**A CLOUD ENVIRONMENT BASED ON CONTAINERS EXAMINING NEW TECHNIQUES TO PREVENT LOW RATE DDOS ATTACKS**

**ABSTRACT**:

DDoS attacks are rampant in cloud environments and continually evolve into more sophisticated and intelligent modalities, such as low-rate DDoS attacks. But meanwhile, the cloud environment is also developing in constant. Now container technology and microservice architecture are widely applied in cloud environment and compose container-based cloud environment. Comparing with traditional cloud environments, the container-based cloud environment is more lightweight in virtualization and more flexible in scaling service. Naturally, a question that arises is whether these new features of container-based cloud environment will bring new possibilities to defeat DDoS attacks. In this paper, we establish a mathematical model based on queueing theory to analyze the strengths and weaknesses of the container-based cloud environment in defeating low-rate DDoS attack. Based on this, we propose a dynamic DDoS mitigation strategy, which can dynamically regulate the number of container instances serving for different users and coordinate the resource allocation for these instances to maximize the quality of service. And extensive simulations and testbed-based experiments demonstrate our strategy can make the limited system resources be utilized sufficiently to maintain the quality of service acceptable and defeat DDoS attack effectively in the container-based cloud environment.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * DDoS attacks are rampant in cloud environments and continually evolve into more sophisticated and intelligent modalities, such as low-rate DDoS attacks. But meanwhile, the cloud environment is also developing in constant. * Now container technology and microservice architecture are widely applied in cloud environment and compose container-based cloud environment. Comparing with traditional cloud environments, the container-based cloud environment is more lightweight in virtualization and more flexible in scaling service. Naturally, a question that arises is whether these new features of container-based cloud environment will bring new possibilities to defeat DDoS attacks. | * In this paper, we establish a mathematical model based on queueing theory to analyze the strengths and weaknesses of the container-based cloud environment in defeating low-rate DDoS attack. Based on this, we propose a dynamic DDoS mitigation strategy, which can dynamically regulate the number of container instances serving for different users and coordinate the resource allocation for these instances to maximize the quality of service. * And extensive simulations and testbed-based experiments demonstrate our strategy can make the limited system resources be utilized sufficiently to maintain the quality of service acceptable and defeat DDoS attack effectively in the container-based cloud environment. |
| **EXISTING ALGORITHM:-**  DDoS attack | **PROPOSED ALGORITHM:-**  Container Technology |
| **ALGORITHM DEFINITION:-**  The main aim of DDoS attacks is exhausting the resources of victims, such as networking resources or computing resources. When DDoS attacks spreading to cloud environment, a series of solutions have been proposed to defeat them based on the features of cloud environment. Explored an idea using abundant resources in cloud environment to defense DDoS attacks. And Yu et al. Proposed a dynamic resources allocation strategy based on queueing theory to mitigate the DDoS attacks with idle resources in cloud environment. Due to the resources are not free in cloud environment, the DDoS attacks gradually evolved into EDoS attacks that aim to the economic resources of victims. For the EDoS attacks. | **ALGORITHM DEFINITION:-**  As the OS-level virtualization technology, container presents an alternative to the VM in cloud environment. Unlike VMs running the whole OS on virtual device, containers share kernel with the host system and support minimum runtime requirements of the application. Due to the difference in the level of virtualization between VM and container, containers depend more on kernel features such as namespace and control groups (cgroups) to achieve isolation and resource control instead of requiring hypervisors. With the namespace, processes in a container are isolated from other containers and host system. Moreover, cgroups use scheduler features in the kernel to control the amount and priority of resources usage for each container. Therefore, combining with these kernel features can achieve the fine-grained runtime isolation and resources control to containers. |
| **DRAWBACKS:-**   * Networking resources or computing resources. * resources are not free in cloud environment | **ADVANTAGES:-**   * View and sharing. * Dividing. * Extract valuable information. |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE

**System Architecture.**

