Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks

S VivinSandar
Department of Information Technology
Karunya University
Coimbatore ,India.

SudhirShenai
Department of Information Technology
Karunya University
Coimbatore, India

ABSTRACT
"Cloud Computing", a new wave in the Internet revolution, transforms the kind of services provided over the Internet. The Cloud Services can be viewed from two perspectives, one as Cloud Service Provider and the other as Cloud Service Consumer. Assurance of security in the Cloud Service is a major challenge for the Providers, as it's the biggest concern for the Consumers to opt for the service, which in turn decides the prospects of the business in Cloud Service. The Security can be administered in the Cloud at various levels and for several types of attacks. The threats and the attacks on the Cloud service can be common prevailing attacks in the internet or can be cloud specific. This paper deals about the threats and the counter measures of the prevailing DDoS attacks on the Cloud Environment as well as the Cloud Specific Vulnerabilities to these attacks. In specific, HTTP and XMLbased DDoS attacks on the cloud service are experimented under proposed security framework for EDoS Protection. A Cloud Service was hosted on Amazon EC2. The Service was targeted by HTTP, XML DDoS attacks from several nodes, which lead to the scaling of the service by consuming more Amazon EC2 resources, which in turn lead to Economic Denial of Sustainability to the Cloud Service under attack. Thus this paper explores the transformation of traditional Distributed denial-of-service (DDoS) attack into cloud specific Economic Denial of Sustainability (EDoS) attack.

KEY WORDS
Cloud Service Security, DDoS attack, EDoS attack

1.INTRODUCTION
Cloud Computing is a heterogeneously distributed environment, which provides highly scalable, elastic and always available resources as service through Internet. The cloud computing provides everything as a service. In cloud computing, large pools of resources are available and it is allocated dynamically to the applications. The cloud infrastructure is fully virtualized to utilize the hardware effectively. The cloud infrastructure supports all hardware architectures [1].The cloud middleware provides an abstraction to the underlying physical cloud resources. Thus providing security to cloud is a complicated issue. The papers [4][5][6][7] give an clear idea about the security issues related to cloud computing. DimitriosZissis,DimitriosLekkas[8] has classified the security requirements and threats exist at variouscloud service levels. Further Cloud Security Alliance (CSA) give us the areas for security needed in cloud computing [9].

Cloud is prone to varieties of attack such as the wrapping attack [22], Malware Injection Attack, Metadata Spoofing attack [21], SQL injection attack, Cross site scripting, DDoS attack and DNS attack. In specific, Cloud services are vulnerable to DDoS attacks. It's very difficult to identify the legitimate traffic from the attack traffic. Detecting and filtering the attack is a challenging task in an environment like cloud where everything is virtualized. There is no one technique available, which can completely eliminate the DDOS attacks. The paper [10] elicits the details of the recent DDoS attack on the web. The BitBucket a Code hosting web service running on the amazon cloud was down for more than 19 hours due to the DDoS attack[11]. Most of the vulnerabilities pertaining to Traditional Distributed Environments are applicable to Cloud Computing environment as well. So all the vulnerabilities in the cloud are not necessarily cloud specific. As noted in the paper [3], a vulnerability is cloud specific if it

- is intrinsic to or prevalent in a core cloud computing technology,
- has its root cause in one of NIST's essential cloud characteristics,
- is caused when cloud innovations make tried-and-tested security controls difficult or impossible to implement, or
- is prevalent in the established state-of-the-art cloud offerings.

Further chapters, give detail about the DDoS attack on Traditional Distributed Environment and Cloud Computing Environment. Finally, the paper highlights how the Traditional DDoS attack is transformed into cloud specific EDoS attack.

2.DDOS ATTACK
A denial-of-service (DoS) attack is an attempt to make a computer resource (e.g. the network bandwidth, CPU time, etc.) unavailable to its intended users. To overload the necessary network and CPU resources, attackers tend to use a large number of machines to launch the Distributed DoS (DDoS) attacks [2].The DDoS attack in a non-cloud environment may not necessarily disturb the service, but it may contribute to economic loss. As the cloud environment is highly scalable, the service will consume more resources during attack period to maintain the SLA, which in turn contributes to the revenue loss. Thus the traditional DDoS attack can be transformed into an Economic Denial of Sustainability attack (EDoS) in the cloud Environment. The EDoS attack is a new breed of attack specifically targets the cloud environment

