International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Enhancing Cloud Security by analyzing venerability of cloud server In D-Dos Attack

Vilas R. Bodkhe
Department of Computer Science and Engineering
Wainganga College of Engineering & Management
(Approved by AICTE, DTE, Govt. of Maharashtra, Affiliated to RTM Nagpur University, Nagpur)

ABSTRACT

Now a day's more and more services and applications are emerging in the Internet, exposing sensitive electronic data in the internet has become easier. Web services cause's personal data to be cached, copied, and archived by third parties, often without our knowledge or control. To provide confidentiality and privacy is very important today to enterprises and other users to use cloud services. Cloud is becoming a dominant computing platform. Researchers have demonstrated that the essential issue of DDoS attack and defense is resource competition between defenders and attackers and maintain data venerability in the cloud. Major problem in clouds are load balancing and sharing the data to the particular user. In our project will propose a job scheduling and attribute base data sharing.

Keywords: *Cloud computing, DDoS attacks, mitigation, system modeling, resource investment.*

I. INTRODUCTION

The contributions of this paper are summarized as follows: We point out that DDoS attacks do threaten individual cloud customers. However, by taking advantage of the cloud platform, we can overcome DDoS attacks, which is difficult to achieve for non-cloud platforms. To the best of our knowledge, this paper is an early feasible work on defeating DDoS attacks in a cloud environment. We propose a dynamic resource allocation mechanism to automatically coordinate the available resources of a cloud to mitigate DDoS attacks on individual cloud customers. The proposed method benefits from the dynamic resource allocation feature of cloud platforms, and are easy to implement. We establish a queuing theory based model to estimate the resource allocation against various attack strengths. Real-world data set based analysis and experiments help us to conclude that it is possible to defeat DDoS attacks in a cloud environment with affordable costs.

Distributed Denial of Service attacker gain illegal access to some of the compromised system all over the world and use them synchronically to flood a particular target at the same instance of time. DDoS Attack traffic is less on the source node so it is not possible to detect it over there. Meanwhile the synchronize attack by multiple compromised system at the same instance of time is sufficient to make the target network overwhelmed and deny its service to their legitimate user.

