Detect and Filter Traffic Attack through Cloud Trace back and Neural Network

Mansaf Alam, Kashish Ara Shakil, Mohd. Salman Javed, Manzoor Ansari and Ambreen

***Abstract*—Cloud computing is one of the major technologies predicted to revolutionize the future of computing world. The concept of delivering IT as a service has several astounding features and advantages. Cloud is an enchanting option for small and medium enterprises to reduce upfront investment, enabling them to use sophisticated business intelligence applications that only large enterprises could previously afford. Cloud computing has huge potential to improve overall productivity and reduce cost. It is a new consumption and delivery model for IT services but its security is still a pitfall. Cloud computing is threatened by several security issues although most of them are already in place but there are still many attacks that need to be taken care of. Out of all the attacks in cloud environment one of the most serious attack to cloud is DDOS attack (H- DoS and X-DoS). This paper tries to find out the root cause for such attacks and suggests particular solutions regarding the same. The proposed solution is based on Cloud TraceBack (CTB) and Network Neural.**

***Index Terms*—Network security, DDoS, X-DoS, H-DoS, Cloud computing, Trace Back, Black hole.**

I. Introduction

Cloud computing works on an abstraction based model which runs on a distributed network using physical resources and offers these resources in a virtual manner. Cloud is the latest model for provisioning resources and provides a platform independent user access to services offered by the cloud service providers [3], [9], [22]. Cloud services can be offered in various forms and the applications that run on cloud may or may not be delivered by cloud service providers. The current cloud hosted services also offer interesting reuse opportunities and design challenges for application developers and platform providers. Cloud computing systems also offer a wide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit [1]. The services that are provided by these vendors can vary from dynamically virtual machines to flexible hosted software services [2].

In cloud computing the services are fully managed by the service providers. Users can consume these services at a rate depending upon their own requirements. This on demand service provisioning is highly elastic and flexible in nature but there are many questions that arise as to whether a cloud is secure enough, even basic services such as an e-mail service requires a thorough review before moving the service to cloud. While some organizations are starting to move their e-mail to cloud services hosted by providers such as Gmail, Yahoo e-mail, and others, there are still many issues that must be taken into consideration. In February 2009, Gmail reported an outage that affected its EU users. In January2010, it was reported that Gmail had been targeted by attackers seeking to gain access to Chinese human rights activists. It was further reported by MSNBC that foreign correspondents may have been targeted. Although these services have many in built controls, it is not impossible for them to be compromised [17].

In addition, Kazi Zunnurhain and Susan V. Vrbsky [4] have discussed that if any kind of failure occurs, it is not possible to know the party which is responsible for this failure. There can be several reasons due to which a failure can occur such as hardware may be responsible for a failure i.e. in the Infrastructure as a Service (IaaS) layer of the cloud, malware in software may be responsible i.e. in the Software as a Service (SaaS) layer of the cloud apart from these running applications of customer may be responsible for some kind of malicious code, this can be due to the malfunctioning of the customer's applications by injection bogus data. This paper shows that, a failure can result in a dispute between the provider and the clients. The clients view point, data loss or interruption in computation can affect the business both financially as well as affect the goodwill of an organization. From the point view of provider, the quality of service (QoS) is generally hampered, leading to unnecessary charges to be borne by the customers for whom the customer is not responsible as per the Service Level Agreement (SLA) which is not satisfactory. In order to overcome this when the customer connects to the cloud provider's site via an Internet, the server's public key and the digital certificates are sent to the customers end. The customer may verify the provider's identity (i.e. through the trusted third party).After the verification, the customer sends

Manuscript received February 17, 2014; revised March 25, 2014

Mansaf Alam is with Department of Computer Science, Jamia Millia Islamia (A Central University), New Delhi , India (corresponding author phone: +91-9810650497; e-mail: malam2@jmi.ac.in).

Kashish Ara Shakil is with Department of Computer Science, Jamia Millia Islamia (A Central University), New Delhi , India (e-mail: kashish127408@st.jmi.ac.in).

Mohd. Salman Javed is with Department of Computer Science , Jamia Millia Islamia (A Central University), New Delhi , India (e-mail: Salman.javed039@gmail.com).

Manzoor Ansari is with Department of Computer Science, Jamia Millia Islamia (A Central University), New Delhi, India (e-mail: manzoor.ans@gmail.com).

