Enhancing cloud security by analyzing vulnerability of cloud server in DDoS attack

Vilas R. Bodkhe
vilasbodkhe01@gmail.com
Wainganga College of Engineering and Management, Nagpur, Maharashtra

ABSTRACT

Nowadays more and more services and applications are emerging on the Internet, exposing sensitive electronic data on 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 vulnerability in the cloud. A major problem in clouds are load balancing and sharing the data with 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, intrusion, attribute sharing.

1. 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 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 systems 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 systems 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
In this section; we propose a mechanism to dynamically allocate extra resources to an individual cloud-hosted server when it is under a DDoS attack. First of all, we examine the features of a cloud-hosted virtual server in a non-attack scenario. As shown in Fig. 1. A 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 are 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 beginning 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.

2.1 Block Diagram

Client requests for resources or services control system first perform the authentication after that load balancing algorithm will check for the available server then allocate a free server to the client to serve the resources & services. If it is found that the requesting client is a 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 the control system will allocate the requested resources to the client.

2.2 Flow Chart D-DoS 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 a legitimate user then grant the request by allocating requested resources or services.
3. SYSTEM MODELLING AND ANALYSIS

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

To detect intrusion patterns by inspecting the network packets.
To implement prevention mechanism for blocking the upcoming network packets from the specific attacking system.
To maintain data integrity verification by keeping transaction log of the user.
To provide security over the data stored in the cloud using the cryptographic algorithm.

4. LITERATURE REVIEW

Some researchers proposed a system that dynamically allocates resources to attacking user called the malicious user to detect DDoS attacker from available cloud customers. When a DDoS attack happens, simply allocate the idle resource of the cloud to the victim in order to quickly sort out attack packets and assure the quality of the service for legitimate users simultaneously. This system needs to improve the M/M/m model to a general model, such as the M/G/m model. As well as we want to discover what should we do if a cloud data center runs out of resources during a DDoS attack [1]. When cyber-attacks and cyber interruptions happen, millions of users are affected & the associated security threats prevent this progression. Characteristics of our method and determining how an attack against the cloud’s infrastructure would affect performance. New algorithms optimized for detecting cloud attacks in an efficient manner are needed, and this is something we will explore further [2]. Some author proposed a system to allocate virtual machines to build side channels to extract private information from virtual machines on same servers [3]. Cloud computing is also suffering from some weaknesses like security & privacy, Internet Dependency, confidentiality, reliability, Availability, And Enterprise Applications Can’t Be Transferred Simply. Author concludes that security is the biggest hurdle in acceptance of cloud computing. Cloud service users are in fright of data loss, security, data reliability, and availability issues. The developed application needs to be much secure. Identify Techniques to enhance resources along with better performance. To reduce the disadvantage of cloud computing and work to provide excellent services to the cloud user in cost-effective manner [4]. Clients require their data to be safe and secure from any modifications or changes or unauthorized access to cloud computing. Various algorithms and protocols are applied by the various mechanisms of this archetypal to provide the maximum levels of integrity for data stored in public cloud for eg. Amazon S3. The major weakness of existing data integrity checking techniques is that they introduced privacy violation during integrity verification [5]. Some author discussed what is cloud computing and the part of cloud storages centers in cloud computing and describing the most important safety threat of cloud storages which is data integrity and data privacy or confidentiality, the proposed mechanisms for integrity assurance and the difficulties being faced in this mechanism. Security & privacy is a problem with rising security, the breaking points in security also occur. The mechanism author proposed can be implemented using much better encoding techniques so that the security rises more as well as data integrity enhances more [6]. Data protection & security is used to assure secure in communication, data storage, and data broadcast. Security of hypermedia data is an imperative issue because of fast analysis of digital data uses the permutation step of Data Encryption Standard (DES) algorithm. Theoretical study and experimental results prove that this method provides high speed of encryption as well as rarer exchanges or transfer over the unsecured network. Modified-AES algorithm is a fast and lightweight encryption cryptographic algorithm for the security of multimedia data [7].
5. PROPOSED SYSTEM

In our proposed system we are going to divide our implementation module into two main parts first is DDoS attack detection & prevention. Second is Applying data integrity on services provided like uploading & downloading Data from the server.

