

The initial report for a dissertation to be submitted in partial fulfillment
of a University of Greenwich Masters Degree

Design and Development of IoT Security system for Cyber Security Exercise System using Blockchain Technology

Name: Panaganti Saiteja Reddy

Student ID: 001212172

Program of Study: MSc in Computer Science (Network Engineering)

Initial Report

Date Proposal Submitted: 08-06-2022

Project Hand-In Date: 25-06-2022

Supervisor: Dwijen Shilu

The Initial Report

I am presently learning the in-depth concepts of blockchain and IoT Technologies. The CyExec, Assuming the introduction of higher education institutions and small and medium-sized businesses, is the exercise system to learn the fundamental strategies of cyber-attack and defense. The characteristics of the CyExec include

- Highly portable exercise environment with low cost
- An exercise environment of proper flexible development and resource utilization.
- Not only suitable for the single organization but also for related organizations.

Hence, our designed system should possess the above specifications.

The next part of the project is integrating IoT Technology with the proposed CyExec.

Depending on the configuration of the lowest layer, the IoT system architecture can be divided into three types.

(1) Data processing issues with IoT devices. Without being processed, the collected data is sent through the IoT gateway to cloud computing. For instance, there are weather sensors and computerized water temperature systems. Install IoT devices into an IoT area network made up of close-range communications, like wireless LAN and Bluetooth.

(2) IoT gadgets are unable to process data. Data is processed by an edge server before being sent to a cloud computer. There are systems for managing products that use IC tags or smart appliances, for instance.

(3) An IoT device serves as an edge server and processes data that has been collected. The data that has been processed is delivered to cloud computing. Network cameras and multi-function printers are two examples.

Therefore, based on the pre-survey conducted through port scanning and the data gathered, we would like to create a scenario in which a backdoor is installed utilizing the FTP server's vulnerability. Also, by integrating Metasploitable2 with Kali Linux, CyExec users can independently create the fundamental exercises they require.

The key objectives of the proposed project are

1. To learn how blockchain technology controls the IoT
2. To implement a highly portable exercise environment at a low cost using Blockchain for IoT
3. To create an environment conducive to proper development and utilization. CyExec improves exercise program implementation through collaborative development and use of not only a single organization but also a related organization.
4. In order to rejoin development and use by multiple higher education institutions, it is necessary to efficiently develop and use exercise programs between different institutions. The basic exercise part aims to learn essential vulnerability detection and countermeasures using WebGoat.
5. To learn the attack method while conducting IoT security exercises, I would like to create a scenario in which a backdoor is installed by exploiting a vulnerability in the FTP server based on the pre-survey by port scanning and the survey information. Furthermore, CyExec users can create their own basic exercises by combining Metasploitable2 and Kali Linux.

We will be assumed to implement the system in such a way that the machine is connected to the network, and that the administrator can log in remotely and update the display contents using HTTP communication. By simulating images stored by digital signage devices and presenting them against the user's wishes, the student will practice cyberattacks and defense by changing the passwords on these devices without authorization (administrator).

1. Current situation

At present, I am presently learning the in-depth concepts of blockchain and IoT Technologies. The literature on various concepts of IoT and Blockchain was done. Raj et al. [1] describe recent proposals for such systems. The authors established a basic blockchain-based communication system between two smart devices. They use the Ethereum blockchain to provide all of the communication system's security benefits.

I came to know the principle of CyExec. It is an exercise system for learning the fundamentals of cyber-attack and defense. I want to develop with the inclusion of higher education institutions and small and medium-sized businesses. I will complete this task by utilizing container technology such as Docker. Therefore, I am learning now how the Docker technology integrates with IoT and Blockchain.

- I gained knowledge on Blockchain technology and the integration with IoT. I have made literature with many available textbooks, websites, and internet sources too.
 - At last, I employed a hardware platform such as Raspberry Pi for the development of this project with the Linux platform.
 - To use CyExec, I learned how to install CyExec on PCs and then run OWASP-created attack exercise environment containers within CyExec and on Docker.

2. Problem Areas

Till now no critical factors are not identified to develop this project. This project will be developed on time without any further extension. If any difficulties are identified I won't hesitate to notify the corresponding problem to my supervisor. I am expecting that there will be a problem arising at the implementation of CyExec. "When the attacker wishes to install the attack file on the trap server, sends a hyperlink linked the attack file to the user (administrator) who logged in to digital signage. When the user clicked the link, the attacker (learner) performs exercises of exploiting CSRF vulnerabilities to change passwords and falsification of the display images." The implementation of this scenario will arise a problem.

Based on the possibility and situation I may alter changes or make some kind of notice to the supervisor and wait for his valuable suggestions.

3. Key work during the next period

I expected to complete this project within six (July 22-Sept 22) months. During the initial 2 weeks, I will learn the concepts related to in-depth knowledge of this project. In the next upcoming weeks, I planned to implement the project and write the dissertation part. The hardware implementation of the project may little difficult, since, I am very new to using embedded hardware circuits. This is the only stage that may deviate according to the expected time frame. Integrating the designed IoT with Blockchain techniques is a little bit risky. This may lead to making me deviating from the original proposal and plan. But, With proper plan and execution, the risk in the project can be achieved and I have confidence that I can successfully implement this project within a time frame.