New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment

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

Abdulaziz Aborujilah *abdulazizh@unikl.edu.my*
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

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

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

Abstract

As a result of integration of many techniques such as grading, clustering, utilization computing and resource's sharing, cloud computing has been appeared as multi element's composition technology, it offers several computing services such as IaaS (infrastructure as service), PaaS (platform as service) and SaaS (software as service) based on pay as you use rule, but nevertheless, and because of cloud computing end users participate in computing resources (co_ tenancy) , and by which infrastructure computing can be shared by a number of users, and as a result to this feature, some security challenges has been existed and one of the most serious security threats is flooding attack, which prevent other users from using cloud infrastructure services, that kind of attack can be done by a legitimate or illegitimate cloud computing users.
To overcome this problem various approaches have been proposed based on Artificial intelligence and statistical methods, but most of them concentrate on one side of problem and neglect the other aspects.
In our proposed approach, the focusing will be more in overcoming the problem in all its aspects, in attack detection stage covariance matrix statistical method will be applied and to determine attack source TTl (Time_to_Life) value counting method will be used, and the attack prevention will be based on Honeypot method, and initial simulation to this approach using UML class diagram and sequence diagram showed where our proposed framework can be done in cloud environment.

Keywords: Flooding based denial-of-service (DDoS) attack, Covariance matrix, TTl, Honeypot, cloud computing, virtual machine.

1. INTRODUCTION

Because of current powerful computing capabilities (CPU, memory, storage media) and also as a result to networking capabilities such as grade [1] and cluster computing [2] and due to vitalization techniques [3] as in Figure 1, cloud computing services have taken a place in modern computing technology. Cloud computing can be defined as in [4] “Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast microprocessor, huge memory, high-speed network and reliable system architecture."

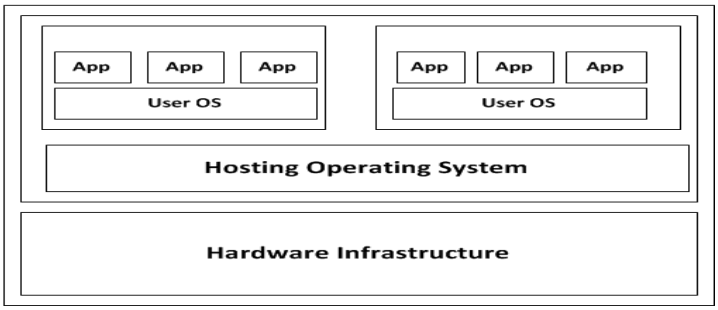

FIGURE 1: cloud computing virtualization

In this paper, we first present a general background about cloud computing architecture after that cloud computing challenges will be highlighted, then we will start in literature review and related works which concentrate on DoS detecting and prevention method, finally we describe our proposed defense framework and initial simulation, we use flooding based attack and DoS attack interchangeably .

2. CLOUD COMPUTING ARCHITECTURE

The cloud computing as new technology help the end user to reducing required computing effort to achieve his goals .and because of cloud computing services provided to the user such as IaaS (infrastructure as a service) [5], the end user is no longer needs to purchase computer equipment necessary to accomplish his goal, but he can rent all equipment he needs then use them as much as he needs.

In addition to IaaS provided by cloud computing providers, computer application developers can take advantage of the multiple development platforms available on the cloud to develop their own applications and deployed them online, which is known as PaaS(platform as the service) [6] .
In addition to IaaS and PaaS services, the end user can use several application's software in different fields available on cloud by so-called SaaS (software as services)[7], and cloud computing application software provided by main cloud providers can reduce the cost of rent or purchase those applications to the end user.

Although these services offered by cloud computing provides, but the most important shortage in cloud services is the security side which is mentioned in details in [8-11], and one of the most serious security problem in cloud computing is related to availability of cloud infrastructure, because of many cloud user can share the same infrastructure, that can cause security threat such as denial of service attack [10-16].

3.CLOUD COMPUTING CHALLENGES

Cloud computing implementation is facing several challenges in different aspect [17] and According to the survey conducted in 2008 by IDC survey about cloud computing challenges, cloud computing security challenges is on the top most threat to cloud [18], and became well known that cloud computing paradigm is a kind of virtualization environment with another technology such as grade and clusters and distributed computing, all these technologies has his own security disadvantages. In addition to the threats coming from cloud component, therefore securing issues is not related to cloud just but also related to other technologies and most dangers threat to cloud is vitalization security.

