I.J. Wireless and Microwave Technologies, **2021, 1, 28-46**
Published Online February 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.01.04

An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)

Asifa Nazir, Sahil Sholla, Adil Bashir
Department of Computer Science &Engineering
Islamic University of Science &Technology, Awantipora, India
Email: {malikasifa356[1], sahilsholla[2], adilbashir.445[3]}@gmail.com

Received: 01 September 2020; Revised: 13 October 2020; Accepted: 03 November 2020; Published: 08 February 2021

Abstract: Due to increased number of IoT devices, the marketplace is showing significant growth of sensor deployments around the world. The context involved in any IoT environment needs proper storage, processing and interpretation to get deeper insights from it. Previous research has not focussed much on context-ware security in IoT environment and has primarily relied on context-ware computing methods. In this research paper we implement logical decisions among IoT nodes in healthcare system using ontological approach. With the help of ontological method collected data is transferred between various healthcare devices to the knowledge base thereby achieving security of context like patient data by providing deeper insights, so as to generate intelligent suggested solutions. Incorporation of context-aware rules based on common experience for specific healthcare scenario is done to get implicit insight among IoT nodes. This work designs security ontology using Security Toolbox: Attacks & Countermeasures (STAC) framework that is implemented in Protégé 5. Moreover, Pellet (Incremental) reasoned is used to evaluate the ontology. Emergency ontology that can prove helpful at emergency times has also been designed. Different parameters addressed in this work are authentication, access-control, authorization and privacy using context-awareness methodology that can enable naive users make informed security decision.

Index Terms: IoT, semantic web, attacks, counter-measures, context-aware security

1. Introduction

Internet of Things (IoT) is the concept of pervasive interconnected computing things, services and humans each provided with unique identifiers to achieve common goal of data transmission in smart applications without requiring human intervention. IoT has become particularly popular because of the speedy development of small sized and low cost sensor devices in market. Typical applications of IoT practices include smart home, smart healthcare monitoring systems, smart agriculture system etc. IoT aims to create an environment where various things flawlessly interact with each other to provide advanced smart services for humans. The interconnected devices such as sensors at perception layer of IoT monitor and hence collect data from particular environment and then after in-depth analysis of the data useful information is extracted to enable promising smart civic amenities available at application layer [1].IoT framework helps services, device and humans to communicate using existing communication technologies (like Bluetooth, Zigbee etc.). According to experts the estimated amount of IoT devices in world is exceeding world's population [2]. In 2017, it has been estimated that the number of connected IoT devices in world is about 8.4 billion and is expected to grow in future. According to predictions made by Cisco's, the number of devices associated to the internet will be more than 50 million by 2020[3]. Movement of the data in context-aware system is determined by context-aware life cycle comprising of four phases. The first phase called context acquisition is accountable for data collection from various physical or virtual sources. The second phase known by the name of context modeling is responsible for modeling data in well-defined manner. This modeled data is processed further to derive high-level situational information from low-level situational information which is done in third phase called reasoning phase. Lastly, distribution of high as well as low–level context is done in fourth phase known as dissemination/distribution phase [4].

Context-awareness is the process of analyzing the changing behavior of surroundings in which IoT devices are to be deployed. This term was first introduced by Schilit and Theimer in 1994, later redefined by Ryan et al. [5, 6]. In both cases main emphasis is on computer applications. Abowd et al. stated that these definitions are too specific and can't be used to specify whether a given system is situation-aware or not. The more appropriate definition of context-awareness is as follows:

