IJCTA, 10(03), 2017, pp. 39-47

SDN Based DDoS Attack Detection and Mitigation in Cloud

Sindia* and Julia Punitha Malar Dhas**

Abstract : Cloud computing has almost swept the IT industry replacing the enterprises' traditional computing. With the recent developments in cloud computing has also grown the threats to the security of cloud services and data. Amongst the many security issues, DDoS has its way in threatening the availability of the services provided by the cloud to the intended users. To detect and mitigate these attacks, a classifier algorithm and a forecasting algorithm are used respectively. With these algorithms deployed in SDN architecture, we can greatly reduce the DDoS attacks in the cloud thereby providing the cloud users uninterrupted services.

Keywords : Cloud storage, DDoS attacks, availability, SDN, classifier algorithm, forecasting algorithm.

1. INTRODUCTION

Cloud computing is an emerging technology now widely being adapted by companies and organizations which helps them to reduce operating costs while increasing efficiency. Eventhough used by many, still security needs to be focused on to make the tenants to use the resources free of threats and attacks to the data stored in the cloud.

Cloud computing is fast replacing the traditional way of computing and storage of data. What hinders the even faster migration is the security issues in the cloud. Threats to the security of data in cloud has been almost addressed. Yet newer, more efficient solutions are evolved day by day.

Low-cost, pay-by-use models can be used to deploy and scale services and benefits in cloud computing. Meanwhile the users who use the services can also enjoy the flexibility provided by the Internet based computing. Users enjoy the on demand provisioning of computing, storage and networking resources according to a pay-per-use business model. Most of the enterprises embrace the paradigm of cloud computing by moving their database and their applications into the cloud.

In the recent years, cloud computing has become a widely accepted computing paradigm built around core concepts such as on-demand computing resources, elastic scaling, elimination of up-front investment, reduction of operational expenses and establishing a pay-per use business model for information technology and computing services. Cloud computing makes it possible for content providers to quickly deploy and scale services and benefit from low-cost, pay-by-use models, while service users enjoy the flexibility that Internet-based computing provides. Cloud computing enables users to benefit from on demand provisioning of compute, storage and networking resources according to a pay-per use business model[10][8].

Resources can be shared from the pool of resources in cloud computing. Cloud computing aims to cut down costs while resources are used as needed. Cloud computing adopts concepts from the service oriented architecture. This helps the user to break the problems into services that can be integrated to provide a solution. The advantages of the cloud computing are: agility, cost reductions, device and

* Department of Information Technology, Noorul Islam University, Kumaracoil, Tamilnadu, India. *E-mail : sindiatv@gmail.com*

** Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, Tamilnadu, India. *E-mail: julaps113@yahoo.com*

location independence, easy maintenance, multitenancy, increased productivity, reliability, scalability and elasticity. As per NIST's definition, the five characteristics of the cloud are: on demand self service, broad network access, resource pooling, rapid elasticity, measured service.

There are three service models in cloud. They are SaaS, PaaS and IaaS. SaaS stands for Software as a Service. The consumer can use the provider's application running on a cloud infrastructure. IaaS stands for Infrastructure as a Service. In IaaS the user is abstracted from the infrastructure like physical computing resources, location, data partitioning, scaling, security etc. PaaS stands for Platform as a Service. In this model cloud providers deliver a computing platform typically including OS, programming language execution environment, database and web server.

Cloud storage has become a faster profit growth point by providing a low cost, scalable, position independent platform for clients' data. It enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. The risk faced by the organization in using the cloud is the security of data that is outsourced. Therefore secure and efficient data exchange across the enterprise and clouds, as well as secure application connectivity becomes the major security concerns.

Cloud computing provides enormous benefits including on-demand, elastic and pay-as-you-go based accessible computing. Amidst all these benefits presented to the user, there are a lot concerning about security and privacy issues in the cloud. The prevalence of cloud computing is blocked by its security to a great extent. When data is stored in cloud, the risk of data being safe is higher as it is prone to many accesses.

DDoS is the acronym for Distributed Denial of Service. It is an attack to make the online services unavailable by overwhelming it with traffic from multiple resources. In this attack, usually Trojan infected multiple systems are used to target a single system which provides service so that the service is denied to the legitimate users.

