International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

DDoS Spyware for Cloud Computing Environment

Prof. Harish Barapatre[1], Jai Deshmukh[2], Vikrant Kapse[3], Pritam Patil[4]
[1,2,3,4] Computer Department,Yadavrao Tasgaonkar Institute Of Engineering & Technology.
Karjat, Maharashtra, India.

Abstract— Cloud computing is becoming one of the next IT industry buzz word. However, as cloud computing is still in its infancy, current adoption is associated with numerous challenges like security, performance, availability, etc. In cloud computing where infrastructure is shared by potentially millions of users, Distributed Denial of Service (DDoS) attacks have the potential to have much greater impact than against single tenanted architectures. This paper tested the efficiency of a cloud trace back model in dealing with DDoS attacks using back propagation neural network and finds that the model is useful in tackling.
Distributed Denial of Service attacks This paper sets to address this important problem. We start by examining the security impact, in particular, the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted. We find that SDN technology can actually help enterprises to defend against DDoS attacks if the defense architecture is designed properly.
Keywords— Denial of Service, Cloud Computing, Cloud Trace Back Model, Cloud Protector, Neural Network.

I. INTRODUCTION

Networking principles have remained mostly unchanged over the past decade. Networks are built using more or less sophisticated switches and routers. These devices are being developed by tens of vendors usually using proprietary operating system and interfaces. Building heterogeneous networks on devices from different vendor's means that organization have to employ a specialist on every router brand. Configuration of different systems also increases the probability of configuration mistakes. This issue coupled with incompatibility of different versions of systems from one vendor make heterogeneous networks difficult or very expensive to manage. There is a need for a new technology to make networks more scalable, dynamic and to allow easier management of network devices from different vendors. These needs could be fulfilled by programmable networks, i. e., by **S**oftware **D**efined **N**etworking (SDN). SDN could replace traditional networking. It is based on the abstraction of a control and a data plane. The main idea is to produce less sophisticated data plane devices, e. g., switches, which only forward the traffic according to a set of rules defined by the software in the control plane. This should remove the differences in proprietary interfaces of devices and makes the network administration independent of data plane devices vendors. SDN also enables applications and network services to treat the network as one logical entity and grants unified access to all devices through the SDN control plane. This opens the upper layer of the network to software that can manage how a traffic in the network is forwarded. Alongside the evolution of networking is the evolution of network attacks. One of the current threats are Distributed Denial of Service (DDoS) attacks.
A DDoS attack is an attempt to make a network or server resource unavailable to its intended users. This attack is relatively easy to perform, hard to defend against, and the attacker is rarely traced back. This attack was performed manually by users refreshing their browsers. Since the first attack, there have been many other more or less sophisticated DDoS attacks. Average DDoS attack bandwidth increased from 2.88 Gbps in Q3 2013 to 13.93 Gbps in Q3 2014. There were 17 attacks with bandwidth higher than 100 Gbps. Even though there are many proposed detection methods and mitigation techniques, we cannot say that the DDoS attacks are a solved problem or do not present an immense threat to the current Internet. The research in the field of SDN and general security in SDN

is still in its early phase. The SDN will not erase the DDoS attacks from the Internet. Moreover, every new technology and level of abstraction opens new attack vectors. However, we believe that the attributes of SDN can help to detect and mitigate the attacks. Currently, there are several papers analyzing DDoS attack vectors and proposing new solutions of mitigation of DDoS attacks in SDN environment. Our research will be dedicated to an analysis of security challenges in SDN from the point of view of DDoS attacks and development of a new DDoS attacks mitigation technique. We believe that SDN gives us a new powerful tool against DDoS attacks. The higher flexibility and easier management of networks could be a powerful tool for detection and mitigation of DDoS attacks. However, one should be aware of upcoming security threats accompanied with the deployment of SDN. The research focused on the security in SDN is still in its early phase. The research groups are focused on the security of the data plane, security of the control plane, security of the communication between these planes and on enhancing the network security using SDN, which is also our goal. The result of our research is going to be a novel method for mitigation of DDoS attacks using the benefits of Software Defined Networking, which enhance the network security. Combination of the existing detection methods and management of SDN forms a new way of DDoS mitigation in future networks.