3.EDOS ATTACK

Many organizations move their business into cloud for the following reasons. They no need to buy the entire infrastructure. The maintenance cost is nill.There by the organization can reduce the purchasing and operational costs. They need to pay for only the resources used [1].Cloud services are provided in the form of service level agreements (SLA).The SLA defines the level of service required by the user. Some SLA will restrict the use of cloud resources to the customers. Some SLA provides infinite amount of resources to customers for QoS. The Cloud services are provided as Pay-per-Use. Therefore the resource utilization and the processing power are charged to the customer by the provider. The DDoS attack aims to utilize the cloud resources there by denying the service to the legitimate users. In the absence of any proper mechanisms to counter DDoS attack the resources can be allocated to the DDoS requests.

As mentioned earlier identifying the attack traffic from the legitimate traffic is a difficult one and also there is no one technique which will completely eliminate the DDoS attacks. Therefore the DDoS attack may deplete the cloud resources rapidly. To provide 100% availability the provider may allocate more and more resources to the attack itself. More instances of the services may be launched according to the customers SLA. Finally the resource utilization and the processing power are charged to the customer. Thus a traditional DDoS attack can be transformed into an Economic Denial of Sustainability attack (EDoS) in the cloud Environment. If vulnerability is prevalent in the state-of-the-art cloud offerings, it must be regarded as cloud-specific. Thus the cloud is vulnerable to EDoS attack, the EDoS attack can be cloud specific.

4.COUNTER MEASURES

We must know the security requirements or security objective for the cloud.It is important that the security mechanism should satisfy the security requirements.

According to DimitriosZissis,Lekkas, the security objectives within a distributed system are essentially[8]:

- To ensure the availability of information communicated between or held within participating systems;
- To maintain the integrity of information communicated between or held within participating systems, i.e. preventing the loss or modification of information due to unauthorized access, component failure or other errors;
- To maintain the integrity of the services provided, i.e. confidentiality and correct operation;
- To provide control over access to services or their components to ensure that users may only USC services for which they are authorized;
- To authenticate the identity of communicating partners (peer entities) and where necessary (e.g. for banking purposes) to ensure non-repudiation of data origin and delivery;
- Where ever appropriate, to provide secure interworking with the non-open systems world.
- To ensure the confidentiality of information held on participating systems.
- Clear separation of data and processes on the virtual level of the cloud, ensuring zero data leakage between different applications.
- To maintain the same level of security when adding or removing resources on the physical level.

There are many mechanisms which serve as a counter to the attacks which disturb security objectives of Cloud. Some few security mechanisms used in cloud such as Intrusion detection system, Packet Filtering, Virtual machine monitoring, Packet marking and trace back, trust and on demand mitigation techniques are discussed in the following section.

4.1 Distributed Cloud Intrusion Detection Model [12]

The Distributed Cloud IDS is a multi-threaded IDS. This uses sensors to sense and monitor the network traffic and checks for malicious packets. The system sends alarm to the third party monitoring organization who reports to the cloud service provider,

- It consist of three phases
- Processing and Querying
- Analyzing and Processing
- Reporting

4.2 CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment [14]

Confidence-Based Filtering has two periods, attack period and non-attack period. When the non-attack period is enabled the normal profile is generated.During attack period the CBF stops generating the profile and extracts the attributes from the packet and checks it legitimacy then decides to drop the packet or to allow it.

4.3 Defend Against Denial of Service Attack with VMM[15]

A virtual machine monitoring mechanism is proposed to protect the cloud from the DoS attacks. The VMM works in an isolated environment and detects the attack when it occurs. If the available resources are less than the threshold, the VMM suspects the existence of the DoS attack. Then the guest OS and the application are duplicated in the isolated environment

4.4 EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing [16]

EDoS-Shield is a mechanism to protect the cloud from the EDoS attack. This architecture consists of two components they are virtual firewall and the cloud verifier node. The virtual firewall acts as a filter. The VF uses the whitelist and Blacklist for making decision. The V nodes use the graphic Turing tests such as CAPTCHA to verify legitimate requests at the application.

4.5 Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks[17]

A mechanism which involves the determinist packet marking and service oriented trace back architecture is used to protect from the XML DoS attack. This is a track back mechanism which identifies the source of the attack and filters it. Here cloud trackback and cloud protector are used. Cloud trace back marks the incoming packets and the cloud protector filters the packets. The cloud protector is a trained back propagation neural network.