Distributed Denial of Service (DDoS) attacks are launched with the intent of negatively impacting the availability of the targeted applications, data or services. With explicit multitenant environment, an attack against one tenant or customer is an attack against all end customers making use of the same shared infrastructure.

Both the end targeted system and the systems that are maliciously used and controlled by the hacker in a distributed manner are the victims of the DDoS attack. DDoS attacks are the ones which threatens the availability of cloud services. DDoS attacks are detected, mitigated and avoided to make sure that the services are always available to the customers.

DDoS attack is a major threat since cloud is a resource pool wherein the resources are shared at host level, browser level, network level and server level. It is an attempt to make a service unavailable to its intended user by draining the system or network resources. Many compromised systems are used to send malicious traffic to the target server so that the server would process the malicious traffic instead of servicing the requests from the users. The two main objectives of the DDoS attacks are to overwhelm the server resources and then to hide the identity of the hackers. These attacks affect the organizations costing them more time and money.

By exploiting the flaws or vulnerabilities in a computer system, a malicious hacker is able to perform DDoS attack. In such case, a web site or a web server is posed as a master system. Further compromise can be done by the hacker after identifying and communicating with other systems when posed as the master system.

The taxonomy[5] of the contributions made in the area of DDoS attacks in cloud is divided into three parts: attack prevention, attack detection, attack mitigation and recovery. Prevention of DDoS attacks is done as a proactive measure. Here the suspected attacker's requests are filtered or dropped before they affect the server. Attack detection is finding that an attack is occurred. Mitigation is a stage which enables the network to continue its services amidst the presence of attacks.

When the hacker has control of multiple compromised systems, he can instruct the machines to launch one among the many flood attacks which floods the targeted system which targets the system with bogus traffic requests causing a denial of service for users of the system. This flood of incoming messages from the compromised systems will make the targeted system to shut down making it impossible for the genuine users to use the services provided. Therefore, time and money of the organization will be wasted.

The important features of cloud computing that are affected by DDoS attacks are discussed in section 2. Section 3 introduces SDN and SDN's role in DDoS attack mitigation. The system for DDoS attack detection and mitigation is discussed in section 4. Performance evaluation is done in section 5 and finally conclusions are drawn.

2. FEATURES OF CLOUD COMPUTING AFFECTED BY DDOS ATTACKS

The pay-as-you-go model of the cloud computing has been exploited by DDoS attacks. The features that are the success factors of cloud computing are also helpful to DDoS attackers in getting their attacks successful. They are auto scaling, pay-as-you-go accounting and multitenancy[5].

Scalability in cloud computing has been a boon to the IT industry. Cloud infrastructure is capable of auto scaling. Resources can be expanded or shrinked with hardware virtualization. Additional resources can be added when necessary and they can be removed as and when they are of no need. This can be made automatic in which cloud consumers are allowed to automatically increase the resources on the basis of utilization or requirement. This scaling can be done horizontally over the data center or the cloud level, or vertically over the machines.

Resources can be consumed from the providers or the third party vendors on a pay per use basis. This allows the customers to utilize the resources without the need of buying them. They can make use of the resources until they need, pay the bill for the resource they use. They need not worry about the power, space and cooling arrangements.

Cloud computing provides excellent features to consumers which are also useful for DDoS attackers. Fake requests can be sent to victim server to achieve DDoS. This would result in heavy resource utilization on the victim server. The auto scaling property of cloud takes these fake requests as input and adds more and more resources. Ultimately there are resources extra to our necessity and these extra resources will also be billed. Thereby there is a heavy economic loss. This will continue till the service provider is able to pay or cloud service provider consumes all the resources. At the end it leads to denial of service.

DDoS attacks targeted towards cloud platforms are quite similar to the attacks on fixed infrastructures. The attack consequences in cloud are not limited to the victim VM and its resources.

The Effective Resource Allocation Time is the time difference between two events, the first being when the VM gets overloaded and the second event is when the cloud resource allocation algorithm diagnoses the utilization and allocates new resources and new resources become active. During this period of Effective Resource Allocation Time, the service may become unavailable or there may be large response times and even request timeouts.