A. Economic Distributed Denial of Service (eDDoS)

In existing system, the Cloud-based DDoS attacks or outside DDoS attacks can make ostensibly legitimate requests for a service to generate an economic Distributed Denial of Service (eDDoS) - where the elastic nature of the cloud allows scaling of service beyond the economic means of the purveyor to pay their cloud-based service bills which leads to Economic Denial of Sustainability (EDoS). Attacks mimicking legitimate users are on the climb. For cloud computing to remain attractive, the DDoS threat is to be addressed before it triggers the billing mechanism. This problem can be addressed by using reactive/on-demand in-cloud eDDoS mitigation service (scrubber Service) for mitigating the application-layer and network-layer DDOS attacks with the help of an efficient client-puzzle approach.

EDoS is "packet flood that stretches the elasticity of metered-services employed by a server, e.g., a cloud-based server". EDoS attack can be generated by distantly run bots "to smoothly (with low rate to avoid triggering security alarms) flood a targeted cloud service by undesired requests". Therefore, the cloud service employment "will be scaled up to satisfy the on-demand requests". As cloud depends on the pay-per-use base, the user's bill will be charged for these faked requests, "leading to service withdrawal or bankruptcy". At the end, the cloud provider will lose its customers, as they will believe that the on premise data center is better and cheaper for them than the cloud, which enforce them to pay for services they did not request. Moreover, the cloud provider must pay, to the vendors, for the infrastructure regardless their clients' withdrawal. Hence, the providers are affected negatively by EDoS attacks more than their customers. Distributed Denial of Service (DDoS) solutions can be classified into two categories; reactive and proactive solutions. Reactive solutions mean that the defense system is waiting the attack to occur then try to mitigate its impacts. On the other side, proactive solution involves treating the source of packets before reaching to the protected server. The filtering systems are considered as reactive solutions. However, Overlay-based techniques are considered as proactive solutions. These techniques include other components beside the filters. They depend on distributed firewalls or nodes (the node can be a virtual machine or an application), and hiding the location of the protected server.

Cloud computing is not a new technology; it is a new way of delivering computing resources. Elastic cloud computing enables services to be deployed and accessed globally on demand with little maintenance by providing QoS as per service level agreement (SLA) of customer. The Cloud-based DDoS attacks or outside DDoS attacks can make ostensibly legitimate requests for a service to generate an economic Distributed Denial of Service (eDDoS) --where the elastic nature of the cloud allows scaling of service beyond the economic means of the purveyor to pay their cloud-based service bills which leads to Economic Denial of Sustainability (EDoS). Attacks mimicking legitimate

users are on the climb. For cloud computing to remain attractive, the DDoS threat is to be addressed before it triggers the billing mechanism. This problem can be addressed by using reactive/on-demand in-cloud eDDoS mitigation service (scrubber Service) for mitigating the application-layer and network-layer DDOS attacks with the help of an efficient client-puzzle approach. Index Terms—Cloud computing, Economic Denial of Service (EDoS), Mitigation, Distributed Denial of Service (DDoS), cryptographic puzzles.

