Detecting Flooding based DoS Attack in Cloud Computing Environment using Covariance Matrix Approach

Mohd Nazri Ismail
Malaysian Institute of Information Technology (MIIT) University Kuala Lumpur,Malaysia
mnazrii@miit.unikl.edu.my

Abdulaziz Aborujilah
Malaysian Institute of Information Technology (MIIT) University Kuala Lumpur,Malaysia
Azizhadi1981@gmail.com

Shahrulniza Musa
Malaysian Institute of Information Technology (MIIT) University Kuala Lumpur,Malaysia
shahrulniza@miit.unikl.edu.my

AAmir Shahzad
Malaysian Institute of Information Technology (MIIT) University Kuala Lumpur,Malaysia
mail2aamirshahzad@gmail.com

ABSTRACT
The internet is gaining a lot of importance day by day, especially with the emergence of cloud technology. This new technology has made a new computing service to end users that include, PaaS, SaaS. On the other hand, this technology was accompanied with some shortages. The most serious obstacle is the security challenges because of the cloud is characterized by computing resource sharing and multi-tenancy features and as a result flooding based denial of service attack has been observed. This effect on performance and quality of service on cloud. To overcome this security challenge, there are several methods to detect and prevent this kind of attack. Most of these approaches are using statistical and/or artificial intelligence methods.

In this research paper a new model to detect flooding based DoS attack in cloud environment has been suggested consisting three phases. (1) The first-phase is to model the normal traffic pattern for baseline profiling and (2) the second phase is the intrusion detection processes and (3) finally prevention phase. The covariance Matrix mathematical model is used as detecting method. The phase (1) and (2) have been implemented in real test bed. From the result, it is proven that we can detect the flooding attack effectively.

Categories and Subject Descriptors
C.2.3 [**Network Operations**]: Network monitoring.

General Terms
Experimentation,Security,Algorithms.

Keywords
Cloud Computing,Covariance Matrix,DoS Flooding_based Attack, Intrusion Detecting.

ICUIMC (IMCOM) 2013, January 17–19, 2013, Kota Kinabalu,Saba, Malaysia.

1. INRODUCTION
Cloud computing adoption can save costs as numerous of users able to share the same computing infrastructure using virtualization technology as in [1]. The cloud technology also gives end users high availability and redundancy. Furthermore, end users no longer need to purchase expensive application. Instead, they can rent the applications required for a period of time according to their need and paid it accordingly. Cloud computing techniques also provide more storage space than local storages. In addition,making applications software more updated just by update virtual machine's application packages instead of update all single applications alone. Using cloud the organizations can focus on their business needs instead of worry about IT issues. Although all of these characteristics, the most dangerous threat to cloud is denial of service attack [2]. In this article, firstly a brief introduction about cloud computing will be explained. Then, cloud computing intrusion detecting and prevention related work will be discussed, after that, the proposed security framework will be explained with covariance matrix mathematical background, finally initial experiment and the results will be discussed.

2. CLOUD COMPUTING SERVICES MODELS
Cloud computing paradigm offers multiple services by sharing the infrastructure (Infrastructure as a Service) or sharing the platform (Platform as a Service) or in the applications (Software as a Service). Renting this kind of technology can decrease the cost and effort needed to acquire them as well as reduce requirements of managing these computing resources locally.

In (IaaS), cloud providers offer computing physical resources as a service such as processors and memories and storage and network equipment[3].In this model end users are able to install their operating systems and applications on cloud infrastructure according to their need , and they have all permission to manage their virtual machines. The main IaaS provider is Amazon and Google and others [4].In addition to physical computing resources offered by the cloud infrastructure provider, PaaS model also facilitates the application development process by providing the application development platform required on which applications can be developed and run [5], therefore there is no longer crucial need to own computing infrastructure locally.Moreover, SaaS model is a software model where a

collection of applications software available to the end users in the cloud environment or by smart phone and in other data exchanging media.