3. SDN IN DDOS MITIGATION

To make the network management easier, an Internet architecture has come which is known as the Software Defined Networking. SDN stands for Software Defined Networking. In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized and the underlying network infrastructure is abstracted from the applications. The three main functional layers of SDN are the infrastructure layer, the control layer and the data layer. The good features of SDN are offering benefits for defeating DDoS attacks. They are: separation of the control plane from the data plane, a centralized controller and view of the network, programmability of the network by external applications, software based traffic analysis and dynamic updating of forwarding rules and flow abstractions [10].

There are many good features in SDN which are benefits for defeating DDoS attacks. Separation of control plane from the data plane enables to establish large scale attack and defense experiments easily. A logical centralized controller and view of the network helps to build consistent security policy. The programmability of the network by external applications supports a process of harvesting intelligence from existing IDSs and IPSs. The software based traffic analysis improves the capabilities of a switch using any software based technique. The dynamic updating of forwarding rules and flow abstraction helps to respond promptly.

The two important concepts of SDN are control plane abstraction and network function virtualization. The properties introduced by these concepts are centralized network control, simplified packet forward, software based network function implementation, virtualized networks.

SDN holds great promise in terms of mitigating DDoS attacks in cloud computing environments. The security of SDN itself remains to be addressed. Unauthorized access, data leakage, malicious applications, configuration issues are the security issues in SDN.

SDN is a network architecture that decouples the control plane and the data plane of network switches and moves the control plane to a centralized application called network controller. The network controller is in charge of the entire network through a vendor independent interface such as OpenFlow[10], which defines the low level packet forwarding behaviors in the data plane. Developers then can program the network from a higher level without concerning the lower level detail of packet processing and forwarding in physical devices.

SDN influences DDoS attack defense in negative ways when designing a DDoS attack defense solution in SDN, one must take the computation and communication overhead into consideration so that no new security vulnerability is introduced[9].

Based on this, we need to incorporate the DDoS attack defense into cloud computing and SDN. To address the challenges in the new network environment, the solution must be effective and should incur small overhead. The design should be effective in the sense that it is able to protect the services and has the ability to adapt to the network topology changes and mitigate DDoS attacks efficiently. The communication and computation overhead should be small. It is also important to see that the cost of deployment is not too expensive. To make the solution effective the enterprise’s network traffic from the main network can be separated by virtualizing the network. To reduce the communication and computation overhead, an efficient attack detection algorithm should be selected.

A DDoS attack mitigation technique is also proposed which can be included in the SDN architecture. SDN can be exploited to address the cloud computing security challenges and the DDoS attack defense can be made more efficient with proper design.

4. DDOS ATTACK DETECTION AND MITIGATION

A new system for DDoS attack detection and mitigation is proposed. The three layers in the system are: network switches, network controller, network applications. The workflow of the system is given in Fig.1.

The packets arriving in the network is forwarded to the network switch and it is checked if the flow is a new one or not. If the packet is a new flow then it is subjected to classification. To know whether the packet is a normal packet or an attack, this classification is done. The algorithm used for this classification is normally called as classifier algorithm. There are many classifier algorithms namely linear classifiers, support vector machines, quadratic classifiers, kernel estimation, meta-algorithm etc.

The forwarded flow is now forwarded to the network controller. Here it is made to undergo classification. Classification is the problem of identifying to which of a set of categories a new observation belongs, on the basis of a training set of data containing observations or instances whose category membership is known.

As an instance of supervised learning, we are applying the Support Vector Machines (SVM) to classify the packets. In SVM when training data are given, the algorithm outputs an optimal hyperplane in which new examples are categorized. SVM can do both linear and non-linear classification. Non-linear classification is done by using kernel trick.