B. Software Defined Networks (SDN)

In proposed system, first we discuss the new trends and characteristics of DDoS attacks in cloud computing environments. We show that SDN brings us a new chance to defeat DDoS attacks in cloud computing environments, and we summarize good features of SDN in defeating DDoS attacks. Software Defined Networks (SDN) is a new network architecture that provides central control over the network. This control works as if it is an operating system that can send instructions and apply changes through its interface. This operating system is called the controller. Although central control is the major advantage of SDN, it is also a single point of failure if it is made unreachable by a Distributed Denial of Service Attack (DDoS). Two main objectives of this study are utilizing the central control of SDN for attack detection and, proposing a solution that is effective and lightweight in terms of the resources that it uses. This research shows how DDoS attacks can exhaust controller resources and provides a solution to detect such attacks based on entropy variation of destination IP address. This method is able to detect DDoS within the first five hundred packets of the attack traffic. SDN architecture can be a network of several controllers each of which is connected to a network of switches. Each of these networks and its controller can be seen as slice of the network. We are focusing on each of these slices to protect it against DDoS. If the connection between the switches and the controller is lost, the network will lose its processing plane. That means packet processing is no longer done in the controller and by losing the controller, the SDN architecture is lost. One of the possibilities that can cause the controller to be unreachable is a DDoS attack. In DDoS attacks, a large number of packets are sent to a host or a group of hosts in a network. If the source addresses of the incoming packets are spoofed, which theory usually are, the switch will not find a match and has to forward the packet to the controller. The collection of legitimate and the DDoS spoofed packets can bind the resources of the controller into continuous processing that exhausts them. This will make the controller unreachable for the newly arrived legitimate packets and may bring the controller down causing the loss of the SDN architecture. Even if there is a backup controller, it has to face the same challenge. The main goal of this research is detecting a DDoS attack in its early stages. The term early depends on the network itself. Since the controller software can be run on a laptop or a powerful desktop, the term early would depend on the tolerance of the device and traffic properties. However, if the detection happens in the first few hundred packets, the mitigation is applied before the controller is completely swamped with the large number of malicious packets.

The high configurability of SDN offers clear separation among virtual networks, permitting experimentation in a real environment. Progressive deployment of new ideas can be per-formed through a seamless transition from an experimental phase to an operational phase. This feature of SDN offers great convenience in putting forward new thoughts and methods for DDoS attack mitigation. In this paper, we first analyze the impact of the combination of cloud computing and SDN on DDoS attack defense. We discuss the potential issues under this new paradigm as well as opportunities of defending DDoS attacks. Based on our analysis, we claim that if designed properly, SDN can actually be exploited to address the security challenges brought by cloud computing and the DDoS attack defense can be made more effective and efficient in the era of cloud computing and SDN. We then propose a new DDoS attack mitigation architecture using software-defined networking to demonstrate and substantiate our findings. Implementing SDN affects the DDoS attack defense greatly in both directions. On the bright side, SDN makes advanced detection logic and rich subsequent processes easier to implement. On the down-side, the devices or middle-boxes originally distributed within the network now need to be located above NOS. Compared with hardware-based

packet processing, software processes packets is much slower. The network delay and traffic overhead caused by the communications between the control program.

Based on our analysis, cloud computing introduces new DDoS challenges, i.e., extended defense perimeter and dynamic network topology due to its new operation model. To effectively address these challenges, the cloud provider must be able to 1) easily delegate the control of its network to cloud users; 2) fast re-configure the control according to the network topology changes caused by dynamic allocations and migrations. On one side, we could benefit from the centralized network controller and the network virtualization of SDN. The negative impact of SDN mainly comes from the efficiency of processing packets using software, which may generate new attack surface and lead to single-point failure. When designing a DDoS attack defense solution in SDN, one must take the computation and communication overhead into the consideration so that no new security vulnerability is introduced.

II. EXISTING SYSTEM

In existing system, the Cloud-based DDoS attacks or outside DDoS attacks can make ostensibly legitimate requests for a service to generate an economic Distributed Denial of Service (eDDoS) - where the elastic nature of the cloud allows scaling of service beyond the economic means of the purveyor to pay their cloud-based service bills which leads to Economic Denial of Sustainability (EDoS). Attacks mimicking legitimate users are on the climb. For cloud computing to remain attractive, the DDoS threat is to be addressed before it triggers the billing mechanism. This problem can be addressed by using reactive/on-demand in-cloud eDDoS mitigation service (scrubber Service) for mitigating the application-layer and network-layer DDOS attacks with the help of an efficient client-puzzle approach.