And one of the potential attacks to cloud virtualization system is neighbor attacks as in Figure 2, which by any virtual machine can attack its neighbor in same physical infrastructures and thus prevent it from providing its services or, which has been known as denial of service attack DoS attack as has been existed in AWS Amazon [19], that kind of attack can effect on cloud performance in general and can cause financial Losses [20] and can cause harmful effect in other servers in same cloud infrastructure as in [10].

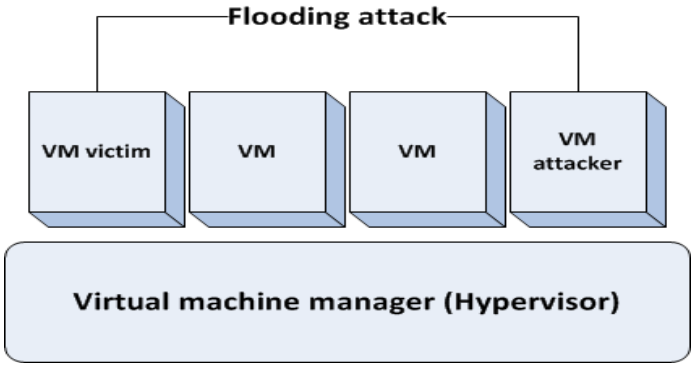

FIGURE 2: Flooding Dos attack in cloud environment

4. LITERATURE REVIEW and RELATED WORK

Denial of service attack poses as one of the most networks famous attacks, by which one victim machine can receive more than its capacity and so other end users requests cannot be served by server, and in the cloud environment, that kind of attack can be most harmful than unclouded environment because of VMs neighboring and resource sharing in cloud computing environment, so one virtual machine can be used as a source of denial of service attack to another virtual machine in same infrastructure and for overcome this security threat , several kind of flooding DoS attacks detecting and prevention approach has been suggested, and every one propose a method to detect or prevent this attack .

4.1 DETECTNG METHODS

Several kinds of flooding DoS attacks detecting approach has been suggested [21], One of these methods has proposed a kind of pattern generation for spatial-temporal traffic pattern in the application layer according to document popularity and also Access Matrix and behavior of web access. This method depends on semi-Markov modeling, and potential DoS attack is identified by entropy of document popularity, which matching the model [22].

In [23] The study pays more attention to service violations as an indicator to DoS attack, then the author explains comparison study to different kind of network monitoring techniques in terms of overhead, finally some of the parameters have been proposed to help in choosing the best monitoring schema according to the requirements and amount of overhead and Permittivity.

In [24] the author proposed framework to detect and trace back the source of attack, the first stage could detect two kinds of attack, logical and DoS/DDoS ,Neural networks used to discover logical attacks while DoS/DDoS can be recognized by CUSUM algorithm and for track backing attack, sources hash tracer is used then the second component of framework is prediction model which focuses on recognize of malicious behaviors for network traffic .

In [25] this research queuing theory model has been suggested to detect DoS attack on line, the proposed approach depends on two models , the first is to detect abrupt change based on some of the parameter and second model is the signal generation module which used for further processing.

In [26] the author has studied the dependency of web page attributes to detect new kinds of application layer attack then multiple principal component analysis is adapted as modeling method to model normal web browsing behaviors and finally, the author conducted some experiments to prove his model.

In [27] the author has developed a simulation to forecast numbers of zombies used in DDoS attack ,the forecasting depend on a polynomial regression model, and several statistical measures have been used for performance evaluation, and NS2 has been utilized as simulation platform and the result has been proven that this detection approach can forecast the number of zombies used in DDoS attack efficiently with low error percentage and prediction number of zombies in a DDoS Attack using Polynomial Regression Model.

in[28] this research paper, packet flows analysis for some network protocol has been suggested to detect DDoS attack and for normal behavior forecasting Gaussian parametric mixture has been utilized finally and for detect DDoS attack queue approach has been implemented, and the results showed that these detecting methods have accepted.

In [29] the author suggest using several computers working together hosted in a cloud to monitoring and analysis network traffic in same time and identify potential attack and for achieving that internet network can be used to link all detection devices systems together.

in [21] covariance-matrix statistical approach has been used for flooding based DoS attack detection, covariance-matrix depend on study and monitor of network traffic features correlativity changes and compare the covariance matrix of normal traffic and any new observed traffic and classify the comparison results according predefined threshold and finding the degree of anomaly of new captured traffic and normal traffic profile, and implementation of this approach has proven more accuracy and efficiency through simulation experiments to two of most famous flooding based attack Neptune and Smurf attacks , and in addition to high accuracy to this approach ,it can also detect second order of features which can be possible attack finally covariance-matrix can be summarized in three spaces, captured traffic space ,which content TCP dump data format and covariance-matrix space and lastly decision space which decide about the traffic either attack traffic or normal traffic as in Figure 3

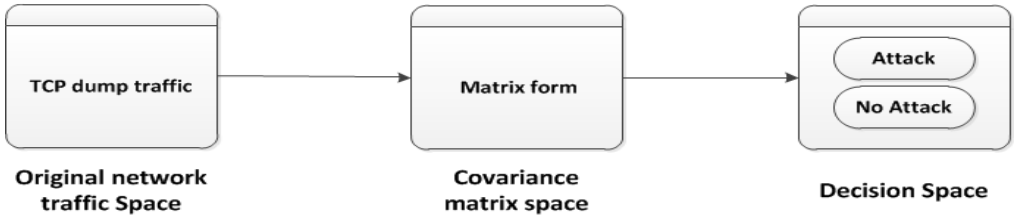

FIGURE 3: Covariance matrix detecting approach spaces

In [30] The author suggested framework depend on sharing IDS warring alerts with each other by set up IDS client tool and estimate the most dangerous attack according to the number of voting obtained by IDS client and simulation of this model has been done in snore environment, and the result has shown that this approach can protect a network from one point of failed

4.2 Prevention Methods

In [31] the author suggests a new approach to mitigate of flooding attack based on users' behavior's history using hidden markov modeling after traffic filtering process and also the author determined the implementation requirement such as firewall and access control setting, and for prove effectiveness of this approach DDoS simulation has been done .

In [32] the author proposes connected firewall to internet trap attack packets before its arrival to its victim. In [14]the author of this paper suggest a prevention strategy to avoid DDoS attack that targets application by shifting any cloud application under attack to another virtual machine in another physical server.

In [33] the author analysis DDoS attacks in random flow network environment, he suggests using this model to evaluate DDoS prevention frameworks, and the simulation has shown the relationship between multi matrixes inferred from the model.

In [34] research paper author suggested a new congestion control mechanism in computer networks to protect it from DDoS attack, this approach depended mainly on filtering mechanism based on time factor, and the author proposed using this protection method before applying queue management rules, and performance of this method using NS2 has done according to IP traces reported in http://www.nlnar.org

In [35] this paper proposed a bandwidth based DDoS prevention method by classify the traffic into three kinds, first is normal, attack and suspicious traffic, attack traffic is restrictive and the if the victim confirmed that arrived traffic is suspicious, then it determines the source of attack to block attack traffic coming from.

In [36] the requirements of the DDoS attack prevention system have been suggested, and the author suggested also DDoS attack prevention platform integration process

In [36] the author suggest finding and prevent TCP Spoofed IP address attack to mitigate TCP SYN flooding attack through TCP specific probing procedure, which forces the end user to modify windows size in packet retransmission through three handshake process in TCP protocol , previous work in mitigate TCP SYN flooding rely on count of SYN flag sent by same IP, but it was weak in order to preventing this attack because attackers using Spoofed IP so needing to this way of preventing TCP Spoofed IP address attack is very necessary

In [37] the author of this paper suggests three procedures to reduce TCP syn attack effects, firstly, utilized router as DoS defense then reduces SYN attack effects by blocking TCP, involving Trusted Platform Module in network infrastructure and Finlay using Certified System Defense.

5. PROPOSED FRAMEWORK

Proposed framework depends on covariance matrix mathematical modeling with three stages, firstly training stage then detecting and prevention stages as the following:

5.1 Training Stage

The first stage is monitoring income network traffic in virtual switch using any flow traffic tool such as wireshark[38] or snort [39] , in normal case or without attack, the traffic behavior has normal data distribution but with attack traffic data distribution change into abnormal form, this assumption can be as rule in detecting process.

