An Efficient Mitigation Plan to Encounter Various Vulnerabilities in Internet of Things Enterprises

Authors : Umesh Kumar Singh, Abhishek Raghuvanshi, Suyash Kumar Singh

Abstract : As IoT networks gain popularity, they are more susceptible to security breaches. As a result, it is crucial to analyze the IoT platform as a whole from the standpoint of core security concepts. The Internet of Things relies heavily on wireless networks, which are well-known for being susceptible to a wide variety of attacks. This article provides an analysis of many techniques that may be used to identify vulnerabilities in the software and hardware associated with the Internet of Things (IoT). In the current investigation, an experimental setup is built with the assistance of server computers, client PCs, Internet of Things development boards, sensors, and cloud subscriptions. Through the use of network host scanning methods and vulnerability scanning tools, raw data relating to IoT-based applications and devices may be collected. Shodan is a tool that is used for scanning, and it is also used for effective vulnerability discovery in IoT devices as well as penetration testing. This article presents an efficient mitigation plan for encountering vulnerabilities in the Internet of Things.

Keywords : internet of things, security, privacy, vulnerability identification, mitigation plan
Conference Title : ICCSCIT 2025 : International Conference on Computer Science, Cybersecurity and Information Technology
Conference Location : Washington, Australia
Conference Dates : April 22-23, 2025