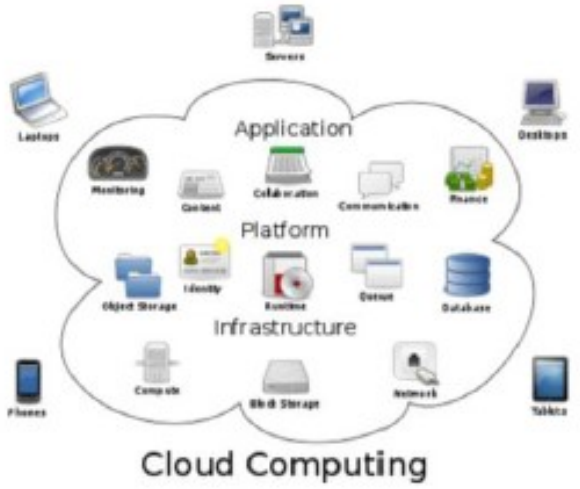


Fig. 1 Architecture of Cloud Computing

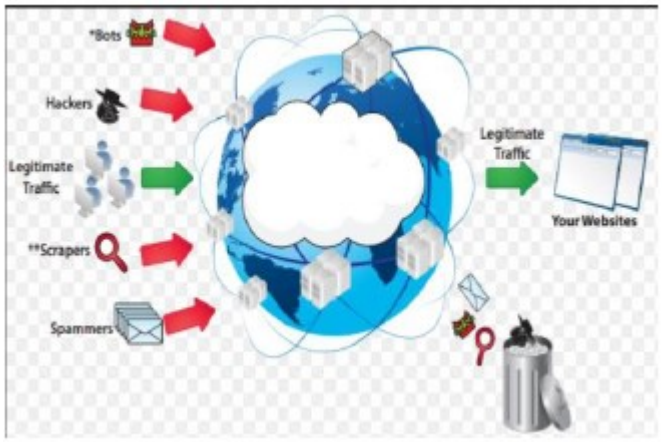


Fig. 2 DDoS attack on Cloud

II. DDOS ATTACK MITIGATION IN CLOUDS

In this section; we propose a mechanism to dynamically allocate extra resources to an individual cloud hosted server when it is under DDoS attack. First of all, we examine the features of a cloud hosted virtual server in a non-attack scenario. As shown in Fig. 1a, similar to an independent Internet based service, a cloud hosted service includes a server, an intrusion prevention system (IPS in the diagram), and a buffer for incoming The IPS is used to protect the specific server of the hosted service. All packets of benign users go through the queue, pass the IPS and are served by the server. In general, the number of benign users is stable, and we suppose the virtual IPS and virtual server have been allocated sufficient resources, and therefore the quality of service (QoS) is satisfactory to users. When a DDoS attack occurs against the hosted virtual server, a large number of attack packets are generated by botnets, and pumped to queue Q. In order to identify these attack packets and guarantee the QoS of benign users, we have to invest more resources to clone multiple IPSs to carry out the task. We propose to clone multiple parallel IPSs to achieve the goal as shown in Fig. 1b. The number of IPSs we need to achieve our goal depends on the volume of the attack packets. As discussed previously, the attack capability of a botnet is usually limited, and the required amount of resources to beat the attack is usually not very large. In general, it is reasonable to expect a cloud can manage its reserved or idle resources to meet demand.

II.1. Block Diagram

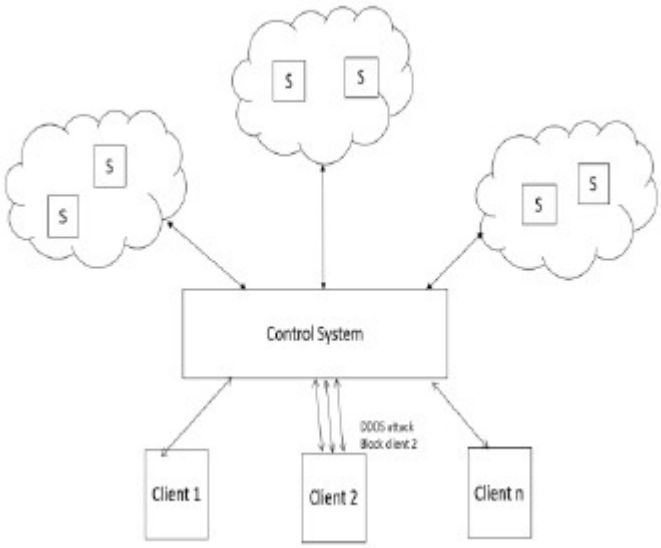


Fig. 3 Control System Architecture

Client requests for resources or services control system first performs the authentication after that load balancing algorithm will check for the available server then allocate free server to the client to serve the resources & services. If it is found that the requesting client is malicious user trying to do DDoS attack will be blocked by the control system for some duration. And if it is a legitimate user then control system will allocate the requested resources to the client.

II.2. Flow Chart DDoS Prevention

In above flow chart whenever client request for service it has to first authenticate from control system after authentication control system will check for the intrusion pattern if it has found it is a malicious user control system will block the user for some period of time. And if the requesting client is legitimate user then grant the request by allocating requested resources or services.