3. CLOUD COMPUTING DEPLOMENT MODEL

Deploying the cloud computing services can be locally inside the organization which is known as private cloud, or can be owned and manage by third parties (public cloud).Several organizations can share their computing resources together (Community cloud), or cloud services can be a mixture of the above models (Hybrid Cloud) [6].

In private cloud computing, single organization owns its cloud infrastructure and operates it by itself or by third party. The cloud infrastructures can be hosted inside the organization's premise or outside. By using private cloud computing the organization can have a secure cloud than the public cloud [7].

While In public cloud, all cloud computing resources are available to the end users via the internet. The cloud infrastructure ownership doesn't belong the organization but belong public providers such as Google, Microsoft Azure and Amazon AWS.

In Community Cloud model , Several organizations can share their computing resources. This kind of cloud model can be hosted and managed locally or in a third party site.

While in hybrid cloud , more than one cloud deployment models can be used at the same time (public, community or private) [6]. This model can support IT organization to achieve their full cloud services [8].

4. RELATED WORK

As the advancement of Internet based technologies and cloud computing especially, several challenges and threats have been identified, especially in security perspectives [9]. One of these threats is associated with the stability of the internet which is denial-of-service attack (DoS) .It is one of the most serious attacks .This kind of attack happens frequently on the internet [10]. DoS attacker uses compromised nodes in the network to target predetermined victim node by a huge quantity of incoming messages, which causes a victim to become unresponsive or become out of service. Because of cloud technology is still in its initial stages, and also it characterized with scalable and multi-shared features, DoS can be more harmful to cloud based network than non-cloud networks. Varieties of research studies have addressed these challenges in different aspects.

In [11], the researchers focus more on cloud computing IDS implementation. They proposed a mechanism to integrate IDS and IPS in one model. They suggested using anomaly and signature base intrusion detecting mechanism in the same model. In addition, they proposed locating IDS in all virtual machines or in hypervisor.

In [12], the authors suggested a new model to group events, and combine them with hypervisor events. This mechanism relied on applying IDS standard and plug-in methods to ensure more flexibility and compatibility .In the experimental side; they implement their proposed model in lock-Keeper and cloud environment.

In another research study[13], they proposed to distribute IDS cooperative agent in all cloud computing regions. Whenever there is an attack in one region, alerts can be sent to the main IDS. Main IDS computes the majority of alerts sent by all cloud region's IDS to determine the degree of attack seriousness. Whenever the alerts sent by most of IDS are the same, then the DoS attack has been detected otherwise no. Implementation of this technique has been proven that no big difference between snort IDS and proposed approach in the computation effort but the main advantage of this method is its ability to prevent the whole system from a single point of failure.

Securing the cloud from DDoSattacks using an intrusion detection system in a virtual machine [15], this article proposes a multi-threaded cloud IDS model, this model integrates the signatures and IDS behavior based on detecting distributed Denial of Service (DDOS) and Cross Site Scripting (XSS).

In [14], a new model to determine the source of XML-based DDoS attack has been proposed, which called Cloud Tracing &Filtering (CTF). For detecting an attack they proposed back propagation neural network (CloudShield) for traffic filtering. They stated that their model is able to detect and filter most of DoS attack and determine the source of the attack. They clime their detection result was around 99%of attacks within almost 10-135 ms.

In [15], they suggest avoiding DoS attack by transfer DoStargeted application to another virtual machine using virtualization strategy mechanism.

In [16], the authors suggested a security framework for economic DoS Protection .To evaluate this framework, XML based DDoShas been implemented to target Cloud Service hosted on Amazon EC2.Finally the researcher concludes that the current DoS protections approaches still need more effort to protect cloud form this attack.

5. COVARIANCE MATRIX MODELING

As in [17] the author explained in detail the detection of various kinds of flooding attack using a covariance matrix model . This kind of modeling relies on investigation and correlation of several features in the IP header as in Figure 1 [22] and Figure 2.

