users regarding its stability. These threats can be of various types like (i) ***Extortionists*** where attacker can use attacks like DDOS to exhaust server resources or (ii) ***Competitors*** where business rivals use known method to interrupt the services. Thus ***cloud computing security*** occurs as a new domain in the field of information security[47]. Cloud computing security depicts set of policies and methodologies which are implemented and enforced to protect data and applications of cloud[3].In cloud the security perspective are broadly divided into two scenarois i.e

- Security issues faced by **providers.**
- Security issues faced by **users.**

In a survey by **Trend Micro: Canadian SME IT Security Survey 2011** the most common concern by the cloud providers and users relates to the privacy and security of company information[4].

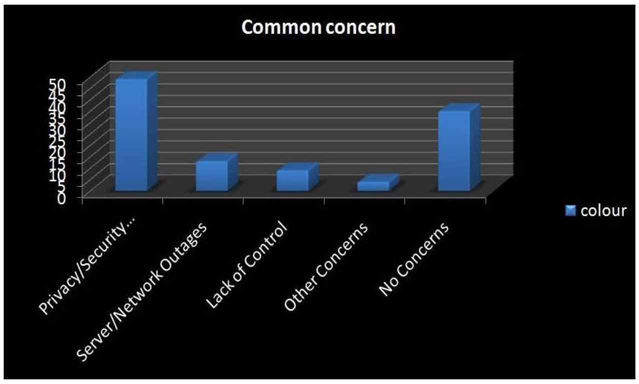


Fig 2.2. Trend Micro Survey

2.1 Recent Security Attacks In Cloud

IDC cloud research shows that there is whooping increase in cloud services reaching to $55.5 billion in 2014. But the hacking attacks and data breaches has drawn lot of concerns regarding the security of cloud[5,6]. Some of the recent security attacks on organisation has showed that lot of the confidential and personal information of customer has been leaked.Some of them are illustrated below[7,8,9,10].

Epsilon Breach : Epsilon a third party email marketing and security provider reported on April 1, 2011 an unauthorized access in its system by finding a vulnerability in its application layer codes. Cyber factors a risk analytics intelligence company study tells that it may have effected 75 companies and 3% of Epsilon customers and may cost it upto $412-$637 million**.**

Amazon Breach : There was a breakdown in Amazon cloud services which affected sites like foursquare and quora. A report from Kaspersky says that Amazon cloud is spreading banking malware which steals information from hardware and software.

Sony Playstation Network Breach: Sony's PSN security breach was one of the biggest data breach that has also been due to Amazon virtual cloud services resulting hackers compromise 77 million playstations customers data**.**

And the attack list continues[11]-

ORGANISATION	FIELD	YEAR	INCIDENTS
Honda Motors	*Automobiles*	*2011*	*4.9 million customers emails compromised*
RSA	*Security Solutions*	*2011*	*RSA's authentication system compromised affecting 40 million employees*
Google	*Multidimensional*	*2011*	*360,000 credit cards customers personal info compromised*
IMF	*Monetary*	*2011*	*Not Disclosed*
NASDAQ	*Stock Exchange*	*2011*	*Not Disclosed*
Lockheed Martin	*Defence*	*2011*	*Secure ID infrastructure Compromised*
Citigroup	*Financial*	*2011*	*Gmail account of US govt & millitary personnels compromised*
JP Morgan Chase	*Financial*	*2012*	*Prevented Customers from banking online.*
Bank Of America[40]	*Financial*	*2012*	*Data Leakeag*

In report "**Assessing the Security Risks of Cloud Computing**" from analyst firm Gartner cloud computing is full of security risks.The customers should make clear all the policies before taking services from cloud providers. Gartner has enlisted seven specific secuirty issues that customers should ask from the vendor before selecting it[48]. These are:

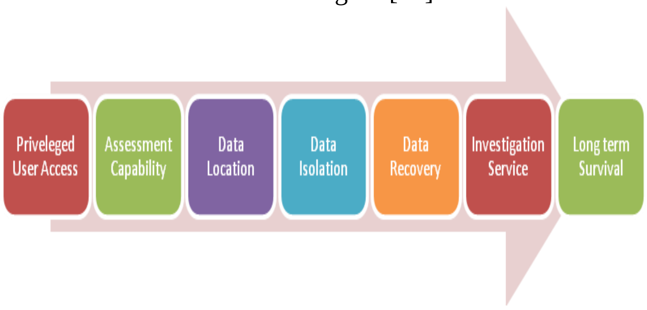


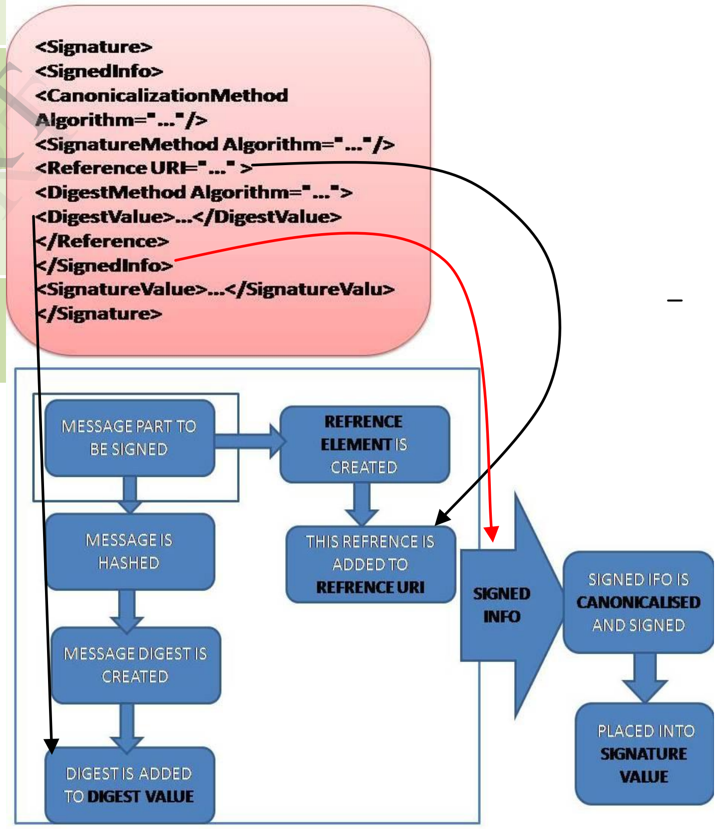
Fig 2.3 Issues that client should Resolve(Gartner)