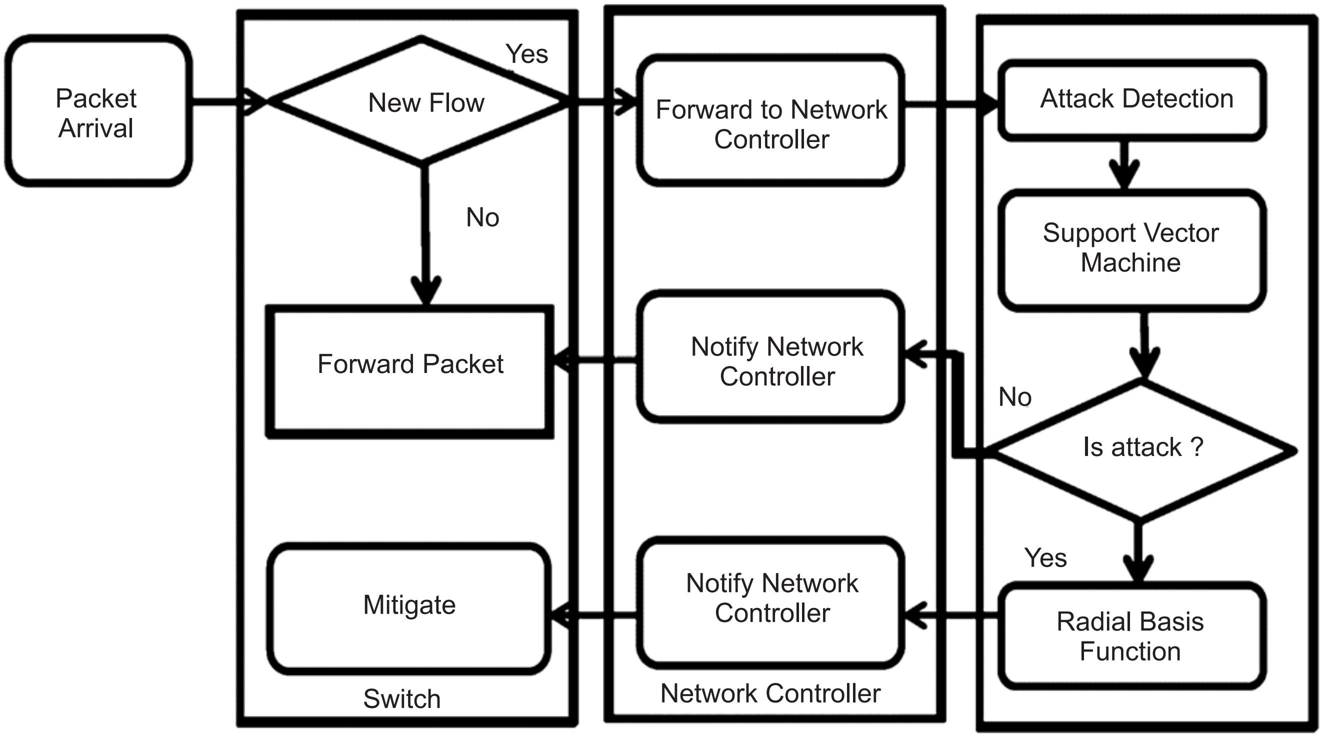

Figure 1: Workflow of the DDoS attack detection and mitigation system

$$k(\vec{x}_i, \vec{x}_j) = \varphi(\vec{x}_i) \cdot \varphi(\vec{x}_j)$$

Where k corresponds to the given kernel function. Kernel trick is applied to maximum margin hyperplanes. This is similar to linear classification except that every dot product is replaced by a non-linear kernel function. The common kernels are polynomial for homogeneous and heterogeneous, guassian radial basis function and hyperbolic tangent. Fig. 2 shows the flow of DDoS attack detection phase.

Attacks are detected using the classifier algorithm. After this the attack needs to be mitigated. Once we identify that there is an attack, we have to take measures to counter it. To reduce its effects on our resources and the services, mitigation needs to be performed. If the packets arriving are found to be normal flow packets, then they are forwarded to the network without any further processing.

SVM can categorize the DDoS attacks too. There are many kinds of DDoS attacks such as SYN floods, UDP floods, ICMP floods, ping of death, smurf attack, HDoS, XDoS. In our classification algorithm, we identify HDoS and XDoS attacks.

