

River Publishers Series in Information Science and Technology

SECURE AND SMART INTERNET OF THINGS (IoT)

using Blockchain and Artificial Intelligence (AI)



Ahmed Banafa



River Publishers

Secure and Smart Internet of Things (IoT)

Using Blockchain and AI

RIVER PUBLISHERS SERIES IN INFORMATION SCIENCE AND TECHNOLOGY

Series Editors:

K. C. CHEN

National Taiwan University

Taipei, Taiwan

and

University of South Florida, USA

SANDEEP SHUKLA

Virginia Tech

USA

and

Indian Institute of Technology Kanpur, India

Indexing: All books published in this series are submitted to the Web of Science Book Citation Index (BkCI), to CrossRef and to Google Scholar.

The “River Publishers Series in Information Science and Technology” covers research which ushers the 21st Century into an Internet and multimedia era. Multimedia means the theory and application of filtering, coding, estimating, analyzing, detecting and recognizing, synthesizing, classifying, recording, and reproducing signals by digital and/or analog devices or techniques, while the scope of “signal” includes audio, video, speech, image, musical, multimedia, data/content, geophysical, sonar/radar, bio/medical, sensation, etc. Networking suggests transportation of such multimedia contents among nodes in communication and/or computer networks, to facilitate the ultimate Internet.

Theory, technologies, protocols and standards, applications/services, practice and implementation of wired/wireless networking are all within the scope of this series. Based on network and communication science, we further extend the scope for 21st Century life through the knowledge in robotics, machine learning, embedded systems, cognitive science, pattern recognition, quantum/biological/molecular computation and information processing, biology, ecology, social science and economics, user behaviors and interface, and applications to health and society advance.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include, but are by no means restricted to the following:

- Communication/Computer Networking Technologies and Applications
- Queuing Theory
- Optimization
- Operation Research
- Stochastic Processes
- Information Theory
- Multimedia/Speech/Video Processing
- Computation and Information Processing
- Machine Intelligence
- Cognitive Science and Brain Science
- Embedded Systems
- Computer Architectures
- Reconfigurable Computing
- Cyber Security

For a list of other books in this series, visit www.riverpublishers.com

Secure and Smart Internet of Things (IoT)

Using Blockchain and AI

Ahmed Banafa

Professor at San Jose State University
USA

and

Instructor at Stanford University
USA



River Publishers

Published, sold and distributed by:

River Publishers
Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers
Lange Geer 44
2611 PW Delft
The Netherlands

Tel.: +45369953197
www.riverpublishers.com

ISBN: 978-87-7022-030-9 (Hardback)
978-87-7022-029-3 (Ebook)

©2018 River Publishers

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Contents

Foreword	xi
Preface	xv
List of Figures	xvii
List of Abbreviations	xix

PART I: What Is IoT?

1 Internet of Things: The Third Wave?	3
1.1 Advantages and Disadvantages of IoT	5
2 The Industrial Internet of Things (IIoT): Challenges, Requirements and Benefits	7
2.1 IIoT, IoT and M2M	9
2.1.1 IIoT Challenges	9
2.1.2 IIoT Requirements	9
2.1.3 IIoT Benefits	10
2.2 The Future of the Industrial Internet of Things	11
3 Internet of Things: Security, Privacy and Safety	13
3.1 IoT's Threats	15
3.2 Threats Are Real	16
3.3 What Can We Do	17
4 Internet of Things: More than Smart “Things”	19
4.1 Industrial Internet	21
4.2 The IoT Value Chain	23
4.3 Internet of Things Predictions	23
4.4 Challenges Facing IoT	24

5	Internet of Things: Myths and Facts	25
5.1	IoT and Sensors	26
5.2	IoT and Mobile Data	27
5.3	IoT and the Volume of Data	28
5.4	IoT and Datacenters	28
5.5	IoT Is a Future Technology	28
5.6	IoT and Current Interoperability Standards	29
5.7	IoT and Privacy & Security	30
5.8	IoT and Limited Vendors	30
5.9	Conclusion	31

