Blockchain Empowered Provenance Framework for Sensor Identity Management and Data Flow Security in Fossil-Based Power Plants

Sachin Shetty, Eranga Herath, Sayyed Ahamed, Old Dominion University

Deepak Tosh, Abel Gomez, University of Texas El Paso

Project Description

- **Project Goal** - Blockchain empowered provenance platform for identity management and process integrity for sensors in *Fossil-based Power Plants* (***FPP***).
- **Strategic alignment with DOE -** Improving electric grid reliability, resilience and availability
- **DOE-NETL** –Dr. Sydni Credle and Maria Reidpath
- **TEAM**
  - Old Dominion University – Virginia Modeling, Analysis and Simulation Center
  - University of Texas at El Paso – Computer Science
- **Partners**
  - Accenture, Argonne National Lab, ReliabilityFirst, Wood PLC
- **Contract**
  - October 1, 2019 – September 30, 2022

Acknowledgement

- "This material is based upon work supported by the Department of Energy Award Number DE-FE0031744."

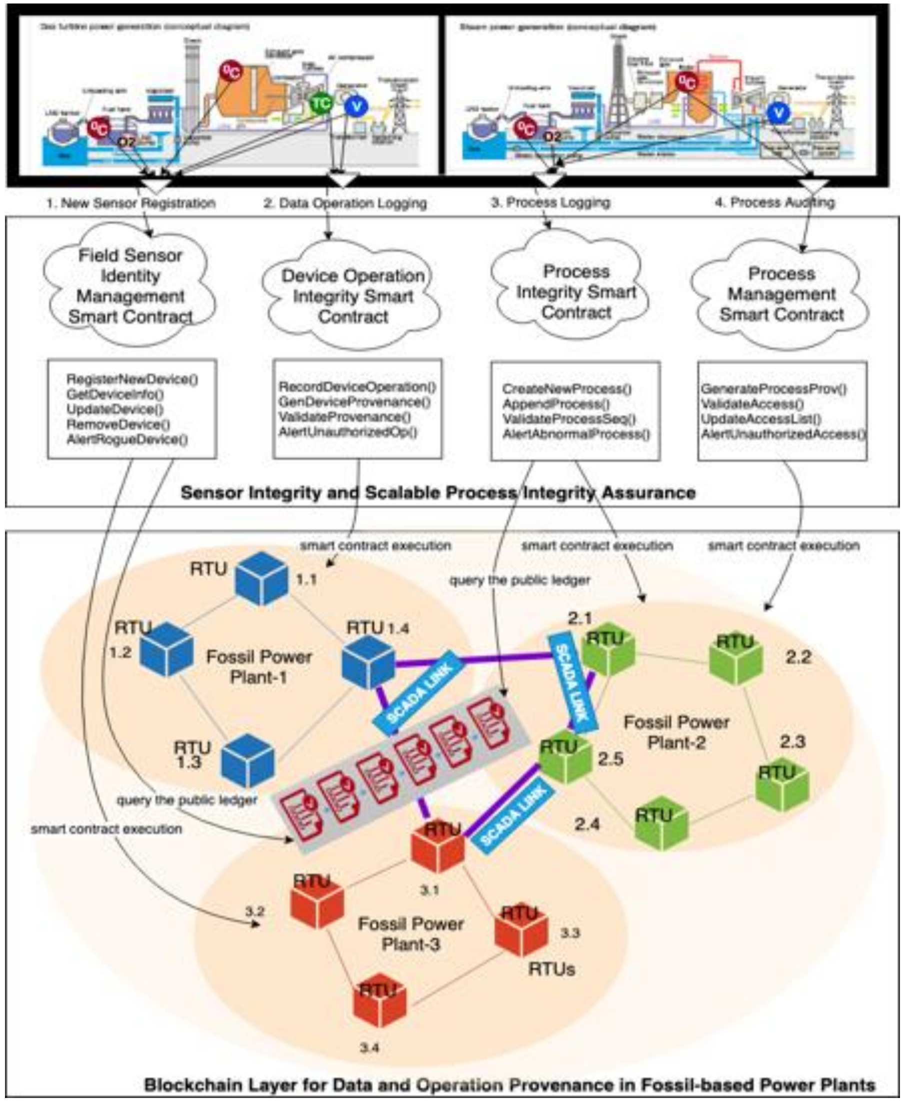
- Disclaimer: "This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."

Project Objectives

Objective 1 - Sensor identity management via establishing a Peer-to-Peer (P2P) SCADA network

Objective-2: Networked Sensor Integrity and Scalable Process Integrity Assurance in FPPs