EDoS is "packet flood that stretches the elasticity of metered-services employed by a server, e.g., a cloud-based server". EDoS attack can be generated by distantly run bots "to smoothly (with low rate to avoid triggering security alarms) flood a targeted cloud service by undesired requests". Therefore, the cloud service employment "will be scaled up to satisfy the on-demand requests". As cloud depends on the pay-per-use base, the user's bill will be charged for these faked requests, "leading to service withdrawal or bankruptcy". At the end, the cloud provider will lose its customers, as they will believe that the on premise data center is better and cheaper for them than the cloud, which enforce them to pay for services they did not request. Moreover, the cloud provider must pay, to the vendors, for the infrastructure regardless their clients' withdrawal. Hence, the providers are affected negatively by EDoS attacks more than their customers. Distributed Denial of Service (DDoS) solutions can be classified into two categories; reactive and proactive solutions. Reactive solutions mean that the defense system is waiting the attack to occur then try to mitigate its impacts. On the other side, proactive solution involves treating the source of packets before reaching to the protected server. The filtering systems are considered as reactive solutions. However, Overlay-based techniques are considered as proactive solutions. These techniques include other components beside the filters. They depend on distributed firewalls or nodes (the node can be a virtual machine or an application), and hiding the location of the protected server.

Cloud computing is not a new technology; it is a new way of delivering computing resources. Elastic cloud computing enables services to be deployed and accessed globally on demand with little maintenance by providing QoS as per service level agreement (SLA) of customer. The Cloud-based DDoS attacks or outside DDoS attacks can make ostensibly legitimate requests for a service to generate an economic Distributed Denial of Service (eDDoS) --where the elastic nature of the cloud allows scaling of service beyond the economic means of the purveyor to pay their cloud-based service bills which leads to Economic Denial of Sustainability (EDoS). Attacks mimicking legitimate users are on the climb. For cloud computing to remain attractive, the DDoS threat is to be addressed before it triggers the billing mechanism. This problem can be addressed by using reactive/on-demand in-cloud eDDoS mitigation service (scrubber Service) for mitigating the application-layer and network-layer DDOS attacks with the help of an efficient client-puzzle approach. Index Terms—

Cloud computing, Economic Denial of Service (EDoS), Mitigation, Distributed Denial of Service (DDoS), cryptographic puzzles.

Software-Defined Networking (SDN) is considered promising to simplify network management and enable research innovations based on the decomposition of the control and data planes. In this paper, we review SDN-related technologies. In particular, we try to cover three main parts of SDN: applications, the control plane, and the data plane anticipating that our efforts will help researchers set appropriate and meaningful directions for future SDN research.

In this section we describe the seven main potential threat vectors we identified in SDNs (Figure 1). Our goal is not to use these potential problems to claim that software-defined networks are inherently less secure than current networks. What we argue is that SDNs pose threats of a different nature that need therefore to be dealt with differently. On the contrary, if the SDN is properly designed and deployed, we believe this new network environment will definitely present a quantum leap in network architecting, not only in functionality but also in resilience. Forged or faked traffic flows, which can be used to attack switches and controllers. This threat can be triggered by faulty (non-malicious) devices or by a malicious user. An attacker can use network elements (e.g., switches, servers, or personal computers) to launch a DoS attack against OpenFlow switches (e.g., targeting to exhaust TCAMs) and controller resources. A simple authentication mechanism could mitigate the problem, but if an attacker assumes the control of an application server that stores the details of many users, it can easily use the same authenticated ports and source MAC addresses to inject authorized, but forged, flows into the network. Possible solutions: The use of intrusion detection systems with support for runtime root-cause analysis could help identify abnormal flows. This could be coupled with mechanisms for dynamic control of switch behavior (e.g., rate bounds for control plane requests).

