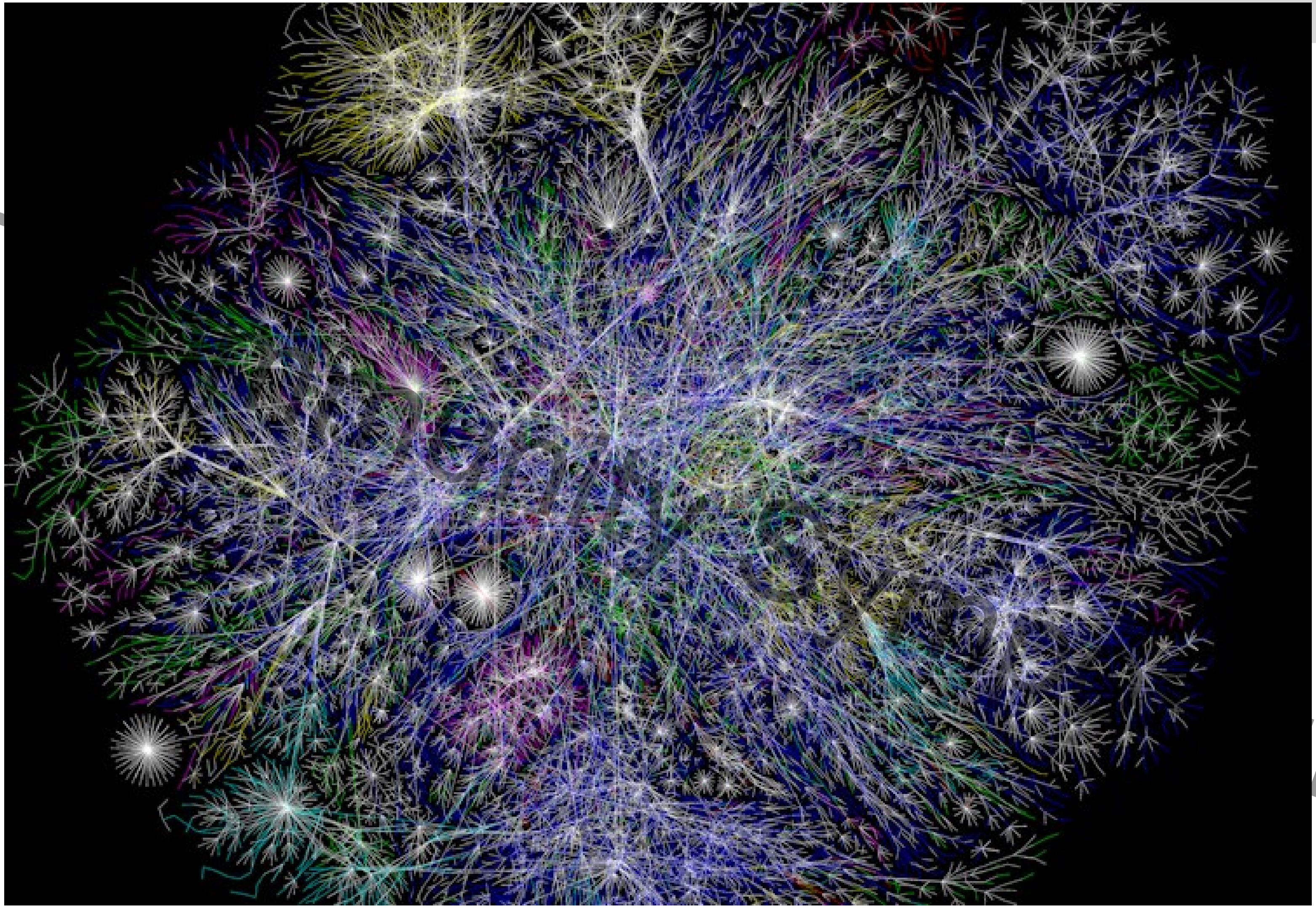
Blockchain-Based Architecture for Secured Cyber-Attack Features Exchange

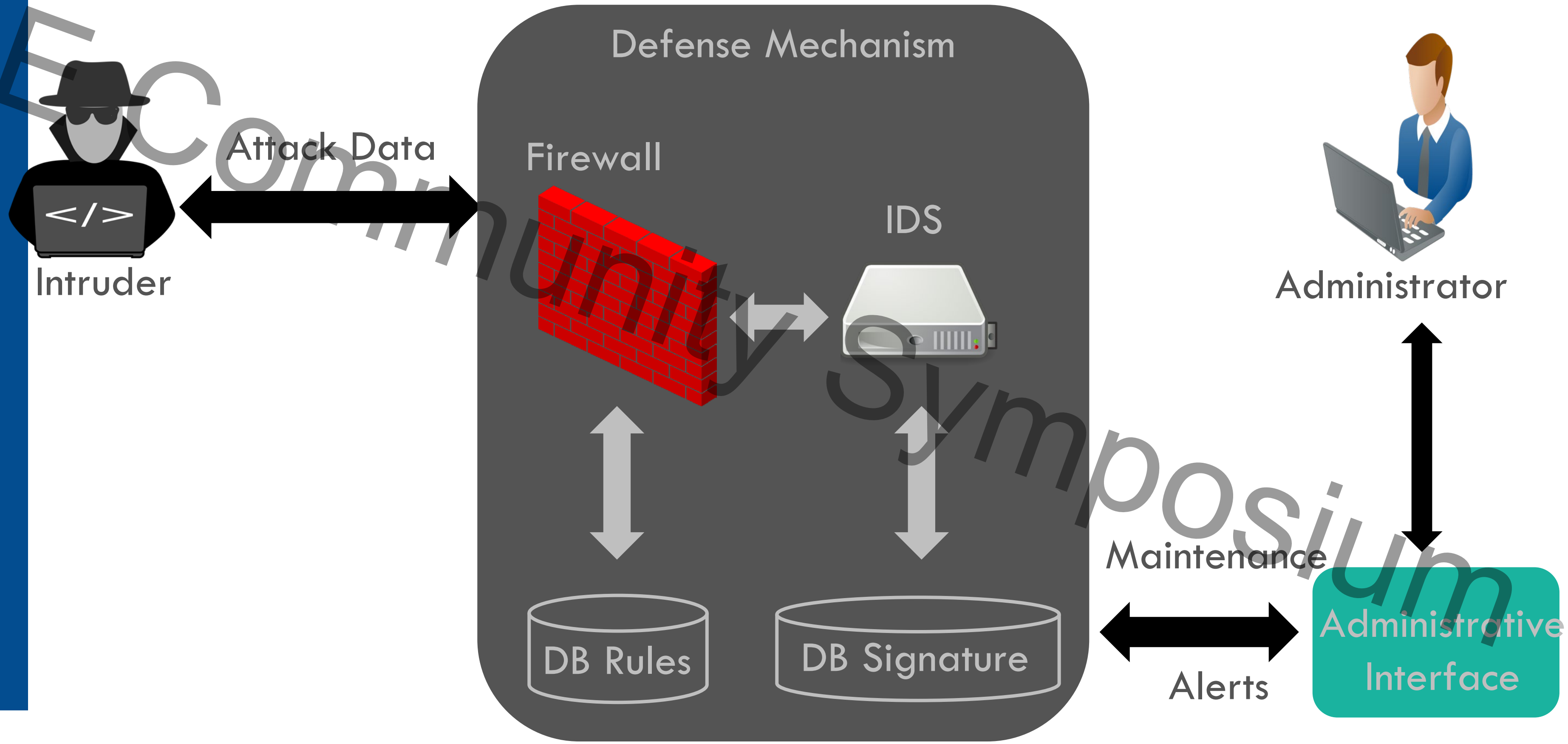
Tarek Saadawi
Co-Founder of Cybersecurity Master's Degree Program
City University of New York, City College (CCNY)
Saadawi@ccny.cuny.edu