Objective-3: Prototype Development and Evaluation

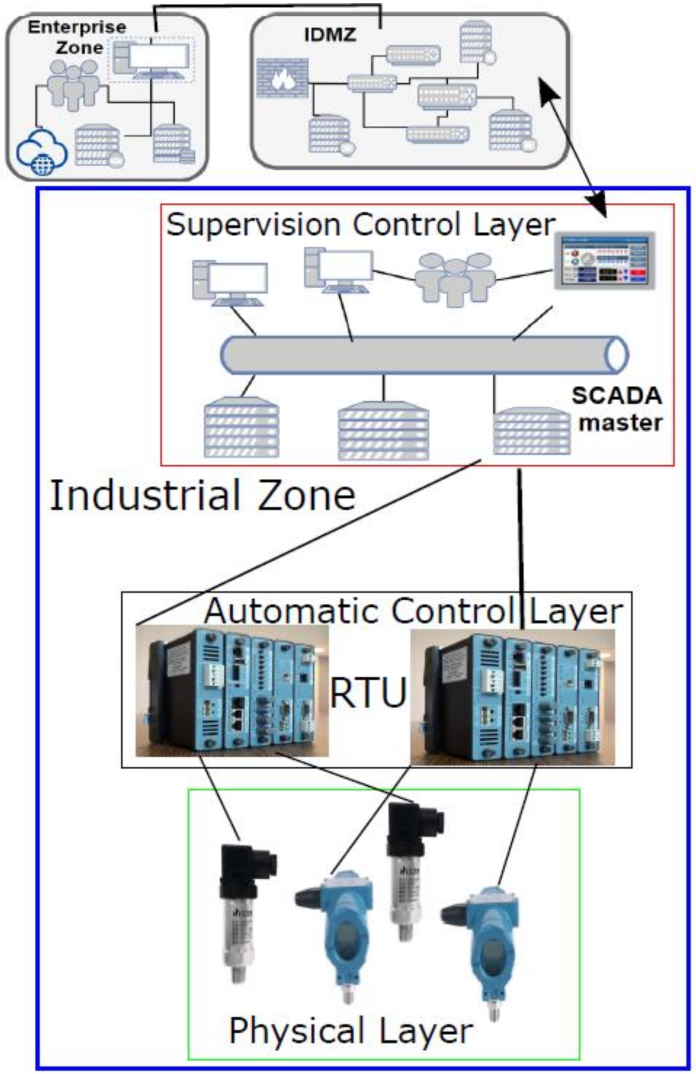


Project Accomplishments

- Developed blockchain-based SRAM PUF Authentication and Integrity (BIoSPAI) protocol
- Implemented the BIoSPAI in Raspberry pi based tested with DHT11 temperature sensors embedded into the boards and a ledger-integrated Hyperledger Fabric (HLF) Network
- Developed a blockchain-based SCADA environment for prototyping
- Published research results for Tikiri, a lightweight and scalable Blockchain platform at Future Generation Computer Systems Journal
- Collaboration with BLOSEM on reliable PUF development
- Planned submission of BIoSPAI paper to Cluster Computing Journal

Resilient Sensor Authentication using PUFs and Blockchain

- Industrial Control Systems (ICS) are integral components of national critical infrastructures
  - Example: Power plants, Water and gas distribution centers, transportation
- Commonly monitored by Supervisory Control and Data Acquisition (SCADA) systems
- Integration of advanced sensors in power plants introduces security challenges:
  - How to ensure authenticity of sensor data?
  - Can the received data be trusted?
  - What lightweight mechanism can verify device identities in such Cyber-Physical Systems?



Resilient Sensor Authentication using PUFs and Blockchain

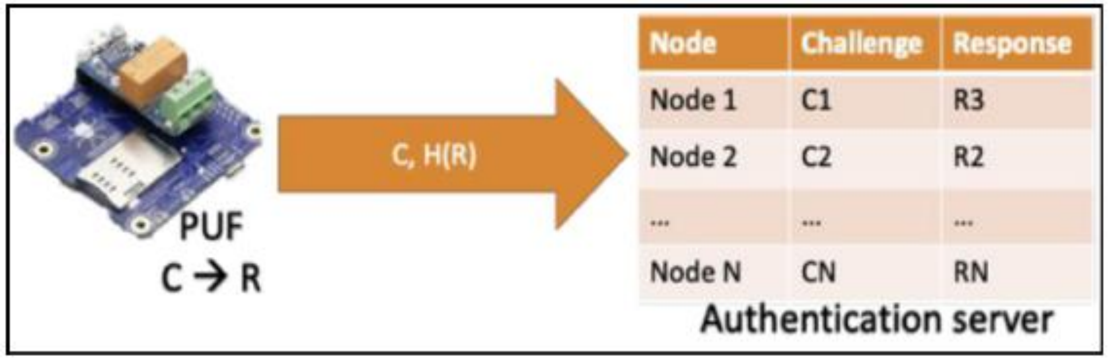
- **Problem Statement:**
  - Given resource constrained IoT nodes,
  - How can we uniquely identify them and perform continuous authentication in order to avoid maliciousness (node & data)?

- **IDEA:**
  - With lightweight hardware security primitive called Physical Unclonable Functions (PUF) to act as a hardware fingerprint generator and use it to dynamically authenticate sensor data through a ledger-integrated distributed network of P2P nodes?

Physical Unclonable Functions (PUFs)

- A hardware security primitive that maps challenges and response

$$y\colon \{0,1\}^n \rightarrow \{0,1\}^m$$



Node	Challenge	Response
Node 1	C1	R3
Node 2	C2	R2
...	...	...
Node N	CN	RN

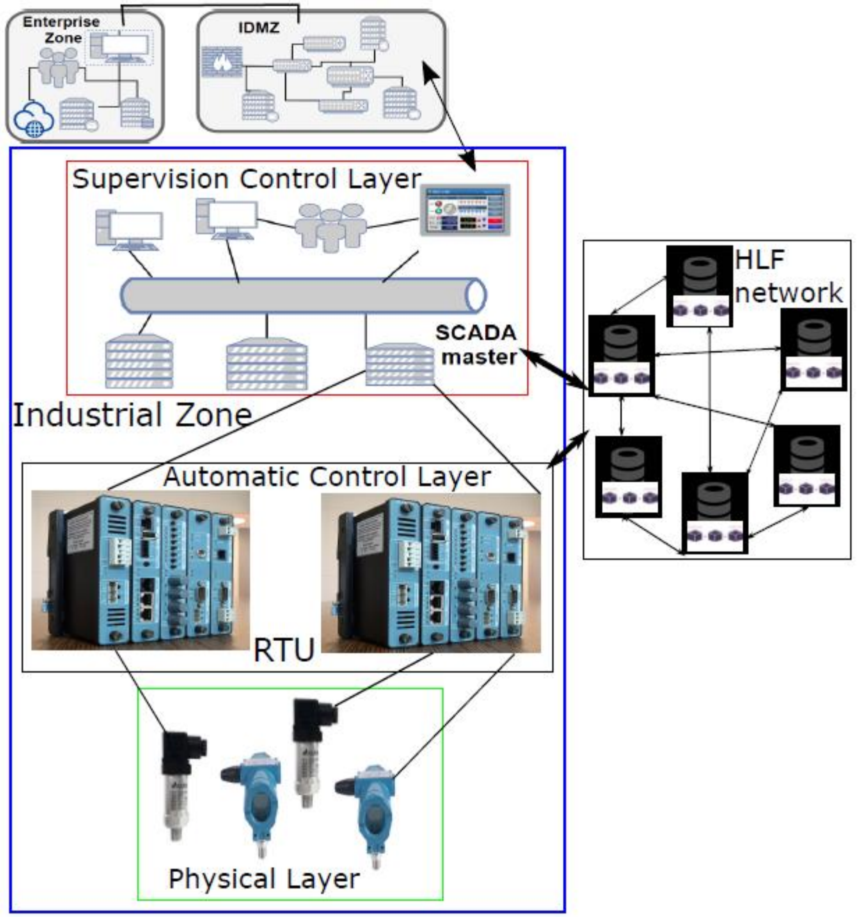
Physical Unclonable Function (PUF)