First stage in detecting stage is summarizing all packets traffic in matrix values form, after that matrix is converted into a covariance matrix (normal traffic profile), finally resulted matrix is stored for further analysis as in Figure 4.

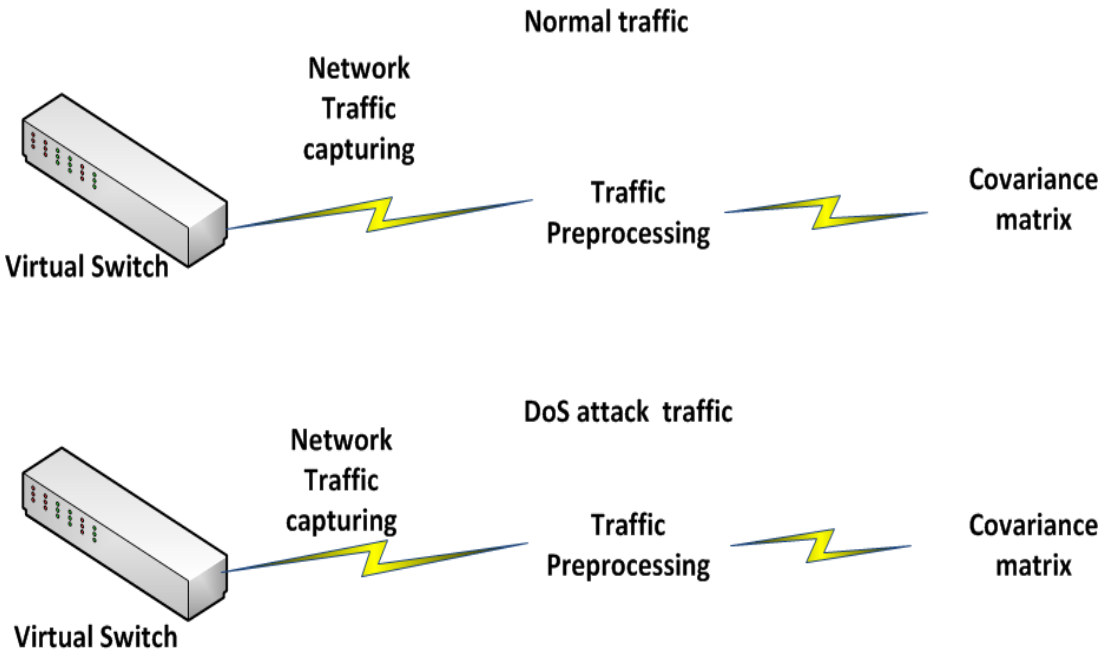

FIGURE 4: DoS attack detecting (Training stage)

5.2 DETECTING AND PREVENATOIN STAGES

In these stage, covariance matrix resulted from new captured traffic is compared with profile of normal traffic(covariance matrix of normal traffic), whenever the result matrix is all zero's values that mean no attack and whenever the resulted matrix not all zeros value and the anomaly degree values more than a predefined threshold, that mean attack has happened and thus detecting signal appears and focus will move into the stage of network protection by finding out attack source IP address.

And to find attack source IP address, number of nodes that attacker pass through until reach victim side is counted by counting value of TTL (Time _to_Life)[40]. After determining the source of attack, all IP address used by an attacker is blocked using honypot network which pings all IP address used by attacker and whenever there is a replay, all responded IP address is blocked [14].