Once the system detects that there is an attack, immediately the next action is to mitigate its effects. To mitigate the DDoS attacks, a forecasting algorithm is used. Forecasting algorithms are mainly used for prediction. In this case, the main aim is not to predict, but to control the system. Based on the training given to the data, the parameters values can be kept in control so that the DDoS attacks are not exploiting the cloud resources. For this we have to alter the parameter values. This is done in the mitigation phase by applying RBF algorithm.

Radial basis function network uses radial basis function as activation functions. The output of the network is a linear combination of radial basis functions of inputs and neuron parameters. Radial basis function networks have many uses including function approximation, time series prediction, classification and system control.

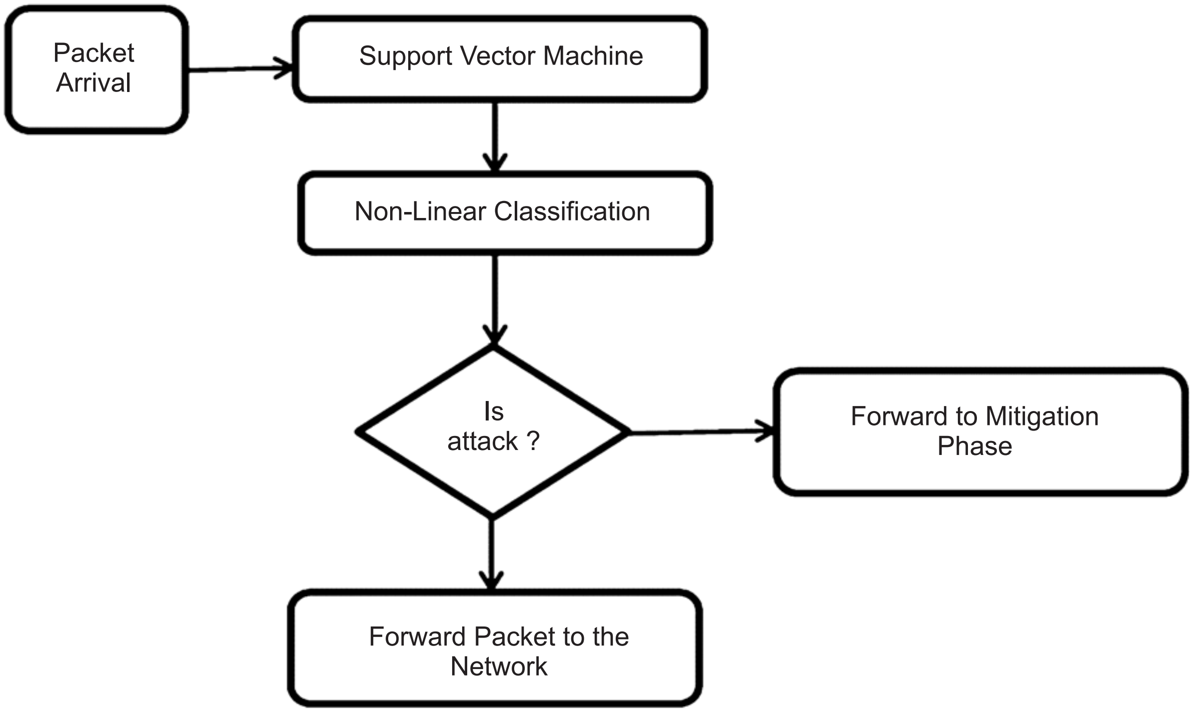
Packet Arrival
Support Vector Machine
Non-Linear Classification
Is attack ?
Forward to Mitigation Phase
Forward Packet to the Network

Figure 2: DDoS attack detection phase

The Radial Basis Function algorithm is used in the control of DDoS attacks. We are providing a set of data samples called training set for which the network outputs are known. This is a supervised learning method. In this case of mitigation, the network parameters are minimized to a certain level so that the attack packets are converted to normal packets.