- Challenge-Response
- Low-Cost fingerprint generator
- Generate unique identities for all devices
- Offload complex state-of-art crypto solutions
- Different types such as SRAM-based
  - High availability and performance

Offloads the complexity of managing and storing keys on constrained devices

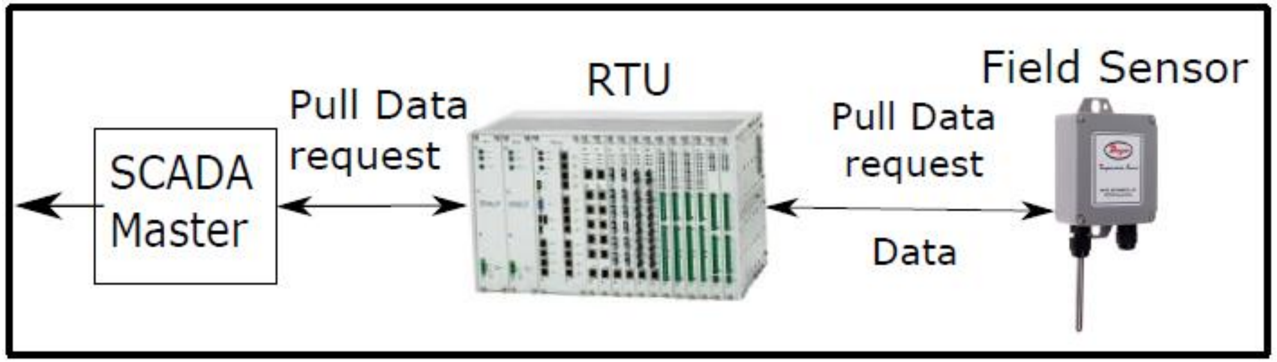
Proposed Approach

- Exploit the fundamental property of embedded sensors to generate unique identity through PUFs and derive hash-key functions
- Address the shortcoming of SPAI protocol by addressing the overhead and space complexity of RTUs.
- Design a blockchain-based SRAM PUF Authentication and Integrity (BloSPAI)
- Sensing data flow integrity assurance
- Eliminates rogue devices from SCADA
- Address overhead issues of SPAI protocol



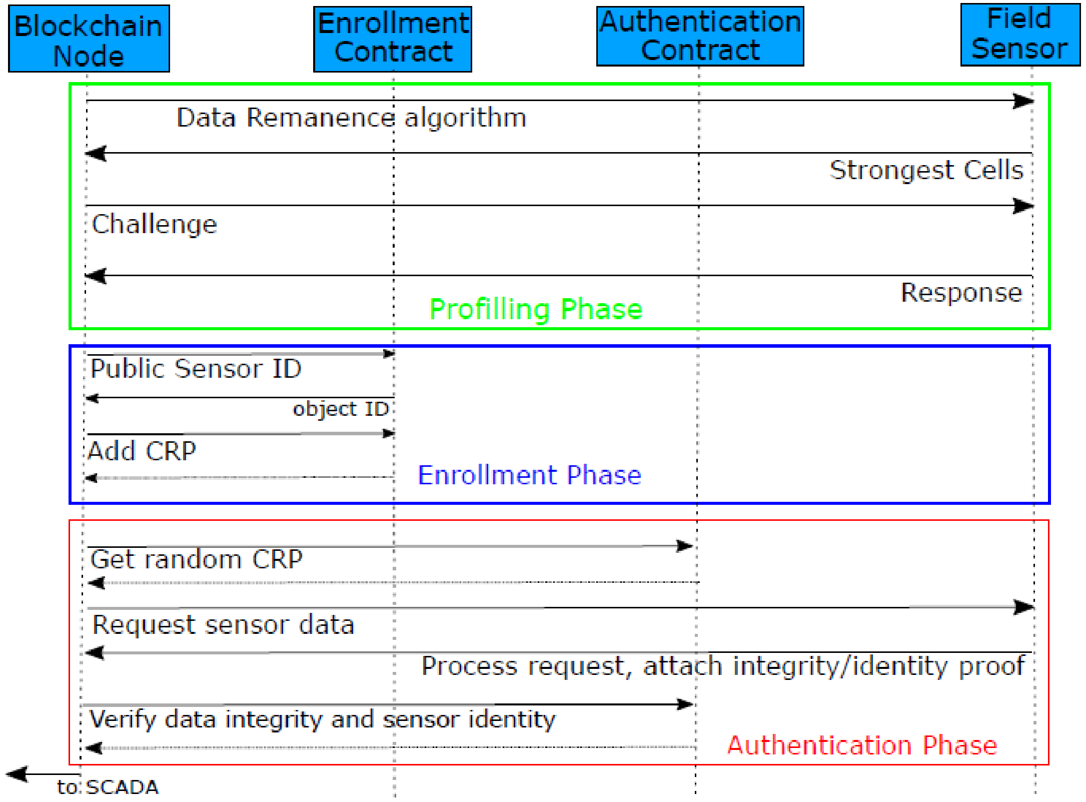
System Overview

- State-of-art SCADA communication
- RTU sends a pull request to a field sensor
- The field sensor read the request and sends the environment data
- Operational and commands are sent in clear text without security