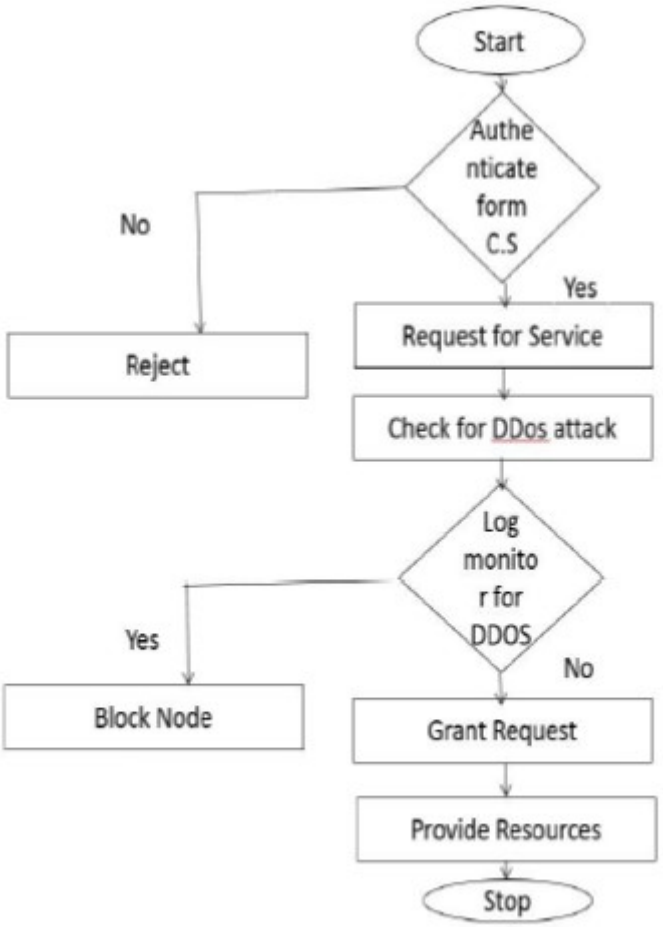


Fig. 4 DDoS attack prevention flow

III. SYSTEM MODELLING AND ANALYSIS

Main Objective of this project to create a scenario of cloud.

To detect intrusion patterns by inspecting the network packets.

To implement prevention mechanism for blocking the upcoming network packets from specific attacking system.

To maintain data integrity verification by keeping transaction log of the user.

To provide security over the data stored on cloud using cryptographic algorithm.

IV. DDOS MITIGATION ALGORITHM FOR A CLOUD

In this section, we present the related algorithm for the proposed mitigation strategy.

4.1DDoS Detection Methods

As aforementioned, DDoS defense in cloud essentially depends on resources no matter which defense methods we use. Therefore, in our mitigation algorithm, we do not involve specific detection methods, rather, we focus on the resource management aspect of detection. In the online supplementary file, we list a few DDoS detection methods that could be implemented in cloud for interested readers.

4.2 DDoS Mitigation Algorithm in Cloud

In the algorithm, we first observe the arrival patterns in nonattack cases for a protected server, and extract the parameters and Moreover, we also identify the resources for the current IPS, RIPS, and the available or idle resources Rc of the cloud. When a DDoS attack is detected by the original IPS, we then clone one IPS based on the image of the original IPS, and calculate the average time in system for the current status. If Taðt; mÞ 9 Tn, then we clone one more IPS for the filtering task. As the battle continues, and we find Taðt; mÞ G Taðt; m 1Þ, then it is time to reduce one IPS and release the resources back to the cloud available resource pool.

The details of the dynamic resource allocation algorithm against DDoS attacks on a cloud customer can be found from the online supplementary file of this paper.

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed dynamic resource allocation method for DDoS mitigation in a cloud from various perspectives. We first study the performance for nonattack scenarios, then investigate the performance of the proposed mitigation method against an ongoing DDoS attack, and then estimate the cost for the proposed mitigation methods. First of all, we summarize the key statistics of DDoS attacks in a global scenario from highly referred literature [6], [28], and present them in Table 1.