5.1 Intrusion Detection & Prevention Mechanism

The d-dos attack is detected by keeping log monitoring system. Below flowchart shows the DDoS detection & prevention. In flow chart shown in fig. 3 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 a legitimate user then grant the request by allocating requested resources or services. One more option for non-registered users is also available. Non-registered users can also upload or download data on the cloud is also provided in public upload and download section. And it is also possible that non-registered user can try to do a DDoS attack on the cloud. Then detected malicious user will also be blocked for some period of time & if it is a legitimate user then grant the request by allocating requested resources or services.

---

![Flowchart](image.png)

Fig.5. Intrusion Detection & Prevention Mechanism
5.2 Attribute Sharing

After detecting legitimate user from malicious user to enhance the data integrity whenever legitimate user request for the data stored on the cloud at the time of data storage owner of data will allocate attribute to the user with whom owner wants to share the data. So whenever users other than owner tries to access the shared data user has to enter the shared attribute to get the access after validation of attribute user can access the data. For further security, owner stores encrypted data on the cloud so that if an untrusted third party gets access to data will not be able to understand the stored data.

Proposed system to detect & prevent DDoS attack can be used by both registered & non-registered user. So there is the possibility of happening or performing a DDoS attack by any of the users like registered or non-registered. Now the question arises why there are two types of user like registered & non-registered? What is the difference between registered & non-registered user? So the difference is that registered user can share files with other registered users on cloud application this feature is not available to non-registered user. Verification code plays a very important role in the registered user profile as without verification no registered user can be able to use the services of the cloud application.

Whenever a user uploads data in cloud application whenever the user wants to download that uploaded file user has to enter the six-digit key which was shared with the user whenever user or client selects on download. So the key is nothing but one-time password which plays a very important part in upload & downloads service of the proposed system.

Now the question arises what is shared attribute? Whenever registered user shares data with other registered users on cloud application. User or client with whom data is shared will receive a six digits code with code chart as shown in fig. 5 below. User has to enter the initials of the corresponding digit. For example, as given in the figure below six digits code like 813115 users has to enter the corresponding initials like „NYSYYP”. This is how shared attribute works.
6. PERFORMANCE ANALYSIS

In this, we analyzed the performance of the proposed DDoS detection & prevention mechanism for DDoS mitigation in a cloud from varies approaches also analyzed the performance of Data integrity detection. Studies the performance of the existing proposed mechanisms likes to prevent the DDoS attack some researchers used idle server allocation or two tiers CAPTCHA just to differentiate between robots from normal users & some used virtual machine allocation. DDoS can be detected using following parameters like CPU cycles, memory cycles, bandwidth & money. We are mainly focusing on bandwidth attack detection where the attacker tries to target the cloud servers by flooding by consuming all their bandwidth so that no other user can use the services of cloud application

<table>
<thead>
<tr>
<th>COLOR CODE</th>
<th>NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED/orange</td>
<td>1</td>
</tr>
<tr>
<td>YELLOW/yellow</td>
<td>2</td>
</tr>
<tr>
<td>GREEN/green</td>
<td>3</td>
</tr>
<tr>
<td>VIOLET/violet</td>
<td>4</td>
</tr>
<tr>
<td>PURPLE/purple</td>
<td>5</td>
</tr>
<tr>
<td>BLUE</td>
<td>6</td>
</tr>
<tr>
<td>ORANGE/orange</td>
<td>7</td>
</tr>
<tr>
<td>NAVYBLUE/navyblue</td>
<td>8</td>
</tr>
<tr>
<td>WHIT</td>
<td>9</td>
</tr>
</tbody>
</table>

**Fig. 7 Performance Analysis of DDoS Attack Detection**

Considering graph shown in fig. 7, it shows the performance of DDoS attacker detected by using the proposed IDPS (Intrusion Detection & Prevention System) using following parameters like IP Address, host address, type of packet, time and counter to count a number of requests. If the user exceeds the counter limit will be blocked by the IDPS system tentatively. Technically we cannot block DDoS attacker because if the user is trying to open a website but the server is busy as the server is not available to fulfill the request asked by a legitimate user. In such cases, we cannot block a legitimate user from accessing services of a developed application. We developed the machine learning scheme where number of legitimate users” verses number of DDoS
detected user has been shown. Where no of legitimate users are more than a number of the DDoS attackers has been shown. For an example, if there total fifteen users out of which five has been detected as a DDoS attacker.

