ID 587

Enhancing IoT Security: A Framework for Mitigating Vulnerabilities in Industrial Systems

MI Sathsara[1#], A Kurunayaka[1], and R Laveena[1]

[1]Department of Biosystem Technology, Faculty of Technology, General Sir John Kotelawala Defence University, Sri Lanka

[#]40-ict-0003@kdu.ac.lk

IoT-based systems have revolutionized various sectors by improving efficiency and decision-making. However, the increased interconnectivity and complexity have heightened security concerns, including vulnerabilities in communication protocols, inadequate encryption, and insufficient access control mechanisms, risking sensitive data and system integrity. This study proposes a comprehensive security framework tailored for IoT-based systems in industrial environments. By integrating advanced encryption, authentication protocols, and intrusion detection systems this study attempted to develop effective security mechanisms and strategies that can be integrated into IoT-based systems to mitigate potential security threats. The foundation for creating strong security measures that will protect IoT-based systems against various cyberattacks be the outcome of this study. A specific testing environment, utilizing specific tools/technologies, for example, simulated IoT networks and real-time monitoring tools, will be developed to evaluate the effectiveness of the proposed security measures against potential cyberattacks. The suitability and flexibility of the many suggested security improvements in a range of IoT-based systems are further confirmed by case studies. The benefits and drawbacks of the suggested security methods are illustrated by the outcomes of experiments and case studies. In conclusion, this study contributes to the enhancement of security in modern IoT-based systems by providing effective mechanisms to address critical vulnerabilities and enhance system reliability. By implementing these security enhancements, the study provides a framework that ensures the confidentiality, integrity, and availability of data in IoT systems, minimizing risks and enhancing system reliability. These findings have the potential to influence future IoT system designs and contribute to the development of industry-wide security standards.

Keywords: *IoT security, encryption algorithms, vulnerability mitigation, data integrity, Authentication Protocols*