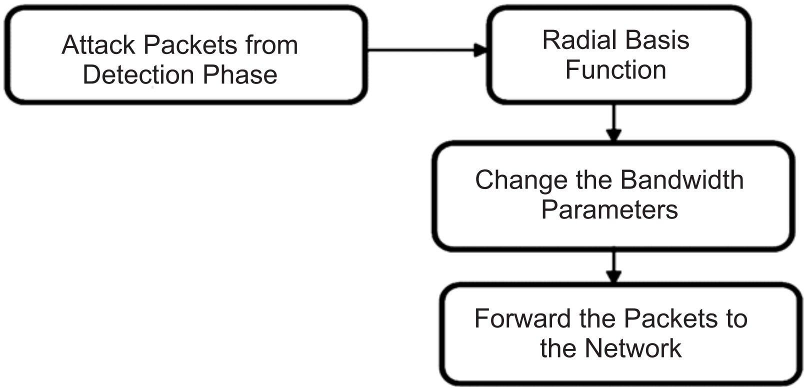
Attack Packets from Detection Phase
Radial Basis Function
Change the Bandwidth Parameters
Forward the Packets to the Network

Figure 3: DDoS attack mitigation phase

$$\min \sum_{i=1}^{Q} (Y_k(X_i) - F_k(X_i))^T \, (Y_k(X_i) - F_k(X_i))$$

The above equation is the minimization function. Here Q is the total number of vectors from a training set, $Y_k(X_i)$ denotes the RBF output vector and $F_k(X_i)$ represents the output vector associated with the data sample X_i from the training set. This minimizes the network parameters such as the bandwidth, mips of the packets arriving in the network as attack. By this mitigation of DDoS attacks is done and the cloud users are saved from denial of services. The flow of the DDoS mitigation phase is shown in Fig. 3.

In the mitigation phase, the attack packets from the network controller are taken as inputs and then the radial basis function is applied to these packets. The bandwidth parameters are changed so that the packets can be further trusted not to create attacks in the network. Once the parameters are changed, there is no panic for attack. The packets will behave as normal packets.

5. PERFORMANCE EVALUATION

The classifier algorithm used for classifying if the packet arriving in the network is an attack or not is found to be efficient in means of computation overhead. The other algorithms which are used for this purpose are found to be having high computational overhead. True positive rate deals with the probability of detection of attacks and measures the proportion of positives that are correctly identified as such. The false positive rate is the proportion of all negatives that still yield positive test outcomes.