4.6 sPoW: On-Demand Cloud-based eDDoS Mitigation Mechanism[18]

Self-verifying Proof of- Work (sPoW) is proposed to overcome the eDDoS attack. On-demand network and application-level eDDoS mitigation Mechanism can be used for sPoW. The main aim is to filter the eDDoS traffic before it triggers the billing Mechanism. The idea behind the sPoW is to transform the network level eDDoS traffic to distinguish a filter and prioritize legitimate traffic.

Table 1. Summary of Countermeasures

Approaches	Focus	Methodology	Distributed approach	Learning ability	Balances the workload	Tolerance to failure	Time response	Scalability
Distributed Cloud Intrusion Detection Model [12]	DDoS attack and cross site scripting	Intrusion Detection system	Yes	Yes	Yes	No	Real Time	Yes
A New Trusted and Collaborative Agent Based Approach [13]	SQL injection attack, Cross site scripting, DDoS.	Trust and Authentication	Yes	No	N o	No	Real Time	No
Implementing Trust in Cloud Infrastructures [20]	DDoS attack	Trust based	No	No	No	Yes	Real Time	Yes
CBF: A Packet Filtering Method for DDoS Attack Defense [14]	Distributed Denial-of-Service attack	Packet Filtering	Yes	Yes	Yes	No	Real Time	Yes
Defend Against DDoS Attack with VMM [15]	DDoS attacks	Traffic monitoring	No	No	Yes	No	-	Yes
EDoS-Shield [16]	EDoS attack	Virtual firewall and authentication	No	Yes	No	No	Real Time	Yes
Cloud Traceback [17]	HTTP and XML based DoS Attack	Packet marking and Traceback	Yes	Yes	Yes	Yes	Real Time	Yes
sPoW: On-Demand Cloud-based eDDoS Mitigation [18]	EDoS attack	Packet Filtering	Yes	Yes	Yes	No	Real Time	Yes
A Layered Security Approach for Cloud Computing [19]	DDoS attack	Security architecture	No	No	Yes	No	-	No
Addressing cloud computing security issues [8]	Common	Trust, cryptography and certificate.	Yes	No	No	No	-	No

4.7Implementing Trust in Cloud Infrastructures [20]

Bonafides system is proposed for remote attestations of security-relevant parts of the cloud infrastructure. It detects the unintended or malicious modifications of cloud infrastructure configurations on runtime. With the trusted computing technology the Bonafides System is protected from Tampering. A DoS attack is carried out to measure the performance of the system.

4.8 A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security [13]

New frame work based on trust is proposed which is trusted and collaborative agent-based two-tier framework. This is used to provide security to the network, infrastructure and for data storage in the cloud platform. This is to protect the cloud service from the SQL injection attack, Cross site scripting, DDoS attack and DNS attack Here two tire architecture is proposed .The tire one consist of proxy server and the tire two consist of the cloud service provider . The working is as follows first the cloud service user (CSU) provides uses the certificate to get information from proxy server. The authenticated CSU updates the data based on the degree of trust. According to the degree of trust operations are performed. A threshold value is maintained for trust .The request having the Degree of trust below the threshold are dropped.

4.9 A Layered Security Approach for Cloud Computing Infrastructure [19]

Dynamic infrastructure Security model is proposed here. This consists of four layers such as network, storage server and application. It has two dynamic security types horizontal and vertical, also, an enterprise level principles. The horizontal is specific to each layer and the vertical is for the interface

between each of the layers. The infrastructure security tools can be used to implement the dynamic configuration request.

4.10 Addressing cloud computing security issues [8]

5. SIGNIFICANT ANALYSIS AND SPECULATION

The major focus of this paper is to find a cloud specific vulnerability.

- The EDoS attack is identified as a Cloud Specific DDoS attack.
- Various techniques that are prevalent today are not up to the mark to protect the cloud from the EDoS attack.
- The counter mechanisms which are implemented only in the target machine are not efficient to defend against the DDoS attack. The approach should be a distributed one.
- On demand mitigation techniques will be well suited for the cloud environment.
- The mechanism which is fully based on trust might not be a good choice.
- The cloud computing is not yet standardized, so the vendors uses their proprietary security mechanisms.
- The Cloud Computing should be standardized soon, so that a solid solution can be proposed and implemented.
- The mechanism should be interoperable between different cloud providers.
- The mechanisms focusing on the identity of the user is a better solution to avoid the EDoS attack.
- Distributed traceback approach can be used to eliminate the attack traffic in the network itself.
- More intelligent traffic monitoring techniques are needed.

