AOI 2: A Novel Access Control Blockchain Paradigm for Cybersecure Sensor Infrastructure in Fossil Power Generation Systems

Rahul Panat¹, Vipul Goyal²

¹Department of Mechanical Engineering, Carnegie Mellon University, Pittsburgh PA
²Computer Science Department, Carnegie Mellon University, Pittsburgh PA

Carnegie Mellon University
Outline

• Background
  – Sensor Systems in Power Plants
• Private Access Controlled Blockchain Concept
• Creating Cybersecure Sensor Networks
• Tasks and Deliverables
• Power generation and distribution infrastructure can experience both external or internal cyberattacks
• Novel methods are required to secure the data, while also controlling its access
Objective of the Project

To design, characterize, and demonstrate a breakthrough secure blockchain protocol, namely smart private ledger with hierarchical access control for fossil power generation systems.

- Build sensor network simulating SCADA system of FE power plant
- Develop blockchain algorithms and codes for smart private ledger
- Simulated cyberattack to test the established blockchain
- Train Students and deliver functioning private blockchain
- Build SCADA System of FE power plant at CMU
- Student training and Deliver secure blockchain system to NETL
- Objective of the Project
Project Timelines and Deliverables
## Tasks and Timelines

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Owner</th>
<th>Year-1</th>
<th>Year-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1.0: Project Management and Planning</td>
<td>Panat</td>
<td>Q1 Q2 Q3 Q4</td>
<td>Q5 Q6 Q7 Q8</td>
</tr>
<tr>
<td>Task 2.0: Create a Sensor Network to Generate Data</td>
<td>Panat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 3.0: Data Transmission to Blockchain Nodes</td>
<td>Panat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 4.0: Development of Blockchain with Computers as Simulated Nodes</td>
<td>Goyal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 5.0: Create Hierarchical Access Control for Data Retrieval</td>
<td>Goyal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain</td>
<td>Panat/Goyal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Project period: 2 years**
  - Data acquisition and transmission system
  - Creation of blockchain protocols
  - Simulate cyberattacks and demonstration lab-scale system
Task-1

- Project Management and Planning
  - The PIs will manage and direct the project in accordance with a Project Management Plan to meet all technical, schedule and budget objectives and requirements. The PIs will coordinate activities in order to effectively accomplish the work. The PIs will ensure that project plans, results, and decisions are appropriately documented and project reporting and briefing requirements are satisfied.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Owner</th>
<th>Year-1</th>
<th>Year-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1.0: Project Management and Planning</td>
<td>Panat</td>
<td>Q1 Q2</td>
<td>Q3 Q4</td>
</tr>
<tr>
<td>Task 2.0: Create a Sensor Network to Generate Data</td>
<td>Panat</td>
<td>Q5 Q6</td>
<td>Q7 Q8</td>
</tr>
<tr>
<td>Task 3.0: Data Transmission to Blockchain Nodes</td>
<td>Panat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 4.0: Development of Blockchain with Computers as Simulated Nodes</td>
<td>Goyal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 5.0: Create Hierarchical Access Control for Data Retrieval</td>
<td>Goyal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain</td>
<td>Panat/Goyal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task-2

- Create a Sensor Network to Generate Data
  - This task will involve the development of sensor networks for the development of the proposed technology. The task will be performed by Panat group
Task-3

- Data Transmission to Blockchain Nodes
  - This task will involve the development of wireless transmission of the signal to the blockchain nodes. The task will be performed by Panat group.
Task-4

• Development of Blockchain with Computers as Simulated Nodes
  - This task will involve the development of the smart private ledger blockchain with hierarchical access control and secret sharing protocols and will be performed by the Goyal group.
• Create Hierarchical Access Control for Data Retrieval
  – This task will develop algorithms to retrieve the data from the blockchain and will be performed by the Goyal group
Simulated Cyberattacks and Demonstration of Robustness of the Blockchain

- PIs will simulate cyberattacks to harden the blockchain system for real world secure deployment
- Common strategies such as those used during the Ukrainian power grid attack will be studied and the blockchain system will be subjected to similar attacks.
- Any changes if needed will be made and the entire process will be repeated. We expect our system to provide very high level of security against such attacks by eliminating a single point of failure.
Building Sensor Network
CMU has developed sensor fabrication methods and testing systems for fossil power plants that can work at temperatures up to 500 C.
CMU has developed sensor fabrication methods and testing systems for fossil power plants that can work at temperatures up to 500 °C.
CMU has developed sensor systems for fossil power plants that can work at temperatures up to 500 °C.
Strain Measurement

1. Installed a commercial strain sensor (VY4 Shear/Torsion full bridge strain gauge) acquired from HBM, USA
2. Integrated the strain sensor with transmitter and base station

Successfully demonstrated strain measurement using Mantracourt T24 telemetry system
| E type beam      | Strain sensor showing good adhesion to beam surface | Strain sensor integrated with transmitter module |
Temperature Measurement

Temperature sensor integrated with transmitter
Data Transmission

Transmitting End
- Strain sensor
- Strain transmitter module
- 4W connection

Receiving End
- Base station mounted in a USB dongle
- Wireless
- Direct connection

Laptop
Data Transmission

- 600 m range in an open field site w/ license free 2.4 GHz direct sequence spread spectrum (DSSS) radio technology
- Data Encryption for complete security (128-bit AES)
- Proprietary protocol based on a 802.15.4 chip allowing T24 range to co-exist with Bluetooth, Zigbee & Wi-Fi devices w/o conflicts!!
Temperature Measurement

Snapshot of temperature data collected in a .csv file
Smart Private Ledger: Blockchains with Private Computation
First successful cryptocurrency

Proposed by “Nakamoto” in 2008, mining started in Jan 2009

Current market cap > 100B, Price > 8-10k

First recorded transaction: mid 2010
- Decentralized, no trusted server
- Miners and users
Need for Private Data

- As of today:
  - All data on public ledger = public
  - Private, access controlled data?

