

## Chapter 5

# IoT Evolution and Security Challenges in Cyber Space: IoT Security

**Uma N. Dulhare**  
*MJCET, India*

**Shaik Rasool**  
*MJCET, India*

### **ABSTRACT**

*The internet of things (IoT) is the network of physical objects accessed through the internet that can identify themselves to other devices and use embedded technology to interact with internal states or external conditions. The IoT is an environment where an object that can represent itself becomes greater by connecting to surrounding objects and the extensive data flowing around it. The number of internet of things (IoT) devices will reach more than 15 billion units by 2021, according to research from Juniper. As businesses and consumers accelerate adoption, we're now on the cusp of an IoT revolution. The chapter walks through the security problems that are seen with IoT devices that continues to highlight how vulnerable these devices are when faced with modern, sophisticated cyber threats. Further, the authors discuss how to solve these security challenges presented by the internet of things.*

DOI: 10.4018/978-1-5225-8241-0.ch005

## **INTRODUCTION**

Human beings were given capable and inquisitive minds, so they endlessly seek better ways of doing things. This kind of drive, along with an inborn curiosity and a strong drive to unlock the secrets of nature, has created a steady stream of technical innovations over the ages. These ground-breaking efforts have focused on the means for endurance, comfort, and accumulation of wealth--with the hierarchy of needs extending from physical basics of existence to higher-level wants associated with self-actualization. A principal push of innovation today carries on toward technological advances that enhance the productivity of labour and free humans of tasks done more economically by machines. A great insatiable appetite for convenience, comfort, and entertainment products and services, as well as for means to overcome natural barriers like geography and travel time, creates a regular pull on technology. The pull is especially strong in areas relating to the quality of life, and there have been many technological innovations to meet that require. But the opportunities are far from exhausted.

Between society's hottest demands on technology is good for the means to handle the huge amount of information made by modern life. This kind of information explosion stems from complex business practices, new residential services, substantially increased record keeping through comprehensive data bases, and the globalization of our advanced society. The information technology has evolved over many years to help a growing portion of the work force devoted to the generation.

Every baby given birth to today under western culture has a life span of around 100 years, which means it will be alive in 2110. It can practically impossible to predict in greater detail life in 2110. However, what we can endeavour to speculation centred on existing drifts is that humans will still inhabit the planet, as drive animals, and we will be combined by simple natural being premeditated naturally in lab, and of course, machines. Equipment will roam the planet, working in factories, taking our children to college, delivering babies, cleaning the streets, and other such tasks, which will make them seemingly indispensable to us (Parag et al, 2016).

We how to start how superior these machines will be a century from today. Some might continue as dumb machines like the methods we have now, assiduously screwing on the caps of Coke containers. Or they might be humanoid robots that look like us and nurse our elderly parents. The cumulative erudition of Technology from the steam engine and encounter of electricity to telecommunications, the Internet and biotechnology is seen as a haphazard confluence of the breakthroughs of geniuses -- or it might be seen as an evolutionary pattern.

Technology, spawns' new generations of products by using existing components, a phenomenon this individual calls combinatorial evolution. The change in 'species' can thus be quite significant in a short period of time. The evolution of technology

27 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/iot-evolution-and-security-challenges-in-cyber-space/222218](http://www.igi-global.com/chapter/iot-evolution-and-security-challenges-in-cyber-space/222218)

## Related Content

---

### Steganalysis: Trends and Challenges

Hafiz Malik, Rajarathnam Chandramouli and K. P. Subbalakshmi (2009). *Multimedia Forensics and Security* (pp. 245-265).

[www.irma-international.org/chapter/steganalysis-trends-challenges/26996](http://www.irma-international.org/chapter/steganalysis-trends-challenges/26996)

### Realistic Spatial Backcloth is not that Important in Agent Based Simulation Research: An Illustration from Simulating Perceptual Deterrence

Henk Elffers and Pieter Van Baal (2008). *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems* (pp. 19-34).

[www.irma-international.org/chapter/realistic-spatial-backcloth-not-important/5256](http://www.irma-international.org/chapter/realistic-spatial-backcloth-not-important/5256)

### An Incremental Acquisition Method for Web Forensics

Guangxuan Chen, Guangxiao Chen, Lei Zhang and Qiang Liu (2021). *International Journal of Digital Crime and Forensics* (pp. 1-13).

[www.irma-international.org/article/an-incremental-acquisition-method-for-web-forensics/284502](http://www.irma-international.org/article/an-incremental-acquisition-method-for-web-forensics/284502)

### Source Camera Identification Based on Sensor Readout Noise

H. R. Chennamma and Lalitha Rangarajan (2010). *International Journal of Digital Crime and Forensics* (pp. 28-42).

[www.irma-international.org/article/source-camera-identification-based-sensor/46045](http://www.irma-international.org/article/source-camera-identification-based-sensor/46045)

### An Analysis of Privacy and Security in the Zachman and Federal Enterprise Architecture Frameworks

Richard V. McCarthy (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 363-374).

[www.irma-international.org/chapter/analysis-privacy-security-zachman-federal/60959](http://www.irma-international.org/chapter/analysis-privacy-security-zachman-federal/60959)