Abstract

Distributed Denial of Service attacks is major threats these days over internet applications and web services. These attacks moving forward towards application layer to acquire and waste maximum CPU cycles. By requesting resources from web services in huge amount using rapid fire of requests, attacker automated programs utilizes all the capability of processing of single server application or distributed environment application. The phases of the scheme implementation are user behavior monitoring and detection. In first phase by gathering the information of user behavior and calculating individual user’s trust score will take place and Entropy of the same user will be calculated. Based on first phase, in detection phase, variation in entropy will be observed and malicious users will be detected. Rate limiter is also introduced to stop or downgrade serving the malicious users. This paper presents the FAÇADE layer for detection and blocking the unauthorized user from attacking the system.

References

- Denial of Service Attacks, "http://www. incapsula. com/ddos/ddos-attacks/denial-of-service. html;"