3.Security Attacks And Solutions In Cloud

The above analysis and survey reports arises many questions that **Whether cloud is secure enough?**With these recent security attacks and data breaches it is now necessary for us to combat these security issues and find out necessary solutions for it. Some of these attacks that how they are performed and what measures should be taken are described below-

3.1 Xml Signature Wrapping Attack / Xml Rewriting Attack

How XML Signature Works- In order to provide integrity, confidentiality and authentication some predefined parts of SOAP(Simple Object Access Protocol) messages are signed.Thus Web Service Security(WS-Security) apply XML Signatures & XML Encryption to SOAP messages. The body of SOAP messages is given below[12,13,14]-



```
<Signature>
<SignedInfo>
<CanonicalizationMethod
Algorithm="..."/>
<SignatureMethod Algorithm="..."/>
<Reference URI="..." >
<DigestMethod Algorithm="...">
<DigestValue>...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...</SignatureValu>
</Signature>
```

MESSAGE PART TO BE SIGNED
REFRENCE ELEMENT IS CREATED
MESSAGE IS HASHED
THIS REFRENCE IS ADDED TO REFRENCE URI
SIGNED INFO
SIGNED IFO IS CANONICALISED AND SIGNED
MESSAGE DIGEST IS CREATED
PLACED INTO SIGNATURE VALUE
DIGEST IS ADDED TO DIGEST VALUE