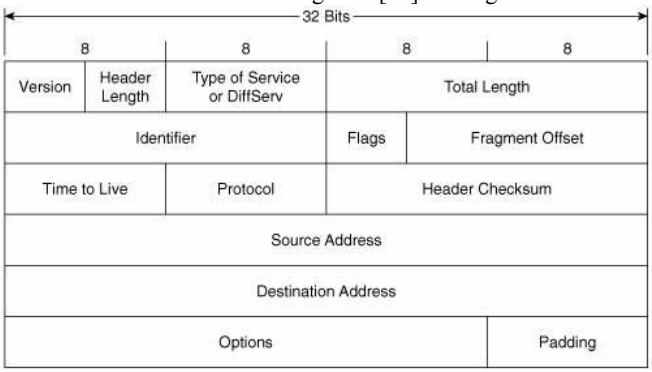
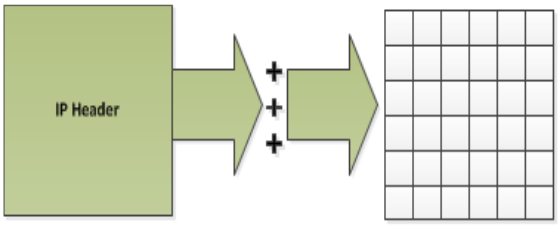


Figure 1. IP header file fields.



IP Header Flags Correlation Covariance Matrix

Figure 2. Covariance Matrix General View.

5.1 Covariance Matrix in Details

The following pseudo code algorithm highlights the steps of the covariance matrix algorithm [17].

This algorithm starts with new captured network traffic as input. Than after traffic processing. Algorithm output is making a decision whether the DoS attack has been occurring is according the values of a binary matrix. When all insides of binary array are zeros, no attack otherwise DoS attack has detected as the following steps:

- Network Traffic Capturing .
- Network traffic sampling,Where every Simple Sequences $y^l=(x_1{}^l,\dots,x^l)^T, x_k{}^l = (f_1{}^{l,k}, f_2{}^{l,k},\dots f_p{}^{l,k})^T, 1 \le k \le n$, *where* $x_1{}^l$ is network segments, $f_1{}^{l,k}$= Network traffic features, k is the number of segments, l network stream length .
- Finding covariance matrixes for every simple as m^l:

$$m^l = \begin{pmatrix} \sigma_{f_1{}^l,f_1{}^l} & \sigma_{f_1{}^l,f_2{}^l} & \cdots & \sigma_{f_1{}^l,f_p{}^l} \\ \sigma_{f_2{}^l,f_1{}^l} & \sigma_{f_2{}^l,f_2{}^l} & \dots & \sigma_{f_2{}^l,f_p{}^l} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{f_p{}^l,f_1{}^l} & \sigma_{f_p{}^l,f_2{}^l} & \cdots & \sigma_{f_p{}^l,f_p{}^l} \end{pmatrix}$$

$$Where\ \sigma_{f_u{}^l,f_v{}^l} = cov\left(f_u{}^l, f_v{}^l\right) = 1/\left(f_u{}^{l,k} - \mu_{f_u{}^l}\right)$$

$$and\ \mu_{f_u{}^l} = Ef_u{}^l = 1/n \sum_{k=1}^{n} f_u{}^{l,k}.$$

- Determine network traffic anomaly according the following formula:

$$(M^{obs}, N; T) = (d_{uv})_{p\times p}$$

$$\forall m_{uv}^{obs} \in M^{obs}, \forall n_{uv} \in N \quad , \quad \forall \delta_{uv} \in T$$

$$if |m_{uv}^{obs} - n_{uv}| \ge \delta_{uv} then \quad d_{uv} = 1$$

$$else d_{uv} = 0$$

Obs.is network traffic observation , v and u are the indexes of feature in covariance matrix, T is the dissimilarity threshold matrix value.

5.2 Features Selecting

Network behavior analysis is based on observing changes in network traffic features. In this approaches covariance-matrix statistical method will be used to network traffic behavior analysis. This study relies on the study of changes of the IP flags behavior such as TCP FIN, RST and FIN [18] and TCP retries flags.

