Workshop on Blockchain Security & Applications

Target Audience: Students & Developers from industry and academia

Summary:

As the technology is changing at the speed of light, the blockchain technologies are also progressing very fast. For software developers who wish to develop on blockchain, this technical workshop will bring you up to the speed.

The workshop will include interesting talks in which you will learn the basics of blockchain, blockchain in cybersecurity, machine learning and vulnerability assessment in blockchain. You will learn the latest trends in blockchain research from the experts at Blockchain Lab. An introductory hands-on training that exposes software developers to the suite of technologies will lay the foundations for Blockchain development. In the training, you will learn to set up your own Ethereum node, write and execute your first smart contract, and expose your smart contract to be executed as a Distributed App on a web browser. We will demonstrate to you the basic concepts behind blockchain architecture and how they might affect your codes. We will discuss some novel challenges with respect to upgrading/migrating smart contracts in Ethereum with solidity. The participants will learn about the storage of critical data on blockchain. Finally, we will make sure that you will leave this workshop with all of the tools that are required to start and produce your own blockchain based applications. In the end, we will conclude this workshop with the closing remarks from Blockchain Lab PI.

Day 1

1. Talks

Talk 1: Dr. Salman Basit: 45 min (10 AM)

- **Title and abstract:** To be decided

Talk 2: Dr. Umar Janjua: 45 min (10:45 AM)

- Introduction of Blockchain Security Lab and Projects
- Introduction of Blockchain

Talk 3: Dr. Basit: 45 min (11:30 AM)

- **Title:** Blockchain based auditable access control for distributed business processes

- **Abstract:** The use of blockchain technology has been proposed to provide auditable access control for individual resources. However, when all resources are owned by a single organization, such expensive solutions may not be needed. In this work we focus on distributed applications such as business processes and distributed workflows. These applications are often composed of multiple resources/services that are subject to the security and access control policies of different organizational domains. Here, blockchains can provide an attractive decentralized solution to provide auditability. However, the underlying access control policies may be overlapping in terms of the component conditions/rules, and simply using existing solutions would result in repeated evaluation of user's authorization separately for each resource, leading to significant overhead in terms of cost and computation time over the blockchain. To address this challenge, we propose an approach that formulates a constraint optimization problem to generate an optimal composite access control policy. This policy is in compliance with all the local access control policies and minimizes the policy evaluation cost over the blockchain. The developed smart contract(s) can then be deployed to the blockchain, and used for access control enforcement. We also discuss how the access control enforcement can be audited using a game-theoretic approach to minimize cost. We have implemented the initial prototype of our approach using Ethereum as the underlying blockchain and experimentally validated the effectiveness and efficiency of our approach.

Break: 30 Min (12:15 AM)

Training-1: Smart Contract Development: Talha Ahmad: 45 min (12:45 PM)

In this training, the participants will learn to develop their own smart contracts. The workshop will provide them a working environment and configured framework. Participants will learn the basic blockchain mechanism – specifically the ones relevant to Ethereum as a virtual machine and they will learn how to write, test, and deploy your smart contracts. In summary, participants will finish the workshop with:

- A running Ethereum node configured on a virtual machine that they can continue to use for their projects
- Samples of Solidity Smart Contracts that they can build further on

A. Requirements for necessary infrastructure

PC having internet connection with one of the following OS

- Windows
- Linux
- MacOS

Day 2

Talk 4: Dr. Taha Ali: 45 min (10:00 AM)

- **Title and abstract:** To be decided

Talk 5: Invited Talk: 45 min (10:45 AM)

Talk 6: Dr. Adnan Noor Mian: 45 min (11:30 AM)

- Blockchain in cybersecurity

Break: 30 Min (12:15 PM)

Demonstration of Ethereum based projects:

Demo 1: ZUBAIR KHALID 15 min (12:45 PM)

PKICHAIN: PKICHAIN is a decentralized and distributed, blockchain-based solution for SSL certificates that is fully compliant with Public Key Infrastructure and X509 standards. Current industry solutions are centralized and vulnerable to the single-point of failure attacks. History has shown us several attacks on leading solutions which resulted in a massive loss. The project is a decentralized solution to this problem where both registration authority and certificate authority are multiple nodes instead of one singular system. Integrity, security, authority, and privacy of data are major issues within a decentralized solution, that is why we are leveraging through the power of blockchain technology to overcome such issues and provide a fair and transparent environment. We are fully compliant with X509 standards which means our issued certificates have the same privileges as traditionally issued certificates and can be used in the same way, no extra efforts or other technical knowledge required. From a development and research perspective, we are using cutting-edge technologies like Blockchain, Self Sovereign Identity (SSI), Decentralized File Storage, Decentralized Validation, Decentralized Signatures, and connecting with the traditionally available standards to provide a solution that is secure, efficient, and compliant with existing solutions. From a user perspective, it is all the same as before, the same interface, same way of issuing certificates, and the same way of installing certificates. We have achieved the issuance

and successful installation of certificates and root certificates and browsers are correctly identifying our certificates. One of the key challenges in this project is building a consensus protocol which must be utilized by distributed nodes to validate a user and issue a certificate against certificate signing request.