Ambreen is with Jamia Millia Islamia (A Central University), New Delhi , India (e-mail: am.cranberry13@gmail.com).

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

the provider a random number as the session key, which can be used to encrypt and decrypt data. This session key sent to cloud provider is encrypted by using the provider's public key and it only can be decrypted by using the provider's private key [10].

Thus, one of the major issues of cloud computing is its security. This paper is an attempt towards spotting some veritable security issues in cloud, make an effort to identify the root cause of failures and offer some specific solutions.

Some security professionals have discussed that the cloud is more vulnerable to DoS attacks, because cloud is shared by different users that make the DoS attacks damaging. Meiko Jensen et al. [19] have discussed that there are high workloads on flooded service; it has been noticed by Cloud Computing operating system. According to them more computation power will be required by it to cope up with the additional workload. By doing this, the boundaries of server hardware will maximize workload to process. In this way, the Cloud system tries to protect itself from attackers, but in reality the biggest threat imposed by the attackers is on the service availability. It gets initiated from a single flooding attack entry point. The attacker does not flood all servers which provide a certain service in target [18] but is more inclined to use the less complicated web based attack tools like Extensible Markup Language (XML)-based Denial of Service (X-DoS) and Hypertext Transfer Protocol (HTTP)-based Denial of Service (H-DoS) attack due to their simple implementation and lack of any real defaces against them. Padmanabhuni et al. [5] have discussed that the X-DoS and its distributed version and Distributed XML-based DoS occurs when an XML message is sent to the Web Server or Web Service with malicious content for using all resources. The Coercive Parsing attack is one example of X-Dos, which manipulates the Web Service Request when a Simple Object Access Protocol (SOAP) is parsed to it, therefore it can transform the content to make it accessible to applications. The continuous sequence is used by Coercive Parsing attack of open tags therefore the CPU usage on an Axis2 web server becomes exhausted.

H-DoS attacks have been discussed and implemented in a web article, which describes the attack as an HTTP Flooder that starts up 1500 threads so that it can send randomized HTTP requests to the victim web server to exhaust its communication channels and also points out there is no way to distinguish between legitimate and illegitimate HTTP. In this paper we have discussed some previous work on service-oriented trace back architecture which is now referred as Cloud Trace Back to defend against X-DoS attacks [6] in cloud computing. We have also discussed the implementation of a previously devastating H-DoS attack affected in Iran. This ongoing cyber-attack was coordinated by the Iranian opposition party that was successful at disrupting access to the pro-Ahmadinejad websites by using a 3 prong attack. We have used this attack as an example for bringing down a cloud system like Amazon EC2, and also for training our back propagation neural network called Cloud Protector (formerly known as X-Detector) to detect this form of attack and remove it from the system. In this paper we have emphasized over how cloud is affected by X-DoS/H-DoS attacks, how attacker attack the source (root node) using some specific tools. We have also proposed a technique through which cloud servers can safeguard against these types of attack. Cloud trace back trace the IP address of intruder and hide its own IP address. Network neural filters this type attack and works as a protectors.

II. Related Work

In this section, we cover briefly X-DoS and H-DoS. X-DoS was a term coined by [13], where web services are prone to XML based Denial of Service (X-DoS). X-DoS according to [13], is defined as a flood of XML messages to a web server network to prevent legitimate users access to the system.

Cloud computing represents a real paradigm shift in the way in which systems are deployed. The massive scale of cloud computing system was enabled by the popularization of internet and the growth of some large services companies. M. Armbrust et al. [20] has discussed that cloud computing makes the long held dream of utility computing [23] possible by paying as per requirement, for infinitely scalable and universally available systems. Cloud computing provides lucrative option for both small enterprise as well as bigger ones and helps them in scaling up their business activities by manifolds. Thus, cloud computing can be thought of as a revolutionary technology.

This section briefly covers some of the attacks that are currently used within cloud computing .It also includes other similar researches such as the ones on SOTA [8], which is based on service-oriented architecture and service-oriented grid architecture [8]. In the concluding part of this section, we will be briefly covering up research done on X-DoS which is a DDoS attack that could affect cloud computing.