PART II: IoT Implementation & Standardization Challenges

6	Three Major Challenges Facing IoT	35
6.1	Technology	36
6.2	Technological Challenges	37
6.3	Business	40
6.4	Society	41
6.5	Privacy	42
6.6	Regulatory Standards	43
7	IoT Implementation and Challenges	45
7.1	Components of IoT Implementation	46
7.1.1	Sensors	46
7.1.2	Networks	47
7.1.3	Standards	48
7.1.4	Intelligent Analysis	49
7.1.5	Intelligent Actions	51
8	IoT Standardization and Implementation Challenges	53
8.1	IoT Standardization	54
8.2	IoT Implementation	55
8.2.1	Sensors	55
8.2.2	Networks	56
8.2.3	Standards	57
8.2.4	Intelligent Analysis	57
8.2.5	Intelligent Actions	58
8.3	The Road Ahead	58

9	Challenges Facing IoT Analytics Success	59
9.1	Data Structures	61
9.2	Combining Multiple Data Formats	61
9.3	The Need to Balance Scale and Speed	61
9.4	IoT Analytics at the Edge	62
9.5	IoT Analytics and AI	63

PART III: Securing IoT

10	How to Secure the Internet of Things	69
10.1	Challenges to Secure IoT Deployments	72
10.2	Dealing with the Challenges and Threats	74
10.3	The Optimum Platform	74
10.4	Last Word	75
11	Using Blockchain to Secure IoT	77
11.1	Challenges to Secure IoT Deployments	77
11.2	Dealing with the Challenges and Threats	78
11.3	The Optimum Platform	78
11.4	Decentralizing IoT Networks	79
11.5	The Blockchain Approach	80
	11.5.1 What Is Blockchain?	81
	11.5.2 What Are Some Advantages of Blockchain?	81
	11.5.3 How Does It Work?	82
11.6	The Blockchain and IoT	83
12	IoT and Blockchain: Challenges and Risks	85
12.1	The Blockchain Model	86
12.2	Principles of Blockchain Technology	87
12.3	Public vs. Private Blockchain	88
12.4	Challenges of Blockchain in IoT	88
12.5	Risks of Using Blockchain in IoT	89
12.6	The Optimum Secure IoT Model	91
13	DDoS Attack: A Wake-Up Call for IoT	93
13.1	Security Is Not the Only Problem	95
	13.1.1 Security Concerns	95
	13.1.2 Privacy Issues	96
	13.1.3 Inter-Operability Standard Issues	96

13.1.4	Legal Regulatory and Rights Issues	97
13.1.5	Emerging Economy and Development Issues	97
13.2	How to Prevent Future Attacks?	97

PART IV: AI, Fog Computing and IoT

14	Why IoT Needs Fog Computing	101
14.1	The Challenge	101
14.2	The Solution	102
14.3	Benefits of Using Fog Computing	103
14.4	Real-Life Example	103
14.5	The Dynamics of Fog Computing	104
14.6	Fog Computing and Smart Gateways	105
14.7	Conclusion	105
15	AI Is the Catalyst of IoT	107
15.1	Examples of IoT Data	109
15.2	AI and IoT Data Analysis	110
15.3	AI in IoT Applications	110
15.4	Challenges Facing AI in IoT	111
15.5	Conclusion	112

PART V: The Future of IoT

16	IoT, AI and Blockchain: Catalysts for Digital Transformation	115
16.1	Digital Transformation	116
16.2	Internet of Things (IoT)	117
16.3	Digital Transformation, Blockchain and AI	118
16.4	Conclusion	118
17	Future Trends of IoT	121
17.1	Trend 1 – Lack of Standardization Will Continue	122
17.2	Trend 2 – More Connectivity and More Devices	122
17.3	Trend 3 – “New Hope” for Security: IoT & Blockchain Convergence	123
17.4	Trend 4 – IoT Investments Will Continue	124
17.5	Trend 5 – Fog Computing Will Be More Visible	124
17.6	Trend 6 – AI & IoT Will Work Closely	125

17.7	Trend 7 – New IoT-as-a-Service (IoT-a-a-S) Business Models	125
17.8	Trend 8 – The Need for Skills in IoT’s Big Data Analysis and AI Will Increase	126