April 16-18, 2024 Louisville, KY



INTERNET MAP

Intrusion detection system (IDS) model



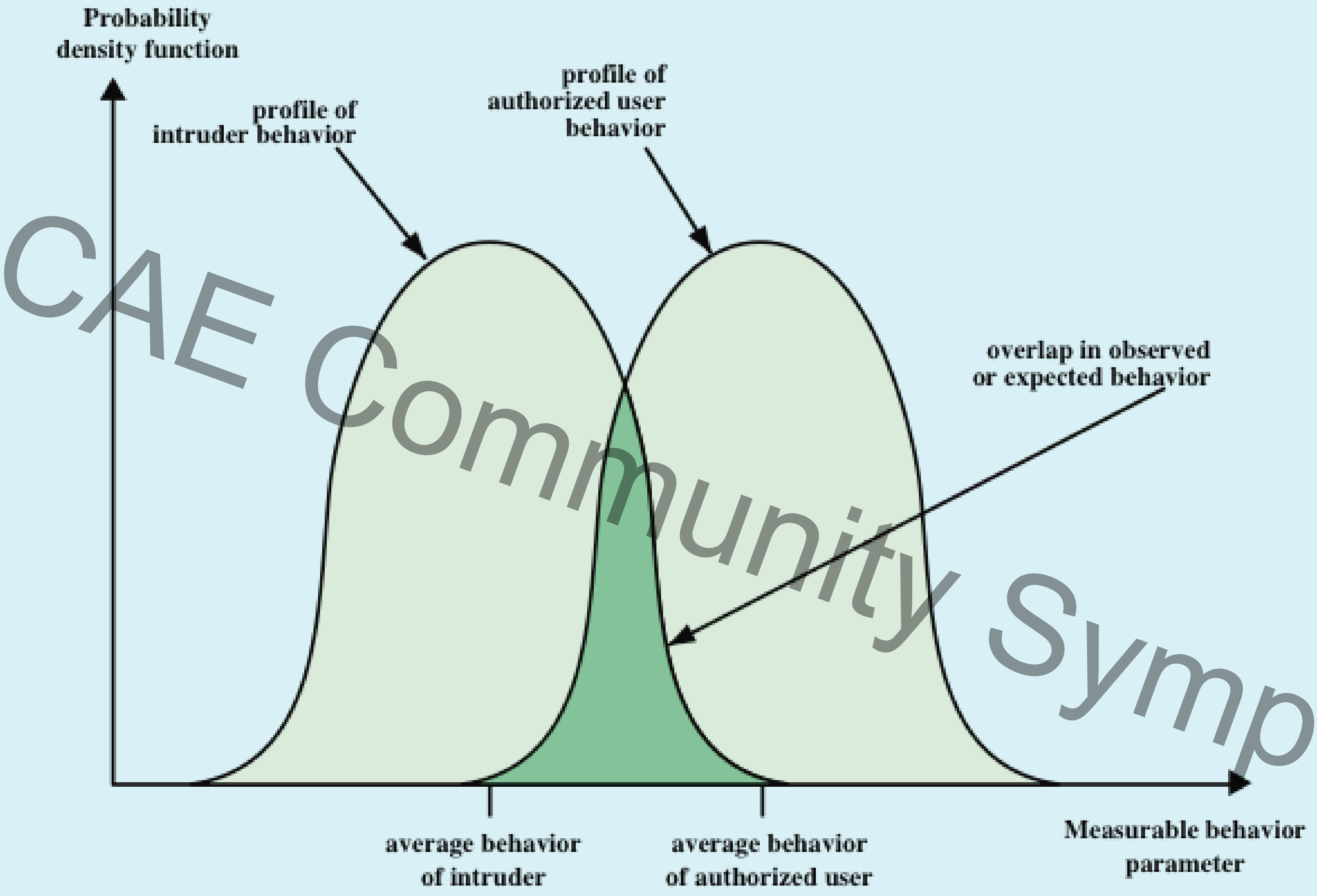

Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

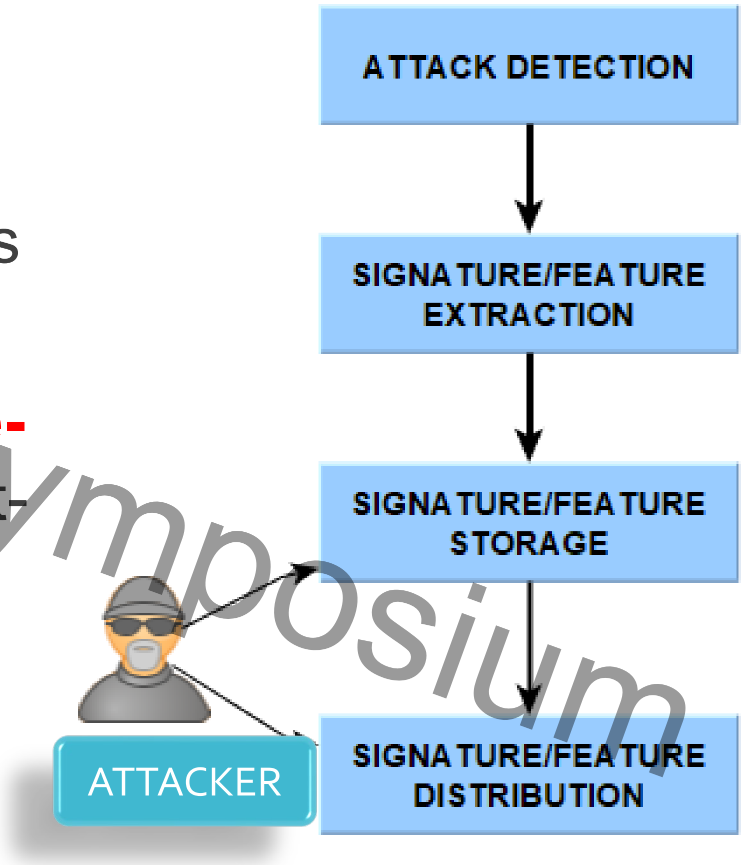
Figure 11.1 Profiles of Behavior of Intruders and Authorized Users

Cooperative Intrusion Detection System (Cooperative IDS)

- ❑ Threat information is needed to be exchanged among the organization's IDS so that **more malicious activities** can be stopped by coordinating efforts of participating IDS.
- ❑ Also, a **zero-day attack** (attack without known signature) experienced in an organization's IDS located say in New York, might be different from that experienced in another organization's IDS located say in London, or another company located in the same region
- ❑ Cooperative intrusion detection system was adopted because it **enhances detection rate of single IDS**.
- ❑ However, data security such as **fake data injection**, **data manipulation** or **deletion** and **data consistency** are some of the major problems facing this approach

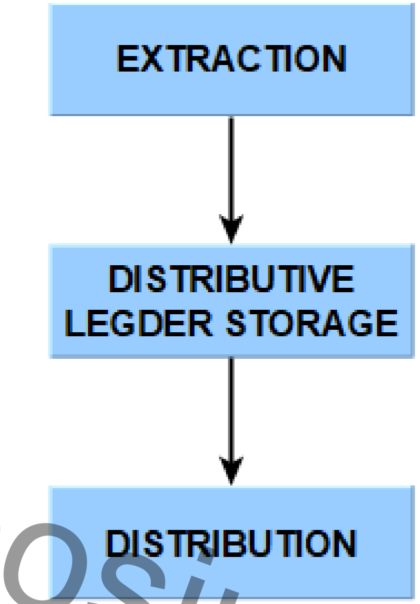
Problem Statement/ Motivation

- Cyber-attackers exploit vulnerabilities of **data storage and distribution stages** of the existing cooperative intrusion detection system to gain unauthorized access to data.
- Most of effective existing solutions uses **centralized** approach.
- This exposes data to **man-in-the-middle** or network to single-point-of-failure attacks .
- Others that use decentralized approach cannot guarantee **the consistency and integrity of shared data**.

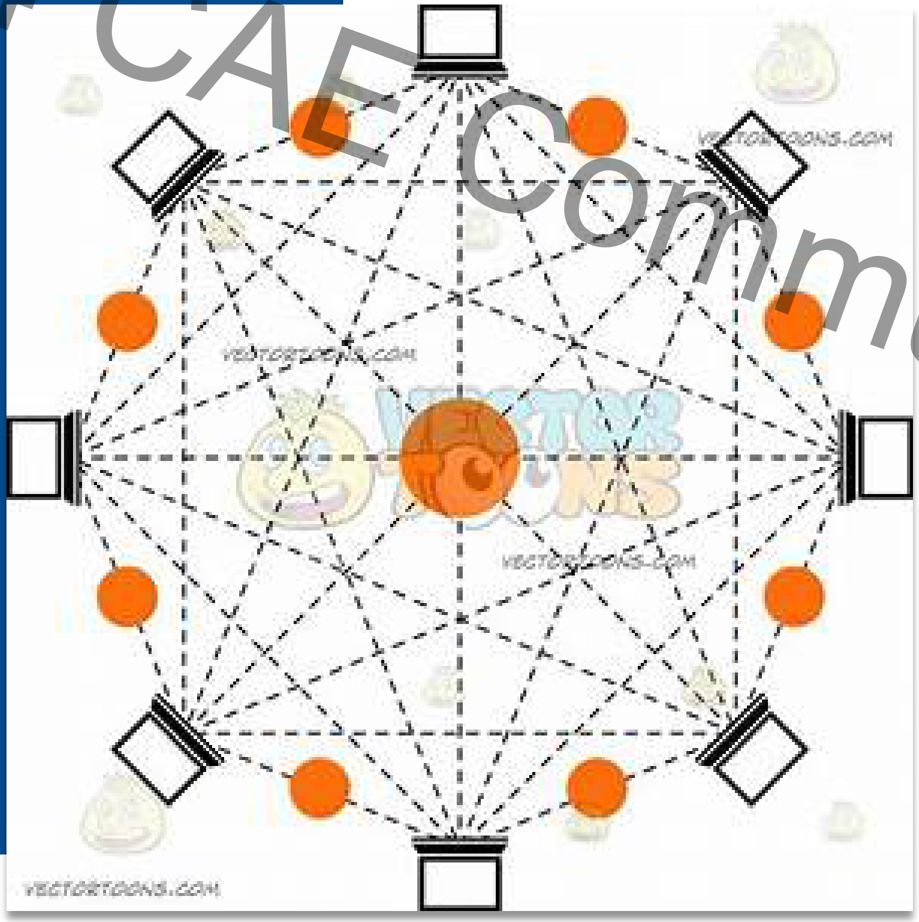

ATTACK DETECTION
SIGNATURE/FEATURE EXTRACTION
SIGNATURE/FEATURE STORAGE
SIGNATURE/FEATURE DISTRIBUTION
ATTACKER

Architecture’s Framework

- The architecture is built on **Ethereum** blockchain platform
- It combines the characteristics of both **public and private** blockchain
- Ethereum features **smart contract**.
- Smart contract is an agreement among the members of consortium which is stored **on the chain** and **run by all participants**

