



Network of 'Things'

The National Institute of Standards and Technology (NIST) has released a new publication that provides a basic model aimed at helping researches better understand the Internet of Things (IoT) and its security challenges. Expected to approach nearly \$2 trillion in market value by 2020, the IoT covers an incredibly large range of technologies – everything from smart homes, wearables, smart factories and building, self-driving cars to health care monitors.

Given the breadth of devices involved, NIST computer scientist Jeff Voas determined that "there is no formal, analytic or even descriptive set of building blocks that govern the operation, trustworthiness and lifecycle of IoT components." Instead, Voas has created a new model called the Network of Things (NoT) based on distributed computing, which has been in use for decades. In distributed computing, computer components are networked and share messages about tasks to operate efficiently. A simple example is the local area network in an office where computers share a printer. The Network of Things (NoT) model is based on four fundamentals at the heart of IoT— sensing, computing, communication and actuation.

This document offers an underlying and foundational understanding of IoT based on the realization that IoT involves sensing, computing, communication, and actuation. The material presented here is generic to all distributed systems that employ IoT technologies (i.e., 'things' and networks). The expected audience is computer scientists, IT managers, networking specialists, and networking and cloud computing software engineers.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- NetworkOfThings.pdf