Abstract

The enhancement in digital technologies has been amplified drastically and it made a lot of changes in the entire life cycle of people. Such a fast development in technology also contains a chance of attacks from direct or indirect security attacks such as gaining physical access to the targeted computer and cyber-attacks like DDoS (Distributed Denial of Service) attacks. In recent years, Cloud services are increasing in public and business ventures for production tasks. So cloud computing needs a lot of security to secure the data of other businesses and also itself. DDoS attacks are major security risks in the cloud environment. It happens by sending thousands of requests to flood the server and prevent it from processing requests.

DDoS attack is a significant cybersecurity challenge and is a network threat that makes a particular system or network out of reach and unusual for a period of time. It affects the server's resources such as bandwidth and buffer size. To detect such types of attacks we need to utilize advanced algorithms and a high level of accuracy which keep the computation cost under control. These are detected by using Machine Learning algorithms like Naïve Bayes, Hybrid computation, KNN algorithm, Random Forest algorithm, etc…

Keyword :

Distributed Denial of Service, Machine Learning, Cloud

References :

[1] https://www.hindawi.com/journals/cin/2022/9151847/ Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier

[2] https://ieeexplore.ieee.org/document/9716094A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks

[3] https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00616-0 Detecting Denial of Service attacks using machine learning algorithms

[4] https://www.jetir.org/papers/JETIR2207531.pdf Detection of DDoS Attack using Machine Learning Algorithms

[5]