Chapter 7
Botnet and Internet of Things (IoTs):
A Definition, Taxonomy, Challenges, and Future Directions

Kamal Alieyan
Universiti Sains Malaysia, Malaysia

Rosni Abdullah
Universiti Sains Malaysia, Malaysia

Ammar Almomani
https://orcid.org/0000-0002-8808-6114
Al-Balqa Applied University, Jordan

Badr Almutairi
Majmaah University, Saudi Arabia

Mohammad Alauthman
https://orcid.org/0000-0003-0319-1968
Zarqa University, Jordan

ABSTRACT

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.

INTRODUCTION

In this digital world where everything is connected through the internet, the Internet of Things (IoT) plays a major role. Most of the people get attracted towards this innovative approach which helps the people to enjoy their life in their hectic routine. For instance, just imagine if refrigerators will be able to monitor their content and can place the order to a retailer shop if any food item is running out or imagine if you would be able to order your Sunday breakfast from your bed through a gesture or a voice command like the intelligent assistants Google Assistant, Apple Siri or Amazon Alexa. All these thoughts are not only some science fiction story but is now becoming a reality just because with use of smart devices such as Google Home, Amazon echoes with Alexa, etc., smart television, smart phones, etc. (Engrish, 2017).

In 1999, the concept of IoT was proposed by Kevin Ashton. IoT was refereed as the objects that are interoperable and exclusively identifiable and are connected with radio-frequency identification technology. Though, IoT is defined by in many forms by the various researchers as (Ray, 2018):

- ''A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies'' (ICTP Workshop, 2015).
- ''3A concept: anytime, anywhere and any media, resulting into sustained ratio between radio and man around 1:1'' (Srivastava, 2006).
- ''a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network'' (Kranenburg, 2008).

Evolution of Internet of Things (IoT)

As shown in Figure 1 that is how the Internet of Things actually evolved with the advent of time. At the era of pre-internet, which is also known as "H2H" or "Human-to-Human" era, people had the fixed or mobile telephony. Except that one of the primary ways of communication was through SMS services. After that with the incorporation of smart networks when the internet came into existence, the "www" or "world wide web" era the communication as well as information and entertainment etc. gets better through the internet. Furthermore, smart IT platforms and services were added to "www" that results in "web 2.0" era that totally converts everything into digital transformation like e-productivity, e-commerce, etc.

Figure 1. Evolution of IoT

Related Content

Artificial Intelligence and Facial Recognition in an IoT Ecosystem: The Impact on Data Protection and Privacy and the Relevance of Ethics
Nicola Fabiano (2022). *International Journal of Cyber Warfare and Terrorism (pp. 1-11).*
www.irma-international.org/article/artificial-intelligence-and-facial-recognition-in-an-iot-ecosystem/305862

Transformation of the Terrorist Threat: A Case Study of the "Islamic State" of Iraq and Syria (ISIS)
Diana Jalagania (2023). *Global Perspectives on the Psychology of Terrorism (pp. 89-121).*
www.irma-international.org/chapter/transformation-of-the-terrorist-threat/314670

Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP)
John S. Hurley (2017). *International Journal of Cyber Warfare and Terrorism (pp. 23-34).*
www.irma-international.org/article/quantifying-decision-making-in-the-critical-infrastructure-via-the-analytic-hierarchy-process-ahp/190589

Understanding Media during Times of Terrorism
Robert Hackett (2014). *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia (pp. 33-43).*
www.irma-international.org/chapter/understanding-media-during-times-of-terrorism/106147

Analysis of Success of Mobilization to Terror using Tools of Neuro-Linguistic Programming (NLP)
Marina Shorer-Zeltserand Galit M. Ben-Israel (2016). *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare (pp. 127-143).*
www.irma-international.org/chapter/analysis-of-success-of-mobilization-to-terror-using-tools-of-neuro-linguistic-programming-nlp/140518