Cloud Computing is used to access the services using Internet based pay per usage model. The various facilities, Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are available in Cloud environment. The various Cloud based products can be used for elimination of overheads for installation and management of client rich applications. In the current scenario the Cloud Service providers are providing services to companies which help them to reduce the high expenditure for installation of infrastructure and other maintenance costs. The customers have to pay charges only for the resources consumed in a utility like manner. Data is considered as the most valuable assets in present scenario today as it plays an important role for decision making in organizations. The Security is one of the most common problems in the cloud environment [14]. Ashley Chonka et al.[11] have also explained another attack called Xml-Based Denial of Service (X-DoS) which is another lethal attack

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

which aims at the services that cloud provides. They have discussed about defend against such attacks, they have also brought forward SOTA model and implemented it on a cloud system, that is called a CloudTraceBack (CTB). CTB can be used in an actual X-DoS attack so the cloud victim could trace the attack back to the source. Their results showed that CTB is able to find the source of an attack within a matter of few seconds.

III. Cloud Computing Attack

The security responsibilities of both the providers and the consumers greatly differ between cloud service models. Amazon's Elastic Compute Cloud (EC2) [1] is offering infrastructure as a service, as an example, it also considers vendor responsibility of security for the hypervisors, that means they can only address security concerns pertaining to virtualization level security, physical level security, and environmental level security. The consumer is responsible for the security controls that relate to the information technology system which also includes the operating system, applications and data [12]. Jianhua Che et al.[15] have surveyed the various existing popular security models of cloud computing for example risk accumulation model, multiple-tenancy model , cube model of cloud computing and have provided some of the main security risks in cloud computing. Finally, they have given some security strategies from the view of build up, operation and security response to relieve the common security concerns of cloud computing environment.

In the current research on cloud computing [7], cloud computing is thought of as virtualization on-demand, elastic, scalable, resource as service. But as Balding pointed out in his Rivest, Shamir, and Adelman (RSA) conference presentation on cloud computing, it is actually an abstraction of services since cloud computing security follows the idea of cloud computing, there are two main areas that security experts look at securing in a cloud system: These are VM vulnerabilities and message integrity (Availability, Integrity and Confidentiality) between cloud systems. SOTA does not directly eliminate an X-DoS or DX-DoS attack message. It will be discussed further in the filter section of a defense system called Cloud Protector.

A. X-DoS Attacks (Coercive Parsing attack)

An X-DoS attack is a content-borne attack whose purpose is to shut down a web service or system running that service. A common X-DoS attack occurs when an XML message is sent with a digital signatures and a naive parser. It would look at every signature and CPU cycles used by all the resources. These are less common than inadvertent X-DoS attacks that occur when a programming error trusted customer causes a handshake to go into an infinite loop.

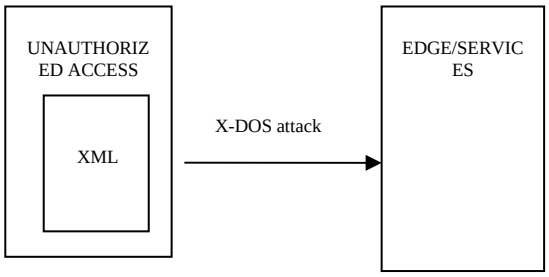

Fig. 1. Illustration of an X-DoS attack[21]

The Problem

Arnon[21] illustrates the type of attacks a malicious sender can cause, this can also be depicted by Fig. 1. [21] shown above through an XML Denial of Service (X-DoS) attack. In this attack a malicious sender creates an XML which appears to be valid one but is loaded with different digital signatures. An unsuspecting parser then verifies these signatures leading to stealing of CPU cycles which can make the services unavailable. A service firewall is used in this concept to intervene incoming and outgoing messages and later on inspects them through a dedicated software component or hardware. Since the parsers are not ready for this type of attack, where each of these signatures are examined therefore it leads to slow down of services under high load conditions.

Thus an attack due to incoming messages is a type of threat demonstrated by this example and it needs to be handled, another related type of problem is related with outgoing messages. It requirement is to make sure that private information does not leak outside of the service. In such a situation, it is mandatory to find a way to make sure that they hold only information allowed in the contract flows out of the service.

The first line of defence for the service is achieved through a Service Firewall. This has also been depicted by Fig. 2. , according to this when a request arrives, it is first screened by Service firewall for validity and authorization, and only the authorized requests are routed for receiving services.

