A Literature Survey on IoT Botnet Detection Techniques

Umar Maikudi
Department of Computer Science
Federal University of Technology
Minna, Nigeria
maikudiumar509@gmail.com

Opeyemi Aderiike Abisoye
Department of Computer Science
Federal University
of Technology
Minna, Nigeria
o.abisoye@futminna.edu.ng

Shefiu Olusegun Ganiyu
Department of Information and Media Technology
Federal University
of Technology
Minna, Nigeria
shefiuganiyu@futminna.ed.ng

Sulaimon A. Bashir
Department of Computer Science
Federal University of Technology
Minna. Nigeria.
bashirsulaimon@futminna.edu.ng

***Abstract*—** One of the significant security concerns in the Information Technology community is Botnet, which could be used by adversaries to launch different kinds of attacks from compromised IoT devices. Botnets were initially created for positive purposes, not until cybercriminals began to take advantage of their potentials and started programming malicious software for malicious intent thereby, making detection and mitigation difficult. The rapid rise in the development of IoT products has made cyber-attack permutations unpredictable and availed cybercriminals of new techniques for security breaches of such products. Hence, the motivation for this research is premised on the incessant increase in the botnet attacks on IoT-based products. Thus, this paper offers a comprehensive literature overview of current IoT botnet detection techniques with a focus on revealing the strengths and weaknesses of the existing techniques in the research area. In line

with this, some selected techniques were retrieved and analyzed in the summary table and a conclusion is drawn which exposed the need for more robust detection techniques to detect and prevent the emerging sophisticated botnet versions in the domain. Therefore, the findings from this review will benefits researchers who are engaged in detecting and preventing botnet attacks over IoT devices and network.