Chapter 3
Consumer Trust, Security, and Ethical Considerations in IoT Markets

Nitika Malik
http://orcid.org/0009-0006-3991-9526
Maharshi Dayanand University, India

Shivangi Rapria
http://orcid.org/0009-0002-2778-8443
Institute of Management Studies and Research, India

Dinesh Aleria
http://orcid.org/0009-0006-1289-1850
Institute of Management Studies and Research, India

Mohit Sharma
http://orcid.org/0009-0007-2280-8077
Institute of Management Studies and Research, India

ABSTRACT

The Internet of Things (IoT) is revolutionizing industries by enhancing connectivity and consumer experiences. However, widespread adoption is hindered by concerns over consumer trust, primarily due to security vulnerabilities, data privacy issues, and ethical dilemmas. This chapter explores the foundational elements of trust in IoT environments, focusing on transparency, cybersecurity, regulatory compliance, and corporate digital responsibility. It examines how breaches and ethical lapses undermine user confidence and emphasizes the importance of transparent data practices

DOI: 10.4018/979-8-3373-3441-7.ch003

and responsible AI use. Consumer psychology is also addressed, illustrating how perceptions of risk, control, and accountability shape trust. The chapter provides an in-depth analysis of security challenges inherent in interconnected IoT systems, highlighting vulnerabilities that cybercriminals exploit. Through case studies, it reviews common threats and presents best practices, including robust cybersecurity frameworks, encryption, and risk mitigation techniques.

INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative innovation across various industries, allowing interconnected devices to communicate, exchange data, and automate processes with remarkable efficiency. Its applications extend to diverse domains such as smart homes, healthcare, transportation, agriculture, and industrial automation, positioning IoT as a key driver of how societies function, how businesses create and deliver value, and how consumers engage with their surroundings. However, the widespread adoption and long-term success of IoT systems depend largely on one essential factor: consumer trust. In the absence of trust—particularly in the areas of data security, privacy, and ethical handling of information—consumers may hesitate to adopt or continue using IoT technologies, hindering the overall development and sustainability of this dynamic ecosystem (Lee & Lee, 2015; Roman et al., 2013). Consumer trust in IoT is influenced by a multifaceted combination of technological, psychological, legal, and ethical factors. While IoT promises enhanced convenience, personalization, and operational efficiency, it simultaneously introduces significant risks such as data breaches, unauthorized surveillance, algorithmic bias, and misuse of sensitive personal data (Weber, 2010; Zeng et al., 2017). These challenges are not hypothetical—real-world incidents, including the Mirai botnet attack that exploited security vulnerabilities in IoT devices, have demonstrated the fragility of existing systems and weakened public confidence in their safety (Antonakakis et al., 2017). As IoT technologies continue to integrate more deeply into daily life, establishing transparent, secure, and ethically responsible frameworks has become a critical imperative for ensuring both consumer protection and sustained technological progress.

The Evolution and Impact of IoT on Consumers

The proliferation of IoT has accelerated rapidly, with billions of devices currently connected worldwide and projections indicating exponential growth in the coming years. According to Statista (2023), the number of connected IoT devices is expected to surpass 30 billion by 2030. From wearable fitness trackers and voice assistants to