System Overview (cont)

- BIoSPAI Protocol Overview
- RTU sends a pull request to a field sensor. It appends a CRP from the HLF network.
- The field sensor uses the CRP to generate a unique response through the PUF
- The prover appends the unique response while sending the sensor data
- The verifier validates the identity of the sensor and integrity of data through the authentication smart contract



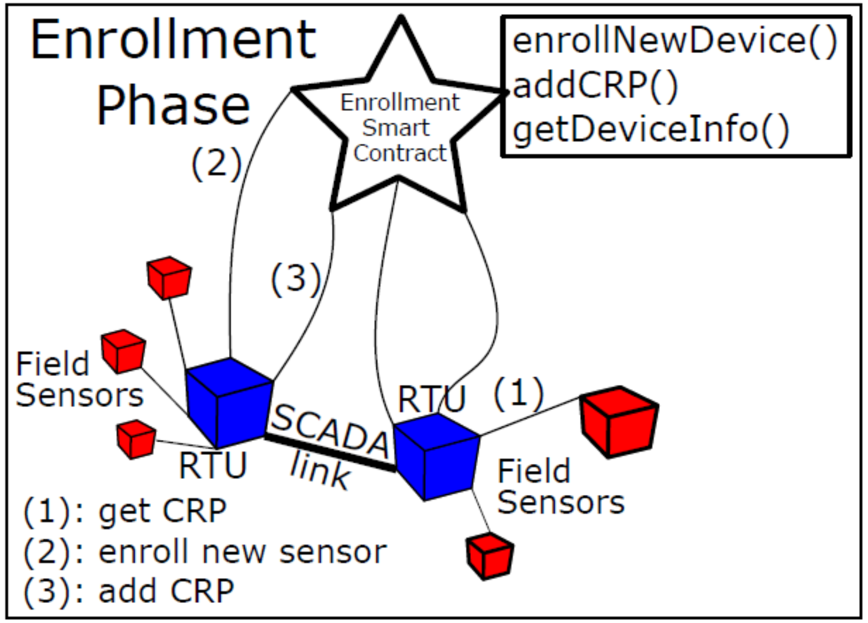
BIoSPAI protocol

Three-phase protocol

- Profiling
- Enrollment
- Authentication

Enrollment

- Generate and store CRP
- Enrollment Smart Contract



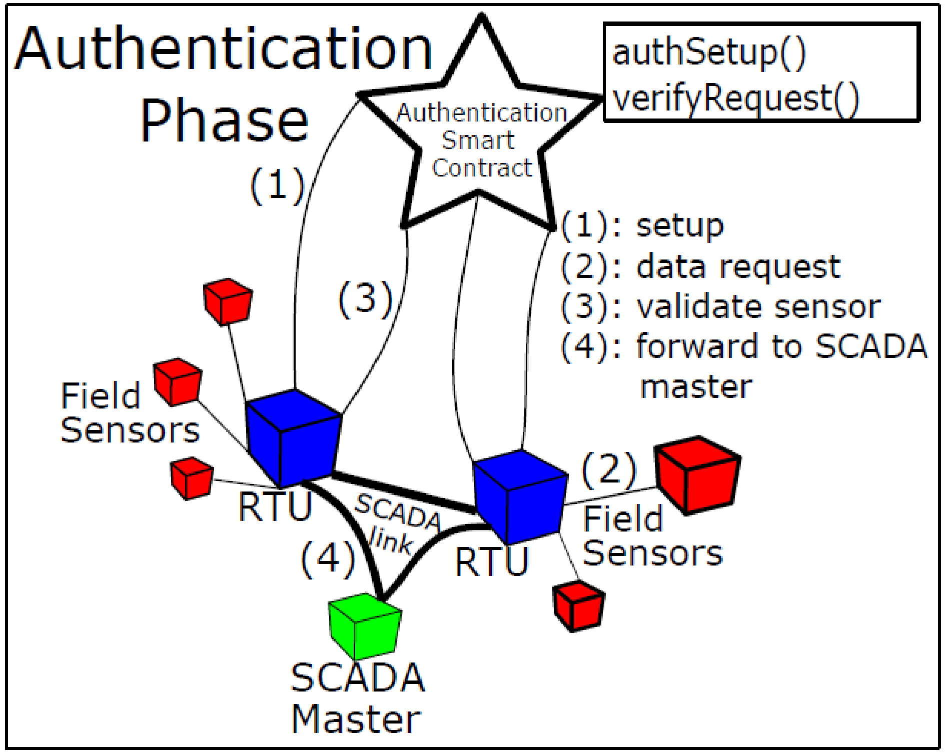
Profiling

- Identify strong cells by integration of data remanence algorithm.