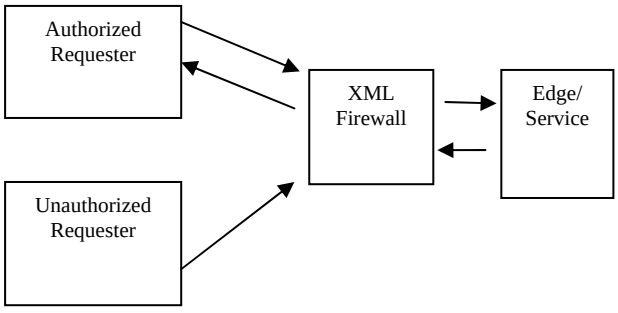

Fig. 2. [21] When a request arrives at a Service Firewall (an XML firewall in this illustration) it is screened for validity, for example the firewall can check for an XML matches the predefined XSD. The Authorized requests get passed and unauthorized requests are blocked.

A Denial of Service (DoS) is where an attacker attempts to deprive legitimate users of their resources. An X-DoS attack, according to Padmanabhuni et al. [5] is where a

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

network is flooded with XML messages instead of packets in order to prevent legitimate users to access network communications. Further, if the attacker floods the web server with XML requests, it will affect the availability of the web services.

The X-DoS is adopted into a Distributed Denial of Service paradigm that is known as Distributed XML based Denial of Service (DX-DoS). The attacker uses multiple hosts to attack the victim with an X-DoS attack, though none of these attacks have been reported as yet, but if these attacks occur in future they can be a very serious threat to cloud computing.

B. Handling Web Server Attacker

Handling of web server attacker can be done either directly through a module handler model or by using a CTB and protector along with the handler. Fig. 3 explains how a web server can directly handle the attacker with a module handler model.

Fig. 4. on the other hand is an extension as well as a modification of module handler model elicited by Fig. 3, and has CTB and a protector between handler modules and web server to handle and protect the attacks which may arise from varied sources.