Then finally when the attack has been known, the legitimate traffic to victim's virtual machine is shifted to same virtual machine but in another physical machine [14], because cloud computing environment located multiple copies for one virtual machine to strengthening reliability of computing as in Figure 5

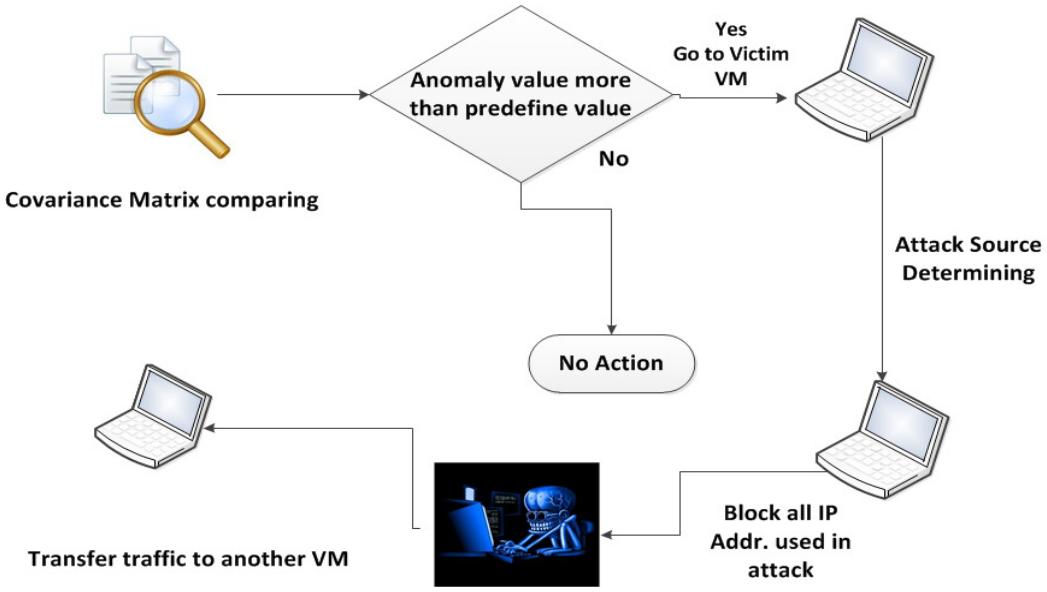

FIGURE 5: DoS attack prevention stage

6. PROPOSED FRAMEWORK TEST BED

To implement the proposed framework, simple cloud environment can be built, which consists of three web server virtual machine and user can access to web server by internet gateway and virtual switch as in Figure 6

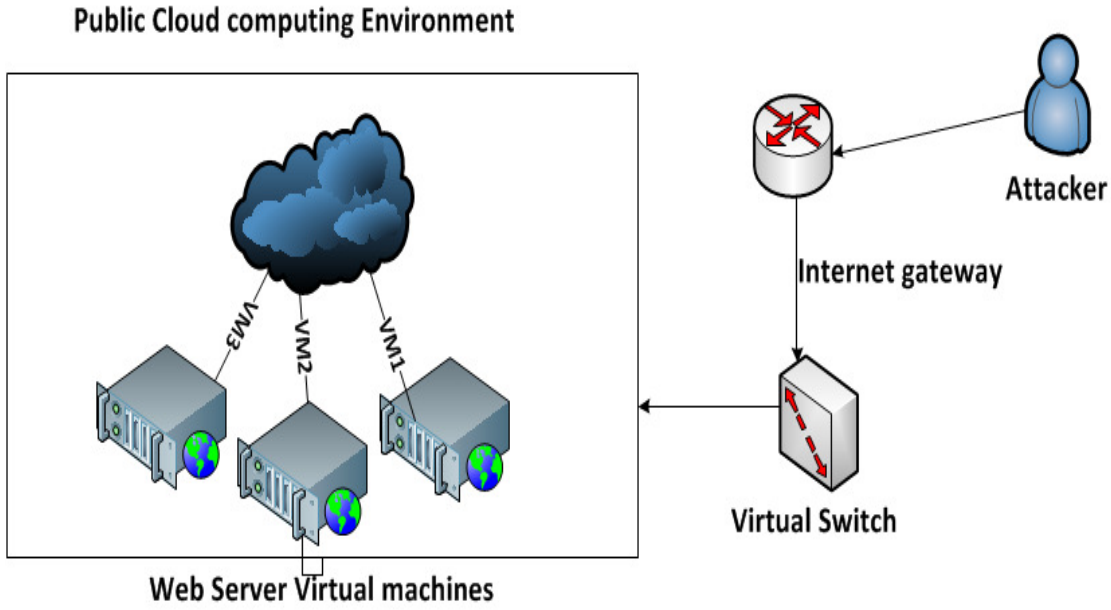

FIGURE 6: Framework experiment test bed

7. IMPLEMENTATION

Proposed framework can be simulated Initially in conceptual level , using class and sequences UML diagrams [41] and Covariance mathematical model can be involved in cloud environment

simulating to detect flooding DoS attack as in Figure 7 and Figure 8 and all detailed of simulation in [40].

