Vulnerable Paths Assessment in Cloud for DDoS Attacks

TREO Talk Paper

Manas Tripathi  
Indian Institute of Management, Rohtak, India  
manas.tripathi@iimrohtak.ac.in

Arunabha Mukhopadhyay  
Indian Institute of Management, Lucknow, India  
arunabha@iiml.ac.in

Abstract

Cloud computing is a subscription-based technology which provides services to its users on demand basis. Companies are migrating towards cloud at a fast pace because it is based on ‘pay-as-you-go’ model. In cloud computing, resource management and maintenance are done by the Cloud Service Provider (CSP), and users can access these services from anywhere at any time through the internet. Unfortunately, with all these benefits, cloud computing is also prone to various security threats. These threats are related to compromise of confidentiality, integrity, and authentication (C-I-A). This, in turn, impacts the trustworthiness of the CSP. Distributed Denial of Service (DDoS) attacks can adversely impact the availability of a cloud computing service. DDoS floods the CSP with illegitimate traffic which may lead to congestion of its critical resources. Organizations may lose millions of dollars due to unavailability of services at the required time which may even force them to churn away to other CSPs. This will adversely affect the reputation of that CSP.

DDoS attacks increase congestion in the network which in turn increase the network packet travel time (latency). Amazon has noted the cost of network latency and its direct consequences on business. They have found that there is a drop of 1% in their sales for every 100 milliseconds (MS) of latency. Google has found that there is 20% drop in traffic if end-user faces 0.5 seconds extra time for searching a webpage. It is clear from the above facts that low latency is an essential element for success in business. Organizations these days have started prioritizing the low latency in network. To evaluate the cost of network latency, we can take the example of Amazon. The sales figure for this tech giant was around $89 billion in 2014. If for an example, Amazon faces 100 MS of latency in their transactions. 100 MS of latency would cost them to 1% drop in sales which is equivalent to staggering $889 million.

An important step for protecting the CSP’s resources from these DDoS attacks is to detect the source or path of the malicious traffic. But the attacker usually masks the source information or uses multiple sources. Researchers have tried to find solutions for the DDoS problem using computer science based algorithm approach. These approaches require high memory consumption, computational and communicational overhead, cost and usage of critical cloud resources itself for discriminating the legitimate traffic from the illegitimate one. Most of the methods allow the attack traffic to arrive at CSP and then propose corrective actions against it.

In this study, we wish to identify the most vulnerable paths that a DDoS attacker may choose to attack a CSP. Afterwards, we want to compute the probability of compromising vulnerable paths and expected loss for the firm due to DDoS attacks. The knowledge of these vulnerable paths and the knowledge of associated loss will help the chief technical officer (CTO) to device preventive mechanisms in advance that will reduce the impact of the DDoS attacks. This is in contrast to the existing literature that focuses on waiting for the packets to arrive at CSP, before taking corrective measures. In this study, we have proposed a proactive cloud vulnerable paths assessment system (P-CVPAS) which will help the security personnel to analyze the various vulnerable network paths, compute the probability of compromising vulnerable paths, and find the expected loss due to DDoS attacks. The attacker may opt for over flooding the destination through these vulnerable paths.