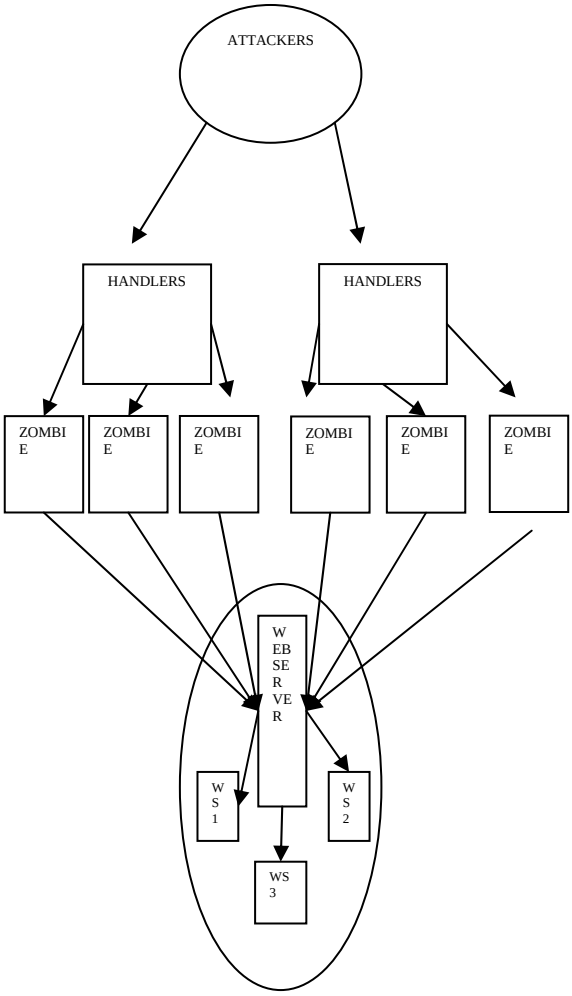

Fig. 3. Web server directly handling the attacker with a module handler model

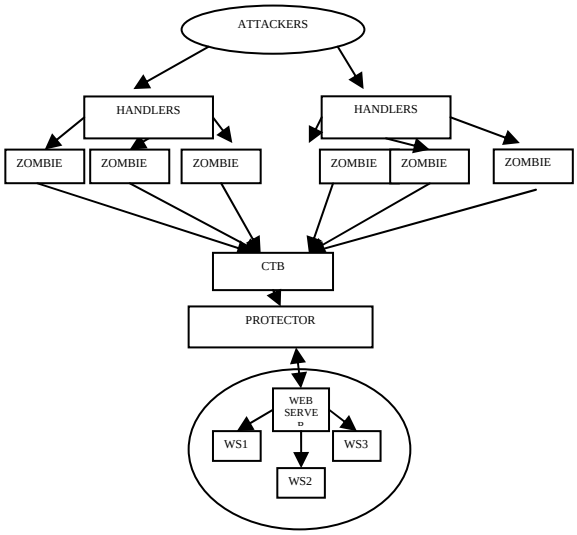

Fig. 4. Module Handler with a CTB and Protector

IV. TRACEBACK

One of the reasons why attackers are so successful is because of the internet characteristic, which includes limited consumable resources. Attackers can target bandwidth, processing power and storages capacities of a cloud network. Ashley Chonka et al. [11] have explained that the cloud computing has limited number of resources so it has to provide a high quality of service, these services can be exhausted with a sufficient number of customers. With this particular knowledge, attackers can instigate an X-DoS or DX-DoS attack. For example, an attacker can open up a number of browsers in virtual machines so that it can send multiple requests to the2 victim's web server over a period time.

A. Cloud Trace Back description

Cloud Trace Back (CTB) [11] can be used either in a network structure, such as a LAN, or a grid network structure. CTB is made within a virtual machine to make placement within the cloud network compatible, flexible and scalable whilst it still remains an SOA security product.

B. *CTB placement within Cloud System Infrastructure*

Deployment of CTB is at the edge routers in order to bring it close to the source of the cloud network. Generally, if the services of security are not in place for web services, as seen in most of the systems, then such systems become highly vulnerable to attacks. Definition Language (WSDL) to the CTB instead of the web server is accomplished by attaching the Web Service.

As a result, requests of all services are firstly sent to the CTB for marking, thereby effectively removing the service provider's address and thus a direct attack is prevented. The victim will be able to recover and reconstruct the CTBM tag if an attack is discovered or was successful at bringing down the web server, and as a result reveal the actual identity of the source.

In an attack scenario, the attack client will request a web service from CTB and after that the request will be routed to the web server. The attack client will then formulate a SOAP request message based on the service description

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

formulated by WSDL. Upon receipt of SOAP request message, SOTA [11] is placed at SOTM within the header section. It is assumed that WS-Security is replacing wsse username tag with its own username tag.

Once the CTBM has been successfully placed, the SOAP message is sent to the Web Server. By the discovery of an attack, the victim would ask for rebuilding an extract mark and inform them about the origin of the message. This rebuilding also starts filtering out the attack traffic.

If the message is in normal form, then the SOAP message is forwarded to the request handler for processing. After the SOAP request is received, the Web Service prepares a SOAP response. The web server than takes the SOAP response and sends it back to the client as part of the HTTP response. CTB will not interfere with the response requests or any outgoing message.

V. Protector

The Cloud Protector is a trained back propagation neural network (NN), to help detect and filter out X-DoS messages. A neural network is a set of connected units made up with input, hidden and output layers. Each of these connections in a neural network has a weight associated with it. In a neural net the focus is on the threshold logic unit (TLU). The TLU inserts input objects into an array of weighted quantities and then sums them up to see if they are above the threshold.

There are several approaches we can adopt to defend against a DDOS attack.

Black-holing or sink holing: - Black –holing or sink holing approach blocks all traffic and diverts it to a black hole, where it is discarded. The down side is that all traffic is discarded both good and bad and targeted business is taken off-line. Similarly packet-filtering and rate–limiting measures simply shut everything down, denying access to legitimate users as well [16].

Black holing initiates the service provider to block all the traffic directed to a target enterprise if possible, and it then directs and diverts traffic to a “black hole” where it is discarded in an effort to save the provider’s network and other clients. Since, legitimate packets are also discarded along with malicious attacking traffic, black holing is not an answer because its victims loose all their traffic and their attacker wins in the end [16].

Routers and firewalls:-Routers are configured to stop simple ping attacks by filtering unimportant protocols and also by stopping invalid IP addresses.

Intrusion-detection System: It has the ability for anomaly-detection; therefore it is recognized when valid protocols are being used as an attack vehicle. It is used in conjunction with firewalls to block-traffic automatically.

VI. Conclusions and Future Work

In this manuscript we have discussed our work on service-oriented architecture and its security applications to cloud computing. We have also covered two threats that pose a very serious danger to cloud based environment, namely H-DoS and X-DoS attacks. If one of these attacks hits the cloud, it could potentially cripple to a business like Amazon EC2.