6. SECURITY FRAMEWORK FOR EDOS ATTACK PROTECTION

Considering the requirements that are necessary for the countermeasure, new security architecture is proposed. This frame work can be implemented to protect the cloud services from the EDoS attacks. The proposed framework consists of firewall which is the entry point for the cloud and Client puzzle server, which is a well-known technique used in mitigating the DDoS attack. The working of the EDoS Protection framework is explained with two scenarios, one with a legitimate user and another with an attacker accessing the service.

6.1 Scenario 1: Legitimate User

The legitimate user access the cloud services

The solution uses the public key cryptography. Here the solution is based on the trust. The trusted third party will provide certificates to all the layers such as hardware, virtual, user and network layers of the cloud architecture. Here the certificate based authentication is used .Each layer will use the other layer certificate for authentication.

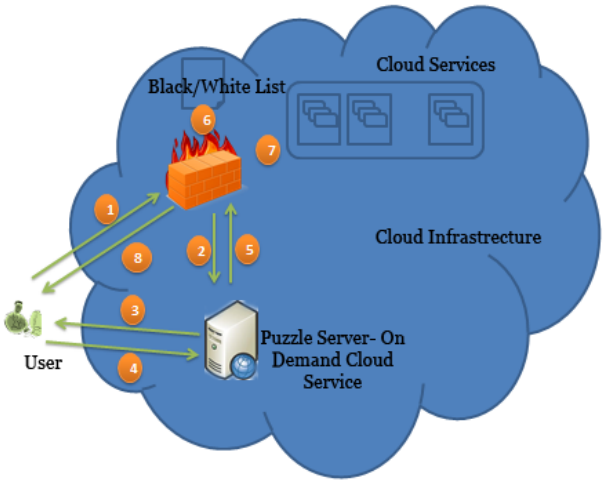

Fig 1: Scenario User

1:The user request to access cloud service is first intercepted by the firewall
2: The firewall then redirects the request to the puzzle server which is an on demand cloud service
3: Puzzle server sends the client a puzzle to solve.
4: The user solves the puzzle and sends the result to the puzzle server
5: The puzzle server verifies the result if correct, sends positive acknowledgement to the firewall
6: The fire wall adds the client's IP to its white list
7: The firewall redirects the user to access the cloud services
8: The service is offered to client by the provider

6.2Scenario 2: Attacker

Attacker access the cloud services

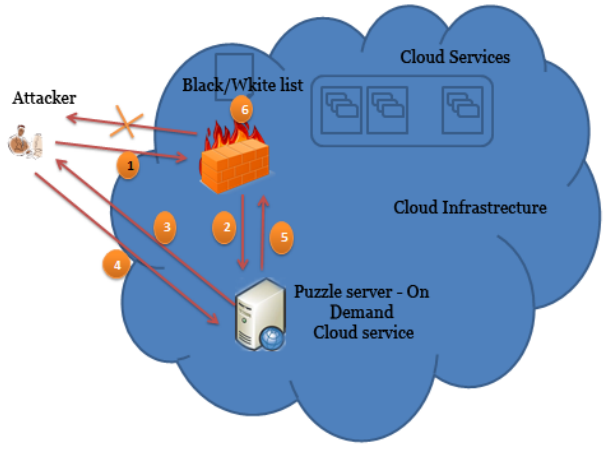

Fig 2 Scenario Attacker

1: The attacker request to access the cloud services is first intercepted by the firewall.
2: The firewall then redirects the request to the puzzle server which is an on demand cloud service
3: Puzzle server sends the client a puzzle to solve.
4: The user solves the puzzle and sends the result to the puzzle server

5: The puzzle server verifies the result, if wrong, sends the negative acknowledgement to the firewall
6: The firewall adds the client's IP to its black list

The packets identified as the attack can be dropped by the firewall. The requests fail to satisfy the puzzle can be considered as an attack .The source address of the attacker can be stored in the black list. Hence the future packets from the blacklisted IP can be dropped by the firewall.