Fig 3.1 Process Of Xml Signature Header In SOAP

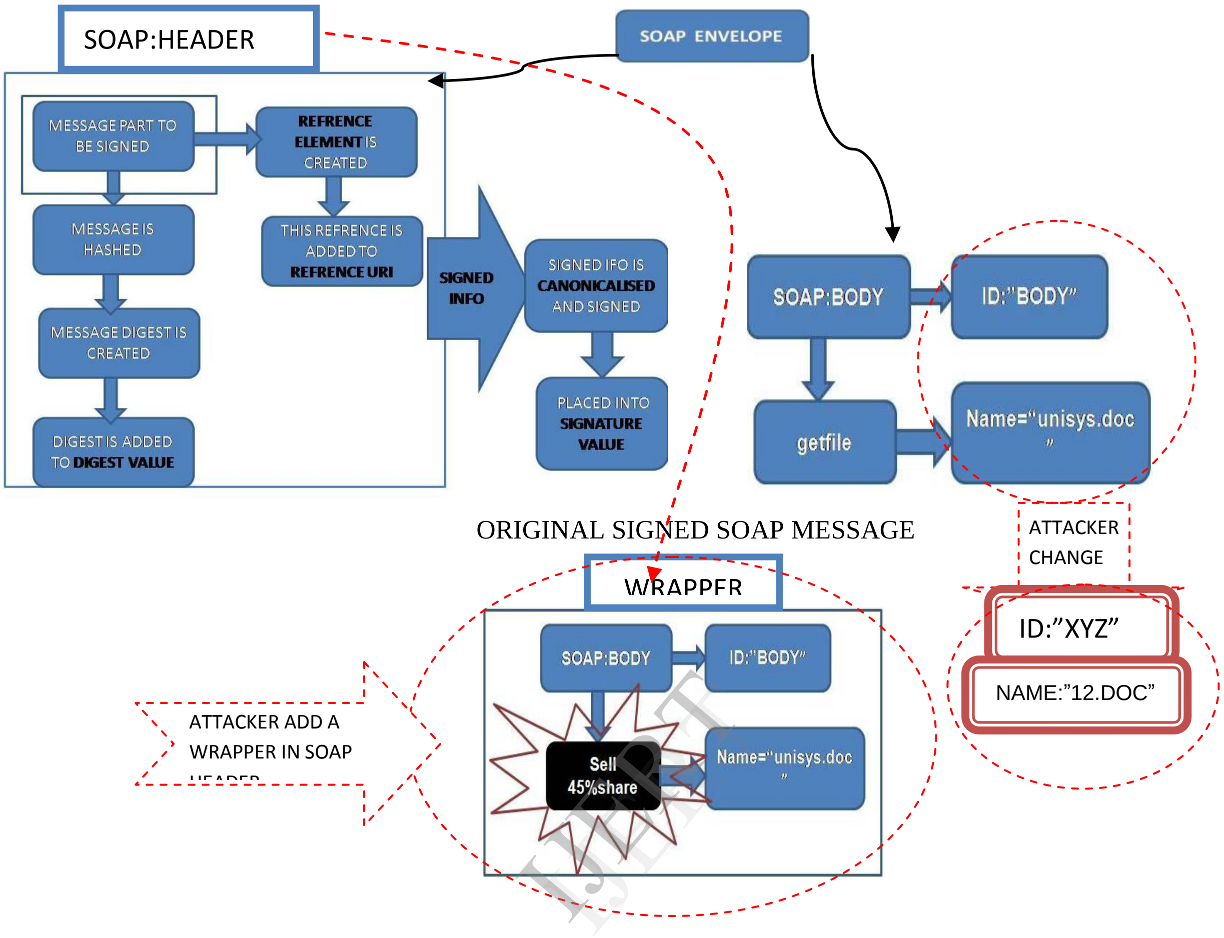

SOAP:HEADER
SOAP ENVELOPE
MESSAGE PART TO BE SIGNED
REFRENCE ELEMENT IS CREATED
MESSAGE IS HASHED
THIS REFRENCE IS ADDED TO REFRENCE URI
MESSAGE DIGEST IS CREATED
DIGEST IS ADDED TO DIGEST VALUE
SIGNED INFO
SIGNED INFO IS CANONICALISED AND SIGNED
PLACED INTO SIGNATURE VALUE
SOAP:BODY
ID:"BODY"
getfile
Name="unisys.doc"
ORIGINAL SIGNED SOAP MESSAGE
ATTACKER CHANGE
WRAPPER
ID:"XYZ"
NAME:"12.DOC"
ATTACKER ADD A WRAPPER IN SOAP HEADER
SOAP:BODY
ID:"BODY"
Sell 45%share
Name="unisys.doc"

Fig 3.2 Changes Done In Soap Envelope During Wrapping

3.1.2 How Wrapping Attack Is Done

The attacker should know certain things before attack-

1) Atacker shold know the endpoint of webservice.

2) Attacker must have information that whether the web service process the signature of security headeror not.

When a user makes a request(e.g browser) to webserver, a SOAP message is generated by webserver. The attack is done during translation of SOAP message in TLS(Transport Layer Security) layer .The attacker create a duplicate message by manipulating SOAP message and copy the target elements and moving it somewhere else in message and inserting something malicious at the original place and sent to webserver. The server authenticates it by signature value and thus integrity checking process is done. After that attacker can run the malicious code on the server. The Fig 3.2 illustrated above will make the picture more clear.

Solutions Of Wrapping Attack-

- The security of TLS layer should be increased when the SOAP header is passed in transition[13].
- There should be some checksum or redundant bit(STAMP bit) in header so that if there is any change in the header then the signature should not be validated[13].
- *Best Practise-*

  i) Fetch validation key by establishing trust ,validating X.509 certificates etc.

  ii) validate **Signed info** with that key.

  iii)validate the refrences.

3.2 Malware Injection Attack /Cross Cloud Injection

Malware- Malware are **malicious codes** that are designed to compromise the confidentiality, integrity, authenticity,availability etc of the system. Malware can *be worms, trojans, viruses, spyware, adware, crimeware,botnets, scareware* etc[15]. Thus , malware can result into diruption in network services, computer operations, data breaches , theft & intrusive pop ups etc.

*Malware Injection***-** Its an act of injecting malicious code into cloud through web applications or others so that when user browse the content his system or application get infected.

Malware Injection Process [Advance Persistent Malware (Apt Malware)]- This attack is done by dynamically generated APT to compromise data of multiple cloud vendors firstly follow the principle of *esclation of privelage* by gaining the administrative rights and then modifying cloud applications[16]. The process how malwares spread is shown below-

Create Malware- When a client access a cloud, the cloud provider creates an image of customers virtual machine (VM) in the image repository of cloud. So, the attacker first create an image to be deployed in the cloud. This image (any OS) also contain the malicious content(script).

Seeding Malware -The attacker then upload the image to a public cloud .this requires authentication but attacker has already got the legitimate user ids and passwords

Executing Malware- The attacker integrate malware with web 2.0 apps like social networking site. When the user access that applications the malware code executes .This malicious code now access applications within the users virtual private cloud.

SOLUTIONS FOR MALWARE INJECTION-

- Use only secure web browsers and trusted applications.
- Malware analysers should be deployed.
- Return address , function pointers and global offset tables should be masked[17].
- Javascript countermeasure- validate input and do clientside encoding[18].
- Cryptographic hashing should be done because its provide integrity by matching the hash of new images[14].

3.3 Flodding Attacks [Dos/Ddos Attacks]

Flodding- Flodding is a DOS(Denial of Service) Attack to take the network down by routing the large traffic on destined server which results in network disruption , incomplete request, server outages and unavailability etc[19].

How Flodding Attack Works- Normally when a web server in cloud is overloaded or reach to certain thresold it transfer some of it instances to other server in order to get flexibility in server functionality but when attacker creates unnecessary packets of garbage data and increase traffic then server has to check authenticity of all these illegetimate packets which unnecessarily consumes memory and CPU utilisation of server. So, in order to attack, attacker firstly infects various machines and then redirects packet to single destination resulting server becomes busy. (DDOS Attack). Once the resources of server depleted , the server starves resulting in its breakdown . Flodding attacks are basically done through UDP(User Datagram Protocol) and ICMP(Internet Control Message Protocol)packets which are termed as[20]-

1) ***Udp Flood Attack***- Here large number of UDP packets are sent on random or destined port of victims machine. It also consumes large bandwidth.

2) ***Icmp Flood Attack-*** In this the malicious code do large volumes of pinging to the victim system thus the network bandwidth of victim system goes down.

3) ***Extensible Markup Language (Xml) Based Denial Of Service (X-Dos)-*** It is a coercive parsing attack which open Xml tags and exhaust CPU usage. Thus the network is flooded with illegitimate XML messages instead of packets which leads to communication failure[47].

4) ***Hypertext Transfer Protocol (Http) Based Denial Of Service (H-Dos)-*** It is using HTTP flooder and starts upto 1500 threads and sends randomized HTTP requests to web severs making the channel busy. This attack was recently done on Iranian security systems to infect their cloud data[47].

3.3.1 Flodding Tools

Agobot: It is a family of computer worms written in C++. These worms has various features like packet sniffing, keylogging, remotely update and remove installed bot , DDOS attack etc[42].

