CSE3501

Information Security Analysis and Audit

J-Component Review-1

Quantum Cryptography to secure

Cyber Physical Systems

Performed Under:

Dr. Sendhil Kumar K.S

Associate Professor Grade 1 (SCOPE)

Team members:

- Moitrish Sinha 18BCE0617
- Abhinav 18BCE0641
- Shaik Haseeb Ur Rahman 18BCE0646
- Lakshit Dua 18BCE0824

Abstract:

Cyber-physical systems (CPSs) refers to the tight conjoining of and coordination between computational and physical resources. Some of the CPSs are smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics. CPSs will be deployed for decades, thus they should be secure against malicious cyberattacks. Quantum cryptography is one of the emerging topics in the field of the computer industry. Quantum Computers have made it easier to crack existing cryptography techniques. Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. Thus, on this project we will try to apply Quantum cryptography on the Cyber-physical systems in order to make them more secure.

Methodology:

In this project, we will apply Quantum cryptography on the Cyber-physical systems in order to make them more secure. Using Quantum Key Exchange, the keys can be exchanged over a network and connection can be secured. Since Cyber-Physical Systems require hardware implementation, in this project we will be proposing only a certain architecture. This architecture will explore how to provide security or how to create a secure communication channel for a Cyber-Physical System or between multiple systems.

Quantum Cryptography involves sending photons from where according to the spin or the configuration, the procedure is further carried on. This also cannot be practically carried out so instead of that, we will be including an algorithm for demonstration purposes.

To illustrate the application of Quantum Cryptography on the Cyber-Physical System, firstly we will create an algorithm for Quantum Cryptography in python. Next, for a dummy Cyber Physical System, which can either be one to one or one to many, we can create a client-server system. For one to one system, we can have one client and one server. Similarly, for one to many, one server and multiple clients. So, when the client(s) request the server for any data, it can be sent directly. But for the communication to be secure we will import the Quantum Cryptography code for the servers as well as the clients. Using the imported code, we will encrypt the data that the server is sending and decrypt it at the client end. Likewise, if the client wishes to send data to the server, the same encryption will be applied.
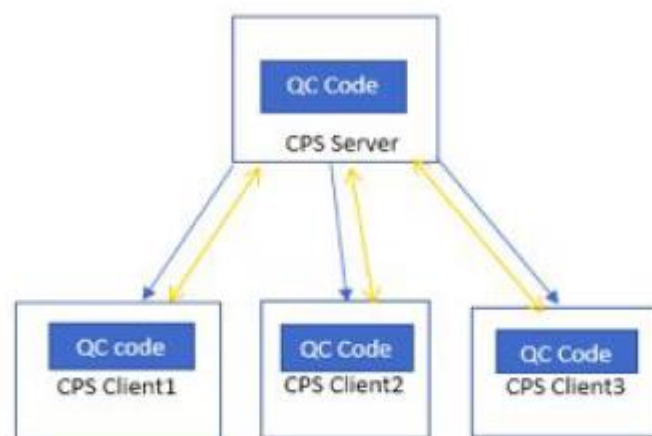
Tools:

- Python 3.7
- PyCharm IDE

Modules:

- **Client Module:**
  Emulation of a CPS device that is to be connected to server and in network to other similar devices. Basically, a node in the network grid of multiple CPS devices communicating with server.
- **Server Module:**
  Responsible for supplying instructions (in real-time applications) to CPS devices. Here, the server will act as a hub for communication between the devices.
- **Encryption/Decryption Module:**
  Algorithm that will act as middle-ware between the server and client device (and vice-versa) and encrypt/decrypt outgoing/incoming messages with quantum algorithm.