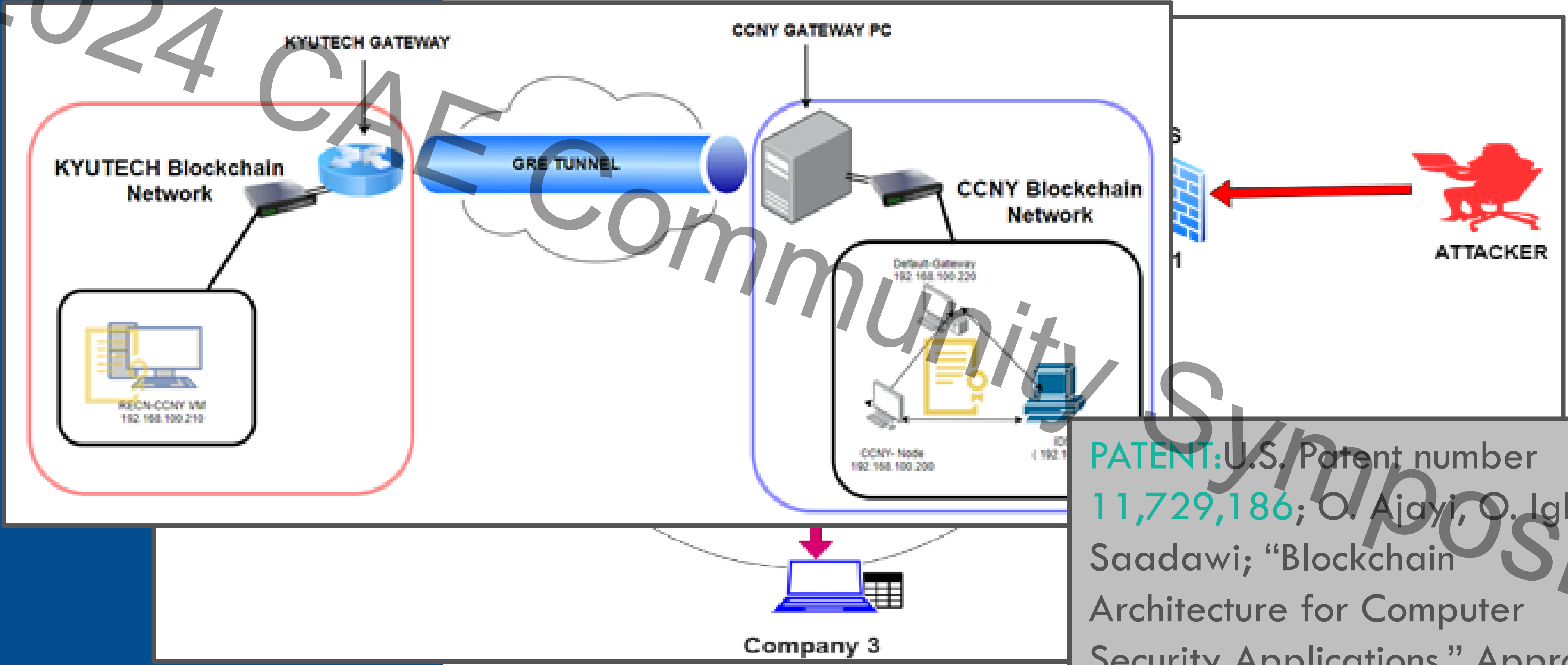


BLOCKCHAIN: Introduction



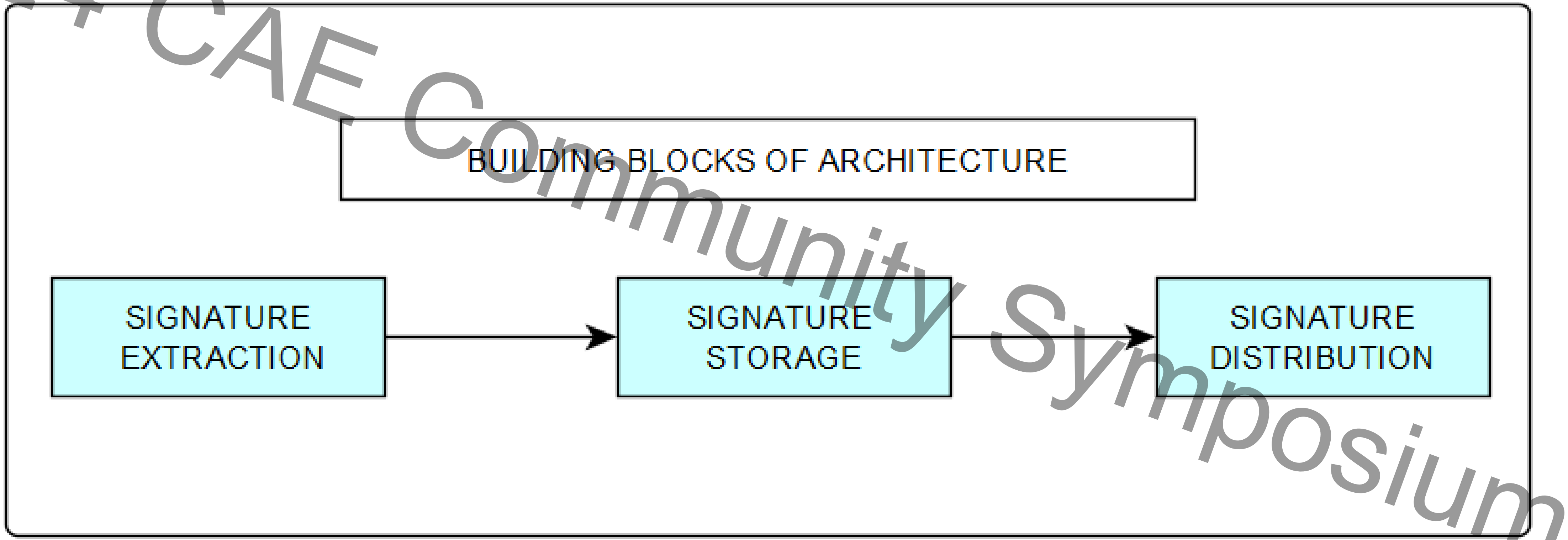
- Network of Computers called Nodes
- Append-only **public ledger**
- It is **Secure** (bit coin example), **distributed**
- It **keeps track** of every transactions **ever made** by participants

Cooperative IDS


KYUTECH GATEWAY
CCNY GATEWAY PC
KYUTECH Blockchain Network
GRE TUNNEL
CCNY Blockchain Network
Default-Gateway 192.168.100.220
RECN-CCNY VM 192.168.100.210
CCNY-Node 192.168.100.200
ATTACKER
Company 3

PATENT:U.S. Patent number 11,729,186; O. Ajayi, O. Igbe, T. Saadawi; "Blockchain Architecture for Computer Security Applications," Approved 8/15/2023

Architecture Building Blocks



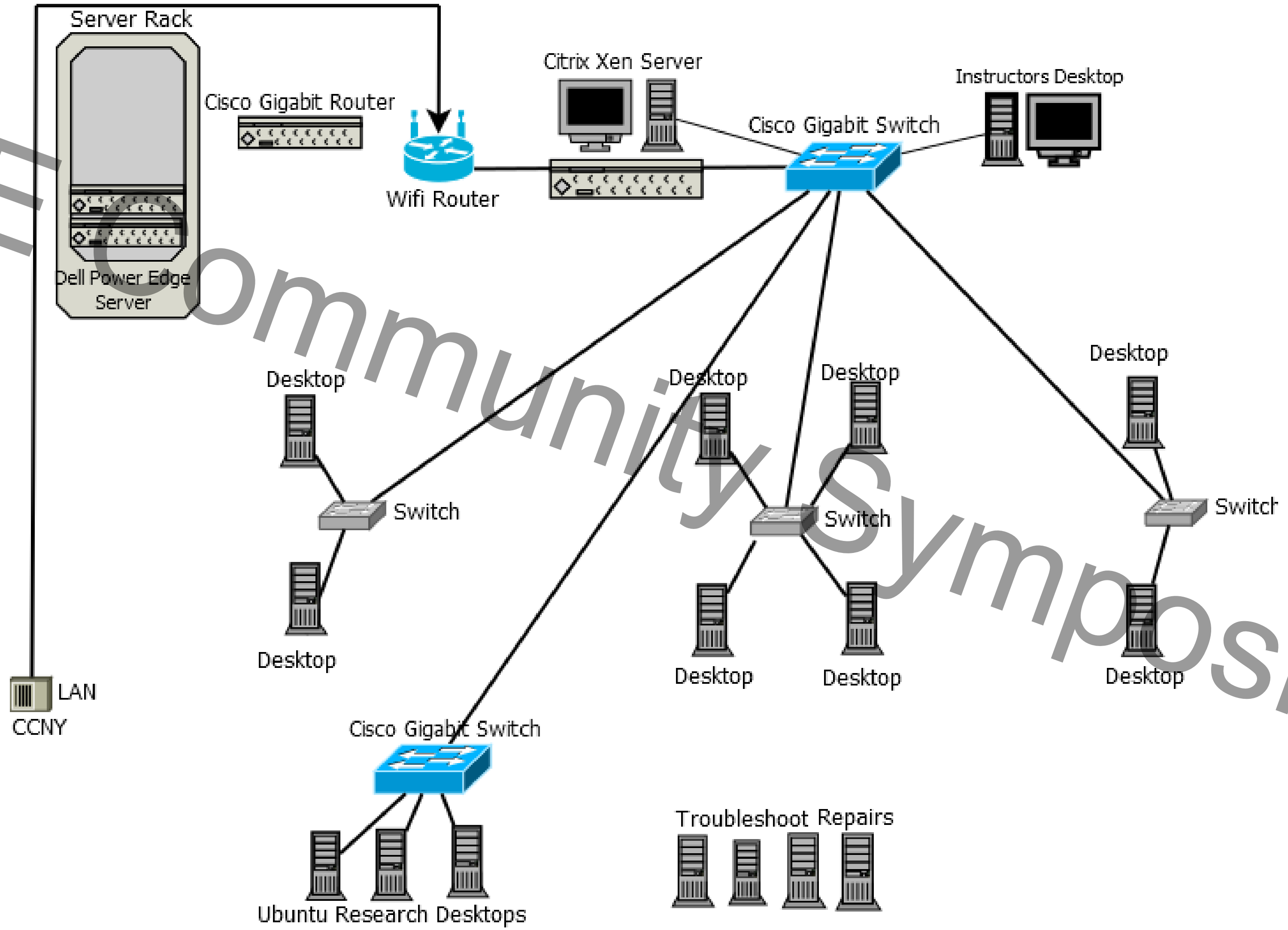
Connection Features

S/N	Feature Name	Definition
1	Source Port	Port from which attack is launched.
2	Destination Port	Target port in target network.
3	Source IP	IP address of attack node.
4	Destination IP	Target IP address in target network
5	Source Bytes	Total number of bytes sent from attack nodes during attack period.
6	Destination Bytes	Total number of bytes sent from target network to attack nodes during attack period.
7	Source Packets	Total number of packets sent from attack nodes during attack period.
8	Connection	Total number of connections initiated with target network by attack node.
9	Duration	Total time elapsed during attack.
10	Packets/second	Number of packets sent by attack node within 1 second.
11	Source Host count	Total number of attack nodes connecting to target network.
12	Destination Host Count	Total number of target nodes in target network.
13	Throughput	Rate at which attack nodes sends bytes to target node.(measured in kbps).
14	Service Count	Total number of ports connected to by attack nodes during attack period.
15	Same service count	Total number of connections to the same port number during attack period.
16	Different Host rate	Percentage of attack nodes attacking different target nodes.
17	Same service rate	Percentage of attack nodes attacking same port during attack period.
18	Same Host rate	Percentage of attack nodes attacking the same target node during attack period.

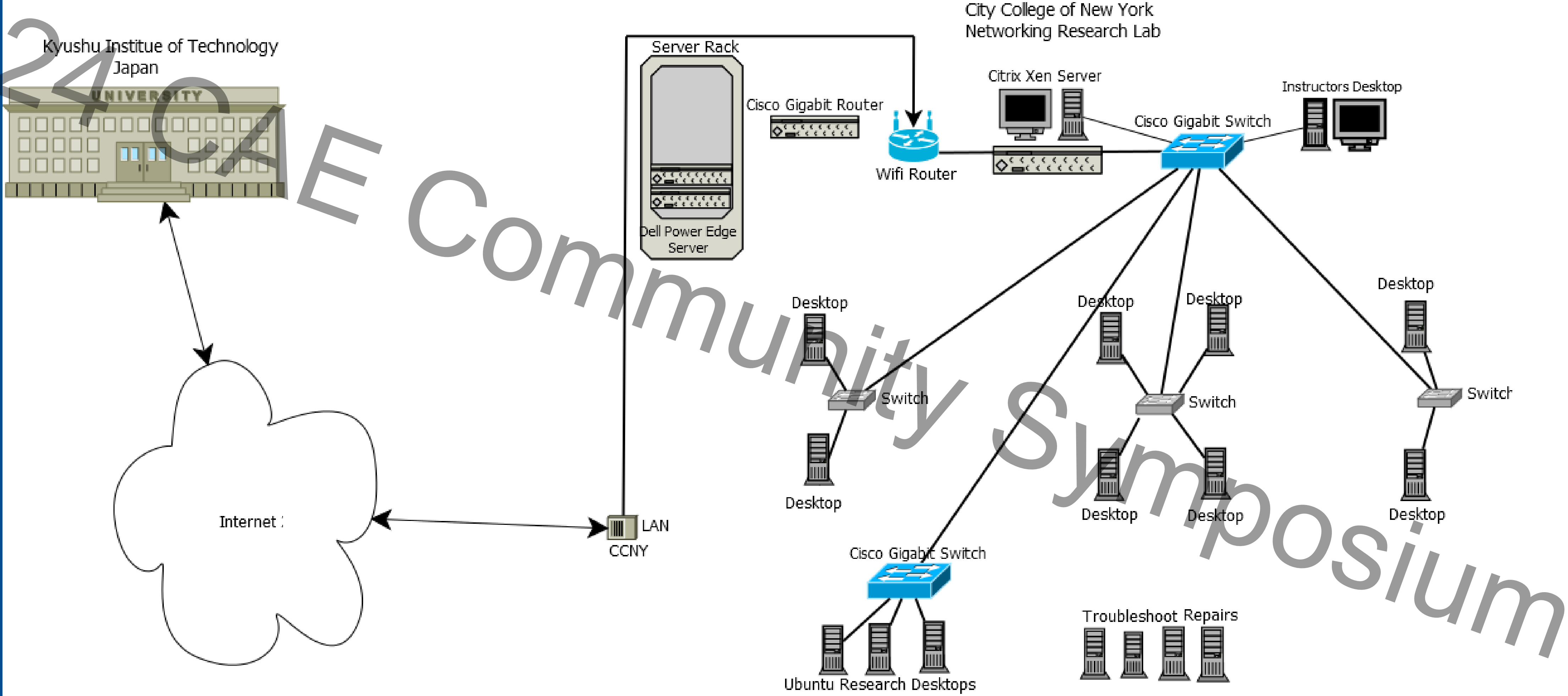
Packet Features

S/N	Feature Name	Definition
1	Land	‘1’ if source and destination IP and ports are the same; otherwise ‘0’.
2	Type of service	Class of traffic assigned to attack packet
3	Protocol	Higher layer protocol used in data portion of attack packet
4	Ip flags	How packet should be routed or processed by higher layer
5	TCP Flags	Defines type of packet sent by attack node
6	Urgent (urg)	Indicates priority of handling packets by router
7	Time to Live	Time left for packet to be discarded
8	Checksum	Error checking in packet header
9	Wrong Fragment	‘1’ if checksum is ‘incorrect’; otherwise ‘0’