7. EXPERIMENT

The experiment was conducted in the amazon EC2 cloud to demonstrate the EDoS. The Fig 3 gives the experimental setup. The high end instances such as the large and extra-large instances are used for creating the experimental setup. Four extra-large EC2 instances are clustered together using a load balancer to form a Server Cluster. The Web service applications are loaded in the Server Cluster. A group of four large EC2 instances are used as the AttackerNetwork, and a large instance is used as the legitimate user. To simulate the attack, HTTP requests to the web service are continuously given to the server cluster in a large scale.The experiment results were taken from the AWS monitoring system, and the incoming packets are monitored trough the packet capturing application wireshark. The number of HTTP requests and response are tracked. The SOAP messages are also tracked.

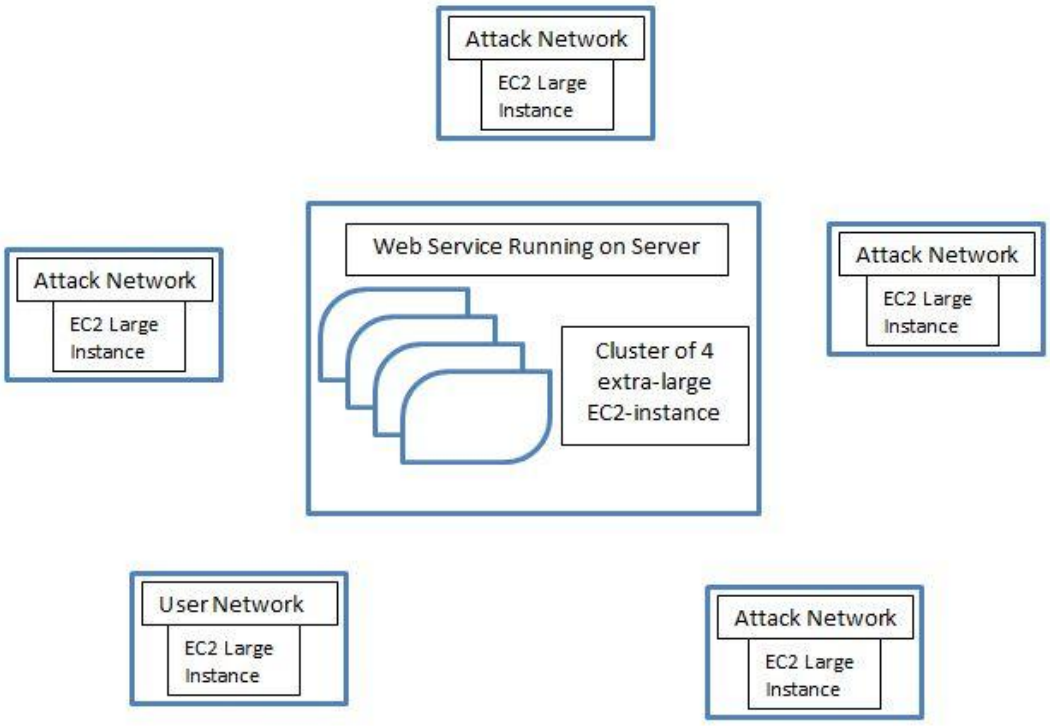

Fig 3: Experiment Setup

The average response time for each request to be processed by the server is also calculated. The graph drawn from the data obtained from the experiments shows the occurrence of Economic Denial of Sustainability for the DDoS Victim. When the numbers of attacks increase, the load balancer distributes the load to more instances, hence incurring cost for the extra instances.An increase in the attack, increases deployment of instances to meet the SLA and hence the cost also increases. Thus the traditional DDoS attack in the cloud can be transformed into an EDoS attack. The Fig 4 shows the cost escalation of the service for one day.

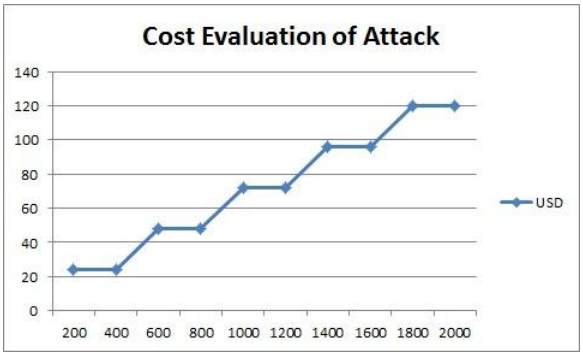

Fig 4: Number of Attack vs. Cost (USD)

8.CONCLUSION

Cloud Computing provides a wide range of services. Existing Security mechanisms are not up to the mark .New approaches are needed which should be a distributed and scalable approach. New form of attacks is possible in the cloud. One such kind of attack is EDoS attack which is a new breed of DDoS attack. The EDoS attack exists only in the cloud so it can be termed as one of the cloud specific attack. A new security EDoS protection frame work is proposed. Also, an experiment is conducted to demonstrate the EDoS attack.The existing approaches are not capable of completely eliminating the EDoS attack. Research is still needed to provide a better mechanism to protect the cloud from EDoS attack.