TABLE 1
Key Statistics of DDoS Attacks

Feature	Attack duration [28]	Attack rate [28]	Sources per attack session [6]
Value	5 minutes	500 requests/s	Around 1000

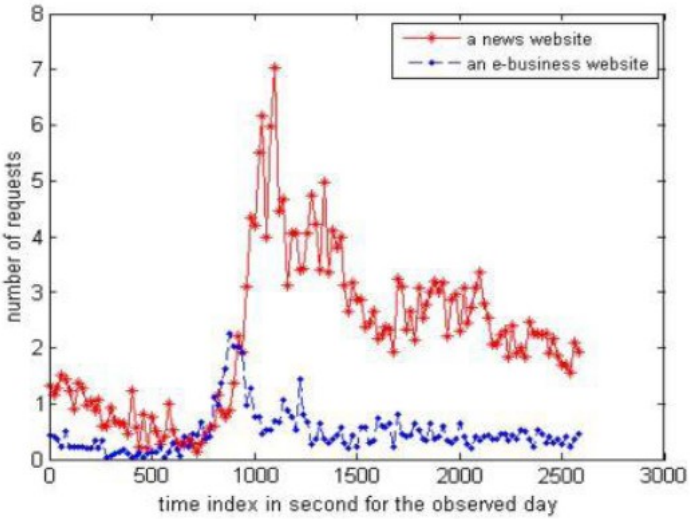
We use the Amazon EC2 as an example and show the related Data in Table 2

TABLE 2
Estimated Key Resources of Amazon EC2

Resource	Servers	Bandwidth
Value	500,000	1Gb/Instance

5.1 Observation

We prefer the busy rate as high as possible under the condition that the average time in system is acceptable.



Secondly, we studied the performance when a DDoS attack was ongoing. As previously discussed, we have multiple IPS servers in this case, and the model is M/M/m. For the system of multiple IPS servers, 0 is an important element, and is also involved in the calculation of other items. We expect a good understanding of 0 against the number of duplicated servers ðm) for a given busy rate. The experiment results are shown in Fig. 4. In contrast to 0, mþ is also important to us because it is a critical point where incoming packets have to wait for service, which is expressed in (16), and the experimental results are shown in Fig. 5. The results indicate that: 1) for a given number of duplicated IPS servers, the higher is, the less probability of packet queueing; 2) for a given , the probability of packet queueing decreases when there are more duplicated servers (this is intuitively straightforward). From this perspective, we obtain the following observation.

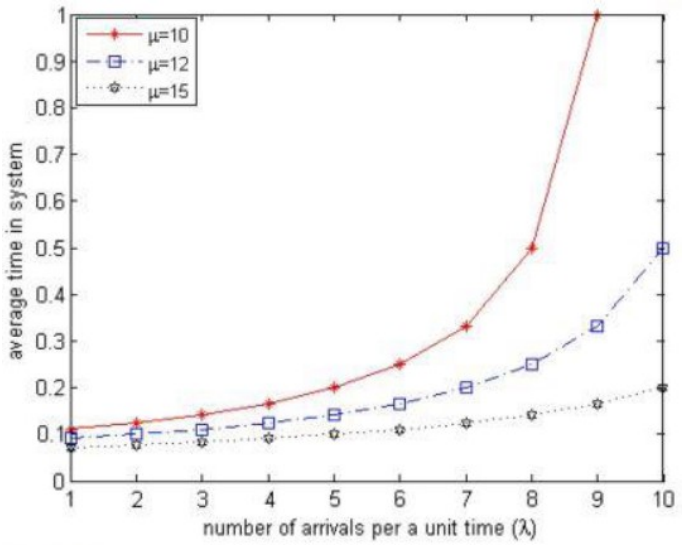


Fig. 3. Average time in system against arrival rate under different service rates for nonattack cases.