6. PROPOSED MODEL ARCHITECTURE

The proposed detecting model consists of three phases. Firstly is the training phase, which focuses on constructing a profile of a normal network traffic behavior (baseline profile). It can be done by capturing the normal traffic than transfers it into the matching covariance matrix.

Secondly, the resulted covariance matrix from the first phase is compared with a new covariance matrix of new traffic which can be normal or abnormal.

To implement this proposed model in cloud environment, we suggest adding it in a cloud environment as in [19] as in Figure 3

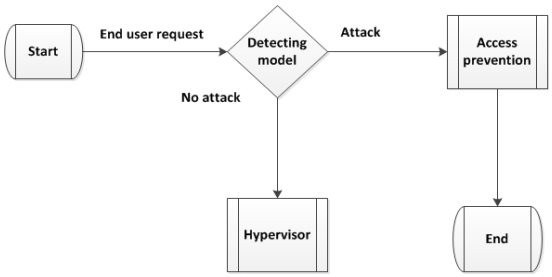


Figure 3. Integrate Proposed Security Model in the Cloud Environment.

7. EXPERMENTS AND ANALYSIS

The aim of this experiment is to examine the effectiveness of the covariance matrix method to detect flooding based DoS attack.

The test bed topology contains tow PCs connected to the same router. One of them is a victim and one is an attacker.

The victim is using a virtual machine run hosted in VMware Player and has on Ubuntu 10.11 operating system IP address 192.186.5.129 and IP address of the attacker is 192.186.0.101.

For generating attack Hyenaetool has been used [20] and for traffic monitoring and capturing network traffic AthTekNetWalk network tool has been used [21].

Network traffic capturing and IP flags statistical value calculation are done in five minutes for every single minute independently. Covariance matrix calculated for all, similarly as in [17].

The Figure 4 summarized the steps of experiments data flow

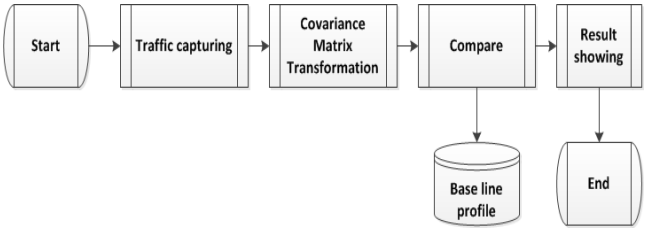


Figure 4. Experiments Data Flow.

7.1 Experiments Methodology

In this research paper, implementation part has been accomplished in two phases.

Training phase, which focus on the baseline profile constructing and second phase which focuses on detecting part.

The implementation depends on the network traffic stream as input and anomaly matrix as output according the following Phases .

Training phase:

- Normal Network Traffic stream Capturing.
- Normal Network Traffic Segmentation.
- Normal Network Traffic Summarization.
- Normal Network Traffic Covariance Matrixes Calculation(Baseline constructing).

Testing phase:

- Abnormal Network Traffic Capturing.
- Abnormal Network Traffic segmentation.
- Abnormal Network Traffic Summarization.
- Abnormal Network Traffic Covariance Matrixes Calculation.
- Network Traffic Anomaly detecting , when resulted matrix all zeros no attack otherwise attack.

7.2 Experiments Methodology

The first two experiments are capturing normal traffic in different internet access rate and the third one is capturing abnormal traffic after generating attack. Than all captured traffic is converted into matching covariance matrixes, finally the three covariance matrix is compared to detect anomaly between normal and abnormal traffic and thus DoS attack detecting.

7.3 Experimental Test Bed

The following test bed has been used in detection model implementation. It includes local network infrastructures connected with the internet. This small network includes two PCs, One of them is an attacker and one as a victim. The victim PC is a virtual machine with Ubuntu 10.11 OS. Moreover, the attacker uses an internet access to attack its victim.

The Test bed experiment consists of AthTekNet Walk tool for traffic capturing and filtering and MSExcel for covariance matrix analysis. As in Figure 5.