III. PROPOSED SYSTEM

In proposed system, first we discuss the new trends and characteristics of DDoS attacks in cloud computing environments. We show that SDN brings us a new chance to defeat DDoS attacks in cloud computing environments, and we summarize good features of SDN in defeating DDoS attacks. Software Defined Networks (SDN) is a new network architecture that provides central control over the network. This control works as if it is an operating system that can send instructions and apply changes through its interface. This operating system is called the controller. Although central control is the major advantage of SDN, it is also a single point of failure if it is made unreachable by a Distributed Denial of Service Attack (DDoS). Two main objectives of this study are utilizing the central control of SDN for attack detection and, proposing a solution that is effective and lightweight in terms of the resources that it uses. This research shows how DDoS attacks can exhaust controller resources and provides a solution to detect such attacks based on entropy variation of destination IP address. This method is able to detect DDoS within the first five hundred packets of the attack traffic. SDN architecture can be a network of several controllers each of which is connected to a network of switches. Each of these networks and its controller can be seen as slice of the network. We are focusing on each of these slices to protect it against DDoS. If the connection between the switches and the controller is lost, the network will lose its processing plane. That means packet processing is no longer done in the controller and by losing the controller, the SDN architecture is lost. One of the possibilities that can cause the controller to be unreachable is a DDoS attack. In DDoS attacks, a large number of packets are sent to a host or a group of hosts in a network. If the source addresses of the incoming packets are spoofed, which theory usually are, the switch will not find a match and has to forward the packet to the controller. The collection of legitimate and the DDoS spoofed packets can bind the resources of the controller into continuous processing that exhausts them. This will make the controller unreachable for the newly arrived legitimate packets and may bring the controller down causing the loss of the SDN architecture. Even if there is a backup controller, it has to face the same challenge. The main goal of this research is detecting a DDoS attack in its early stages. The term early depends on the network itself. Since the controller software can be run on a

laptop or a powerful desktop, the term early would depend on the tolerance of the device and traffic properties. However, if the detection happens in the first few hundred packets, the mitigation is applied before the controller is completely swamped with the large number of malicious packets.

The high configurability of SDN offers clear separation among virtual networks, permitting experimentation in a real environment. Progressive deployment of new ideas can be per-formed through a seamless transition from an experimental phase to an operational phase. This feature of SDN offers great convenience in putting forward new thoughts and methods for DDoS attack mitigation. In this paper, we first analyze the impact of the combination of cloud computing and SDN on DDoS attack defense. We discuss the potential issues under this new paradigm as well as opportunities of defending DDoS attacks. Based on our analysis, we claim that if designed properly, SDN can actually be exploited to address the security challenges brought by cloud computing and the DDoS attack defense can be made more effective and efficient in the era of cloud computing and SDN. We then propose a new DDoS attack mitigation architecture using software-defined networking to demonstrate and substantiate our findings. Implementing SDN affects the DDoS attack defense greatly in both directions. On the bright side, SDN makes advanced detection logic and rich subsequent processes easier to implement. On the down-side, the devices or middle-boxes originally distributed within the network now need to be located above NOS. Compared with hardware-based packet processing, software processes packets is much slower. The network delay and traffic overhead caused by the communications between the control program.

Based on our analysis, cloud computing introduces new DDoS challenges, i.e., extended defense perimeter and dynamic network topology due to its new operation model. To effectively address these challenges, the cloud provider must be able to 1) easily delegate the control of its network to cloud users; 2) fast re-configure the control according to the network topology changes caused by dynamic allocations and migrations. On one side, we could benefit from the centralized network controller and the network virtualization of SDN. The negative impact of SDN mainly comes from the efficiency of processing packets using software, which may generate new attack surface and lead to single-point failure. When designing a DDoS attack defense solution in SDN, one must take the computation and communication overhead into the consideration so that no new security vulnerability is introduced.

IV. METHODOLOGY

System Implementation:

Implementation of software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure that the software is meant to make their job easier.

The active user must be aware of the benefits of using the system

Their confidence in the software built up

Proper guidance is impaired to the user so that he is comfortable in using the application

Before going ahead and viewing the system, the user must know that for viewing the result, the server program should be running in the server. If the server object is not running on the server, the actual processes will not take place.

A. User Training:

To achieve the objectives and benefits expected from the proposed system it is essential for the people who will be involved to be confident of their role in the new system. As system becomes more complex, the need for education and training is more and more important.