Mstream: It involves a series of "Zombies," programs planted on compromised systems that can be used to launch an attack against a network. The Zombies are controlled by a program placed on another compromised system called a "Master Controller”.The actual attacker triggers the attacks with a telnet session to the system running the master controller.The stream.c program floods a system with TCP ACK packets sent from random IP addresses. The denial of service occurs on the attacked system(s) that try to cope with the malicious ACK packets and on the network at large where every ACK packet also produces a RST packet and an ICMP host/destination unreachable packet[41] .

Trinoo: It is a set of computer programs to do DDos attack . It is a three stage process to attack the systems. The attacker firstly prepares the list of hosts to be compromised.Then he load scripts on these hosts to make it trinoo masters and lastly launch the attack[44] .

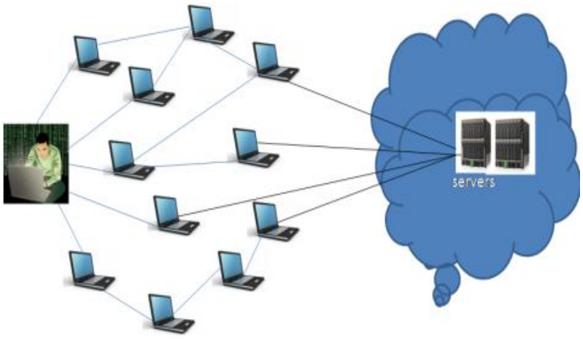


Fig 3.1 DDOS attack

Countermeasures Of Flodding Attack

- Load balancing should be done to mitigate and stop attacks.
- Packet Filtering Firewalls ,software patches should be installed to detect attacks[22].
- Implementing **HONEYPOTS** and **HONEYNETS**. Honeypot is a system that mirrors the attacker that he has compromised the system but in reality honeypots learn the tool and tactics of the attacker. Honeynet are categorised as research honeypots[21].
- DMM(DOS Mitigation Module) should be implemented which can protect environments like firewalls and intrusion detection system.

3.4 Other Security Attacks And Issues

Since with the rapid changes in the technology the nature of attacks are also changing very rapidly. As the new technology develops the attacker find out new loopholes and vulnerabilties in that. The frequency of attacks discussed above are more.Despite of these there is a large list of cloud security issues. Some of them are shown below[12,13,14]-

Man In The Middle Attack -Attacker places himself between users and intercepts the data.

Side Channel Attacks -Attacker can place malicious virtual machine near target cloud sever and can get info from timing information, electromagnetic leaks etc.

Browser Security- Attackers use various exploits of browsers to attack. These exploits are basically done through javascript or cross site scripting. Web browser with latest scripting techniques should be used.

Data Loss/Leakage & Stealing –The attacker get the credentials like ids and passwords through trojans, keyloggers etc and thus steal or destroy the data .this may result in loss of intellectual property which may lead to financial and competitive implications.

3.5 Cloud Tracebacking

The WS(web services) security provides security by placing security header into SOAP but this is not able to prevent DDOS at it can be easily spoofed. ***Service Oriented Traceback Architecture*(SOTA)** is a framework which can identify attacker by tracing back to source of attack. SOTA is based on DPM(Deterministic Packet Marketing) , a packet marketing algorithm which marks IP field and reserved flag within IP header. Each incoming packet which enters the edge ingress router is marked and outgoing packets are ignored. SOTM replace token which contains client authentication and replace with its own header and placed inside SOAP header. It does not change as it traverses through network. Victim of DDOS attack will be able to find the source and can filter it[46].

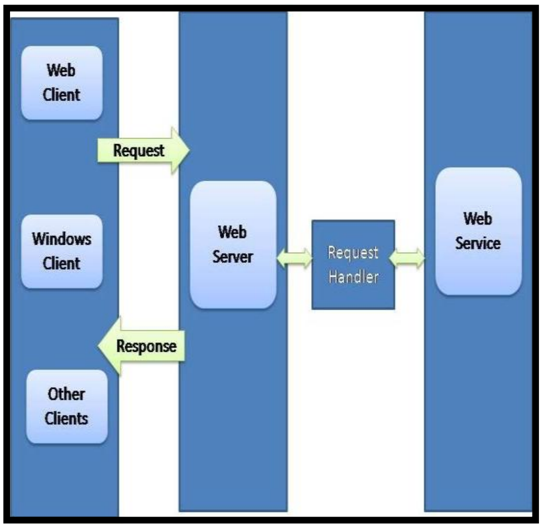


Fig 3.2 Web Service Architecture without SOTA

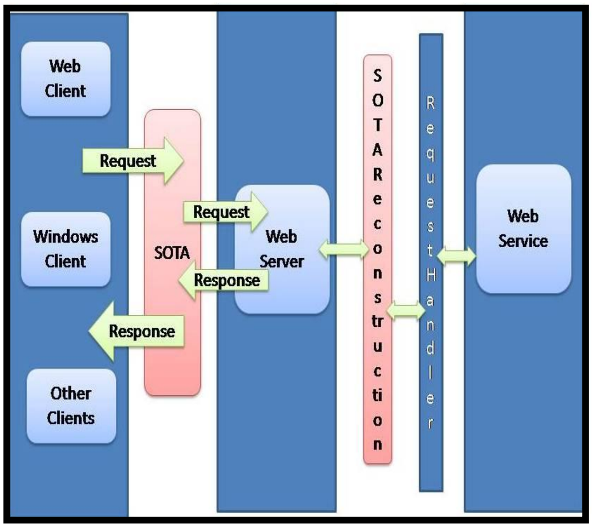


Fig 3.3 Web Service Architecture With SOTA

4.Privacy Issues In Cloud

Privacy means control over information.

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

. ***Alan Westin, Privacy and Freedom, 1967***

"Privacy is considered to be a fundamental human right."