BIoSPAI Protocol: Authentication Phase

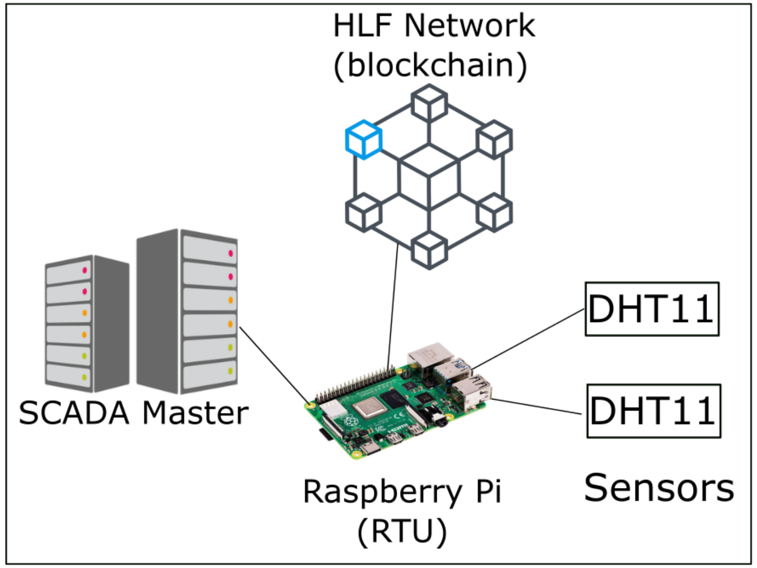
- Ensures the authenticity of request and sensing data flow integrity by integration a HLF network.

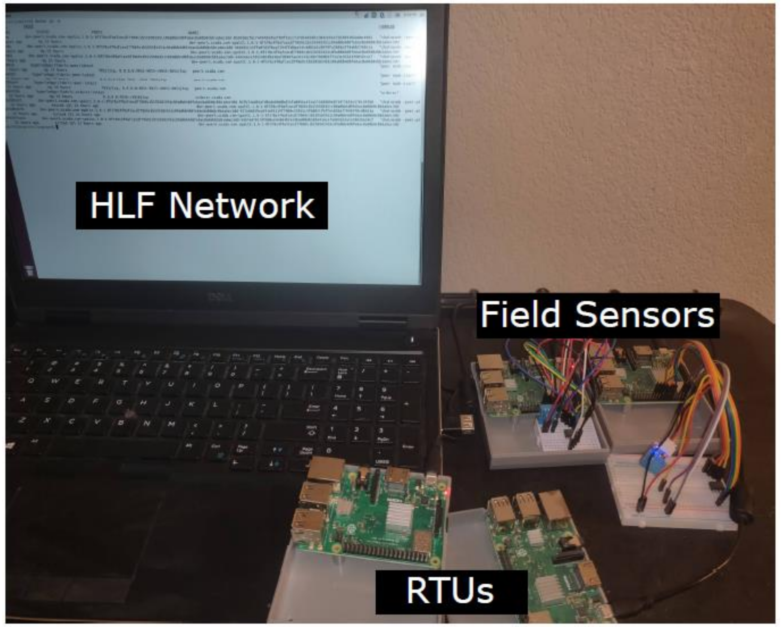
- The authentication phase prevents critical information disclosure through lightweight crypto solutions and ledger-integrated network.



Testbed setup

- Emulated RTU function, in a Raspberry Pi 3 model B.
- Raspberry pi is connected to the external SRAM microchip 23LC1024 and a HLF network.