Education is complementary to training. It brings life to formal training by explaining the background to the resources for them. Education involves creating the right atmosphere and motivating user staff. Education information can make training more interesting and more understandable.

B. Training on the Application Software:

After providing the necessary basic training on the computer awareness, the users will have to be trained on the new application software. This will give the underlying philosophy of the use of the new system such as the screen flow, screen design, type of help on the screen, type of errors while entering the data, the corresponding validation check at each entry and the ways to correct the data entered. This training may be different across different user groups and across different levels of hierarchy.

C. Operational Documentation:

Once the implementation plan is decided, it is essential that the user of the system is made familiar and comfortable with the environment. A documentation providing the whole operations of the system is being developed. Useful tips and guidance is given inside the application itself to the user. The system is developed user friendly so that the user can work the system from the tips given in the application itself.

D. System Maintenance:

The maintenance phase of the software cycle is the time in which software performs useful work. After a system is successfully implemented, it should be maintained in a proper manner. System maintenance is an important aspect in the software development life cycle. The need for system maintenance is to make adaptable to the changes in the system environment. There may be social, technical and other environmental changes, which affect a system which is being implemented. Software product enhancements may involve providing new functional capabilities, improving user displays and mode of interaction, upgrading the performance characteristics of the system. So only thru proper system maintenance procedures, the system can be adapted to cope up with these changes. Software maintenance is of course, far more than “finding mistakes”.

E. Corrective Maintenance:

The first maintenance activity occurs because it is unreasonable to assume that software testing will uncover all latent errors in a large software system. During the use of any large program, errors will occur and be reported to the developer. The process that includes the diagnosis and correction of one or more errors is called Corrective Maintenance.

F. Adaptive Maintenance:

The second activity that contributes to a definition of maintenance occurs because of the rapid change that is encountered in every aspect of computing. Therefore Adaptive maintenance termed as an activity that modifies software to properly interfere with a changing environment is both necessary and commonplace.

G. Perceptive Maintenance:

The third activity that may be applied to a definition of maintenance occurs when a software package is successful. As the software is used, recommendations for new capabilities, modifications to existing functions, and general enhancement are received from users. To satisfy requests in this category, Perceptive maintenance is performed. This activity accounts for the majority of all efforts expended on software maintenance.

H. Preventive Maintenance:

The fourth maintenance activity occurs when software is changed to improve future maintainability or reliability, or to provide a better basis for future enhancements. Often called preventive maintenance, this activity is characterized by reverse engineering and re-engineering techniques.

V. MODULE DESCRIPTION

Server Monitoring:

This module describes to start the cloud server monitoring process. Its watch. The service request from different source and what request come from source IP.

Data preprocess from the Source :

Here Cloud server collect all service request detail, such as type of request , Source Protocol detail, Size of Request, Count of service in same port connection in same time duration to the cloud server and count the request when enter to the service host all those details are frequently sending to the server.

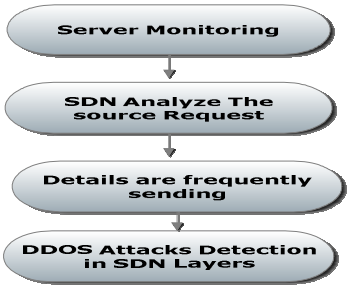
DDOS Attacks Detection in SDN Layers

The SDN contain 3 type of layers. These layers are filter the attack in each level.

Application layer

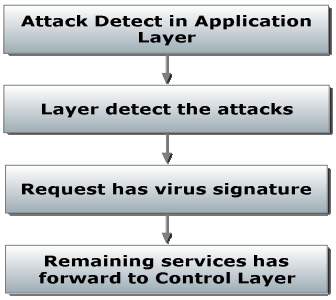
Control layer

Infrastructure Layer



Attack Detect in Trace Back Model

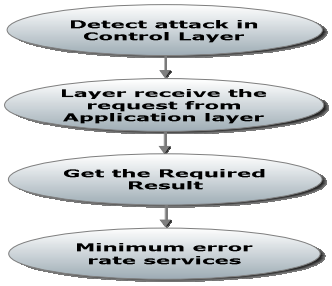
Here The Layer detect the attacks in North bound application level, that's mean SDN find which service Request has virus signature, that indicate in Logging level. If the Logged is '1' that service are not in virus Signature and which is Logged level is '0'that request has attached a virus or malware or botnet Signature. These attacks are filter in this layer and remaining services has forward to Control Layer.



