Title of the Project : A Reliable and Robust DDOS attack in IoT Using Neural network

Name of the Students : S.Varsha , R.Valarmathi

Register Number : 211417104292 , 211417104289

Name of the Guide : R.Devi

**ABSTRACT**

Internet-of-things (IOT) plays a prominent role in the digital revolution . The rapid development of IoT leads to various emerging cybersecurity threats. This is because IoT devices are often limited in making them particularly vulnerable to adversaries Therefore, detecting and preventing attacks in IoT networks have to be noticed by the people in the industry. There are many attacks takes place out of them distributed denial-of-service(DDoS) attack is most challenging.

A distributed denial-of-service(DDoS) attack is a malicious attempt to disrupt normal flow of targeted server, by overwhelming the target or its surrounding with a flood of Internet traffic. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. This could be sending a web server so many requests to serve a page that it crashes under the demand, or it could be a database being hit with a high volume of queries. The result is available internet bandwidth, CPU and RAM capacity becomes overwhelmed. This paper presents Distributed denial-of-service attack detection using Neural network. The main contributions of this project are Data Analysis, Dataset Preprocessing, Training the Model, Testing of Dataset. This method will produce better results compared to other techniques.