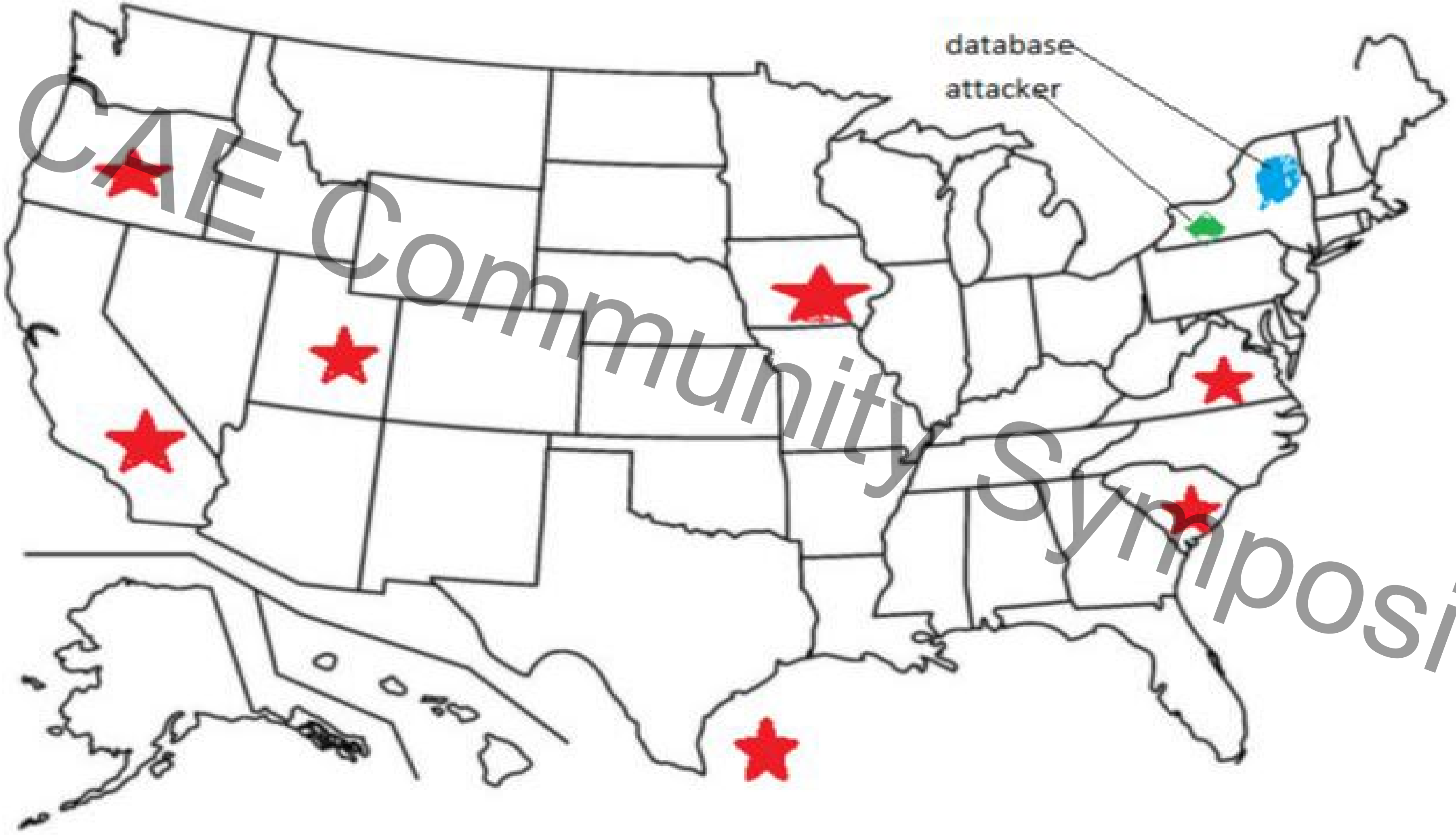
CyberSecurity Network Lab (1/2)



Cyber Security Network Lab (2/2)

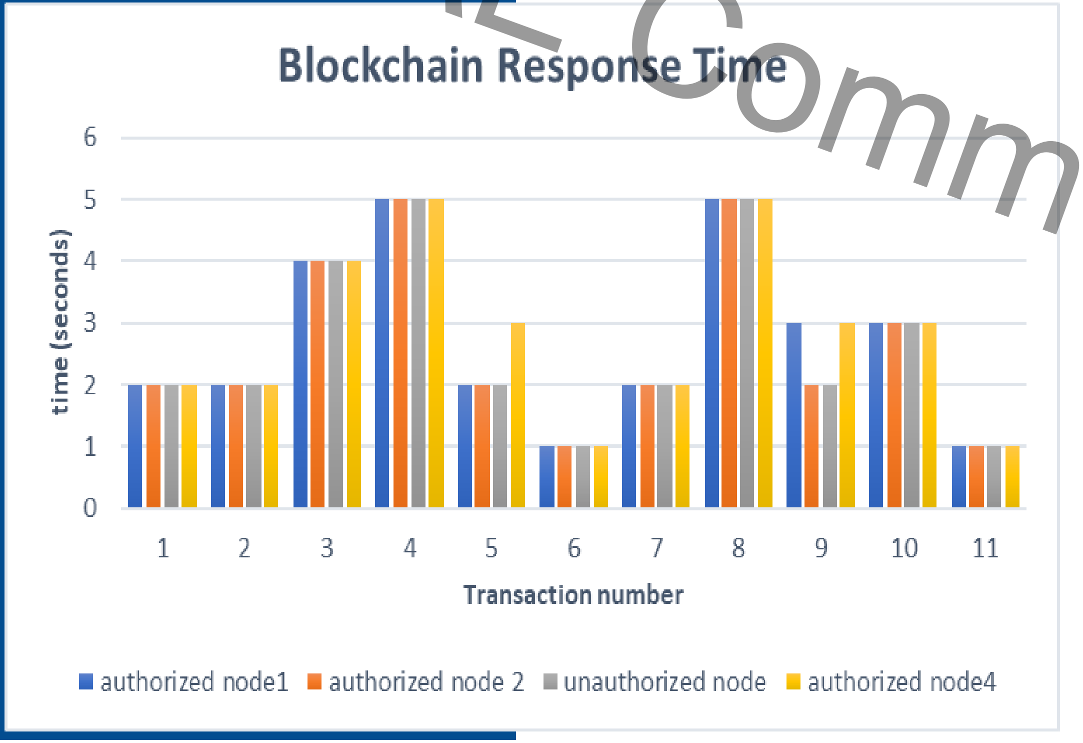


Location of cloud Nodes

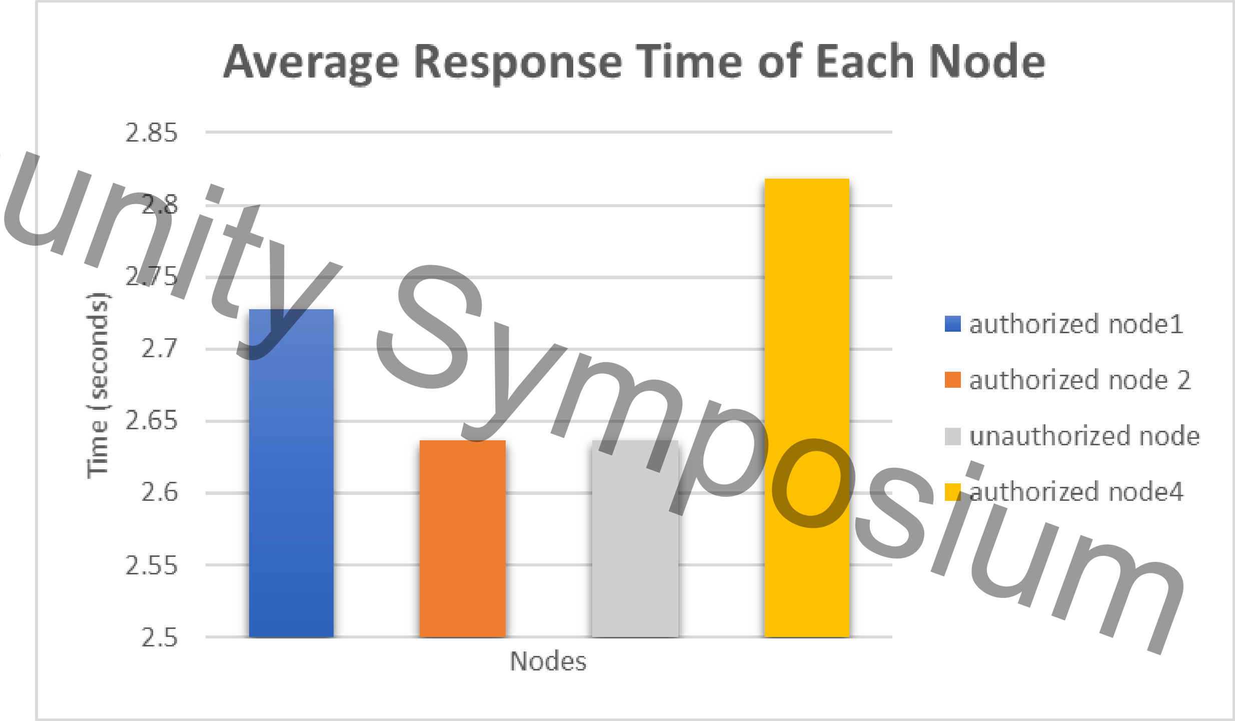


Performance Metrics

Total Latency



Average Latency



Experimentation

- We experimented with three signature-based IDS: **Snort, Bro** and **Suricata**. These are installed on the blockchain nodes
- Rule to **detect DoS** was set on the snort rule file of one of the authorized nodes
- DoS attack is launched at the node.
- This attack is detected, **converted to standard format** and **distributed** as explained.
- The experiment was repeated 20 more times.
- We obtain the ***transaction deployment time*** and ***execution time*** for each transaction from each node.

