Abstract

Despite the rapid growth in popularity of cloud computing, securing the availability and usability of data, resources, and services is still a major problem. DDOS (distributed denial of service) assaults are not a new threat. There is a serious concern over the hot topic of research. We'll go through the numerous DDOS intended and launch methods that can be used to combat or facilitate DDOS assaults, as well as intrusion-detection methodologies and defense tactics.

Methods and Materials

An attacker using the second method tries to do one of the following (16): (1) randomly bounce IP addresses, (2) process routing capacities, or (3) network resources; they can be tricked with one set or another. These are currently considered flooding assaults on the network/transport layer. (For example, flooding attacks.) There are several mechanisms available for DoS defense. One known method is to use the DoS prevention techniques and ensure that no normal service can be used. Many in the past ten years have focused on the prevention and response to these attacks. Financial/economic/governmental initiatives, cyber warfare.

Conclusions

We were successful in achieving the accuracy of 0.9999 by using random forest classifier which is slightly better than SVM with the same accuracy. The accuracy of about 0.9999 proves that random forest classifier is a viable alternative to the SVM classifier. We can also consider the use of other machine learning algorithms in the future to achieve even better accuracy.

# References


# Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped to improve the quality of the manuscript.

# Conclusion

In this paper, we have demonstrated that machine learning-based models can be applied for forecasting the next week's highest accuracy results. Based on our findings, we have proven that the proposed machine learning algorithms, specifically the Random Forest classifier, can significantly improve the accuracy of DDOS detection in cloud environments. Future work includes the development of more advanced machine learning models and algorithms that can better handle dynamic and unpredictable network environments.