PART VI: Inside look at Blockchain

18	Myths about Blockchain Technology	129
18.1	Myth 1: The Blockchain Is a Magical Database in the Cloud	132
18.2	Myth 2: Blockchain Is Going to Change the World	132
18.3	Myth 3: Blockchain Is Free	133
18.4	Myth 4: There Is Only One Blockchain	133
18.5	Myth 5: The Blockchain Can be Used for Anything and Everything	133
18.6	Myth 6: The Blockchain Can be the Backbone of a Global Economy	134
18.7	Myth 7: The Blockchain Ledger Is Locked and Irrevocable	134
18.8	Myth 8: Blockchain Records Can Never be Hacked or Altered	134
18.9	Myth 9: Blockchain Can Only be Used in the Financial Sector	135
18.10	Myth 10: Blockchain Is Bitcoin	135
18.11	Myth 11: Blockchain Is Designed for Business Interactions Only	136
18.12	Myth 12: Smart Contracts Have the Same Legal Value as Regular Contracts	136
19	Cybersecurity & Blockchain	137
19.1	Implementing Blockchain in Cybersecurity	138
19.2	Advantages of Using Blockchain in Cybersecurity	139
19.2.1	Decentralization	139
19.2.2	Tracking and Tracing	140
19.2.3	Confidentiality	140
19.2.4	Fraud Security	140
19.2.5	Sustainability	141
19.2.6	Integrity	141
19.2.7	Resilience	141
19.2.8	Data Quality	141

19.2.9	Smart Contracts	141
19.2.10	Availability	141
19.2.11	Increase Customer Trust	142
19.3	Disadvantages of Using Blockchain in Cybersecurity	142
19.3.1	Irreversibility	142
19.3.2	Storage Limits	142
19.3.3	Risk of Cyberattacks	142
19.3.4	Adaptability Challenges	142
19.3.5	High Operation Costs	143
19.3.6	Blockchain Literacy	143
19.4	Conclusion	143
20	Future Trends of Blockchain	145
20.1	Blockchain Tracks	146
20.2	Blockchain Technology Future Trends	147
20.3	Blockchain Skills in Demand	147
20.4	Blockchain and Enterprise Applications	148
20.5	Blockchain and IoT Security	149
20.6	Blockchain and Zero-Trust Model	150
20.7	Final Words	150
	References	151
	Index	159
	About the Author	163

Foreword

The Internet of Things (IoT) connects everything on our bodies, in our homes, cities, and factories to the Internet to create a new reality of a connected world. Imagine a person driving an autonomous vehicle driving through connected traffic lights wearing a connected pacemaker. Every connected thing comes with security risk with the potential for hackers to target the person. Even security updates of AI inference models on these devices can be hacked when the device makers send an OTA or Over the Air update.

Blockchain gives you a distributed ledger in the cloud that is secure from tampering because it is cryptographically secured with transparent access to everyone equally.

Blockchain is used with the Internet of Things (IoT) systems to track every access point of the device thereby ensuring security. Blockchain offers additional transparency to a supply chain or logistics process by offering new insights to where the products originated and how it traveled to the endpoint. Imagine knowing which farm produced the coffee you are drinking and every step it traveled to reach your Barista. Blockchain also helps secure complex systems such as mines, hospitals and critical infrastructures such as water and energy systems.

I have watched Prof. Banafa's passion for IoT over the past years as he researched IoT markets with special focus on Industrial IoT with his articles, talks, and teaching.

Read this book to understand IoT solutions, as Prof. Banafa demystifies the grey areas of Edge, Fog and Cloud and drills down to provide clarity to the integration of new technologies such as Blockchain and Artificial Intelligence on how they fit to make IoT secure. Treasure this book as you will be re-reading and coming back to it several times as you build the connected world of the Internet of Things.

Sudha Jamthe
CEO, Author IoTDisruptions
& Stanford Continuing Studies IoT and AV Business Instructor

We live in exciting times where technology emergence is making us reinvent the world around us. There is no single technology that can help this transformation, but the confluence of many emerging technologies such as IoT, AI, Blockchain, AR/VR, Edge Computing will enable the current generation to visualize and discover new ways of doing things, that were earlier not possible. And this transformation will cut across every aspect of our life: Consumer to Enterprise, Community to Government, Homes to Hospitals, Art to Law, Engineering to Medicine, Infants to Elderly, Poor to Rich, impacting every form of life and resource on this planet and beyond.

And that bring us face to face with the challenges that it will bring relating to privacy and security, and the associated vulnerabilities that the new technologies bring. The human mind has, however, always fought these challenges and emerged successful, rather than letting these challenges consume us. The Blockchain is an ingenious approach that provides secure and trustless decentralized framework that holds the promise to provide an impregnable and transparent transaction system.