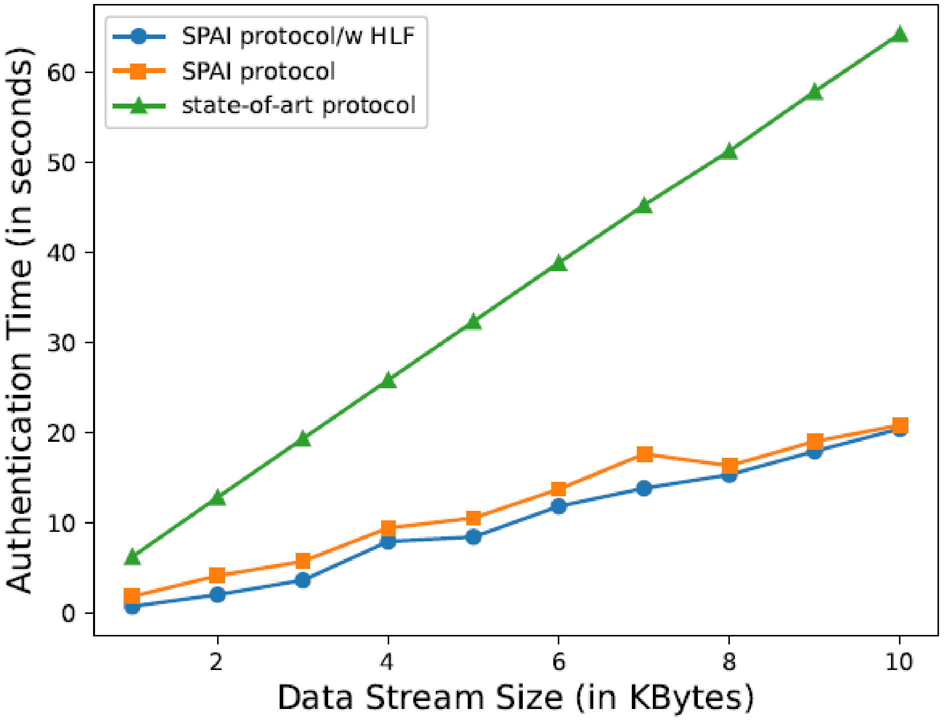




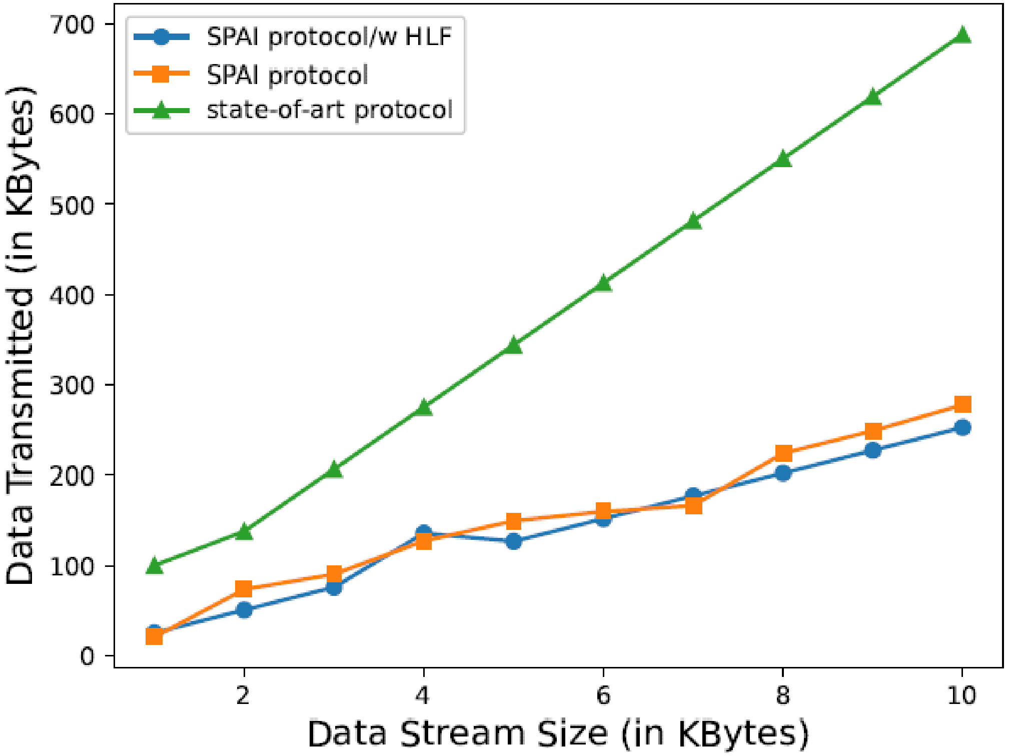
Evaluated the overhead of the BIoSPAI protocol in a temperature and humidity sensor DHT11, the sensors reads and sends data every two seconds.

Evaluation

Time to complete authentication process for continuous data stream

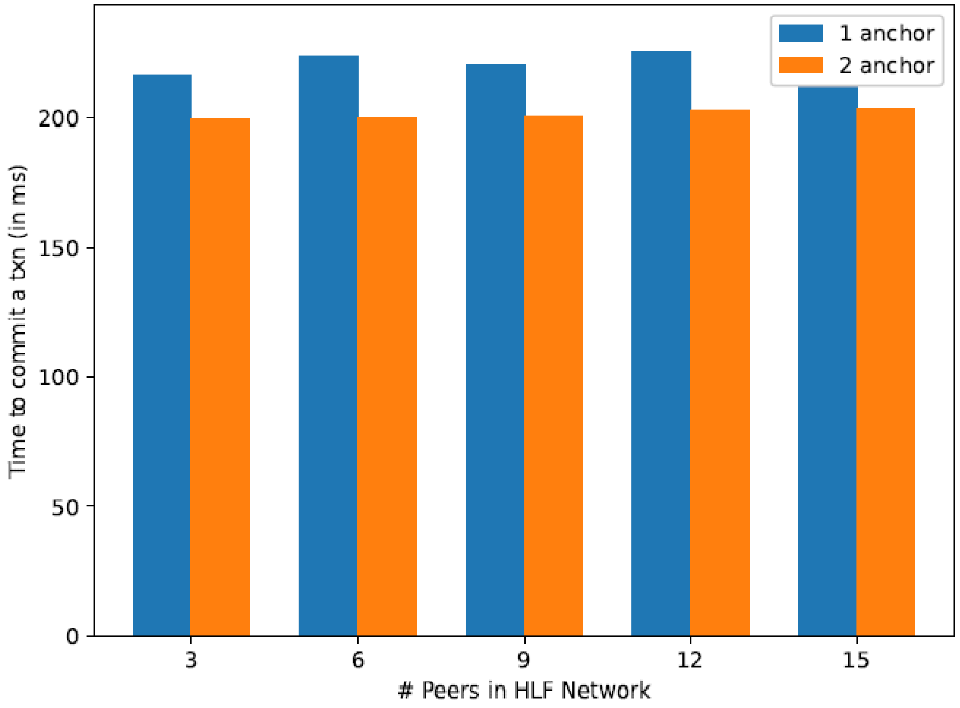


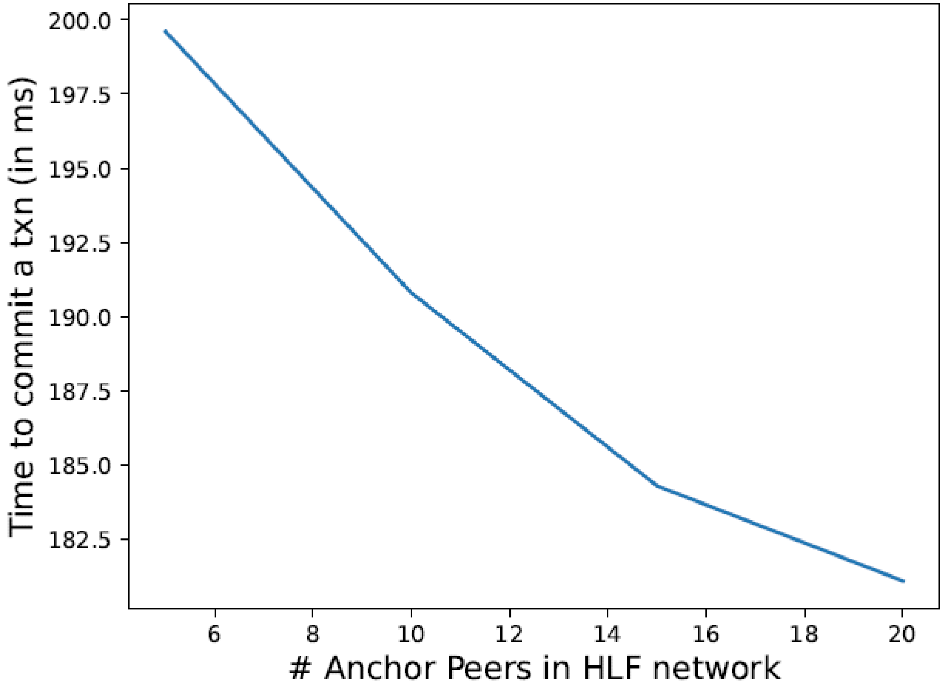
Total data communicated over modbus protocol for continuous data stream