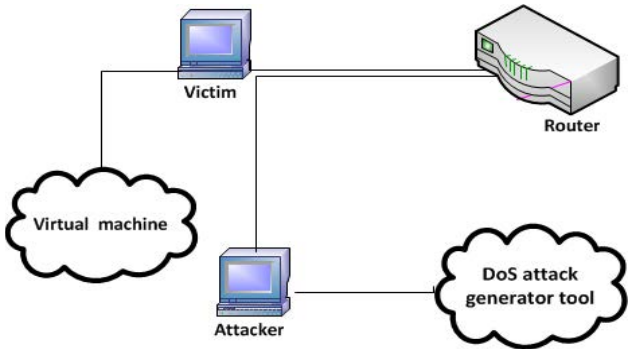


Figure 5. Experiment Test Bed.

8. RESULTS DISCUSSION

Three experiments have been conducted; first one has been done to capture network traffic in normal situation . The result was as the following:

Table1 .Normal Traffic Covariance Matrix (Experiment 1)

	SYN	FIN	RST	TCP Retries	Flags Average
First Minute	1	114	20	17	38
Second Minute	28	9	5	0	11
Third Minute	40	7	0	6	13
Fourth Minute	12	35	0	5	13
Fifth Minute	0	24	3	0	7

Table1 give numerical decryption to covariance matrix under normal condition. Normal traffic captured whereas web site surfing such as google.com, yahoo.com, youtupe.com and others, while capturing tool is running at the same time.
Finally, the covariance matrix of all IP flags is calculated by taking into consideration average of every flag value independently as it is in Figure 6.

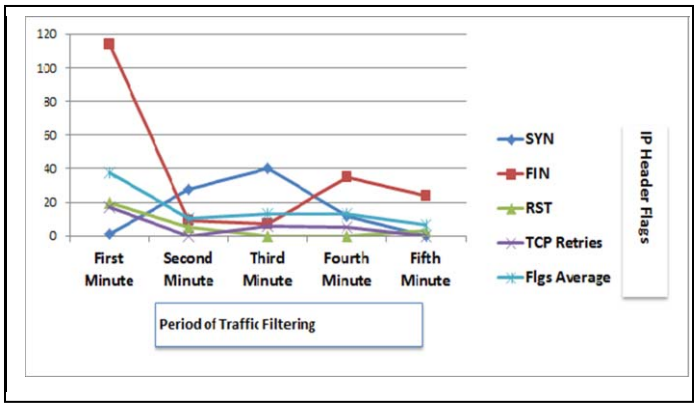


Figure 6 .Normal Traffic Covariance Matrix (Experiment 1).

In Table 2, the same data item statistics are calculated under normal situation by surfing other websites such as www.ikhwanonline.com, www.al-islah.net which are consider as common news web sites . these two web sites contain some animation and normal website content.

By doing the this experiment, normal network traffic pattern constructing has been done (training period).
Then in testing phase, comparing of new observed traffic with normal pattern is done to calculate how much anomaly is. and thus discovering DoS attack accordingly(testing period) .
Figure 7 shows the flags values and average of them as in experiment 2.

Table2 .Normal Traffic Covariance Matrix (Experiment 2)

	SYN	FIN	RST	TCP Retries	Flags Average
First Minute	10	10	4	0	6
Second Minute	4	6	2	2	4
Third Minute	0	0	0	0	0
Fourth Minute	2	2	0	0	1
Fifth Minute	0	0	0	0	0

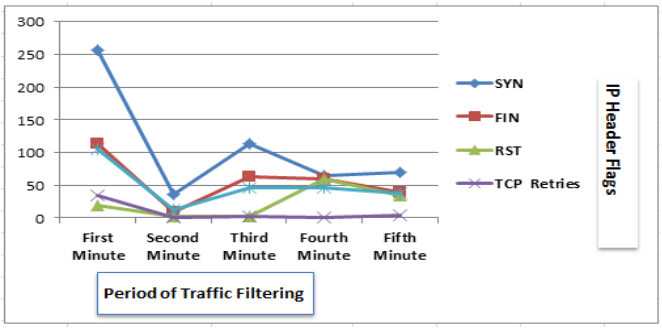


Figure 7 .Normal Traffic Covariance Matrix (Experiment 2).