Experimentation

- We install *tcpdump v. 4.9.2., libpcap v. 1.9.0 , tcptrace v.6.6.0, wireshark v. 3.0.1*. and *scapy v.2.4.0* on all authorized nodes.
- We developed and run connection and packet analyzing scripts on authorized node 2 in addition to **Dendritic Cell Algorithm (DCA)** being run
- DoS attack was launched at **node 2**
- This attacked is detected, features are extracted and arranged in agreed format.
- We further performed Land and port scanning attacks on authorized node 2
- The experiment is repeated 20 times more in each case
- We recorded the ***transaction deployment time*** and ***execution time*** of each transaction from each node

Results –Signature

Attack rule

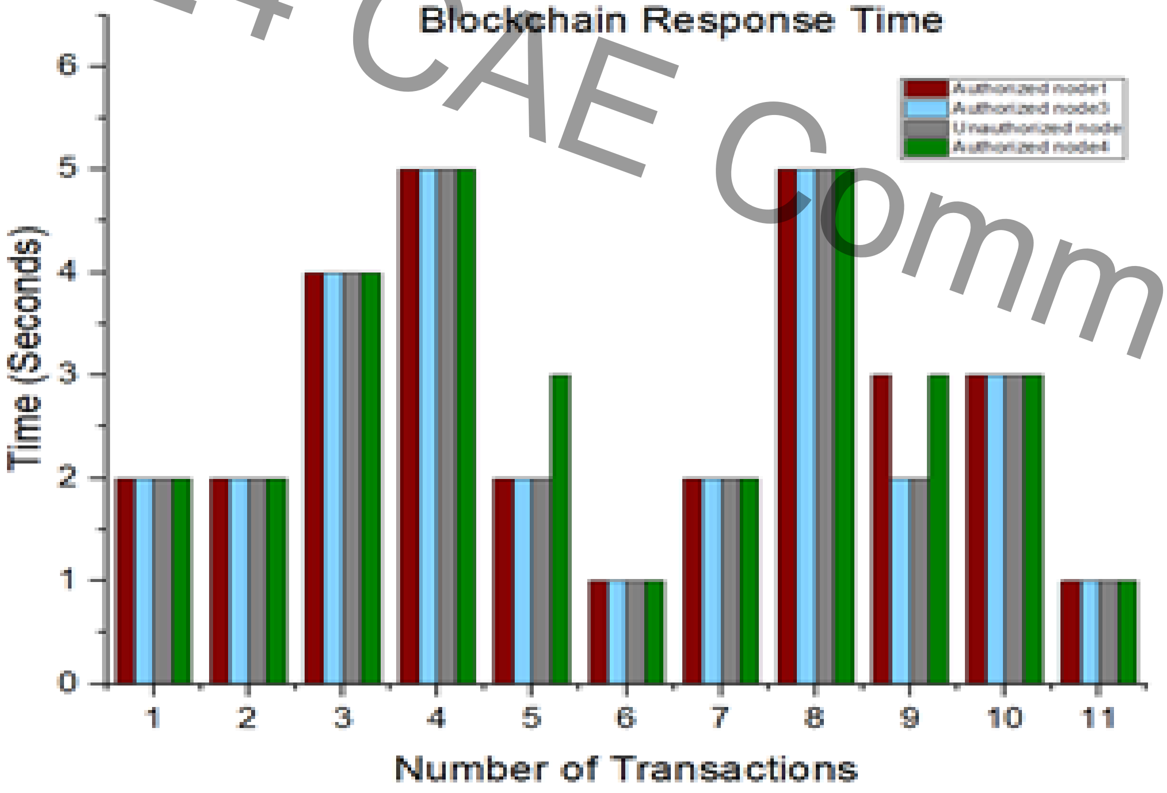
```
alert tcp ! $ any any ->
$HOME_NET 80 (flags: S;
msg:"Possible DoS"; count
70, seconds 10;
sid:10001;rev:1;)
```

Standard Format

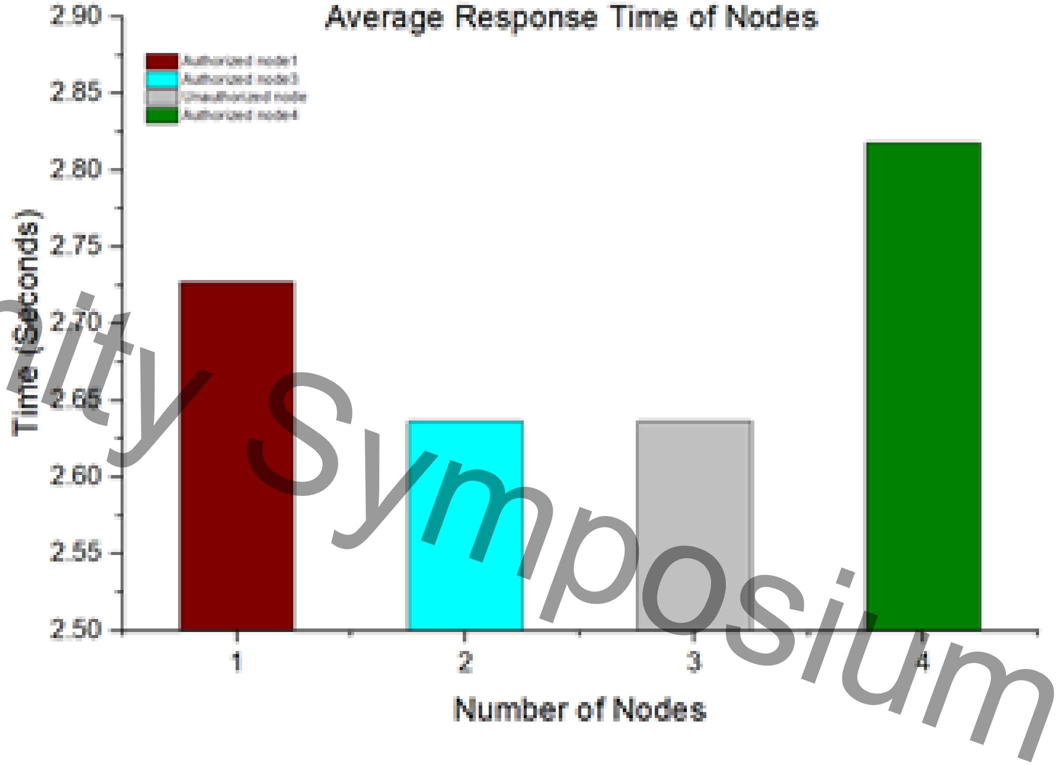
Standard Format Variable	Signature Values
Action	Alert
Protocol	tcp
Source IP	Any
Source port	Any
Destination IP	Home_net
Destination port	80
Flags	S
Message	Possible Dos
flow	------
Packets/sec	70
Time (seconds)	10
sid	10001
rev	1