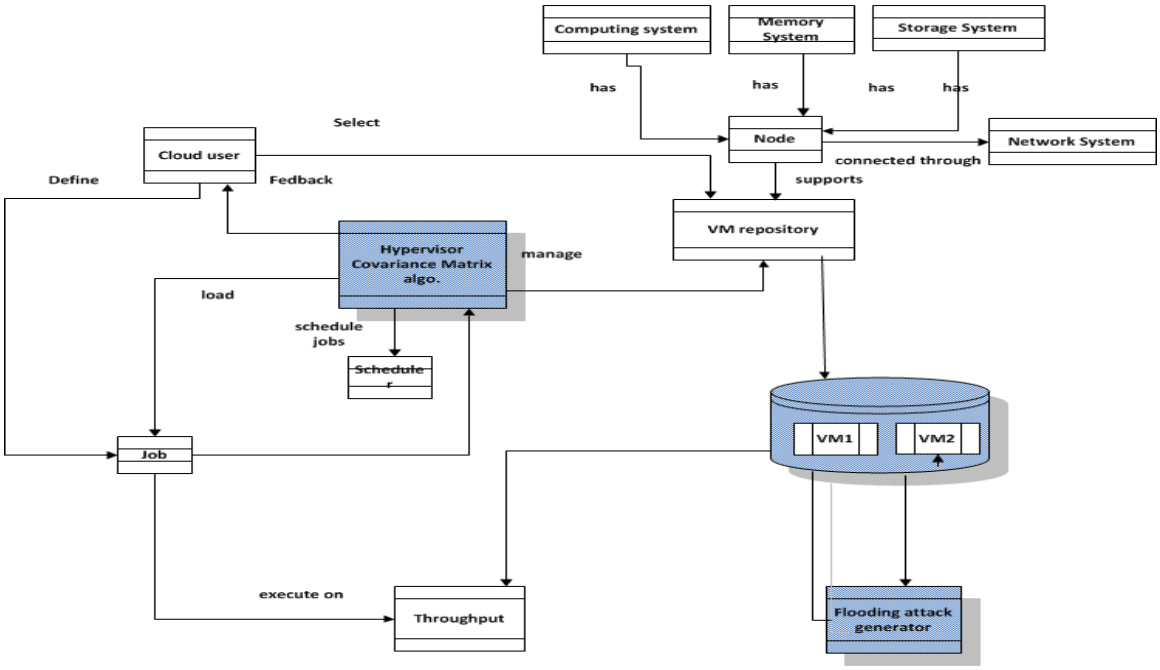

FIGURE 7: Class diagram to cloud environment

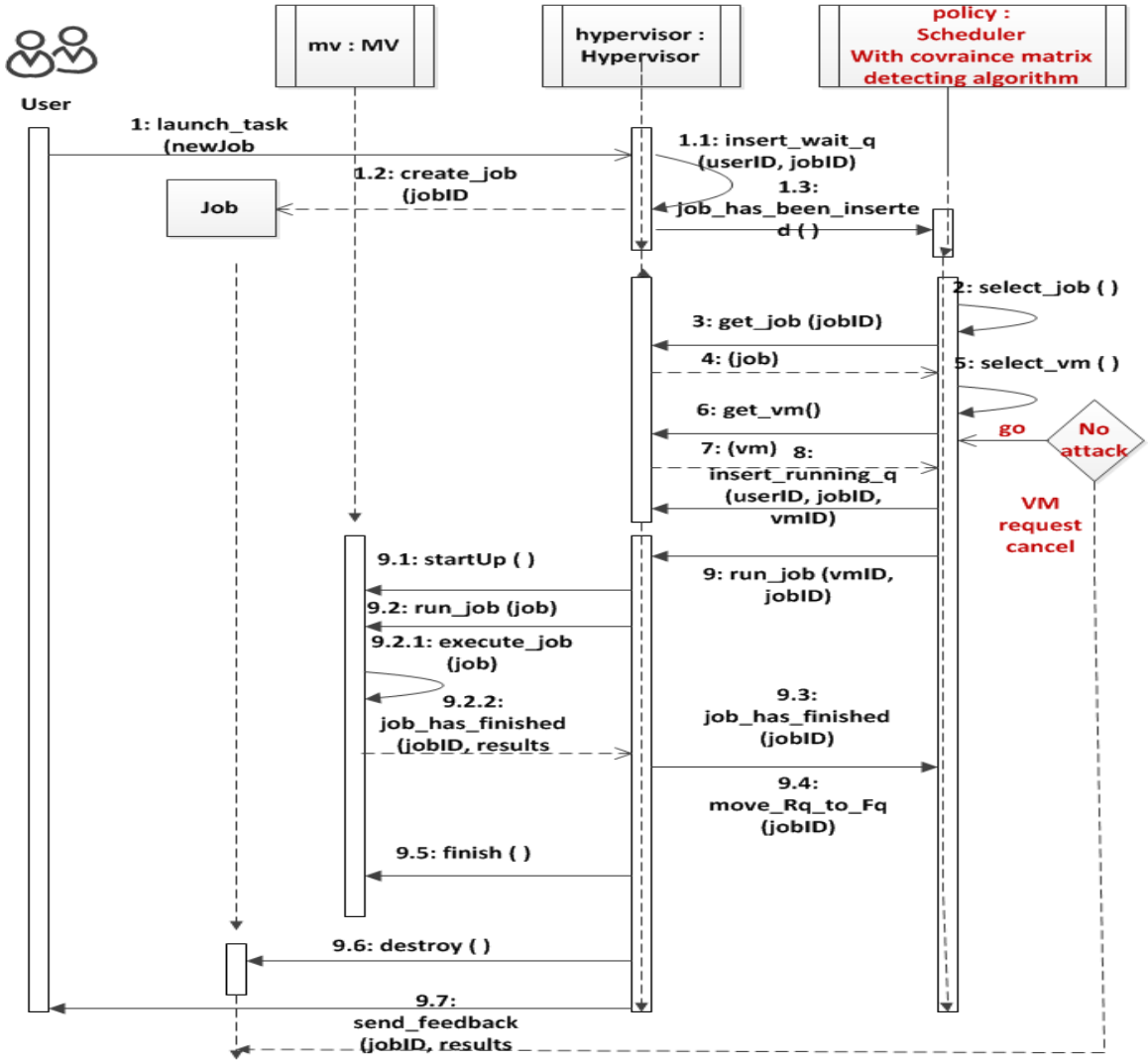

FIGURE 8: Sequence diagram to cloud environment

8. CONCLUSION

Finlay we can conclude that as cloud computing can offer new computing benefits, but it faces high risks, specifically in the security side where DDoS attack can make cloud service unavailable, and several methods have suggested but most of them give more attention to one side either detecting or track backing or prevention, our new frame work focuses on all aspects of the problem. Simulation part we give a conceptual view to location of the covariance matrix in cloud computing environment using class and sequences UML diagram and In future work we plan to performance the simulation mentioned above and implement the proposed frame work in real cloud environment and determine some constraints such as on line detecting constraints and also detecting the attack in different cloud environment such as private, public and hyper environment.

9. REFERENCE

[1] Foster, I. and C. Kesselman, The grid: blueprint for a new computing infrastructure. 2004: Morgan Kaufmann.

[2] Buyya, R., High performance cluster computing: programming and applications, vol. 2. Pre ticeHallPTR, NJ, 1999.

[3] Armbrust, M., et al., A view of cloud computing. Communications of the ACM, 2010. 53(4): p. 50-58.

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

[5] Bhardwaj, S., L. Jain, and S. Jain, Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2010. 2(1): p. 60-63.

[6] Kulkarni, G., P. Khatawkar, and J. Gambhir, Cloud Computing-Platform as Service. International Journal of Engineering. 1.

[7] Kulkarni, G., J. Gambhir, and R. Palwe, Cloud Computing-Software as Service. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2012. 1(1).

[8] Foster, I., et al. Cloud computing and grid computing 360-degree compared. 2008: Ieee.

[9] Ngongang, G., Cloud Computing Security. 2011.

[10] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011. 34(1): p. 1-11.