Demo 2: MAHA AYUB 15 min (1:00 PM)

TRANSPER: Transper is a state extraction and upgradation tool. It applies static/dynamic analysis techniques on a deployed smart contract in order to extract all variable values from its storage state including complex structures like arrays, mappings. Visibility into the actual values of smart contract variables is helpful in improving code comprehension, developer debugging, and testing of contracts. Currently, regular variables in solidity can be easily obtained, but complex structures like mapping require intelligent analysis of storage slots. This is because, complex map variables, the key-value pairs are stored randomly in the Ethereum storage. Transper uses source code-driven algorithms for safe analysis and extraction of index keys of map structure specifically and identifies cases when all variables can be safely extracted. In case, it cannot extract a value (e.g., index key to mapping is not known), it safely reports it. Our initial results show that for 90% of the time, the state of smart contracts with mapping variables can be extracted safely. Further, we have successfully extracted a snapshot of the state of several smart contracts and redeployed a newer version of the smart contract with the snapshot state reinstated.

Demo 3: Sayyaf Haider 15 min (1:15 PM)

Title: Implementation of secure Blockchain using SGX.

Abstract: In recent years, blockchain has received much attention from various fields, including finance, healthcare, supply chain, etc. However, some security challenges hinder the wide adoption of blockchain technology. Especially, the execution of smart contracts raises confidentiality and integrity issues because of processing it on an untrusted large code base including operating systems and hypervisors. Recently, Intel processor introduced software guard extensions (SGX) that isolate the critical program from an untrusted computing base. In this presentation, we discuss the functions of SGX and its usage in blockchain technology to maintain confidentiality and integrity during the execution of smart contracts. In addition to security, SGX also has potential in improving other aspects of blockchain technology including performance, attestation and scalability. We also present these aspects in detail.

Day 3

Talk 7: Invited Talk: 45 min (10:00 AM)

Talk 8: Invited Talk: 45 min (10:45 AM)

Talk 9: Dr. Ali Ahmad: 20 min (11:30 AM)

- Blockchain in Machine Learning

Talk 10: Dr. Khurram Bhatti: 20 min (11:50 AM)

- Vulnerability Assessment in Blockchain

Break: 20 Min (12:20 PM)

1. Demonstration of Critical data storage projects:

A. Requirements for necessary infrastructure

- PC with stable internet connection
- Window/Linux OS
- VSCode
- NodeJS
- MongoDB
- Multichain (Stable Version)

Demo 5: Muhammad Ahtazaz Ahsan: 10 min (12:20 PM)

- Critical Data Storage on Blockchain

Demo 6: Maheen Ayesha: 10 min (12:30 PM)

Critical Data Storage of (FIR Data) on Multichain: In this demo, we will see how practically the critical data is stored on Blockchain. We will use the Multichain platform and Nodejs servers installed on our local machines to broadcast our data transactions onto the network. We will use different commands to analyze blockchain parameters and basics coding skills required to implement the network. We will extend the network to multiple nodes and re-adjust the configurable parameters to analyze the blockchain behaviour.

Demo 7: Hira Ahmad: 10 min (12:40 PM)

Performance Evaluation of Blockchain for Critical data storage: In this demo, we will see the performance of parameters related to the Blockchain network like latency, throughput, or scalability etc. We will also see which factors can be tuned further to

enhance the network performance for critical data storage and what are the trade-off between scalability and performance.

Demo 8: Hira Arshad 10 min (12:50 PM)

IOTA: A DAG-based blockchain for low powered IOT devices: In this demo, we will see another kind of blockchain that is Directed Acyclic Graph based chain, called IOTA. We will see how a node of IOTA is installed and used on local machines and can be connected to IOT devices. Moreover, we will see the key differences between IOTA and Blockchain on the basis of different performance metrics like scalability, computation time, etc.

Demo 9: Aneela Jaffer 10 min (1:00 PM)

Critical Data Storage of FIR Data on Hyperledger: In this demo, we will show how practically critical data like FIRs are stored on blockchain. We have used hyperledger Fabric Network for the storage of FIR data. The basic operations like creating an FIR, updating the status etc will be demonstrated. We will use different commands to analyze blockchain parameters and basic coding skills required to implement the network. We will extend the network to multiple nodes and re-adjust the configurable parameters to analyze the blockchain behaviour.

Closing Ceremony: 20 Min (1:10 PM)