Chapter 11
Security in Internet of Things: Requirements, Challenges, and Open Issues

Said Ul Abrar
The University of Agriculture, Peshawar, Pakistan

Mohib Ullah
The University of Agriculture, Peshawar, Pakistan

Kamran Ullah
The University of Agriculture, Peshawar, Pakistan

Irfan Ullah Khan
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Saleem Zahid
The University of Agriculture, Peshawar, Pakistan

Muhammad Inam Ul Haq
Khushal Khan Khattak University, Karak, Pakistan

ABSTRACT

Recently, electronics devices, cognitive computing, and sensing enable the deployment of internet-of-things (IoTs) with a huge application domain. However, resource constraints such as low computing powers or limited storage leave IoTs infrastructures vulnerable to a variety of cyber-attacks. In dark-net the address space developed as designated unrestricted internet address space anticipated to be used by trustworthy hosts anywhere in the world, therefore, any communication activity is presumed to be unwanted and particularly treated as a probe, backscatter, or miss-configuration. This chapter investigates and evaluates the operation of dark-net traffic detection systems in IoTs networks. Moreover, the most recent work done to ensure security in the IoTs network has been discussed. In particular, the areas of privacy provisioning, lightweight cryptographic framework, secure routing, robustness, and DoS attacks have been addressed. Moreover, based on the analysis of existing state-of-the-art protocols, the security requirements and challenges are highlighted along with identified open issues.

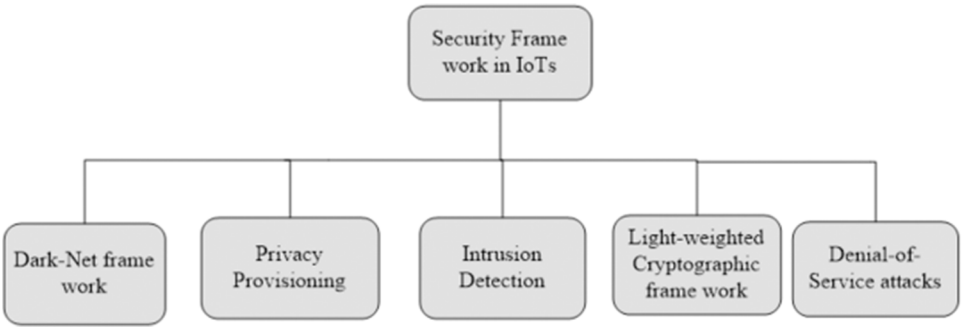
DOI: 10.4018/978-1-6684-6914-9.ch011

1. INTRODUCTION

The emergence of internet of things (IoTs) has been made possible by the modern technological revolution in electronics, cognitive computing, and sensing, which has supplied essential infrastructure for a variety of applications. As the IoT domain expands, it is challenging to devise a reference design that can handle both present functionality and potential improvements. In IoTs, the data are acquired from multiple sources and processed by numerous entities, therefore, the IoTs architecture must be distributed in nature, scalable, interoperable, and capable of delivering Moreover, resource constraints such as limited computing power, storage capabilities and energy prohibit the deployment of sophisticated mechanisms. Therefore, the infrastructures used by IoTs are vulnerable to a variety of cyber-attacks. Likewise, traditional networking security solutions are not applicable in IoTs due to the specific architectural requirements and resource constraints. Therefore, light weighted and scalable solutions, under the resource constraints, are desirable to address the problems of privacy, Integrity, denial-of-service attacks detection, cryptographic framework, secure routing etc in IoTs.

Figure1 shows the security frame work in IoTs. The subsequent sections provide a brief detail of the current state-of-the-art solutions aross the sub domains. Finally, a detail discussion including the open research issues, challenges, requirements and future research directions, concludes each sub-domain.

Figure 1. Security framework in IoTs



1.1 Dark-Net Traffic Detection Systems in IoTs

The Dark Web or Dark-net comprises a network of shared resources (i.e. websites, servers) open to public with hidden identifiers i.e. IPs. Accessing the shared resources needs special tools and applications. The Dark-net uses peer-to-peer networking with encapsulation where the data are transmitted in encrypted form. Likewise, the forwarding takes placed in a layered manner, where forwarding nodes decrypt layers of the encryption. In this manner, the intermediate nodes know only the position of immediate nodes before and after, this mechanism hides the identity of senders. The working principles of Dark-net make enables the users to carry out illegal activities. The most prominent literature exploits machine learning mechanisms to analyze the network traffic and detects Dark-net related activities (Abu Al-Haija et al., 2022; Demertzis et al., 2021). The employed machine learning techniques classify the different Dark-net traffics and detect certain patterns as malicious activities.