“Secure and Smart Internet of Things (IoT): Using Blockchain and AI” by Prof Banafa is one such book that has covered various types of emerging technologies, their convergence, and the supporting technologies like Mist and Fog Computing, that have emerged to take AI from the cloud to the edge. I have known Prof Banafa for many years and have a deep appreciation for his ability to mix academics with industry use-cases to make them relevant for applications in various domains. Apart from being a “#1 Voice to Follow in Tech” on LinkedIn, his prophecies of technology evolution have been very accurate. In this book, he shares his valuable technology insights that will be very useful to aspiring innovators to set them thinking on the right path.

My advice to readers is to relate the technologies discussed here, in context of their own ideas and visions, to discover how they can play an instrumental role in building the emerging new world that will bring peace, joy, and happiness to all.

Sudhir Kadam
Startup Alchemist, Silicon Valley Emerging Tech Expert
Board Member at IIT Startups

In *Secure and Smart Internet of Things (IoT) using Blockchain and AI*, Ahmed, a seasoned and revered stalwart on IoT and cybersecurity chronicles the vanguard of what science fictionists once called Skynet: the set of technologies converging at warp speed to create a massive intelligent machine or device network. The revolution of “Internet of Things” is amassing to some 28 billion devices by 2020 according to some experts. This ubiquity presents a Cambrian explosion: an unprecedented economic opportunity and is consequently poised to spark an arms race in cybercrime or cyberwars. It is crucial to grasp the magnitude of the cybersecurity risks and the challenge device manufacturers face. Imagine for a moment the chaos that would ensue when a rogue entity commandeers a system of autonomous vehicles operating in a smart city. Worse yet, imagine a world of interconnected healthcare systems being hijacked and mission critical information for patient treatment is held ransom or is compromised. There is no question that we approach a world where cybercrime and cyberwar is dire. Its no longer science fiction. Thanks to Ahmed who has done most of the homework for us in presenting a cogent methodology to counter this formidable threat. To anyone from (smart)home-owners to business-owners and in between - *Secure and Smart Internet of Things using Blockchain and AI* is the call to action!

Abood Quraini
Sr. Manager, Hardware Engineering at NVIDIA

Preface

By 2020, experts forecast that up to 28 billion devices will be connected to the Internet with only one third of them being computers, smartphones, smartwatches, and tablets. The remaining two thirds will be other “devices” – sensors, terminals, household appliances, thermostats, televisions, automobiles, production machinery, urban infrastructure and many other “things”, which traditionally have not been Internet enabled.

This “Internet of Things” (IoT) represents a remarkable transformation of the way in which our world will soon interact. Much like the World Wide Web connected computers to networks, and the next evolution mobile devices connected people to the Internet and other people, IoT looks poised to interconnect devices, people, environments, virtual objects and machines in ways that only science fiction writers could have imagined. In a nutshell the Internet of Things (IoT) is the convergence of connecting people, things, data and processes; it is transforming our life, business and everything in between. This book *Secure and Smart IoT* explores many aspects of the Internet of Things and explains many of the complicated principles of IoT and the new advancements in IoT including using Fog Computing, AI and Blockchain technology.

This book is divided into 6 parts:

Part 1: What Is IoT?

Part 2: IoT Implementation & Standardization Challenges

Part 3: Securing IoT

Part 4: AI, Fog Computing and IoT

Part 5: The Future of IoT

Part 6: Inside Look at Blockchain

Audience

This book is for everyone who would like to have a good understanding of IoT and its applications and its relationship with business operations

including: C-Suite executives, IT managers, marketing & sales people, lawyers, product & project managers, business specialists, students. It's not for programmers who are looking for codes or exercises on the different components of IoT.

Acknowledgment

I am grateful for all the support I received from my family during the stages of writing this book, thank you all!