Results

Response Time for the lab experiment

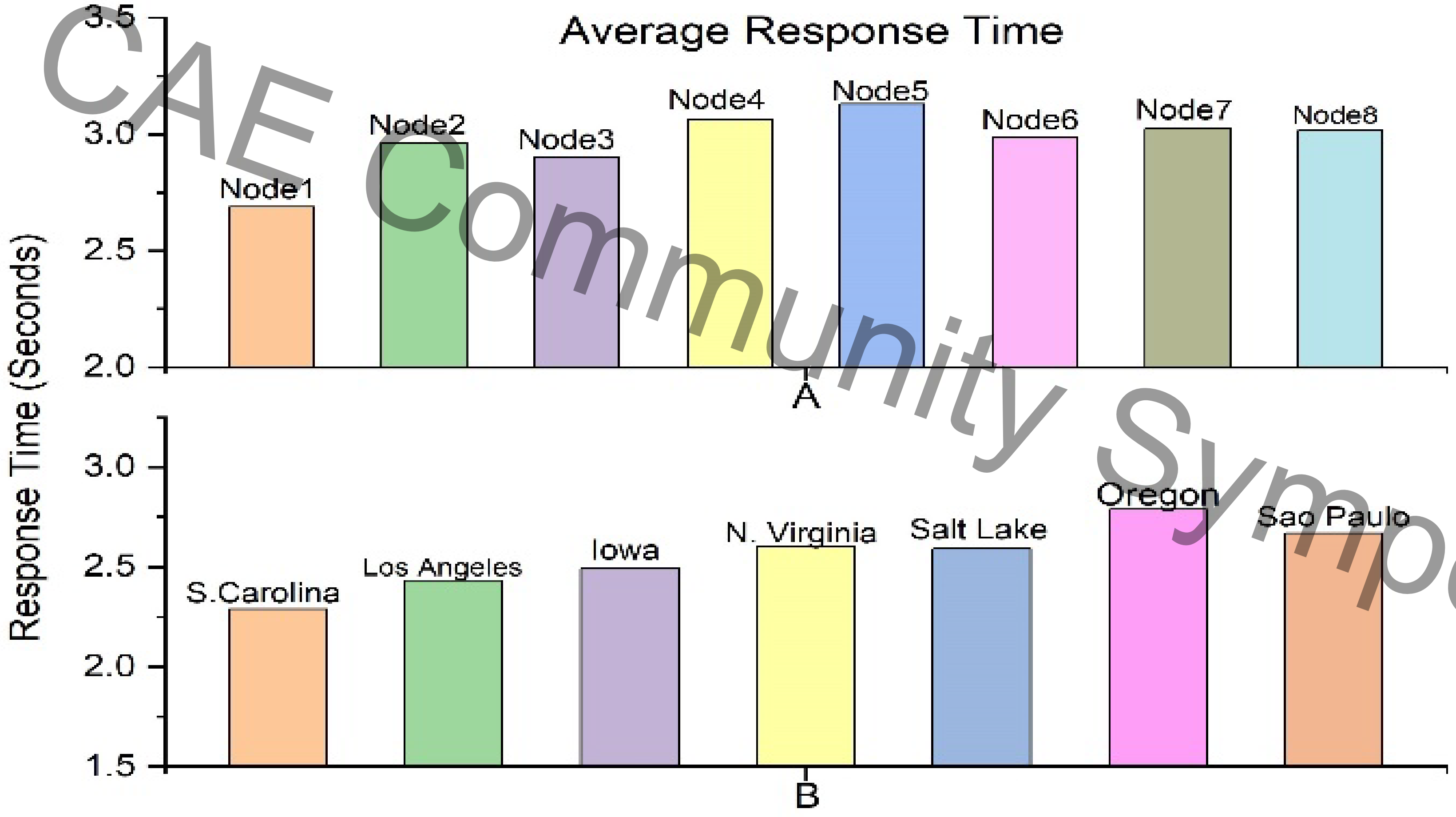


Average Response Time for the lab experiment



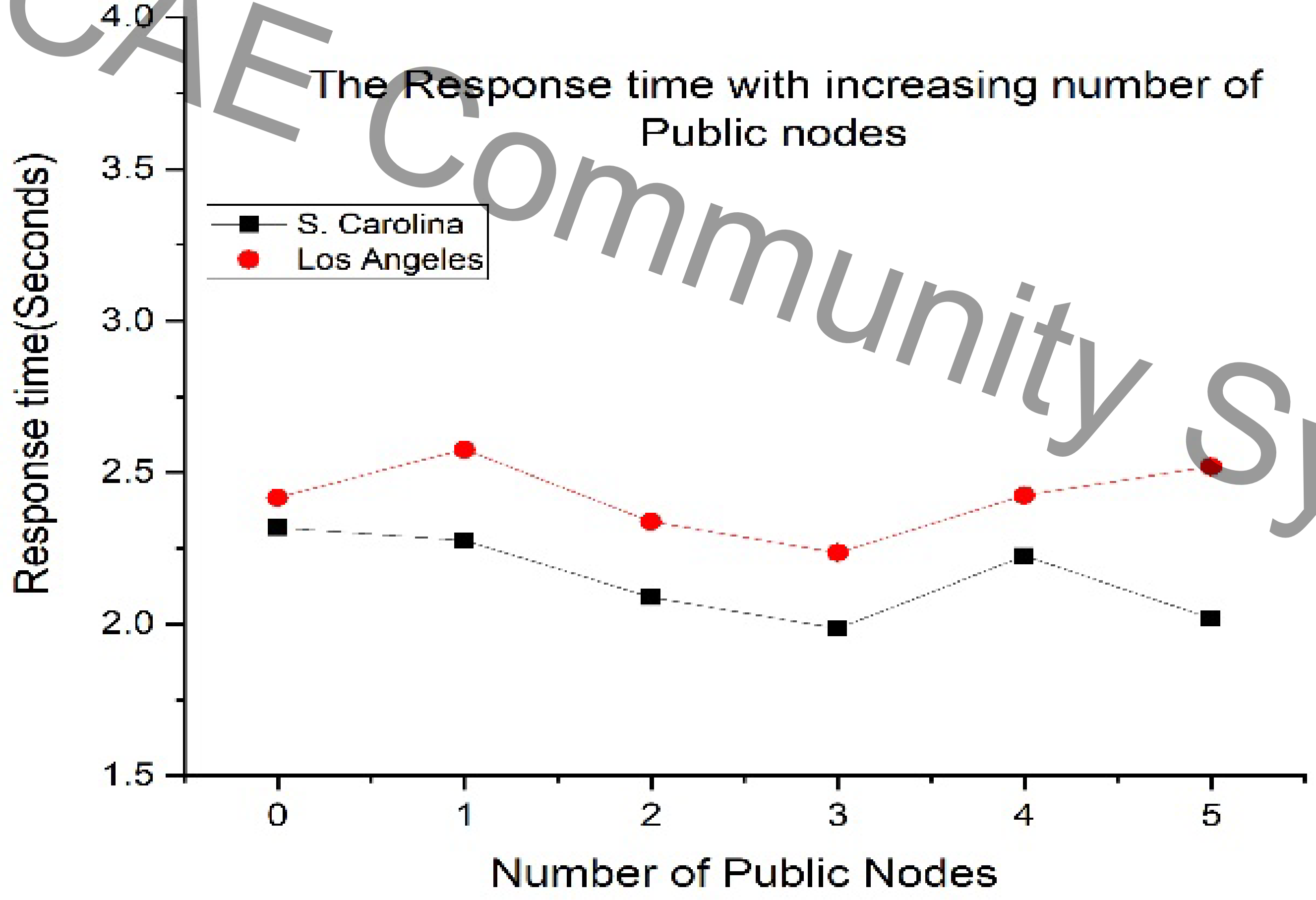
Response Time (New Result)

Average Response Time for Lab experiment and Cloud deployment nodes



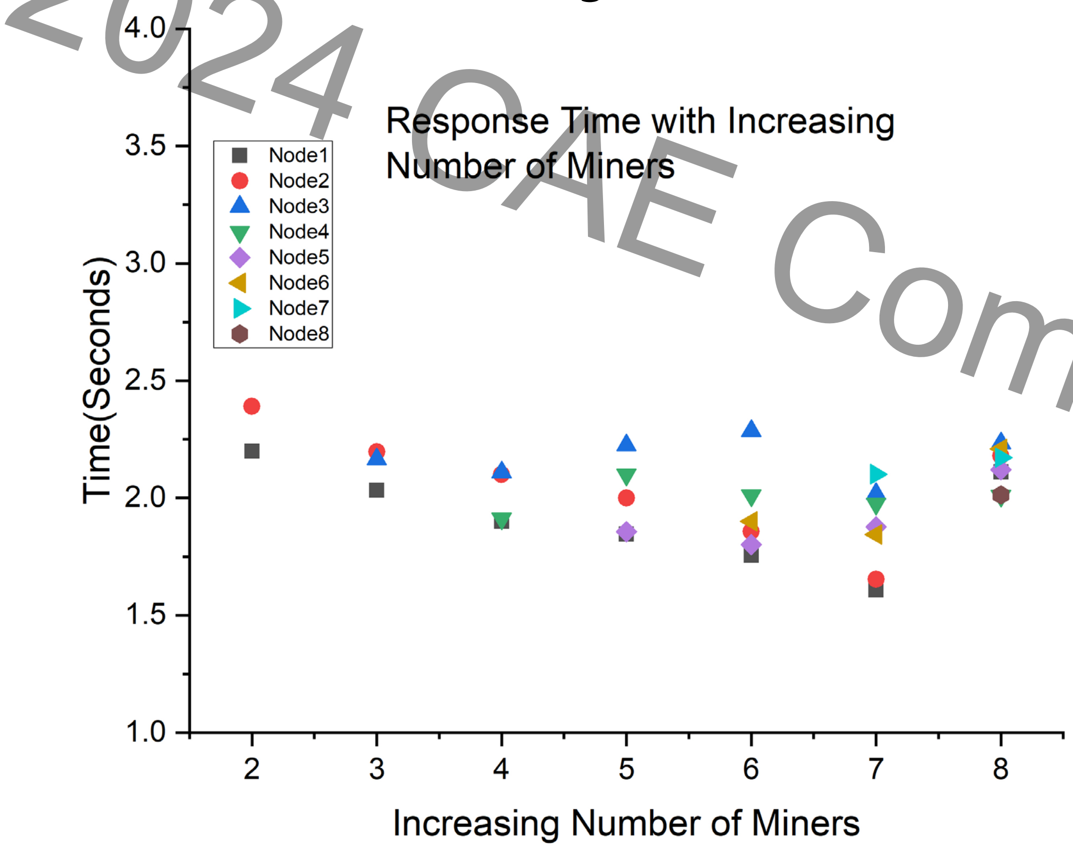
Scalability (New result)

