Preface

Internet of Things (IoT) is the booming technology conquering the technologically compressed ball, the Globe. Changes are inevitable even to a common man in his daily activities and the technology is not exempted. Technology, exempted from vagaries will become extinct. Before Cloud computing conceals the globe, IoT swallowed the globe and cloud. IoT incorporates everything under the umbrella of Internet. 5G under study could provide the expected speed and along with IPv6 could enrich IoT to a better podium. At the same time IoT flags flap, intruders try to invade. Propaganda of IoT with its Quality of Service will also drive the researcher to focus on security breaches. IoT provides services to all the sectors including healthcare, vehicular network, industrial trades, Education, locating, tracking and monitoring household, smart cities etc. Exponential increase in the number of devices and the connectivity among them warns the IoT developers about the precautions to be measured on the data stored and retrieved.

Medical transcription in IoT can save the human life during emergencies. None will carry all the medical data always. In case of an accident, the stored data can be retrieved by the doctors and the current condition of the patient can be studied without undergoing multiple preliminary lab tests. At the same time, database should not be accessed by an ill-legitimate. Hence the intended or unintended security breach should be analyzed and an appropriate authentication and authorization mechanisms has to be deployed at the right ratio to protect the data. IoT in transportation is again a flair to track and monitor the smart vehicles. But if the speed of the vehicle is controlled and operated by an intruder, it would lead to malicious behavior.

IoT architecture has been proposed in multiple versions by different experts. IoT comprises many devices and layers. Each device has its own security concerns to be addressed and mitigated to avoid unsolicited activities.

Bursty growth, in Internet of Things (IoT) towards the peak, from the floor is owed by the ease of connectivity. Anything and everything can interconnect and communicate with each other in a smarter way. Devices became smarter, with embedded sensors make every device to talk and operate without human intervention. IoT can be deployed in all real time basic amenities, be it a child care, health care, appliances control, city surveillance or environmental change. IoT could make the human life simple and stress free but not threat free.

Fascinating features of IoT are devices can trigger a warning signal in an emergency situation, vehicles can be auto controlled, electrical appliances can be operated remotely and many more. Threat arises here, who is going to receive and respond to the emergent warning signal, the intended or the attacker. We are happy about automobile control with no think on what happens when the vehicle is controlled by an attacker.

Apart from invaders, illegal users, and misnomers IoT can also be faded away by the signals it receives from. IoT operations wholly depend on the signals received from sensors. Accuracy of sensor signal may be verified and confirmed with redundant sensors, leads to ambiguous values. Hence, IoT should focus on both precision, QoS and threats, Security.

We hope timely publication of this title could serve as an essential reference source, building on the available literature in the field of smart networks, IoT everywhere. It is trusted that this text will provide the resources necessary for students, academia, researchers and industrial experts those who always expect and experience technical challenges.

This book tries to analyze different IoT architecture versions and all possibilities of security breaches in detail. This book carries 10 chapters that address: (1) IoT Architecture; (2) Security Perspectives in IoT: Current Issues and Trends; (3) Security in Network Layer of IoT: Possible Measures to Preclude; (4) Security in Application Layer Protocols of IoT: Threats and Attacks; (5) Security in IoT Devices; (6) Security Threats in Autonomous Vehicles; (7) Intelligent Digital Forensics in the Era of IoT; (8) Mechanisms to Secure Communications in the IoT; (9) IoT in Healthcare: Breaching Security Issues; (10) A Contemplator on Topical Image Encryption Measures.

Chapter 1 discusses the importance of Internet of Things in various application areas. It has been elucidated that how IoT can be used effectively in the smart wireless networks. Most of the devices used in the IoT system are of sensor and actuator devices. The architectural model and communication layout of IoT is explicated through appropriate diagrams.

Chapter 2 focuses on the literature review through a thorough literature consolidation of the IoT and security perspectives. The extensive literature of the IoT and security perspectives provides a contribution to practitioners and researchers by revealing the issues and trends with the IoT and security perspectives in order to enhance organizational performance and reach strategic goals in global operations.

Chapter 3 lights upon the threats in the network layer of IoT, the new objects that enter the network are configured automatically. This characteristic makes IoT highly susceptible to security threats such as Disruption and Denial of Service (DoS), eavesdropping, problems in authentication and physical attacks on devices in different forms, are most common.

Chapter 4 uncovers the cyber-attacks, cyber threats at the application layer and provide the control mechanism or guidelines to combat cyber-attacks, especially in the application layer.

Chapter 5 provides a general survey of the prevailing attack types along with analysis of the underlying structures that make these attacks possible, which would help researchers in understanding the DDoS problem better.

Chapter 6 aims to examine the vulnerability of the systems present inside an autonomous vehicle, and propose solutions to the same. Currently, no official standards exist for the secure functioning of an autonomous vehicle, apart from the 'guidelines' released by the US DOT.

Chapter 7 introduces of internet of things (IoT) forensics, IoT application in forensics field. Art-of-states for IoT forensics are provided. The issues for IoT forensics are identified. Also, introduced the proposed data classification in IoT forensics protocol.

Chapter 8 focuses on existing protocols and different proposed mechanisms in literature to secure communications in the IoT.

Chapter 9 focuses on security by design: better collaboration among industry; manufacturers, regulators, and medical practitioners; a change in the regulatory approval paradigm, and encouraging feedback from patients and families who directly benefit from these devices.

Chapter 10 analyses the image encryption mechanisms which could help in healthcare record transmissions.

Hence, this book could attract academicians, researchers, advanced-level students, technology developers, and curriculum designers.