Evaluation

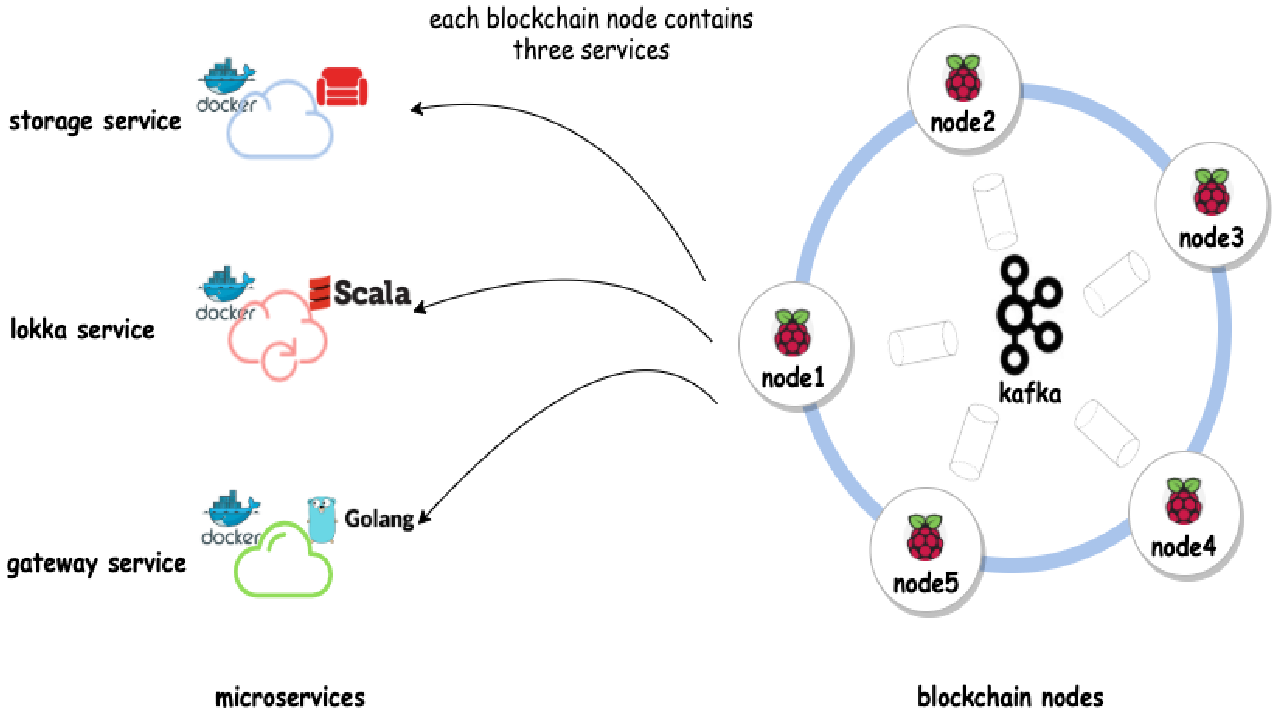
Average time to commit a transaction





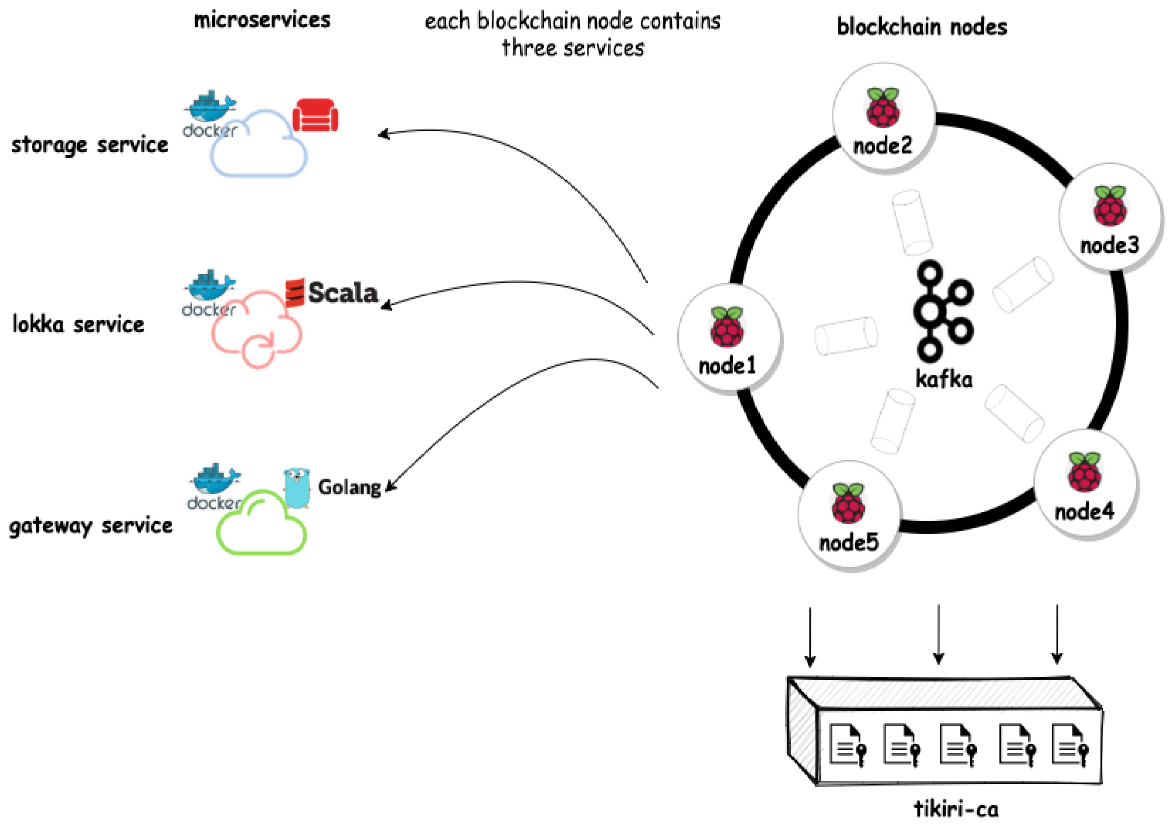
Tikiri - Lightweight and scalable blockchain