According to Chaos theory the computers on a cloud network work on the infrastructure as networks, therefore it introduce inherent non-linear dynamics into the system when an attacker initiates an H-DoS attack they change the initial conditions of the system.

In our future work we have planned to correlate chaos theory and black holing concept together to detect DDOS attack and give a solution, how to protect cloud victim from the introducer. This work will represents a new paradigm of information protection and security in cloud computing.

References

[1] Amazon Web Services (January 2014), *Amazon Elastic Compute Cloud (ec2)*, Available: http://aws.amazon.com/ec2

[2] Enomaly.com (November 2013), *Enomalism elastic computing infrastructure*. http://www.enomaly.com

[3] M. Alam and K. A. Shakil, “Cloud database Management System Architecture,” *International Journal of Computer Science and its Applications*, vol. 3, no. 1, pp. 27-31, Universal Association of Computer and Electronics Engineers(UACEE), 2013

[4] K. Zunnurhain and S.V. Vrbsky, “Security Attacks and Solutions in Clouds, ” Proceedings of 1st International conference on cloud computing”pp. 145-156,2010

[5] S. Padmanabhuni, V. Singh, K .M .S. Kumar, A. Chatterjee, "Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach," icws, *IEEE International Conference on Web Services (ICWS'06)*, pp.577-584 ,2006

[6] A. Chonka, W. Zhou and Y. Xiang, Y."Protecting Web Services with Service Oriented Traceback Architecture", *IEEE 8th International Conference on Computer and Information Technology, IEEE*, 2008.

[7] P. Laplante, J. Zhang and J. Voas, “What’s in a name? Distinguishing between saas and soa”.,*IT Professional,vol.* 10, no. 3, pp. 46–50, May-June 2008

[8] A. Chonka , W. Zhou , Y. Xiang , “ Defending grid web services from X-DoS Attacks by SOTA,” *in Percom 2009: Proceedings of the Seventh Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 1-6, 2009.

[9] B. Alam, M.N. Doja, M. Alam and S. Malhotra, “5-Layered Architecture of Cloud Database Management System,” *AASRI Procedia*, vol. 5, pp. 194-199, 2013

[10] X. Li, “Cloud Computing: Introduction, Application and Security from Industry Perspectives,” *International Journal of Computer Science and Network Security*, vol .11, no.5, May 2011.

[11] A. Chonka, Y. Xiang, W. Zhou, A. Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1097–1107, July 2011.

[12] S. Subashini , V.Kavitha, “A survey on security issues in service delivery models of cloud computing,”*Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, January 2011.

[13] S. Padmanabhuni, V. Singh, K.M Senthil and A. Chatterjee,“Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach”, *International Conference on ICWS apos;06.* , pp 577 – 584, 2006.

[14] B. Loganayagi, S. Sujatha, “Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques,” *Procedia Engineering*, vol. 30, pp. 654-661, 2012.

[15] J. Che, Y. Duan, T. Zhang, J. Fan, “Study on the Security Models and Strategies of Cloud Computing,”*Procedia Engineering*, vol.23, pp. 586–593, 2011.

[16] CISCO(March 2014),*Defeating DDOS Attacks*, Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.pdf

[17] Michael Gregg (January 2014), 10 *Security Concerns for Cloud Computing*, Available: http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf

[18] A. Singh, M. Shrivastava , “Overview of Attacks on Cloud Computing”, *International Journal of Engineering and Innovative Technology (IJEIT)* vol. 1, no. 4, April 2012.

[19] M. Jensen, J. Schwenk , N. Gruschka, L.L. Iacono, “On Technical Security Issues in Cloud Computing,”*IEEE International Conference on Cloud Computing*, pp:109-116, IEEE, 2009.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[20] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, " A view of cloud computing," *Commun. ACM*, vol. 53,no. 4 ,April 2010

[21] K. A. Shakil and M. Alam, "Data Management in Cloud Based Environment using k-Median Clustering Technique", *IJCA Proceedings on 4th International IT Summit Confluence 2013 - The Next Generation Information Technology Summit*, pp.8-13, January 2014

[22] M. Alam, K.A. Shakil, "A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment", *International Conference on Recent Trends in Communication and Computer Networks*, Elsevier, pp. 174-180, November 2013.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)