Botnet and Internet of Things (IoTs): A Definition, Taxonomy, Challenges, and Future Directions

K Alieyan, A Almomani, R Abdullah, B Almutairi, M Alauthman

In today's internet world the internet of things (IoT) is becoming the most significant and developing technology. The primary goal behind the IoT is enabling more secure existence along with the improvement of risks at various life levels. With the arrival of IoT botnets, the perspective towards IoT products has transformed from enhanced living enabler into the internet of vulnerabilities for cybercriminals. Of all the several types of malware, botnet is considered as really a serious risk that often happens in cybercrimes and cyber-attacks. Botnet performs some predefined jobs and that too in some automated fashion. These attacks mostly occur in situations like phishing against any critical targets. Files sharing channel information are moved to DDoS attacks. IoT botnets have subjected two distinct problems, firstly, on the public internet. Most of the IoT devices are easily accessible. Secondly, in the architecture of most of the IoT units, security is usually a reconsideration. This particular chapter discusses IoT, botnet in IoT, and various botnet detection techniques available in IoT.