- Build an intelligent access controlled ledger
  - Different data visible to different parties
  - Even do computation on private data
  - 3rd gen Blockchain tech
The Overall Vision: Create Smart Private Ledger

Secret Sharing Based Consensus

Blockchain Node-1
Data storage 1 linked to SCADA
Sensor-1

Blockchain Node-2
Data storage 2 linked to SCADA
Sensor-2

Blockchain Node-3
Data storage 3 linked to SCADA
Sensor-3

Blockchain Node-n
Data storage n linked to SCADA
Sensor-5
Development of Smart Private Ledger

Our system flow is as follows:

- Generating secret key
- Loading and encrypting csv file containing the data from sensor network (using AES secret key encryption scheme)
Development of Smart Private Ledger

- Generating secret key shares
- Encrypting secret key shares (using RSA algorithm)
- Decrypting secret key shares
- Reconstructing secret key
- Decrypting ciphertext to obtain original file containing data
- Smart contract to store/retrieve data from blockchain
System Design

- Secret sharing and file encryption is implemented to be run locally on a given miner’s machine. Any file type containing the data can be encrypted with this secret sharing algorithm.
- Once this data is generated, it is stored in the smart contract which is deployed on the blockchain (Ethereum).
- Any miner is then able to access the data from the smart contract and decrypt their respective shares.
- With their keys recovered, they are able to decrypt the data file and have access to the sensor network data.
Smart Contract Storage

We create a smart contract which stores a mapping from miner address to secret key share (of type bytes) with the following functions:

- Add share to the mapping
- Store the encrypted file
- Retrieve the share of a given miner address
- Check if an address is in the map
Integration in Data Acquisition System

Sensors

- Temperature sensor
- Strain sensor

Oven for High Temperature sensor Network

T = 500 °C

Smart private ledger Blockchain

Secret Sharing Based Consensus

Node-1

Node-2

Node-3

Node-N
## Deliverables and Timelines

<table>
<thead>
<tr>
<th>Task / Subtask Number</th>
<th>Deliverable Title</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Project Management Plan</td>
<td>Update due 30 days after award. Revisions to the PMP shall be submitted as requested by the NETL Project Manager.</td>
</tr>
<tr>
<td>2.0</td>
<td>Sensor Networks for Fossil Power Generation System</td>
<td>Delivery to NETL 6 months after the start of the project.</td>
</tr>
<tr>
<td>3.0</td>
<td>Secure transmission of sensors to blockchain nodes</td>
<td>Delivery to NETL 3 months after Task-2.0, i.e., 9 months after the start of the project.</td>
</tr>
<tr>
<td>4.0</td>
<td>Smart Private Ledger Blockchain (codes and algorithms)</td>
<td>Delivery to NETL 12 months after the start of the project.</td>
</tr>
<tr>
<td>5.0</td>
<td>Hierarchical Access Control for Data Retrieval (codes and algorithms)</td>
<td>Delivery to NETL 3 months after the Task-4.0, i.e., 15 months after the start of the project</td>
</tr>
<tr>
<td>6.0</td>
<td>Robust Blockchain Including Necessary Modifications Ready to be Implemented in the Field</td>
<td>Delivery to NETL 9 months after the Task-5.0, i.e., 24 months after the start of the project</td>
</tr>
<tr>
<td>No</td>
<td>Risks</td>
<td>Probability</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| i. | Delay in the formation of sensor networks: The PIs propose to create high temperature sensor networks at CMU by leveraging a prior NETL project on sensors and using aerosol jet printing technology. There is a risk for equipment breakdown and the sensor networks not being ready by the end of the third quarter | Low         | High   | 1. Warranties/service agreements with the manufacturers are in place for the equipment.  
2. The PIs will use individual commercial temperature sensors in case the sensor network fabrication is delayed. |
| ii.| Risk for wireless transmission: There is a low probability that the sensor networks cannot send the signal wirelessly to the blockchain nodes. | Low         | Moderate | 1. The PIs will use commercial wireless sensors (two) as a back-up to demonstrate the concept  
2. Multiple suppliers are available in the market with wireless sensors and will be utilized as necessary. |
| iii.| Risk for formation of Blockchains: there is a small probability that the continuous stream of data coming from sensor readings will cause scalability issues in the blockchain | Low         | Moderate | 1. The PIs will increase the block size to handle a larger number of transactions per second  
2. The number of new blocks per unit time could also be increased to improve the scalability of the system |
| iv.| Risk for data retrieval: there is a risk that if a number of nodes on the Blockchain go offline, the data stored could become inaccessible | Low         | Moderate | 1. This risk can be mitigated by increasing the number of nodes. The higher the number of nodes, the better the availability of the system would be. In any case, compared to a centralized data storage, the system will provide much higher level of anonymity. |
Acknowledgements

• NETL for supporting this research under grant # DE-FE0031770
• Dr. Robie Lewis, Dr. Vito Cedro, and Dr. Sydni Credle for help on guidance of the project
Questions?