List of Figures

Figure 2.1	IIoT Challenges.	10
Figure 2.2	IIoT Requirements.	10
Figure 2.3	IIoT Benefits.	11
Figure 4.1	IoT Key Attributes.	22
Figure 6.1	Three Major Challenges Facing IoT.	36
Figure 6.2	Technological Challenges Facing IoT.	36
Figure 6.3	Categories of IoT.	42
Figure 7.1	Components of IoT implementation.	46
Figure 7.2	New trends of sensors.	47
Figure 8.1	Hurdles facing IoT standardization.	54
Figure 8.2	Components of IoT implementations.	56
Figure 9.1	Challenges facing IoT analytics.	60
Figure 9.2	AI and IoT Data Analysis.	64
Figure 10.1	IoT architecture.	70
Figure 11.1	Advantages of Blockchain.	81
Figure 12.1	Challenges of Blockchain in IoT.	89
Figure 12.2	Risks of using Blockchain in IoT.	90
Figure 13.1	How to prevent future attacks.	98
Figure 15.1	Challenges facing AI in IoT.	112
Figure 16.1	Digital Transformation Areas.	116
Figure 17.1	Future Trends of IoT.	121
Figure 18.1	Types of Blockchains.	131
Figure 19.1	Advantages of Using Blockchain in Cybersecurity.	140
Figure 19.2	Disadvantages of Using Blockchain in Cybersecurity.	142
Figure 20.1	Tracks of Blockchain Technology.	146
Figure 20.2	Blockchain Technology Future Trends.	147

List of Abbreviations

AI	Artificial Intelligence
BYOD	Bring Your Own Device
CEP	Complex Event Processing
CSA	Cloud Security Alliance
DDoS	Distributed Denial of Service
DoS	Denial of Service
DX	Digital Transformation
E-a-a-S	Elevator as a Service
ETL	Extract, Transform and Load
FIPP	Fair Information Practice Principles
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronics Engineering
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISA	International Society of Automation
ISOC	Information Security Operations Center
IT	Information Technology
L-a-a-S	Lighting as a Service
LAN	Local Area Network
Li-Fi	Light Fidelity
LTE	Long-Term Evolution
M2H	Machine to Human
M2M	Machin to Machine
MAN	Merto Area Network
OEM	Original Equipment Manufacturer

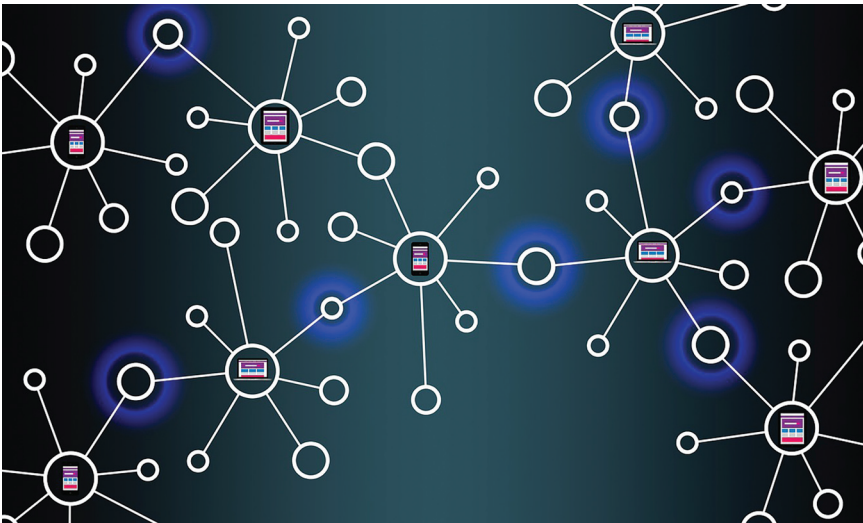
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PSS	Privacy, Security, Safety
R-a-a-S	Rail as a Service
SaaS	Software as a Service
UI	User Interface
UX	User Experience
VUI	Voice User Interface
W3C	World Wide Web Consortium
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
ZTM	Zero Trust Model

PART I

What Is IoT?

1

Internet of Things: The Third Wave?



The Internet of Things (IoT) is the network of physical objects accessed through the Internet. These objects contain embedded technology to interact with internal states or the external environment. In other words, when objects can sense and communicate, it changes how and where decisions are made, and who makes them, for example, Nest thermostats.

The Internet of Things (IoT) emerged as the third wave in the development of the Internet. The Internet wave of the 1990s connected 1 billion users, while the mobile wave of the 2000s connected another

2 billion. The IoT has the potential to connect 10 times as many 20 billion “things” to the Internet by 2020, ranging from bracelets to cars [17]. Breakthroughs in the cost of sensors, processing power and bandwidth to connect devices are enabling ubiquitous connections at present. Smart products like smart watches and thermostats (Nest) are already gaining traction as stated in the Goldman Sachs Global Investment Research report.