. **Movius and Krup ,2009**

The given keywords make the picture of privacy little bit more clear[25]-

- PERSONHOOD
- INTIMACY
- SECRECY
- CONTEXTUAL INTEGRITY
- LIMITED ACCESS TO SELF

Privacy can be in any form like information, communication, territorial(living space), bodily etc. Since in cloud computing the services are outsourced so when user put his information and application on centralised servers then it may be possible that their information may be siphoned to someone else and the reasons for this can be anything like market competition for financial or personal gains. These informations can be personally identifiable or some sensitive informations like users email, his account or his organisations assets etc.Thus it can create great risk for the users. The research by ***Pew Internet And American Life Project*** shows below the concern of cloud users if there information is leaked or given to others without their consent [23].

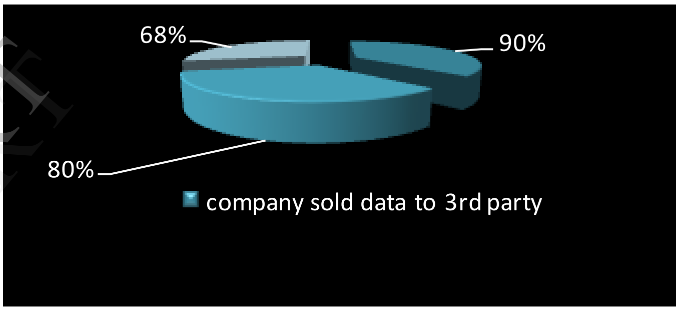


Fig 4.1 Privacy Concern Report by Pew Internet

So it is essential for the user that he should read the *Term Of Service* and *privacy policies* given by the cloud providers. He should understand the *use limitation and security safeguards* before giving his information. The most important thing is the location of data because it has to follow the legal aspects of that country where the data resides.

Countermeasures- Since privacy is believed to be a long term security issue so it is necessary to take actions regarding it[25].

Need Of Strong Governance- A strong governance will help in controlling over policies ,procedures, design, implementation of deployed service. If this is not done then vulnerable systems may be deployed and various legal implications may be overlooked putting data into risk.

Data Location- In-house data and information is more safe and secure as compare to when it crosses the geographical boundary of a country. During transborder flow of information various legal and regualatory regimes can raise variety of concerns. The flow of sensitive data can be issue of national security.So it is necessary to check whether the laws of a country where data is going permits its flow or not[24].

4.1 Privacy Laws

Privacy laws and regulations vary widely throughout the world. US has mostly sector-specific laws, with relatively minimal protections like ***Federal Communications Commission*** regulates telecommunications. In the same way ***European Data Protection Directive*** requires all European Union countries to adopt similar comprehensive privacy laws that recognize privacy as fundamental human right.Privacy commissions in each country are also there (some countries have national and state commissions).

US laws – recent additions[35,36,37,38,39,40]-

HIPAA (Health Insurance Portability and Accountability Act, 1996)-This law protects medical records and other individually identifiable health information.

COPPA (Children‟s Online Privacy Protection Act, 1998)-Web sites that target children must obtain parental consent before collecting personal information from children under the age of 13.

GLB (Gramm-Leach-Bliley-Act, 1999)-Requires privacy policy disclosure and opt-out mechanisms from financial service institutions.

Safe harbor(*Approved July 26, 2000 by EU*)-US companies self-certify adherence to requirements.Signatories must provide notices of data collected, purposes, recipients,choice of opt-out of 3rd-party transfers, opt-in for sensitive data.

FTC(Fair Information Practise Principles,1998)- These are the set of guidelines concerning with fair use of information of individuals .This is enforced in US , Canada and Europe. FIP is based on five principles guidelines which are:

- Notice /Awareness
- Choice/Consent
- Access/ Participation
  - Integrity/Security
  - Enforcement Redress

Fair Credit Reporting Act(FCRA)- It applies to consumer reports of US citizens and covers Credit Reporting Agencies .This act implements all FIP principles.

USA – Patriot Act(2001)- This act was enacted in september 2001 giving powers to US intelligence services to collect data on suspected terrorist actions. This act is now creating headache in US cloud companies as foreign customers concerned that US gov can intercept their confidential data.

In a recent study by ***Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*** by University of Amsterdam has published that this act has eroded privacy regulations on global scale. The study shows that theoritically US government can intercept European Data which has very strong privacy regulations on data leakage. This has raised eyebrows of various privacy policymakers of European nations.

EU Directive 95/46/EC(1995) -This is also known as Data Protection Directive(Birnhock,2008). This directive was implemented to harmonize privacy laws in different states of european union.It addresses personal data and PID(personally identifiable information) .

Payment Card Industry- Data Security Standard(PCI- DSS)- It is a self regulatory standard to protect cardholder data and implements various requirments for secure transmission of cardholder data through encryption . It also includes maintenance of secure system , creation of vaious policies , acess restriction on know basis and physical access restriction etc.

4.2 Adoption Of Privacy Enhancing Technologies

Privacy enhancing technologies should be used to protect the privacy of entities. This can be done through-

- Increase control
- Choose degree of anonymization
- Provide informed consent
- Data minimization
- Online Anonymizers – like Tor
- Privacy policy languages -XACML, P3P

4.3 Legal Implications Between Cloud Provider And User

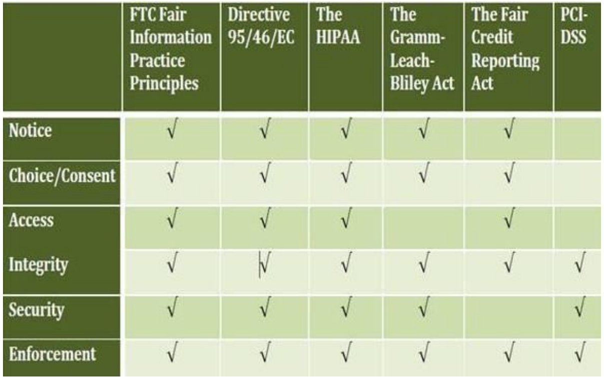
It is very important to have a crystal cut agreement between the provider and the user so that matter can be resolved in any future conflict..Organisations can be held liable if any subcontractor breaches the compilance with legislation[38,39]. It may include contractual questions like :

Service Level Agreements

- Accessibility and reliability of the cloud service
- Maintenance of the cloud service
- Warranty in the case of data disruption
- Liability in the case of third-party attacks

General contractual matters

- Liability in case of a treaty violation ("Data as a hostage")
- Consequences of a merger or an acquisition of the cloud provider .