[11] Chen, Y., V. Paxson, and R.H. Katz, What's new about cloud computing security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 2010. 20(2010): p. 2010-5.

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

[13] Hwang, K., S. Kulkareni, and Y. Hu. Cloud security with virtualized defense and reputation-based trust mangement. 2009: Ieee.

[14] Bakshi, A. and B. Yogesh. Securing cloud from ddos attacks using intrusion detection system in virtual machine. 2010: Ieee.

[15] Almulla, S.A. and C.Y. Yeun. Cloud computing security management. 2010: IEEE.

[16] Iankoulova, I. and M. Daneva, Cloud Computing Security Requirements: a Systematic Review.

[17] Bamiah, M.A. and S.N. Brohi, Seven Deadly Threats and Vulnerabilities in Cloud Computing.

[18] Dillon, T., C. Wu, and E. Chang. Cloud computing: Issues and challenges. 2010: Ieee.

[19] Hovav, A. and J. D'Arcy, The Impact of Denial□of□Service Attack Announcements on the Market Value of Firms. Risk Management and Insurance Review, 2003. 6(2): p. 97-121.

[20] Peng, T., C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 2007. 39(1): p. 3.

[21] 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.

[22] Xie, Y. and S.Z. Yu, Monitoring the application-layer DDoS attacks for popular websites. Networking, IEEE/ACM Transactions on, 2009. 17(1): p. 15-25.

[23] Habib, A., M. Hefeeda, and B. Bhargava. Detecting service violations and DoS attacks. 2003.

[24] Leu, F., Intrusion Detection, Forecast and Traceback Against DDoS Attacks. 2009.

[25] Singh, N., S. Ghrera, and P. Chaudhuri, Denial of Service Attack: Analysis of Network Traffic Anormaly using Queuing Theory. Arxiv preprint arXiv:1006.2807, 2010.

[26] Lee, S., G. Kim, and S. Kim, Sequence-order-independent network profiling for detecting application layer DDoS attacks. EURASIP Journal on Wireless Communications and Networking, 2011. 2011(1): p. 1-9.

[27] Gupta, B., R. Joshi, and M. Misra, Prediction of Number of Zombies in a DDoS Attack using Polynomial Regression Model. Journal of Advances in Information Technology, 2011. 2(1): p. 57-62.

[28] Hao, S., et al. A queue model to detect DDos attacks. 2005: IEEE.

[29] Guilbault, N. and R. Guha. Experiment setup for temporal distributed intrusion detection system on amazon's elastic compute cloud. 2009: IEEE.

[30] Lo, C.C., C.C. Huang, and J. Ku. A cooperative intrusion detection system framework for cloud computing Networks. 2010: IEEE.

[31] Prabha, S. and R. Anitha, Mitigation of Application Traffic DDOS Attacks with Trust and Am Based Hmm Models. International Journal of Computer Applications IJCA, 2010. 6(9): p. 26-34.

[32] Chang, R.K.C., Defending against flooding-based distributed denial-of-service attacks: A tutorial. Communications Magazine, IEEE, 2002. 40(10): p. 42-51.

[33] Kong, J., et al. Random flow network modeling and simulations for DDoS attack mitigation. 2003: IEEE.

[34] Hu, Y.H., H. Choi, and H.A. Choi. Packet filtering to defend flooding-based DDoS attacks [Internet denial-of-service attacks]. 2004: IEEE.

[35] Wuu, L.C., et al. A practice of the intrusion prevention system. 2007: IEEE.

[36] Choi, Y.S., et al. Integrated DDoS attack defense infrastructure for effective attack prevention. 2010: IEEE.

[37] Chao-yang, Z. DOS Attack Analysis and Study of New Measures to Prevent. 2011: IEEE.

[38] Lamping, U. and E. Warnicke, Wireshark User's Guide. Interface, 2004. 4: p. 6.

[39] Roesch, M. Snort-lightweight intrusion detection for networks. 1999: Seattle, Washington.

[40] Wang, H., C. Jin, and K.G. Shin, Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Transactions on Networking (TON), 2007. 15(1): p. 40-53.

[41] Nunez, A., et al. Design of a flexible and scalable hypervisor module for simulating cloud computing environments. 2011: IEEE.