Abstract

Internet of Things (IoT) is an emerging technology it is used for connection of not only computers or mobiles but also buildings, homes, household devices (air conditioner, fridge), fuel stations and for several other industrial purposes. It has also cast its effect on sectors like transportation, healthcare. The connection and communication of these devices, processes and data produces an enormous data set, which needs large datacenters and data warehouses for storage. IoT infrastructure and services needs a great security measure due to a wide and ever increasing attack surface, vast heterogeneity and complexity of dynamism of volumes. This paper explores the challenge involved in ubiquitous computing and the security complications, by providing an overview of threats and vulnerabilities in IoT enabled cyber-physical system. The overview could provide guidance for future work and research on
IoT security and computational intelligence (involving encryption).

Refernces

- ERCIM news: Smart Cities Number 98 2014
- The Internet of Things – Architecture: Final architectural reference model for the IoT v3.
- BRK1552 by Kevin Miller, Principal Program Manager, Azure IoT
- Internet_of_Things_factsheet_Architecture
- On the Application of IOT (Internet of Things) for Securing Industrial Threats By: Muhammad Usman, National University of Sciences and Technology (NUST)
- "Internet of Things: How Much are We Exposed to Cyber Threats?" - InfoSec Resources. http://resources.infosecinstitute.com/internet-things-much-exposed-cyber-threats/
- S. Institute, "SANS Institute InfoSec Reading Room tu-evolution, the history and Evolution of Intrusion Detection," 2001.
- A new approach to investigate IoT threats based on a four layer model
Securing IoT: Threats and Vulnerabilities

- "Internet of Things Strategic Research and Innovation Agenda" Ovidiu Vermesan et. al.

Index Terms

Computer Science Security

Keywords

IoT Ubiquitous Computing Datacenter Data Ware Houses