	FTC Fair Information Practice Principles	Directive 95/46/EC	The HIPAA	The Gramm-Leach-Bliley Act	The Fair Credit Reporting Act	PCI-DSS
Notice	√	√	√	√	√	
Choice/Consent	√	√	√	√	√	
Access	√	√	√		√	
Integrity	√	√	√	√	√	√
Security	√	√	√	√		√
Enforcement	√	√	√	√	√	√

Fig 4.2 Common Principles In Privacy Regulation

In Fig 4.2 horizontal axis represents various Privacy Laws and regulations and vertical axis represents common principles in various privacy laws and regulations.

5.Trust Issues In Cloud

Trust-The origin of trust came from the nature and behaviour of human societies.We can say that trust is an amalgation of mental and emotional attitude. So trust is a subjective notion based on opinion and values of an individual[27].

Thus trust in cloud plays a very vital role because user is accesing and giving information as he is having trust in the service providers of cloud. Thus , lot of factors came into existence in users mind because of which he lacks confidence in cloud[26].

4.4 Trust Management

If these issues are not been cleared **satisfactorily** in users mind till then the real aim of cloud to provide services in form of Saas will not be fully fulfilled. So , there is a need to built a trust in between users and providers and this can be done through trust management and this can be done by[33]-

- Designing the product securely.
- Deploying it in secure state.
- Help customers to keep them secure .

- Client need to know trust in hardware and software that he is using is coming from legitimate source or not.
- Client should know that the data is coming from the person he expects.

Thus end trust is very important as it is an alignment between social, economic, political and IT product &services.So, there is a need to use *socio mechanism* to reinforce value.

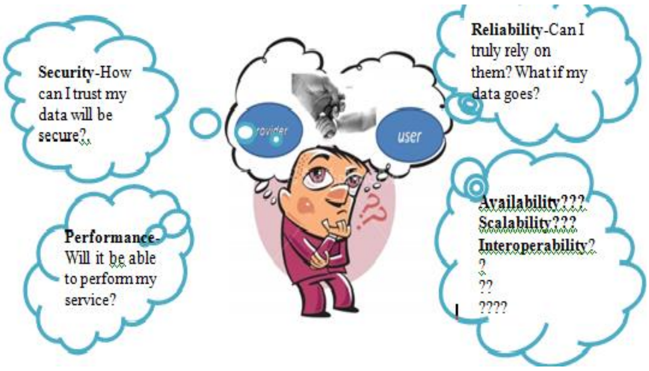

Security-How can I trust my data will be secure?
Performance-Will it be able to perform my service?
rovider
user
Reliability-Can I truly rely on them? What if my data goes?
Availability???
Scalability???
Interoperability?
?
??
????

Fig 5.1 Trust issues in cloud

5.2 Trusted Zones

Trusted zones should be implemented as a part of virtual infrastructure. The applications should be categorised on the basis of their services, users, hardware , software etc and virtual cluster of these should be made.Thus creating trusted zones protect against cybercriminals by use of cyber intelligence and strong authentication.It enforces trust policies on all the three level[28]:

Vm-Level- It is done by grouping VM into trusted zones and controlling it through provisioning policies.

Data Level- It avoid data leakage and control data in cloud provider.

Identity Level- This will manage user access within and out of trusted zones.

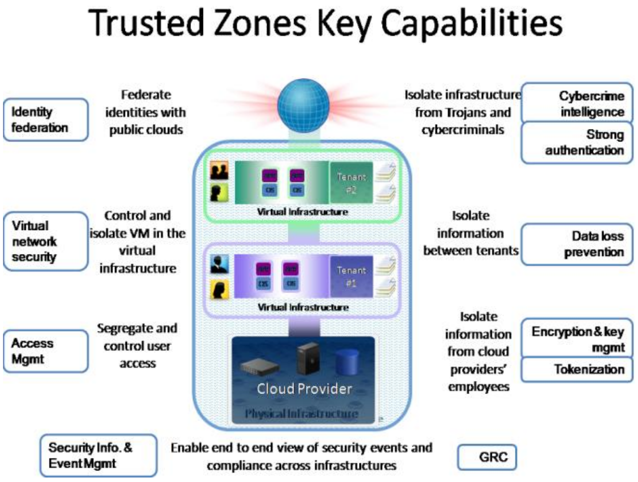

Trusted Zones Key Capabilities
Identity federation
Federate identities with public clouds
Isolate infrastructure from Trojans and cybercriminals
Cybercrime intelligence
Strong authentication
Tenant #2
Virtual Infrastructure
Virtual network security
Control and isolate VM in the virtual infrastructure
Isolate information between tenants
Data loss prevention
Tenant #1
Virtual Infrastructure
Access Mgmt
Segregate and control user access
Cloud Provider
Physical Infrastructure
Isolate information from cloud providers' employees
Encryption & key mgmt
Tokenization
Security Info. & Event Mgmt
Enable end to end view of security events and compliance across infrastructures
GRC

Fig 5.2 RSA Trusted Zones[28]

5.3 Identity Management

It helps in identifying individuals in a system and controlling access to the resources .It is a better way to do identification, authentication, authorization[25] .It can be done in many dimensions like-

- Technical: identity management systems
- Legal: Data protection
- Police: Identity theft
- Social and humanity: privacy
- Security: access control
- Organizations: division of access

These above factors will help in trustworthy computing. The below is shown a trusted and dependable model of cloud architecture where solid lines shows services and data flows while dashed line shows control flows in trust management[30] .

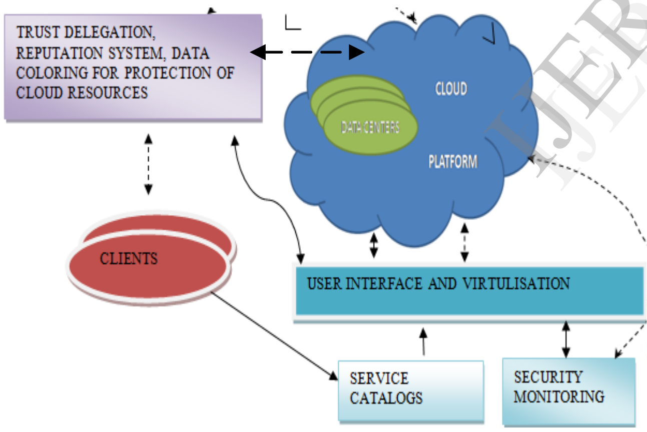

TRUST DELEGATION, REPUTATION SYSTEM, DATA COLORING FOR PROTECTION OF CLOUD RESOURCES
CLOUD
DATACENTERS
PLATFORM
CLIENTS
USER INTERFACE AND VIRTULISATION
SERVICE CATALOGS
SECURITY MONITORING

Fig 5.3 Trust model

6. Accountability Issues

Accountability is a governance concept which has different meanings in different domains like in leadership it relates with responsibility, administration, implementation etc[31]. In computer science it is related to reporting and auditing mechanism. These days more cohesive and practical approach to protect data across different regulatory systems are being developed. According to Galway Project –*"Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."[32].*

So accountability is done to –

- Deal with Faults.
- Deal with Misbehaviours.
- Provides trust.
- Gives transparency
- Incentives to avoid faults.

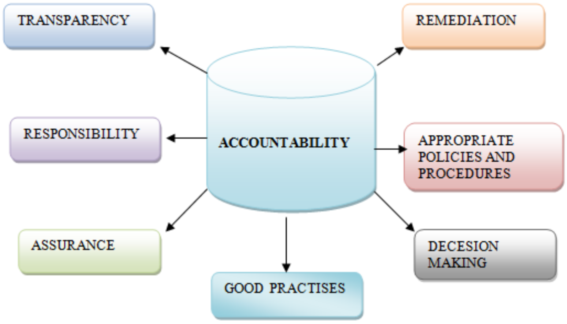


Fig 6.1 Central components of accountability

OECD recommendation council has also given the accountability principle .An accountability situation in a cloud is shown in fig 6.2.Suppose Alice(service provider) and Bob(sevice beneficiary) have face a situation that in which they got a bug in their software then how both they will know that who is accountable for all this happenings.

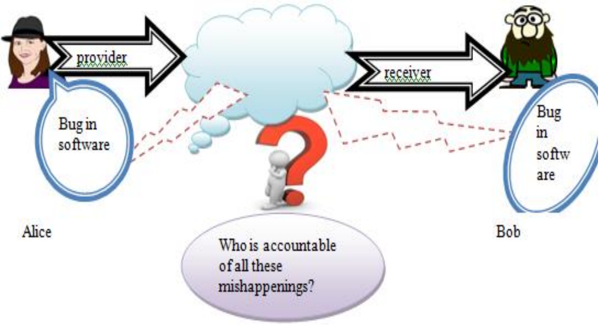


Fig 6.2 An Accountability Scenario

In this condition the cloud should be make accountable to check the accuracy and verifiability that from where the bug has occurred.Since if cloud records all the actions in a tamper evident log then both can audit their logs and check the faults and thus the legal actions can be taken according to the policies and procedures. Thus it will help providers to attract customers and helps them in handling disputes etc. Thus *Accountable Virtual Machines*(AVM) should be deployed[34].

Thus an organisation should appoint someone to ensure that privacy policies and procedures are being followed according to the given rules and regulations. Auditing should be done time to time to cross check the practises that are being performed . Since the laws differ in different geographic area so it is necessary to keep eye on all the things. OECD council has also given accountability principle to check the security and privacy issues.HIPPA(Health Insurance Portability and Accountability Act) has given various safeguard regarding healthcare facilities. So cloud providers should follow these regulatory concerns to follow security and privacy.

7.Conclusion

The issues discussed above tells that cloud inspite of being very productive services has various security loopholes and vulnerabilties. So it is necessary for the users to know about all the terms and services and the legal aspects before going to cloud.It is necessary for the user as well as provider to be alert as attacker can do any innovative malicious activity at any time.So clouds can not deplete if you are vigil.

8. Acknowledgement

I really thanks to Dr. Gaurav Gupta(professor IIIT-Delhi) for his lectures on Digital Forensic and legal issues.

9. References

[1] A history of cloud computing. http://www.computerweekly.com/feature/A-history-of-cloud-computing.

[2] Into the cloud out of the fog. Ernst & Young's 2011 Global Information Security Survey. http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog2011_GISS/$File/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

[3] Cloud Computing Security- Wikipedia. http://en.wikipedia.org/wiki/Cloud_computing_security

[4] Trend Micro- Canadian IT SME Survey 2011. http://ca.trendmicro.com/imperia/md/content/ca/environics_-_trend_micro_it_security_-_final_report_-_jul_18-2011.pdf

[5] Troubles in Clouds. http://www.experian.com/blogs/data-breach/2011/07/19/trouble-in-the-clouds-data-breaches-threaten-cloud-computing/

[6] http://www.idc.com/prodserv/idc_cloud.jsp.

