Systematic literature review on Iot-Based Botnet attack

ABSTRACT

The adoption of the Internet of Things (IoT) technology is expanding exponentially because of its capability to provide a better service. This technology has been successfully implemented on various devices. The growth of IoT devices is massive at present. However, security is becoming a major challenge with this growth. Attacks, such as IoT-based botnet attacks, are becoming frequent and have become popular amongst attackers.IoT has a resource constraint and heterogeneous environments, such as low computational power and memory. Hence, these constraints create problems in implementing a security solution in IoT devices. Therefore, various kind of attacks are possible due to this vulnerability, with IoT-based botnet attack being one of the most popular.In this study, we conducted a comprehensive systematic literature review on IoT-based botnet attacks. Existing state of the art in the area of study was presented and discussed in detail. A systematic methodology was adopted to ensure the coverage of all important studies. This methodology was detailed and repeatable. The review outlined the existing proposed contributions, datasets utilised, network forensic methods utilised and research focus of the primary selected studies. The demographic characteristics of primary studies were also outlined.The result of this review revealed that research in this domain is gaining momentum, particularly in the last 3 years (2018-2020). Nine key contributions were also identified, with Evaluation, System, and Model being the most conducted