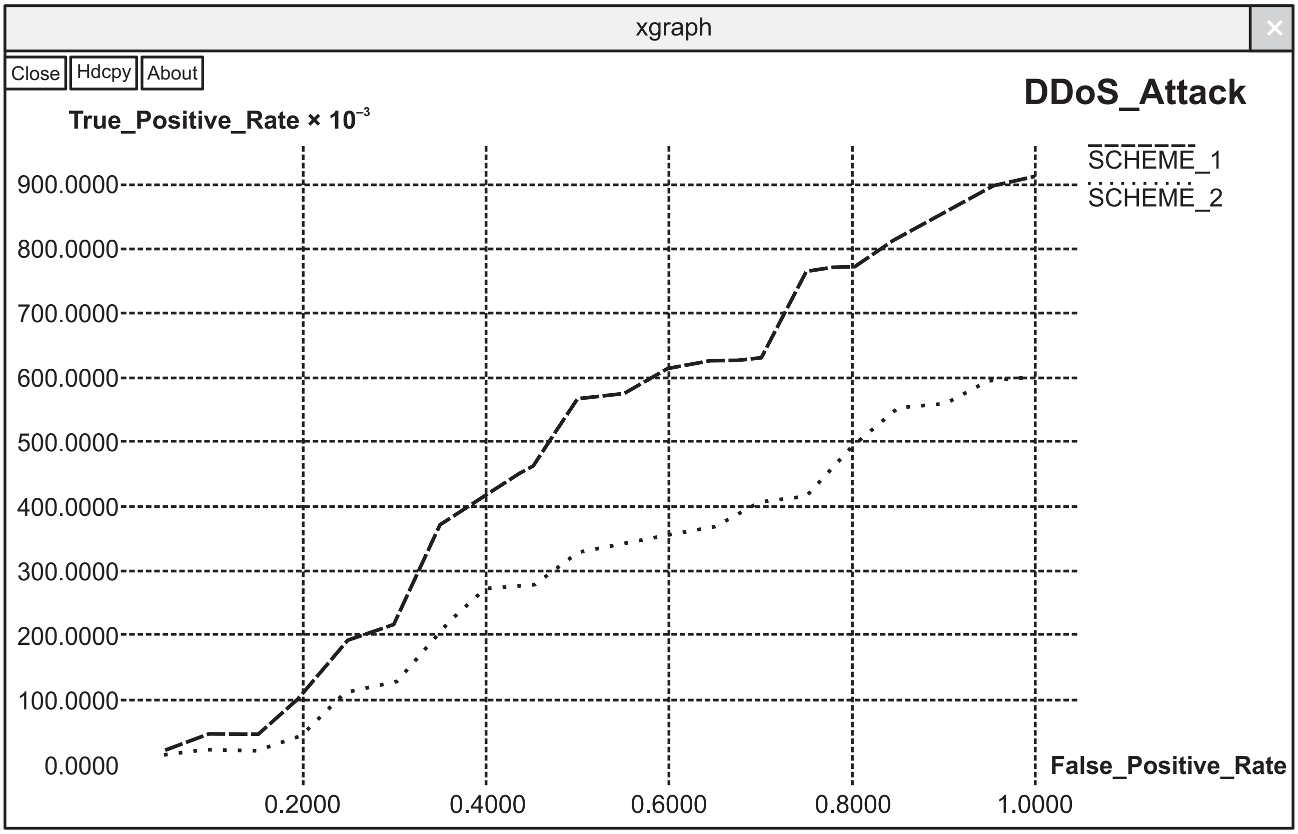

Figure 4: SVM *vs* K-Means algorithm in DDoS attack detection

The graph above shows the performance of two algorithms. Scheme 1 is the performance of K-Means algorithm and scheme 2 is that of support vector machine. The support vector machine is better than the former algorithm. In terms of the computation overhead, the algorithm we use for classification is found to be better than other algorithms.

6. CONCLUSION

Cloud computing has already taken its stand in the IT industry. To make the services even more uninterruptable, certain security measures have to be taken. DDoS attacks concentrate on availability of services and resources. They are still an effective tool for cyber criminals to shut down individual cloud customers. To detect DDoS attacks, support vector machines prove to be a good approach and to mitigate the DDoS attacks another algorithm called as Radial Basis Function algorithm is used. Radial Basis Function algorithm is efficient enough to make the packets like those of normal flow thereby avoiding the effects of the DDoS attacks in the cloud and making the cloud resources and services always available to the end customers.

7. REFERENCES

1. Hakem Beitollahi and Geert Deconinck, A Four-Step Technique for Tackling DDoS Attacks, The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT-2012) Procedia Computer Science 10 (2012) 507 – 516

2. Nagarajukilari, Dr. R. Sridaran, An Overview of DDoS Attacks in Cloud Environment, International Journal of Advanced Networking Applications (IJANA) ISSN No. : 0975-0290 124-127

3. Shui Yu, Song Guo, Can We Beat DDoS Attacks in Clouds?, IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014 2245-2254

4. Zhifeng Xiao and Yang Xiao, Security and Privacy in Cloud Computing, IEEE COMMUNICATIONS SURVEYS &TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013 843

5. GauravSomani,Manoj Singh Gaur, RajkumarBuyyaet.al.,"DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions,ACM Computing Surveys, Vol. 1, No. 1, Article 1, Dec 2015

6. UsmanTariqa1, YasirMalikb, BessamAbdulrazakbandManPyoHongc,Collaborative Peer to Peer Defense Mechanism for DDoS Attacks, The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science 5 (2011) 157–164.

7. Ping Du, Akihiro Nakao, DDoS Defense as a Network Service, IEEE/IFIP Network Operations and Management Symposium - NOMS 2010: Short Papers,894-897

8. UsmanTariqa1 , YasirMalikb, BessamAbdulrazakb, Defense and Monitoring Model for Distributed Denial of Service Attacks, The 2nd International Workshop on Internet of Ubiquitous and Pervasive Things (IUPT 2012) Procedia Computer Science 10 (2012) 1052 – 1056

9. Bing Wang, Yao Zheng, Wenjing Lou, Y. Thomas Hou,"DDoS attack protection in the era of cloud computing and Software-Defined Networking",Computer Networks 81 (2015) 308-319

10. Qiao Yan F, Richard Yu, QingXiang Gong and Jianquiang Li, "Software-Defined Networking and Distributed Denial of Service Attacks in Cloud Computing Environments: A survey, some research issues and challenges", IEEE Communications Surveys and Tutorials, 2015.

11. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, 39th IEEE International Conference on Parallel Processing Workshops, 2010, pp280-284.

12. Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi, Securing Cloud Computing Environment Against DDoS Attacks, IEEE International Conference on Computer Communication and Informatics, 2012.

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

14. E.Anitha, Dr.S.Malliga, A Packet Marking Approach to Protect Cloud Environment against DDoS Attacks, International Conference on Information Communication and Embedded Systems, 2013.

15. TarunKarnwal, T.Sivakumar, G.Aghila, A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack, IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012, vol-01, pp-9-12.

16. S. Renuka Devi and P. Yogesh, Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics, CS & IT-CSCP 2012, pp.217–223.

17. Solomon GuadieWorku , ChunxiangXu, Jining Zhao, Xiaohu He, Secure and efficient privacy-preserving public auditing scheme for cloud storage , Computers and Electrical Engineering 40 (2014) 1703–1713

18. Page, Scott. "CloudComputing-Availability." ACC.

19. Security and privacy for storage and computation in cloud computing, Lifei Wei a, Haojin Zhu a, Zhenfu Cao a, ⇑, Xiaolei Dong a, WeiweiJia a, Yunlu Chen a, Athanasios V. Vasilakos b, Elsevier,2013

20. Ari Juels, RSA Laboratories Cambridge, MA, USA, AlinaOprea, , RSA Laboratories Cambridge, MA, USA , New approaches to Security and Availability for Cloud Data,.

21. Kuyoro S. O., Ibikunle F. &Awodele O., Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

22. H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security Privacy,vol. 8, no. 6, Nov.–Dec. 2010

23. Cloud Security Alliance, Top threats to cloud computing V1.0,https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf(Retrieved 2012-09-22Last access 09/01/2013).

24. Yung-Wei Kao, Kuan-Ying Huang, Hui-Zhen Gu, Shyan-Ming Yuan, "uCloud: a user-centric key management scheme for cloud data protection", IET Inf. Secur., 2013, Vol. 7, Iss. 2, pp. 144–154

25. Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, GuangtaoXue, Minglu Li,“ Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing”, Computers and Security 42 (2014) 151-164

26. A Review of DOS Attacks in Cloud Computing,Vidhya.V, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. II (Sep – Oct. 2014), PP 32-35

27. T. Subbulakshmi; K. BalaKrishnan; S. Mercy Shalinie; D. AnandKumar; V. GanapathiSubramanian; K. Kannathal ,”Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset “,2011 Third International Conference on Advanced Computing Year: 2011 ,Pages: 17 – 22

28. P. K. Agrawal; B. B. Gupta; Satbir Jain,”SVM Based Scheme for Predicting Number of Zombies in a DDoS Attack “, Intelligence and Security Informatics Conference (EISIC), 2011 European Year: 2011, Pages: 178 - 182, DOI: 10.1109/EISIC.2011.19

29. A. Ramamoorthi; T. Subbulakshmi; S. Mercy Shalinie,”Real time detection and classification of DDoS attacks using enhanced SVM with string kernels “,Recent Trends in Information Technology (ICRTIT), 2011 International Conference on Year: 2011 Pages: 91 – 96

30. B. S. Kiruthika Devi; G. Preetha; G. Selvaram; S. Mercy Shalinie,”An impact analysis: Real time DDoS attack detection and mitigation using machine learning “,Recent Trends in Information Technology (ICRTIT), 2014 International Conference on Year: 2014 Pages: 1 – 7

31. Kokila RT; S. Thamarai Selvi; Kannan Govindarajan,”DDoS detection and analysis in SDN-based environment using support vector machine classifier “, Sixth International Conference on Advanced Computing (ICoAC) Year: 2014,Pages: 205 - 210.