Blockchain-based Architecture for Interdomain Cybersecurity Research

[1]Oluwaseyi Ajayi, [1]Tarek Saadawi, [2]Kenichi Kourai and [2]Masato Tsuru

[1] City University of New York, City College (CCNY), New York, USA and [2]Kyushu Institute of Technology, Japan.

Overview: We designed and developed a novel application that applies blockchain technology in cybersecurity. This architecture allows different companies to come together to promptly exchange cyberattack information in a secure way to detect coordinated or distributed attacks. In addition to this, the architecture allows the public node to connect to the blockchain network and retrieve the stored attack information in real-time. The processes involved in exchanging the attack information are: (i) extraction of the attack information, (ii) preparing and submitting it as transactions to a blockchain network, (iii) verification of the submitted information, (iv) validation and chaining the transaction to blockchain and (v) distribution to other blockchain nodes. The novelty in the proposed work is that the architecture facilitates scalable and secured attack features exchange and ensures the integrity and consistency of the shared features. Furthermore, it detects and prevents malicious activities on the stored data from both outsider and insider threats, it presents the features in a standard format which encourages heterogeneous IDS nodes participation, and finally, it is robust to public IDS nodes joining and leaving the blockchain network.

Implementation: A prototype of the architecture has been built and tested in the laboratory. We evaluated the performance in terms of the transaction dissemination latency, security, scalability, and throughput. The preliminary result obtained shows a promising result; however, the result obtained does not depict a real-life scenario. As a result, there is a need to evaluate the performance of the architecture on a global testbed. Testing the architecture across the proposed global network will serve to evaluate its scalability, throughput, and transaction dissemination latency over a wide geographical area. The result of the deployment across the proposed global network gives the architecture's performance in terms of scalability, latency, throughput, and security if industries adopt the architecture. Hence, the importance of testing it across the global testbed cannot be over-emphasized.

Deployment: To evaluate the performance of architecture, we will deploy the architecture to the improved GRE tunnel setup between CCNY and JGN Seattle. The improved tunneling is useful for quick (preliminary) global testbed construction which may include troubleshooting, performance measurement and tunneling functionalities. It is useful as a quick way to extend VLAN, i.e., it keeps the real locations (a geographic relationship). Here, part of the blockchain network is set up at CCNY in the US while the other part will be set up at Kyutech in Japan. These two fragment blockchain networks will be connected through the research networks JGN/TransPAC and the GRE tunnel. The experiment will be carried out, the performance metrics will be evaluated and compared to the values obtained in the earlier experiments from the lab. Furthermore, the CCNY-Japan experiment will be extended to the COSM-IC (COSMOS Interconnecting Continents global testbed). Here, the blockchain nodes will be set up at different regions over the COSM-IC global testbed, which includes CCNY and Kyutech labs. The performance metrics obtained will be compared to the other results mentioned earlier. The purpose of the deployment is to analyze the performance of the architecture when the nodes are in different environments and are running different network traffic.

Facilitators: Oluwaseyi Ajayi and Tarek Saadawi are working on setting up the CCNY part of the tunnel and implementation of the experiment on the tunnel while Kenichi Kourai and Masato Tsuru are working on setting up and facilitating the experimentation on the tunnel at Kyutech side.

This work is partially funded by NSF and NICT