Cybersecurity Challenges in Power Sector: Analysis of DoS and MITM Attacks

Rudrasinh H Rajput
Ph.D. Scholar, National Forensic Sciences University, Gandhinagar, Gujarat, India
Junior Scientific Officer, Centre of Excellence in Cyber Security, National Forensic Sciences University, Gandhinagar, Gujarat, India

Dr. Jay Teraiya
Associate Professor, Department of School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, India

Abstract

Modern power systems are changing very fast with the increasing integration of Information and Communication Technologies (ICT) into power sector. This has significantly improved the efficiency of power system operation and monitoring, allowing for the effective management of electricity generation, transmission, and distribution. Nevertheless, with the rising level of interconnectedness and reliance on digital communication in smart grid operation, there is also the rising threat of potential cyber security risks that may impact power system operation. The most critical of all cyber-attacks in power sectors are Denial of Service (DoS) and Man in the Middle (MITM) attacks. DoS attacks are focused on overwhelming the network infrastructure in order to deny authorized users access to critical services. On the other hand, MITM allows attackers to intercept and/or monitor communications between devices on the network. These cyber-attacks can be launched on essential cyber-physical power system infrastructure, which includes Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Phasor Measurement Unit (PMU), communication systems, and Distributed Energy Resources.

This research aims to provide a narrative literature review that aims to examine the occurrence of DoS and MITM attacks in smart grid systems, methods of performing these attacks, and their possible impacts on smart grid system efficiency and reliability. In addition, it aims to compare both types of attacks based on their characteristics and operational impact and possible difficulties in detecting them. Lastly, it aims to examine various mitigation techniques, which include intrusion detection systems, secure communication protocols, artificial intelligence-based monitoring techniques, and blockchain technology, which can be applied to cybersecurity in power sector systems.

Keywords

Cybersecurity, Cyber-attacks, Power system.