CYBER SECURITY AND INTERNET OF THINGS

Abstract:

The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. The unconscious use, not changing passwords, and the lack of device updates have increased cyber security risks and access to malicious applications to the IoT systems' sensitive data. Such inappropriate security practices increase the chances of a data breach and other threats. Most of the security professionals consider IoT as the vulnerable point for cyber-attacks due to weak security protocols and policies. Even though several security mechanisms were developed to protect IoT devices from cyber-attacks, security guidelines are not appropriately documented. Thereby, end-users could not utilize protective measures to avert data attacks.

Existing Method:

Currently, objects and systems are empowered with network connectivity and have the computing power to communicate with similar connected devices and machines. Expanding the network capabilities to all possible physical locations will make our life more efficient and help us save time and money. However, connecting to the Internet also means to communicate with potential cyber threats. Internet-enabled products become a target for cybercriminals.