Analyzed the performance of Data Integrity Detection which is applied to the data uploaded on cloud application. Studied the presently proposed mechanisms like they just applied encryption algorithms to data in cloud-like DES, RSA, etc. In our proposed system we not only applied advanced encryption mechanism but also one-time password mechanism to the services provided by cloud application. Data Integrity can be detected using various parameters like a number of requests, buffer overflow & last but not the least file size. But we are concentrating mainly on a number of requests to access the services like upload & download data or file from a cloud application.

Fig. 8 Performance Analysis of Data Integrity Detection

Considering graph shown in fig. 8, it shows the performance of the Data integrity detection using the proposed mechanism using the following parameter like file type, number of words, file extension, file size, & number of characters in a file. Data integrity can be maintained, enhanced & detected only by using above mentioned parameters only. As we developed machine learning system where affected original file verses number of the file uploaded has been shown. If there are 11 file uploaded among them 3 can be spoofed, hacked or modified by a hacker or malicious user. This ratio is obtained by considering the above-mentioned parameters only.

Table 1 Comparative Analysis of Encryption Algorithms

<table>
<thead>
<tr>
<th>Parameters</th>
<th>M-AES</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>128, 192, 256</td>
<td>56 bits</td>
<td>1024 bits</td>
</tr>
<tr>
<td>Type of Algorithm</td>
<td>Symmetric</td>
<td>Symmetric</td>
<td>Asymmetric</td>
</tr>
<tr>
<td>Key Generation Time</td>
<td>Less</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Amount of Data</td>
<td>Large</td>
<td>Large</td>
<td>Small</td>
</tr>
<tr>
<td>Computation Time</td>
<td>Less</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Brute Force Attack</td>
<td>Not</td>
<td>Possible</td>
<td>Not Possible</td>
</tr>
</tbody>
</table>

Above table 1 shows the comparative analysis of Cryptographic Encryption Algorithm. We are comparing the existing encryption technique with the one we are implementing in our Data integrity proposed mechanism. Till date, DES & RSA encryption algorithms have been implemented. We are implementing M-AES in our proposed mechanism which takes 128, 192 & 256 bits key. Whereas DES uses 56 bits key & RSA takes 1024 bits key. Brute force attack is not possible on large bits key like the 256-bit key is large enough to avoid this of attack [7]. What exactly brute force attack is a Brute force is a trial and error method to decode encrypted data like passwords or Data Encryption Standard (DES) keys, AES keys & RSA keys through obsessive effort (using brute force).

M-AES & DES are symmetric key algorithm & RSA is an asymmetric key algorithm. Now the question arises what is the difference between symmetric & asymmetric key algorithm. The technically symmetric key algorithm uses the same key at the time of encryption & decryption of data. Whereas asymmetric key algorithm uses different keys at the time of encryption & decryption of data. M-AES takes less time to generate a key as compared to RSA & takes more time as compared to DES encryption algorithm. Whereas DES takes less time to generate a key as compared to both the encryption algorithm M-AES & RSA. And RSA takes more time to generate a key as compared to both algorithms DES & M-AES.
M-AES & DES can be applied on a large amount of data whereas RSA is applied on a small amount of data. M-AES & DES takes less time to compute as compared to RSA encryption algorithm. Proposed mechanism uses 256 bits key to avoid brute force attack as well as it takes less computation time & can be applied on a large number of data & also takes less key generation time as compared to RSA where RSA can be applied on a small amount of data. And we cannot predict how much data user can upload to our cloud application. So we can conclude that M-AES is the best option as compared to existing mechanisms used.

7. CONCLUSION AND FUTURE WORK

In this paper, we discussed the DDoS attack prevention mechanism which is associated with Data Integrity of the data uploaded to our cloud application. DDoS prevention & Data Integrity maintenance is combined for the first time ever. Why are we combining DDoS with data integrity together? As per our research, we are providing services like upload data on cloud & download data form cloud. As data is involved it should be secured on the cloud to maintain confidentiality & reliability of data we are appending Data Integrity to DDoS.

Also used One Time Password concept for downloading of self-uploaded data from the cloud as well as shared attribute concept which is explained above is used for shared data with

8. REFERENCES