Abstract

The exponential growth of Internet of Things (IoT) devices has introduced significant security challenges, particularly in securing token-based communication protocols used for authentication and authorization. This survey systematically reviews the vulnerabilities in token transmission within IoT environments, focusing on various sophisticated attack vectors such as replay attacks, token hijacking, man-in-the-middle (MITM) attacks, token injection, and eavesdropping among others. These attacks exploit the inherent weaknesses of token-based mechanisms like OAuth, JSON Web Tokens (JWT), and bearer tokens, which are widely used in IoT ecosystems for managing device interactions and access control. The impact of such attacks is profound, leading to unauthorized access, data exfiltration, and control over IoT devices, posing significant threats to privacy, safety, and the operational integrity of critical IoT applications in sectors like healthcare, smart cities, and industrial automation. This paper categorizes these attack vectors, explores real-world case studies, and analyzes their effects on resource-constrained IoT devices that have limited processing power and memory, rendering them more susceptible to such exploits. Furthermore, this survey presents a comprehensive evaluation of existing mitigation techniques, including cryptographic protocols, lightweight secure transmission frameworks, secure token management practices, and network-layer defenses such as Transport Layer Security (TLS) and multi-factor authentication (MFA). The study also highlights the trade-offs between security and performance in IoT systems and identifies key gaps in current research, emphasizing the need for more scalable, energy-efficient, and robust security frameworks to address the evolving landscape of token transmission attacks in IoT devices.