In other side experiment 3 describes covariance matrix of IP header flags under attack as in Table 3 and Figure 8.

Table3 .Normal Traffic Covariance Matrix (Experiment 3)

	SYN	FIN	RST	TCP Retries	Flags Average
First Minute	256	114	19	35	106
Second Minute	36	10	2	1	12
Third Minute	114	63	3	3	46
Fourth Minute	64	60	60	1	46
Fifth Minute	70	40	35	4	37

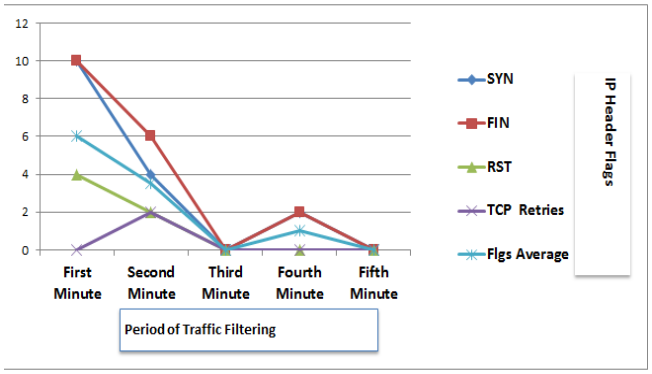


Figure 8. Covariance Matrix of IP Header Flags under Attack (Experiment 3).

In Table 4, anomaly comparing between Covariance Matrixes in experiment1 and experiment 3 is calculated by subtracting the average of the flags values in normal case and under attack as has been highlighted in figure 9

Table 4.A Comparison Between Covariance Matrix of Normal and Abnormal Network Traffic

	SYN	FIN	RST	TCP Retries	Flags Average
First Minute	-9	104	16	17	32
Second Minute	24	3	3	-2	7
Third Minute	40	7	0	6	13
Fourth Minute	10	33	0	5	12
Fifth Minute	0	24	3	0	7

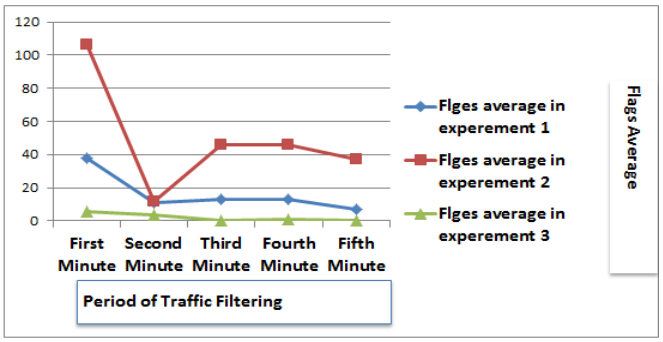


Figure 9.A comparison Between Average of Covariance Matrix of Normal and Abnormal Traffic.

By referring to figure 9, it is clear that the flags average in experiment 1 similarly as in experiment 2. Both of expamen1 and 2 in normal circumstance. At the same time the average of flags in experiment 3 is totally different and experiment 3 is under attack circumstance.

Finally it can be concluded that there is clearly different between normal network traffic and network traffic under flooding based DoS attack.This inference is depending on measuring the similarity between the average of IP flags in typical and untypical network traffic. Thus the covariance matrix mathematical approach can be very useful to detect flooding based DoS attack on cloud environment.

9. CONCLUSION

Cloud computing services are more widely used in several sectors, because of new advantages offered such as reducing cost of computing infrastructure (IaaS). In addition to that cloud computing services such as PaaS, SaaSgives a new way to use and develop cloud based application software instead of traditional application development. Cloud computing provides a new computing services but the main shortage is security of cloud services used, especially in cloud infrastructure aspects.

