Chapter 6
Advanced Cybersecurity and Surveillance in 5G and IoT Ecosystems

Megha Agarwal
https://orcid.org/0000-0002-6300-4207
Department of Computer Science and Information Systems, Shri Ramswaroop Memorial University, India

Vinayak Shukla
Computer Science and Engineering Department, BBDNITM, Lucknow, India

Mritunjay Rai
Department of Electrical and Electronics Engineering, Shri Ramswaroop Memorial University, India

Rajveer Mathur
Department of AI ML Engineering WILP Division, Bila Institute of Technology and Science, Pilani, India

ABSTRACT

The unexpected rise of 5G and IoT technologies has changed communication networks creating unprecedented levels of connectivity. The existing security frameworks often fail to meet these threats, due in part to a lack of scalability and intelligence to address the issues in the 5G-IoT ecosystems. Frequently, key areas of real-time threat identification, device-level security, and data integrity are neglected. The proposed chapter addresses these gaps by applying advanced cybersecurity and surveillance technologies to 5G and IoT environments. Our intention is for these technologies to incorporate machine learning, real-time analyzed, and blockchain, in our efforts to enhance current surveillance systems and improve current cybersecurity principles and practices. AI-driven solutions would remove human dependency and provide a better level of security for IoT devices. This effort demonstrates a bridge between theoretical cybersecurity concepts and real-world applications, allowing us to move the field forward and into the important conversation of a more secure digital future.

DOI: 10.4018/979-8-3373-4277-1.ch006

1. INTRODUCTION

The explosive expansion of 5G technology and the Internet of Things (IoT) have transformed connectivity by allowing previously unrealistic amounts of communication between billions of devices on a single network. This advancement has provided opportunities for exciting new developments in industries like autonomous systems, smart cities, telemedicine, and industrial automation, to name just a few. However, the increasing quantity of connected devices increases the potential for exposure to cyber threats. Numerous IoT devices are inadequately secure and thus become a very simple target for cybercriminals while 5G networks, with their super connections, ultra-deep visibility, and sub-five-millisecond latency, create an entire new level of security challenges with connected devices. Cybersecurity threats such as Distributed Denial of Service (DDoS) attacks, espionage, data breaches, and AI-based attacks can impede personal privacy or jeopardize national security. To mitigate these risks, we need improved cybersecurity solutions involving AI, blockchain, and quantum-resistant capabilities as old security methods cannot keep up with evolving infiltration methods. In this chapter, we address salient security issues in the 5G and IoT (Plata et al., 2023) ecosystems and develop innovative concepts for 1) implementing cybersecurity and surveillance, and 2) creating an effective and secure cybersecurity ecosystem to the next generation of wireless communication by using AI-based threat detection, blockchain security, and privacy technology.

The combination of IoT and 5G has made great strides in areas such as healthcare, transportation, and smart cities by enabling quicker, smarter communication systems that provide significant utility to enterprises. Unfortunately, these utility benefits also create significant security concerns. The decentralized nature of 5G (multiple edge computing capabilities, network slicing, etc.) will require organizations to rethink aspects of their traditional security strategy. Furthermore, the lack of secure implementations that many IoT devices face creates a serious security concern, leaving them open to DDoS attacks, data breaches, data corruption, and unauthorized access. All of the lockdown security systems designed for their data centers, which rely heavily on cloud infrastructure and connected networking systems, are equally at risk. Over the last several years, cyber threat actors have become increasingly sophisticated, with some hijacking surveillance systems through the use of AI and other tools, while others launch hacked ransomware attacks on entire cities or capture and leverage zero-day vulnerabilities. Addressing the [IoT & 5G] risks posed by expected attacks represents a significant shift from traditional solutions. For example, organizations must embrace the use of adaptive security solutions (GDPR, NIST cybersecurity framework, etc.) in order to protect data and infrastructure in a rapidly evolving landscape.

Objectives and Scope

The convergence of 5G (Chen et al., 2021) and IoT is helping to revolutionize environments with reliable, quicker, real-time communication for innovative smart infrastructure, digital healthcare systems, and automated industries. The above effective connectivity also poses greater cybersecurity risks, which require protection strategies that are adaptive and offered as advanced features.

The objective are listed below:

- Leveraging Network Slicing:

Project Management Practices and Project Manager Traits as a Key to Successful Information Systems Implementation
Evon M.O. Abu-Taieh, Jeihan M. Abu-Tayehand Alia Abu-Tayeh (2011). *International Journal of Aviation Technology, Engineering and Management (pp. 37-51).*
www.irma-international.org/article/project-management-practices-project-manager/58945

Project Management Practices and Project Manager Traits as a Key to Successful Information Systems Implementation
Evon M.O. Abu-Taieh, Jeihan M. Abu-Tayehand Alia Abu-Tayeh (2011). *International Journal of Aviation Technology, Engineering and Management (pp. 37-51).*
www.irma-international.org/article/project-management-practices-project-manager/58945