INTERNATIONAL CONFERENCE ON RECENT CHALLENGES IN ENGINEERING, SCIENCE AND INFORMATION TECHNOLOGY (ICRCESIT – 2020)
25TH OCTOBER, 2020

CERTIFICATE NO : ICRCESIT /2020/ C1020702

ANALYZE EXISTING STUDIES RELATING OF MACHINE LEARNING IN BOTNET DETECTION IN SDN SYSTEM

DEEVI HARIKRISHNA

Research Scholar, Ph.D. in Computer Science Engineering,
Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P., India.

ABSTRACT

The security threat is one of the most pressing challenges in today's networks, and it is regarded as the most critical in the management of multimedia data. Bots are a type of security attack that targets a person or a group of nodes in a network, turning them into bots. A botnet is a network of bots that can be controlled by a bot master. These bots are programmed to disrupt network activity. It collects very sensitive data including bank account numbers and personal information. Botnets are now identified utilising an intrusion detection system (IDS), which efficiently monitors network activity in entities and companies on a regular basis. Bots create bogus or undesirable data, which is then passed on to all nodes in the network, lowering network efficiency. The botnet's primary goal is to assault as many devices as possible while also disseminating malicious programmes as much as possible. Botnet assaults infect many types of technology, and even the most basic internet security suites, firewalls, and antivirus software provide some defence. We offered dynamic analysis in advance, looking for signs of infection in behavioural analysis, as well as network and network traffic anomalies. Individual symptoms of botnet attacks are combined with network-level attacks.