Attack Detection From Source Using TCB:

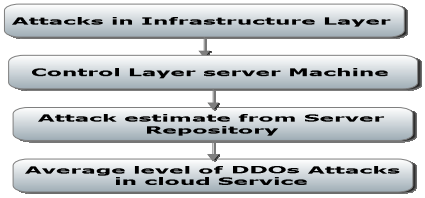
This Layer receive the request from Application layer and control the Request services forward to the server machine for Get the Required Result or Required Cloud service. This Source Request has to forwarding to each control server machine depending upon The Size of Request and Service error

rate. If which is have maximum error rate that type of services are denied in this layer. And minimum error rate services only forward to the Destination server machine.

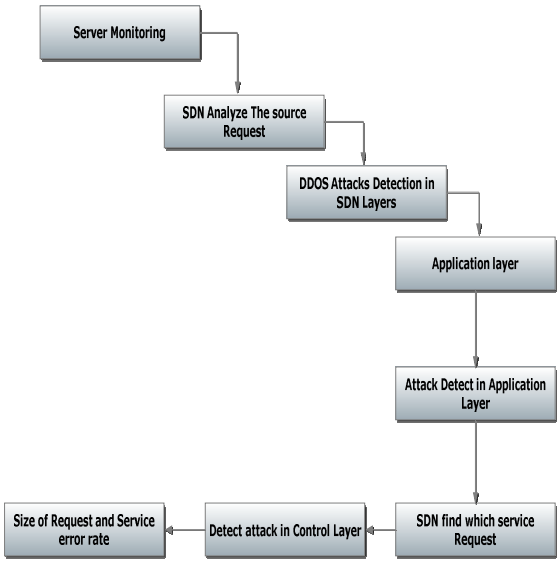


Network Propagation Model

The Infrastructure layer is a Southbound of Network. It Receive the Services Request From Control Layer server Machine .It Generate The Result to each request or Provide The Services To The request IP, but before provide service…it analyze the Destination error rate.. because some of ddos, malware or botnet attack couldn't find out above layers, that's filter maximum level of attack signature request, but still some of malwares no filter proper, so the Server indicate that service request using destination error rate, So maximum level of error request file has denied and finally the cloud service provide for non-attack request IP. The NPM server Calculate No of attack come from which IP and The time duration, Analyze the performance of Each Layer, how much attacks detect and filter in each level. And we have calculate the average level of DDOs Attacks in cloud Service.



