

Chapter 13

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

Kamal Alieyan

Universiti Sains Malaysia, Malaysia

Ammar Almomani

Al-Balqa Applied University, Jordan

Rosni Abdullah

Universiti Sains Malaysia, Malaysia

Badr Almutairi

Majmaah University, Saudi Arabia

Mohammad Alauthman

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.

DOI: 10.4018/978-1-5225-9742-1.ch013

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. (English, 2017).

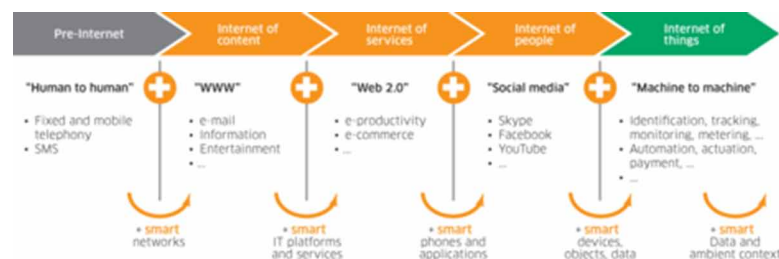
In 1999, the concept of IoT was proposed by Kevin Ashton. IoT was refereed as the objects that are interoperable and exclusively identifiable and are connected with radio-frequency identification technology. Though, IoT is defined by in many forms by the various researchers as (Ray, 2018):

- “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



11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/botnet-and-internet-of-things-iots/234816

Related Content

On the Importance of Framing

Nathan Harter (2011). *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives* (pp. 1-16).

www.irma-international.org/chapter/importance-framing/46338

Risks in Adoption and Implementation of Big Data Analytics: A Case of Indian Micro, Small, and Medium Enterprises (MSMEs)

Rajasekhara Mouly Potluri and Narasimha Rao Vajjhala (2021). *International Journal of Risk and Contingency Management* (pp. 1-11).

www.irma-international.org/article/risks-in-adoption-and-implementation-of-big-data-analytics/284440

An Integrated Machine Learning Framework for Fraud Detection: A Comparative and Comprehensive Approach

Karim Ouazzane, Thekla Polykarpou, Yogesh Patel and Jun Li (2022). *International Journal of Information Security and Privacy* (pp. 1-17).

www.irma-international.org/article/an-integrated-machine-learning-framework-for-fraud-detection/300314

Privacy Preserving Classification of Biomedical Data With Secure Removing of Duplicate Records

Boudheb Tarik and Elberichi Zakaria (2021). *Research Anthology on Privatizing and Securing Data* (pp. 569-588).

www.irma-international.org/chapter/privacy-preserving-classification-of-biomedical-data-with-secure-removing-of-duplicate-records/280193

Identity Management: A Comprehensive Approach to Ensuring a Secure Network Infrastructure

Katherine M. Hollis and David M. Hollis (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 2641-2649).

www.irma-international.org/chapter/identity-management-comprehensive-approach-ensuring/23246