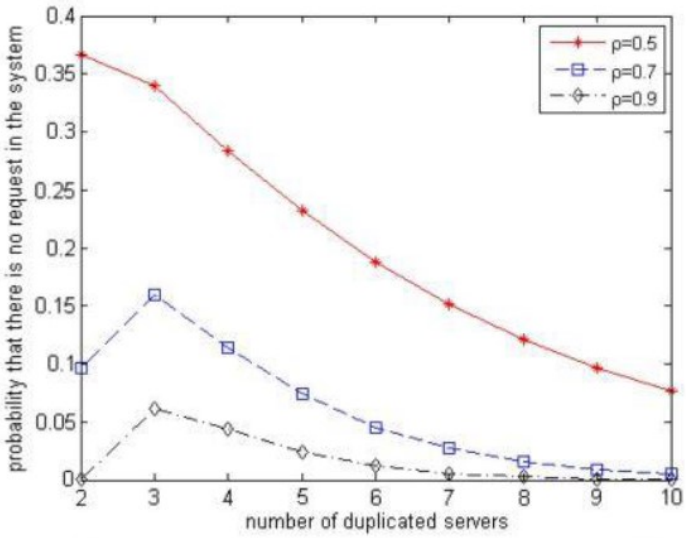


Fig. 4. Relationship between π_0 and the number of duplicated IPS servers for a given busy rate.

METHODOLOGY

➢ Control system detects intrusion patterns by inspecting the network packets. Implement prevention mechanism for blocking the upcoming network packets from attacking system.

➢ To maintain data integrity in cloud data storage owner of data will allocate attribute to the user with whom owner wants to share the data. After entering particular shared attribute users other than owner will get access to data.

➢ Provide security over the data stored on cloud using cryptographic algorithm. Whenever client stores data in cloud it will first encrypt it using

cryptographic algorithm then stores encrypted data on cloud.

➢ This section illustrates the prototype system implemented to elaborate the architecture, design and algorithms used in this model. The implementation of the prototype system and the performance testing and evaluation are explained.

SUMMARY

In this papers to detect DDoS attack they have used Intrusion detection system & to prevent attack by using different mechanisms like dynamic resource allocation, generate alert logs, using CAPTHA identify Techniques to optimize resources along with better performance, using potential loopholes in the migration algorithm to prevent the attack. Also to improve data integrity against unauthorized parties. Effective mechanism that provides data integrity verification without allowing third party to violate the privacy of data.

We establish a queueing theory based model for the proposed DDoS attack mitigation strategy in a cloud environment. We thoroughly analyze the proposed method. Extensive real-world data set based experiments and simulations confirm our claim that we can beat DDoS attacks on individual cloud hosted services with an affordable cost to cloud customers. As a rarely explored new area of research, there is plenty of work expected to be completed in the near future. As future work, we firstly attempt to improve the M/M/m model to a more general model, such as the M/G/m model. Secondly, we want to explore what should we do if a cloud data center runs out of resources during a battle. Thirdly, we would like to discover whether it is possible for attackers to rent the resources of a cloud to carry out their attacks on servers hosted by the same or other clouds. Finally, real cloud environment tests for the proposed method are expected in the near future.

ACKNOWLEDGMENT

Y. Tian is the corresponding author REFERENCES

The authors would like to acknowledge the University Teknologi Malaysia (UTM), Research Management Center (RMC) and K-Economy Research Alliance (RAKE) in supporting this study.

REFERENCES

1) Shui Yu, Yonghong Tian, Song Guo, and Dapeng Oliver Wu, Fellow,“Can We Beat DDoS Attacks in Clouds?”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014.

2) Aine MacDermott, Qi Shi, Madjid Merabti, and KashifKifiyat, “Considering an Elastic Scaling Model for Cloud Security”, International Conference for Internet Technology and Secured Transactions (ICITST-2013)

3) Yi Han, Jeffrey Chan, Tansu Alpcan, Christopher Leckie , ” Using Virtual Machine Allocation Policies to Defend against Co-resident Attacks in Cloud Computing”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 2015

4) Poonam Yadav, Sujata ,” Security Issues in Cloud ComputingSolution of DDOS and IntroducingTwo-Tier CAPTCHA” , International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013

5) Mohammed Faez Al-Jaberi and Anazida Zainal, “Data Integrity and Privacy Model in Cloud Computing”, 2014 International Symposium on Biometrics and Security Technologies (ISBAST).