VI. DESIGN



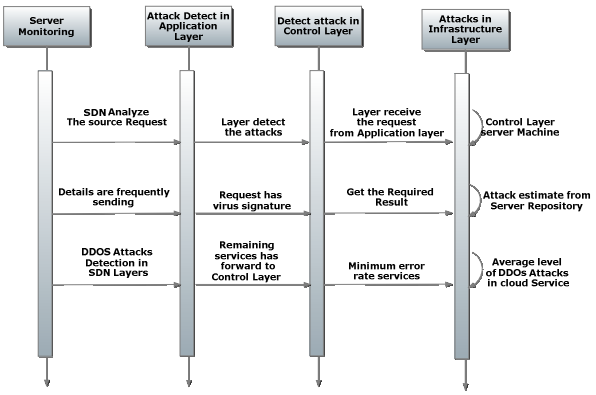


Figure : SEQUENCE DIAGRAM

VII.CONCLUSION

Cloud computing is already here to stay and SDN is gaining increased popularity. With both of the technology emerging as the future enterprise IT solutions, it is worthwhile to look at the implications of the combination of the two, particularly on the enterprise network security. In this paper, we analyze the impact of cloud computing and SDN on DDoS attack defense. Based on our analysis, we identify the challenges and the benefits raised by these new technologies. We claim that with careful design, SDN could help with DDoS attack protection. To substantiate our finding, we proposed our solution of defending DDoS attack— DaMask architecture. Compared to the existing solutions, DaMask requires little effort from the cloud provider which means few changes are required from the current cloud computing service architecture. The SDN-based network monitoring and control mechanism allow companies to control and configure their defense mechanisms in the cloud effectively without affecting other cloud users. We also carried out a simulation study using real network traces to evaluate the performance. The results show that our proposed DaMask is successful in dealing with the new challenges raised. The SDN-based network management can rapidly adapt to the network topological changes.

In the first phase of research, we focused on the literature dedicated to SDN and the problem of DDoS attacks. This helped us to gain thorough understanding of the current state of the art in SDN and proposed future research by the SDN research community. It showed us that security in SDN is one of the crucial problems that must be dealt with before the deployment of SDN infrastructure into production networks. Even though we do not want to secure the SDN itself, it is important to describe all DDoS attack vectors emerging in SDN. Current DDoS attacks independent of used network infrastructure, that could be used in SDN environment were also in the focus of our research.

REFERENCES

1. Z. Xiao and Y. Xiao, “Security and Privacy in Cloud Computing,” IEEE Commun. Surveys & Tutorials , vol. 15, no. 2, 2013, pp. 843–59.
2. S. T. Zargar, J. Joshi, and D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Ser-vice (DDoS) Flooding Attacks,” IEEE Commun. Surveys & Tutorials , vol. 15, no. 4, 2013, pp. 2046–69.
3. W. Xia et al., “A Survey on Software-Defined Network-ing,” IEEE Commun. Surveys & Tutorials , 2014, to be published.
4. S. Scott-Hayward, G. O’Callaghan, and S. Sezer, “SDN Security: A Survey,” Proc. IEEE SDN for Future Networks and Services (SDN4FNS) , 2013, pp. 1–7.
5. R. Shea and J. Liu, “Performance of Virtual Machines under Networked Denial of Service Attacks: Experi-ments and Analysis,” IEEE Systems J. , vol. 7, no. 2,2013, pp. 335–45.
6. S. Sezer et al., “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks,” IEEE Com-mun. Mag. , vol. 51, no. 7, 2013.
7. A. TaheriMonfared and C. Rong, “Multi-Tenant Network Monitoring Based on Software Defined Networking,” Proc. OTM Conf. Move to Meaningful Internet Systems, 2013.

8. C.-J. Chung et al., "Nice: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," IEEE Trans. Dependable and Secure Computing , vol. 10, no. 4, July 2013, pp. 198–211.
9. R. Jin and B. Wang, "Malware Detection for Mobile Devices Using Software-Defined Networking," Proc. IEEE 2nd GENI on Research and Educational Experiment Wksp. (GREE), 2013, pp. 81–88.
10. Y. Yu, Q. Chen, and X. Li, "Distributed Collaborative Monitoring in Software Defined Networks," arXiv preprint arXiv:1403.8008, 2014.17
11. S. Shin and G. Gu, "Attacking Software-Defined Net-works: A First Feasibility Study," Proc. 2nd ACM SIGCOMM Wksp. Hot Topics Software Defined Networking, 2013, pp. 165–66.
12. P. Porras et al., "A Security Enforcement Kernel for OpenFlow Networks," Proc. 1st Wksp. Hot Topics in Software Defined Networks, 2012, pp. 121–126.
13. D. Kreutz, F. Ramos, and P. Verissimo, "Towards Secure and Dependable Software-Defined Networks," Proc. 2nd ACM SIGCOMM Wksp. Hot Topics in Soft-ware Defined Networking, 2013, pp. 55–60.
14. B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Network-ing: Past, Present, and Future of Programmable Net-works," IEEE Commun. Surveys & Tutorials, vol. 16, no. 3, Third Quarter 2014, pp. 1617–34.

