|  |  |  |  |
| --- | --- | --- | --- |
| Title | A Comparative Review on DDoS Attack Detection Using Machine Learning Techniques | | |
| Author(s) Name | Zerin Hasan Sahosh, Azraf Faheem, Marzana Bintay Tuba1, Md. Istiaq Ahmed, and Syeda Anika Tasnim\* | | |
| Contact Email(s) | anika.tasnim@aiub.edu | | |
| Published Journal Name | Malaysian Journal of Science and Advanced Technology | | |
| Type of Publication | Online | | |
| Volume | 4 | Issue | 2 |
| Publisher | Penteract Technology | | |
| Publication Date | 2024-03-09 | | |
| ISSN | 2785-8901 | | |
| DOI | https://doi.org/10.56532/mjsat.v4i2.208 | | |
| URL | https://mjsat.com.my/index.php/mjsat/article/view/208 | | |
| Other Related Info. |  | | |
|  | | | |

|  |  |
| --- | --- |
| Abstract |  |
| The rapid growth of the internet and the increasing reliance on digital infrastructures have posed significant challenges to cybersecurity. Among the other variants of attacks, Distributed Denial of Service (DDoS) attacks have emerged as one of the most destructive and common threats. These attacks disrupt or slow down network services by overwhelming the network infrastructure with a massive volume of malicious traffic. To effectively identify and mitigate DDoS attacks, machine learning techniques have been extensively employed in intrusion detection systems. Machine learning approaches offer the advantage of automating the detection process by learning patterns and characteristics of DDoS attacks from historical data. Researchers have explored various machine learning algorithms such as K-Nearest Neighbours (KNN), Support Vector Machine (SVM), Random Forest (RF), and Naïve Bayes to classify and detect DDoS attacks. These algorithms leverage features extracted from network traffic data, including packet size, packet delay patterns, and traffic behaviour, to differentiate between normal and malicious traffic. | |