In cloud infrastructure service, several users can share the same infrastructure, which can cause DoS attack. In this paper covariance matrix approached has been suggested to detect this kind of attack. According the initial experiments conducted, it can be concluded that this approach can detect this kind of attack effectually, to refer to Figure 9, it is clear that the two experiments which implemented on normal traffic are similar in the flags average regardless of the amount of traffic and in other hand, the average of flags in abnormal traffic is totally different from normal traffic as in third experiment. Therefore the covariance matrix approach can be effectively used to detect abnormal traffic (DoS attack).

In future work we suggest investigating the performance the covariance matrix approach in an online environment.

10. ACKNOWLEDGMENTS

Sincerely, I would like to thank my parents first than my wife, my children Hamza and Omar, also my best friend Abdulkarem Alsharafi and my supervisors for their supporting me to make this successful research.

11. REFERENCES

[1] Vouk,M.A.,Cloud computing–Issues, research and implementations. Journal of Computing and Information Technology, 2004. 16 (4): p. 235-246.

[2]Ismail, M.N., et al., New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment.International Journal of Computer Science and Security (IJCSS). 6 (4): p. 226.

[3]Mell, P. And T. Grance, Draft NIST working definition of cloud computing.Referenced on June.3rd, 2009.

[4] Zhang, Q., L. Cheng, and R. Boutaba, Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 2010. 1 (1): p. 7-18.

[5] Shelke, M.P.K., M.S. Sontakke, and A. Gawande, Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

[6] Mell, P. And T. Grance, The NIST definition of cloud computing.National Institute of Standards and Technology, 2009. 53 (6): p. 50.

[7] Mell, P. And T. Grance, Effectively and securely using the cloud computing paradigm. NIST, Information Technology Lab, 2009.

[8] Zhang, H., et al., Intelligent workload factoring for a hybrid cloud computing model. IEEE Computer Society Washington, DC, USA, 2009.

[9] Bamiah, M.A. And S.N. Brohi, Seven Deadly Threats and Vulnerabilities in Cloud Computing. International Journal of Advanced engineering sciences and technologies, 2011

[10] Xia, Z., et al., Enhancing DDoS Flood Attack Detection

Via Intelligent Fuzzy Logic. Informatics: An International Journal of Computing and Informatics, 2010. 34 (4): p. 497-507.

[11] Alsafi, H.M., W.M. Abduallah, and A.S.K. Pathan, IDPS: An Integrated Intrusion Handling Model For Cloud Computing Environment. International Journal of Computing & Information Technology (IJCIT), 2012.

[12] Roschke, S., F. Cheng, and C. Meinel, An Advanced IDS Management Architecture. Journal of Information Assurance and Security, 2010. 5: p. 246-255.

[13]Lo, C.C., C.C. Huang, and J. Ku. A cooperative intrusion detection system framework for cloud computing Networks.Parallel Processing Workshops (ICPPW), 2010.

[14] Chonka, A., et al., Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 2010.

[15] Bakshi, A. and B. Yogesh. Securing cloud from DDoS attacks using intrusion detection system in virtual machine.Second International Conference on Communication Software and Networks, 2010.

[16] VivinSandar, S. and S. Shenai, Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks. International Journal of Computer Applications, 2012. 41(20): p. 11-16.

[17] Yeung, D.S., S. Jin, and X. Wang, Covariance-matrix modeling and detecting various flooding attacks. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 2007. 37(2): p. 157-169.

[18] Bridges, S.M. and R.B. Vaughn. Fuzzy data mining and genetic algorithms applied to intrusion detection.National Information Systems Security Conference (NISSC), 2000.

[19] Nunez, A., et al. Design of a flexible and scalable hypervisor module for simulating cloud computing environments.International Symposium onPerformance Evaluation of Computer&TelecommunicationSystems (SPECTS), 2011.

[20] Hyenae, H.p.h. , 2010. Retrieved September 1, 2012.http://sourceforge.net/projects/hyenae.

[21] AthTekNetWalk, 2012. Retrieved September 1, 2012.http://www.athtek.com/netwalk.html.

[22] IP Packet Header.Retrieved September 1, 2012. http://pekoktenan.wordpress.com/2009/03/31/ip-packet-header.