IoT has key attributes that distinguish it from the “regular” Internet, as captured by Goldman Sachs’s S-E-N-S-E framework: *Sensing, Efficient, Networked, Specialized, Everywhere* [1]. These attributes may change the direction of technology development and adoption, with significant implications for Tech companies – much like the transition from the fixed to the mobile Internet shifted the center of gravity from Intel to Qualcomm or from Dell to Apple.

A number of significant technology changes have come together to enable the rise of the IoT. These include the following [1]:

- *Cheap sensors* – Sensor prices have dropped to an average 60 cents from \$1.30 in the past 10 years.
- *Cheap bandwidth* – The cost of bandwidth has also declined precipitously, by a factor of nearly 40 times over the past 10 years.
- *Cheap processing* – Similarly, processing costs have declined by nearly 60 times over the past 10 years, enabling more devices to be not just connected, but smart enough to know what to do with all the new data they are generating or receiving.
- *Smartphones* – Smartphones are now becoming the personal gateway to the IoT, serving as a remote control or hub for the connected home, connected car or the health and fitness devices that consumers have increasingly started to wear.
- *Ubiquitous wireless coverage* – With Wi-Fi coverage now ubiquitous, wireless connectivity is available for free or at a very low cost, given Wi-Fi utilizes unlicensed spectrum and thus does not require monthly access fees to a carrier.

- *Big Data* – As the IoT will, by definition, generate voluminous amounts of unstructured data, the availability of Big Data analytics is a key enabler.
- *IPv6* – Most networking equipment now support IPv6, the newest version of the Internet Protocol (IP) standard that is intended to replace IPv4. IPv4 supports 32-bit addresses, which translates to about 4.3 billion addresses – a number that has become largely exhausted by all the connected devices globally. In contrast, IPv6 can support 128-bit addresses, translating to approximately 3.4×10^{38} addresses – an almost limitless number that can amply handle all conceivable IoT devices.

1.1 Advantages and Disadvantages of IoT

Many smart devices like laptops, smart phones and tablets communicate with each other through the use of Wi-Fi Internet technology. Transfer these technological capabilities into ordinary household gadgets like refrigerators, washing machines, microwave ovens, thermostat, door locks among others; equip these with their own computer chips, software and get access to the Internet, and a “smart home” now comes to life.

The Internet of Things can only work if these gadgets and devices start interacting with each other through a networked system. The AllJoyn Open Source Project [2], a nonprofit organization devoted to the adoption of the Internet of Things, facilitates to ensure that companies like Cisco, Sharp and Panasonic are manufacturing products compatible with a networked system and to ensure that these products can interact with each other.

The advantages of these highly networked and connected devices mean productive and enhanced quality of lives for people. For example, health monitoring can be rather easy with connected RX bottles and medicine cabinets. Doctors supervising patients can monitor their medicine intake as well as measure blood pressure and sugar levels and alert them when something goes wrong to their patients online.

In the aspect of energy conservation, household appliances can suggest optimal setting based on the user's energy consumption like turning the ideal temperature just before the owner arrives home as well as turning on and off the lights whenever the owner is out on vacation just to create the impression that somebody is still left inside the house to prevent burglars from attempting to enter.

Smart refrigerators, on the other hand, can suggest food supplies that are low on inventory and needs immediate replenishment. The suggestions are based on the user's historical purchasing behavior and trends. Wearable technology are also part of the Internet of Things, where these devices can monitor sleeping patterns, workout measurements, sugar levels, blood pressure and connecting these data to the user's social media accounts for tracking purposes.

The most important disadvantage of the Internet of Things is with regard to the privacy and security issue. Smart home devices have the ability to devour a lot of data and information about a user. These data can include personal schedules, shopping habits, medicine intake schedule and even location of the user at any given time. If these data fall are misused, great harm and damage can be done to people.

The other disadvantage is the fact that most devices are not yet ready to communicate with another brand of devices. Specific products can only be networked with their fellow products under the same brand name. It is good that The AllJoyn Open Source Project [2], is ensuring connectivity, but the reality of a "universal remote control" for all these devices and products is still in its infancy.