[7]Epsilon breach http://www.infosecisland.com/blogview/12814-Epsilon-Breach-Deals-Another-Blow-to-Cloud-Security.html

[8]Epsilon breach .http://www.insideprivacy.com/data-security/data-breaches/epsilon-data-breach-highlights-security-challenges-in-the-cloud

[9] Epsilon breach .http://bizcloudnetwork.com/epsilon-and-amazon-cloud-security-issues-not-adequately-addressed

[10]Citigroup acknowledges Breach http://searchsecurity.techtarget.com/news/2240036729/Citigroup-acknowledges-data-security-breach

[11]http://www.ciphercloud.com

[12] Meiko Jensen, Jorg Schwenk,Nils Gruschka, Luigi Lo Iacono-"*On Technical Security Issues In Cloud*".2009 IEEE International Confrence on Cloud Computing.

[13]Kazi Zunnurhain and Susan V. Vrbsky."*Security Attacks And Solution In Clouds*". The University of Alabama ,Tuscaloosa, AL 35487-0290. http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf

[14] Danish Jamil, Hassan Zaki-"*Security Issues In Cloud Computing And Countermeasures*". Danish Jamil et al. / International Journal of Engineering Science and Technology (IJEST).

[15]Malware Injection Attack- http://www.w3.org/TR/xmldsig-bestpractices/

[16]TD Dave".Cross Cloud Injection in multiple vendors leading to advance persistent threat.http://lists.webappsec.org/pipermail/websecurity_lists.webappsec.org/2011-April/007675.html

[17]Thorsten Holz, Herbert" *Detection of Intrusions and Malware, and Vulnerability Assessment*".

[18] Nimrod Luria."Security in Web 2.0 World".Microsoft Tech Israel.

[19]Flodding.http://www.webopedia.com/TERM/F/Flooding.html

[20] Stephen M. Specht, Ruby B. Lee." *Distributed Denial of Service:Taxonomies of Attacks Tools And Countermeasures.".* http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf

[21]NathalieWeiler."*Honeypots for Distributed Denial of ServiceAttacks*".http://www.csl.mtu.edu/cs6461/www/Reading/Weiler02.pdf

[22] Ezaz Ahmed ,George Mohay,Alan tickle, Sajal Bhatia." *Use of Ip Address for High Rate Flodding Attack Detection*". Queensland University of technology.

[23]Cloud Computing.http://epic.org/privacy/cloudcomputing/#Issues

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

[25]Lecture Notes Of Dr Gaurav Gupta and Dr Ponnurangam Kumarguru[IIIT-Delhi].

[26]In Cloud We Trust. http://blog.kawaobjects.com/?p=134

[27] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan**."** *Trust and Trust Management in Cloud Computing – A Survey***".** University Utara Malaysia

[28] Bernard Montel "*RSA Approach for Securing The Cloud*". July 2010.

[30] *Kai Hwang, Deyi Li "Trusted Cloud Computing with Secure Resources and Data Coloring"* http://gridsec.usc.edu/hwang/papers/trusted-cloud-computing.pdf

[31]Accountability- Wikipedia.

[32]Siani Pearson**.***"* *Towards Accountability in the Cloud*" ,HP laborataries.http://www.hpl.hp.com/techreports/2011/HPL-2011-138.pdf

[33]RSA conference 2010- Creating A Safer and more Trusted Internet. http://www.youtube.com/watch?v=X6XBgOzwZ9Q

[34]Peter Druschel joint work with Andreas Haeberlen^1, Petr Kuznetsov^2, Rodrigo Rodrigues
Accountable distributed systems and the accountable cloud".

[35]Avoiding US based clouds, CSK guide http://ccskguide.org/avoiding-us-based-clouds/

[36] Europeans outraged over the us using patriot act for worldwide spying http://rt.com/usa/us-patriot-act-cloud-381/

[37] *Cloud Computing and Privacy Laws!* Prof. Dr. Thomas Fetzer, LL.M. Technische Universität Dresden Law School.

[38] *Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice* : Joep Ruiter and Martijn Warnier. http://homepage.tudelft.nl/68x7e/Papers/spcc10.pdf

[39]*Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications*: Dr. Mohammed A. T. Alsudiari1, Dr. TGK Vasista ,College of Business Administration, King Saud University, Riyadh, KSA,

[40] 3 more major US banks for possible cyber attacks http://www.nbcnews.com/technology/technolog/3-more-major-us-banks-report-possible-cyber-attacks-6126050.

[41]DDOS mstream handler agent Command http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20045.

[42]AGOBOT http://en.wikipedia.org/wiki/Agobot

[43]*Computational Grids****:*** Ian Foster, Carl Kesselman, University of southern California http://www.globus.org/alliance/publications/papers/chapter2.pdf.

[44]Trinoo http://en.wikipedia.org/wiki/Trinoo.

[45] Security Guidance for Critical Areas of Focus In Cloud Computing V3.0 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[46]*Protecting WebServices with Service Oriented Traceback Architecture* : Ashley Chonka,Deakin University and Yang Xiang Central Queensland University. http://dro.deakin.edu.au/eserv/DU:30018209/Zhou-protectingwebservices-2008.pdf

[47]Overview of Cloud Computing attack ijeit.com/vol%201/Issue%204/IJEIT1412201204_57.pdf

[48]IEEE: A research on the indicator system of Cloud Computing security risk assessment, Jijun Zhang,Dejain Sun,Donhang Zhai, Library Airforce Aviation University China. http://toc.proceedings.com/15402webtoc.pdf