IIoTShield: Securing Industrial IoT Networks with a Hierarchical Authentication and Session Key Generation Mechanism

Abstract

Industrial Internet of Things (IIoT) has transformed industries by enabling seamless data collection, storage, and communication to enhance efficiency, safety, quality, and sustainability. However, IIoT networks face critical challenges, including device interoperability, heterogeneous environments, and security concerns such as unauthorized access, intrusion, and data breaches. Traditional authentication mechanisms often rely on complex cryptographic operations or fail to address timeliness and security comprehensively, resulting in vulnerabilities to attacks and system inefficiencies. These drawbacks, coupled with significant computational, communication, and energy overheads, hinder the widespread adoption of IIoT systems. To address these challenges, this project proposes a lightweight and robust device authentication mechanism and session key generation scheme for IIoT networks. The proposed system organizes devices into a hierarchical structure comprising devices, intermediate nodes, and a central server. By utilizing efficient operations such as one-way hash functions, bitwise XOR, and concatenation, the mechanism ensures secure authentication while minimizing overhead. During deployment, authentication parameters are pre-stored, and session keys are dynamically generated using random values and identifiers without exposing sensitive data. This ensures confidentiality, integrity, and resistance to known security attacks. The proposed solution outperforms existing methods by eliminating illegitimate device access, ensuring timely and secure communication, and providing a scalable framework for secure IIoT operations. It addresses critical security requirements while being lightweight, making it an ideal choice for real-time industrial applications.

Software and Packages

- **Programming Language**: Python 3.8 or later
- **Python Libraries**: NumPy, Pandas, Matplotlib, Scikit-learn
- **Cryptography Libraries**: PyCryptodome (for implementing security measures)
- **Database**: MySQL (for storing device authentication parameters, session keys, and logs)
- **Web Framework**: Flask (for building the web-based interface and device communication)
- **Authentication Libraries**: Hashlib (for implementing one-way hash functions used in device authentication)