9.REFERENCES

[1] Xue Jing, Jens Nimis, Zhang Jian-jun,"A Brief Survey on the Security Model of Cloud Computing" *2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.*

[2] Denial-of-service attack ,Wikipedia,

http://en.wikipedia.org/wiki/Denial-of-service_attack

[3] Bernd Grobauer, Tobias Walloschek, and ElmarStöcker "Understanding Cloud Computing Vulnerabilities" *Cloud Computing, Copublished By The IEEE Computer And Reliability Societies*

[4] KrešimirPopović, ŽeljkoHocenski "Cloud computing security issues and challenges", *MIPRO 2010*, May 24-28, 2010, Opatija, Croatia

[5] Paul Wooley ,Tyco Electronics ,"Identifying Cloud Computing Security Risks"University of Oregon ,Applied Information Management Program, Feb 2011

[6] V VenkateswaraRao , G. Suresh Kumar, Azam Khan, S SanthiPriya,"Threats and Remedies in Cloud"*Journal of Current Computer Science and Technology*, Vol. 1 Issue 4[2011]101-106

[7] A Survey on Cloud Computing Security,Challenges and Threats", *Journal of Current Computer Science and Technology* Vol. 1 Issue 4[2011]101-106

[8] DimitriosZissis , And DimitriosLekkas,"Addressing cloud computing security issues Future Generation Computer Systems", *Future Generation Computer Systems.*

[9] Cloud Security Alliance,"Critical Areas of Focus in Cloud Computing" ,*Prepared by the Cloud Security Alliance* ,December 2009

[10] KetkiArora ,Krishan Kumar, And Monika Sachdeva ," Impact analysis of DDOs Attack", *International Journal on Computer Science and Engineering* (IJCSE)- Vol. 3 No. 2 Feb 2011

[11] Metz C "DDoS attack rains down on Amazon cloud", The Register,Online Article, http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage,

[12] IrfanGul, M. Hussain "Distributed Cloud Intrusion Detection Model" *International Journal of Advanced Science and Technology* Vol. 34, September, 2011

[13] Shantanu Pal, SunirmalKhatua, NabenduChaki, SugataSanyal ,"A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", *Annals of Faculty Engineering Hunedoara International Journal of Engineering*; scheduled for publication in Vol. 10, Issue 1, February, 2012. ISSN: 1584-2665.

[14] Qi Chen, Wenmin Lin, Wanchun Dou , Shui Yu "CBF A Packet Filtering Method for DDoS Attack Defense in Cloud Environment"*2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.*

[15] Siqin Zhao, Kang Chen, WeiminZheng ,"Defend Against Denial of Service Attack with VMM" , *Eighth International Conference on Grid and Cooperative Computing*

[16] Mohammed H. Sqalli Fahd Al-HaidariKhaledSalah,"EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing ",*Fourth IEEE International Conference on Utility and Cloud Computing.*

[17] Ashley Chonka,Yang Xiang n, Wanlei Zhou, AlessioBonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", *Journal of Network and Computer Applications* 34 (2011) 1097–1107

[18] Soon HinKhor Akihiro Nakao, "sPow On-Demand Cloud-based eDDoS Mitigation Mechanism"*Fifth Workshop on Hot Topics in System Dependability*

[19] Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth,"A Layered Security Approach for Cloud Computing Infrastructure", *10th International Symposium on Pervasive Systems, Algorithms, and Networks.*

[20] Ricardo Neisse, DominikHolling, Alexander Pretschner,"Implementing Trust in Cloud Infrastructures",*2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.*

[21] Meiko Jensen, J¨orgSchwenk , Nils Gruschka, Luigi Lo Iacono ,"On Technical Security Issues in Cloud Computing", *IEEE International Conference on Cloud Computing*.

[22] Nils Gruschka and Luigi Lo Iacono,"Vulnerable Cloud: SOAP Message Security Validation Revisited", *IEEE International Conference on Web Services*