- With

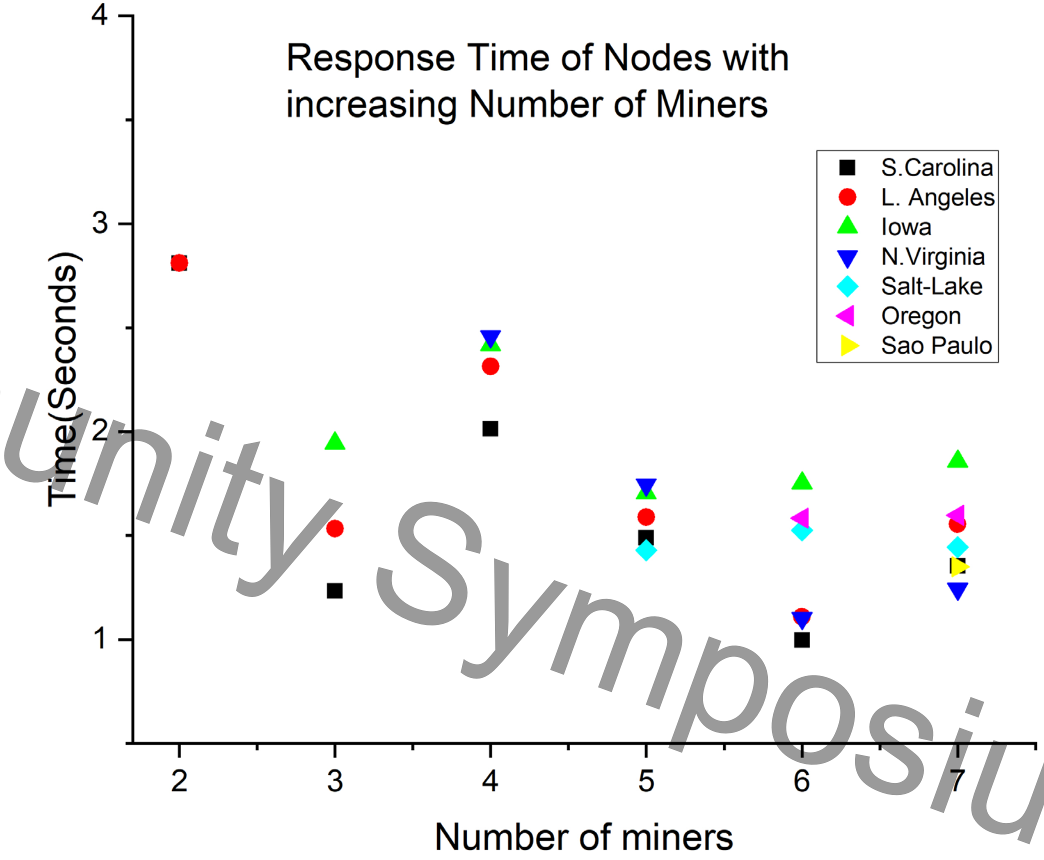


Scalability (new result)

- With increasing number of miners

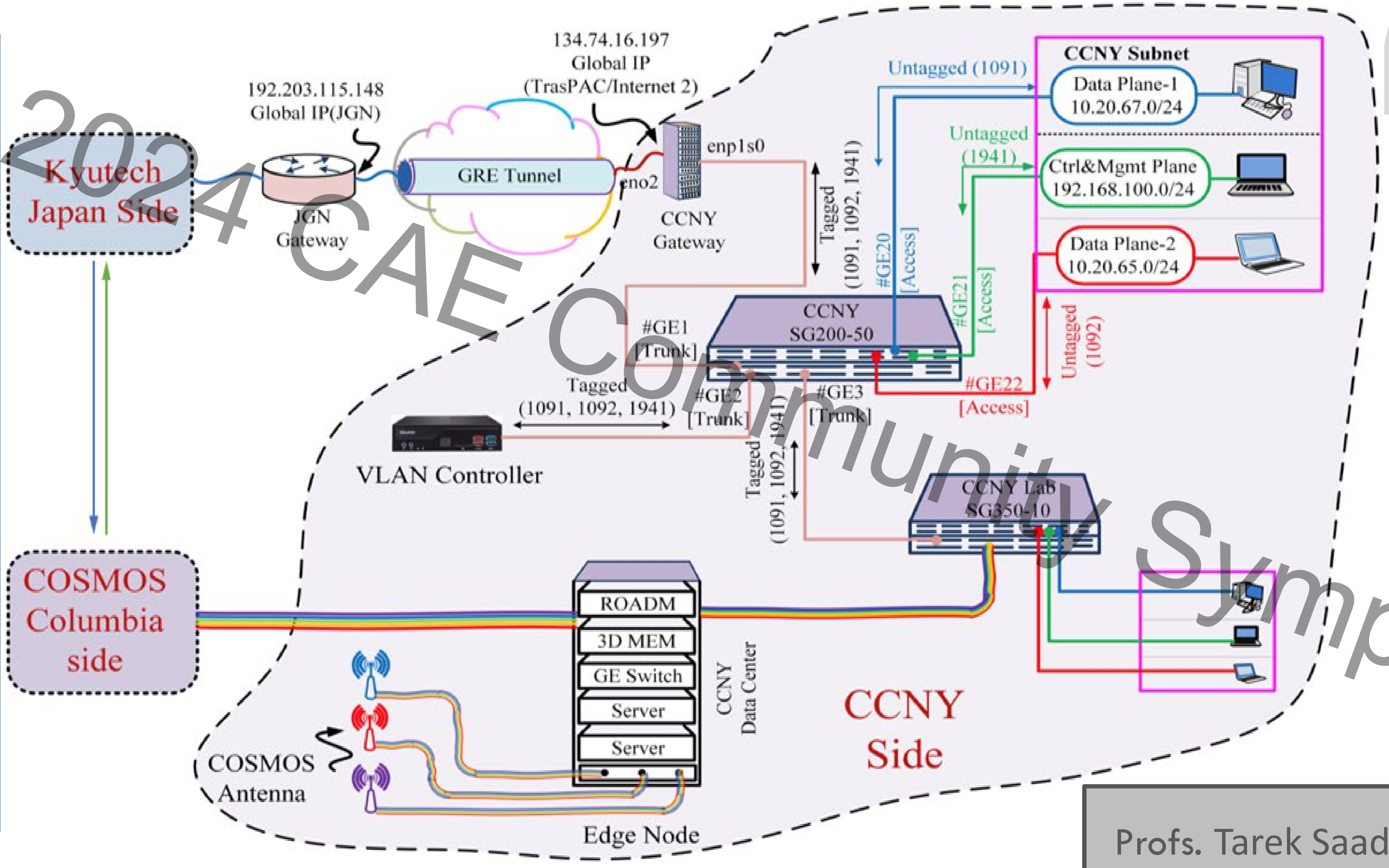


Lab Experiment



USA Experiment

NSF COSMOS: Cloud-Enhanced Open Software-Defined Mobile Wireless Testbed for City-Scale Deployment



Profs. Tarek Saadawi and Myung Lee

Conclusion

- **Private-public** blockchain-based architecture.
- It enhances the security of data shared in **cooperative intrusion detection system**
- It is **robust to public nodes** leaving and joining the network
- Performance is evaluated using **response time** and **security against fake attack injection**
- The architecture shows promising results.

O. Ajayi, O. Igbe and T. Saadawi, "Consortium Blockchain-Based Architecture for Cyber-attack Signatures and Features Distribution" 2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON 2019), Oct 10th – 12th 2019, Columbia University, New York, USA

Cybersecurity Patents:

CAE
IN CYBERSECURITY
COMMUNITY

1) Blockchain Co-IDS

U.S. Patent number 11,729,186; O. Ajayi, O. Igbe, T. Saadawi; "***Blockchain Architecture for Computer Security Applications***," Approved 8/15/2023

2) VM Keylogger Detection

U.S. Patent application number 17,723,937; H. Huseynov, K. Kurai, T. Saadawi, O. Igbe; "***Anomaly Based Keylogger Detection Through Virtual Machine Introspection***," Filed: 04/19/2022

3) AI-based IDS

U.S. Patent application number 15,633,056; O. Igbe, I. Darwish, T. Saadawi, "***Digital Immune System for Intrusion Detection in Data Processing Systems and Networks***," Filed: 06/26/2017

Questions

?