- Support real-time transaction
- Concurrent execution of blockchain transactions
- Support sharding based data replication to reduce the communication overhead
- Apache kafka based consensus to increase the scalability and throughput



Tikiri - Lightweight and scalable blockchain

- Microservices based smart contract architecture saas(smart actors as a service)
- Tikiri-ca certificate authority for zero trust architecture based security and privacy in tikiri blockchain



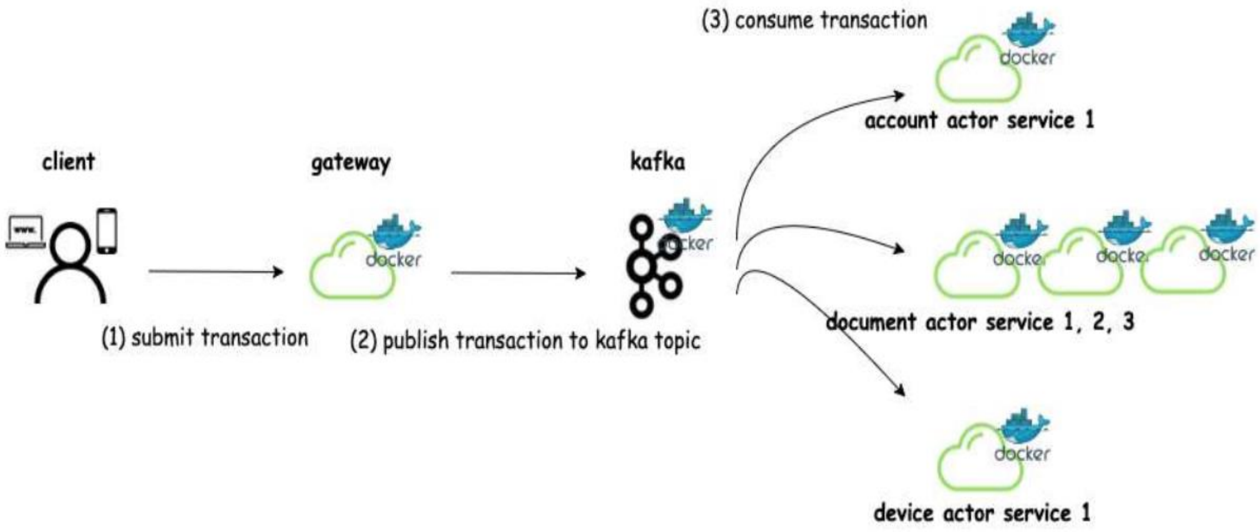
E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, Tikiri-towards a lightweight blockchain for iot, Future Generation Computer Systems (2021).

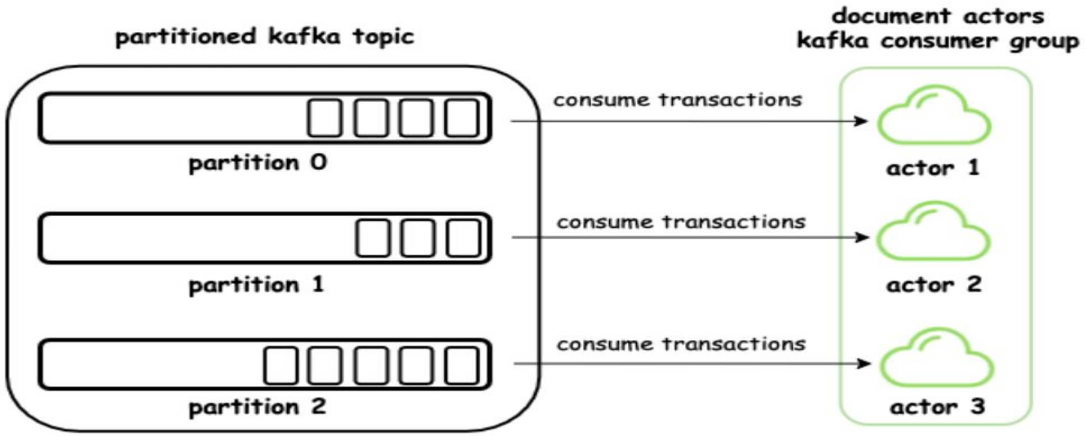
Tikiri - Lightweight and scalable blockchain

- Implemented on raspberry-pi cluster
- Apache kafka(zab) used as the consensus
- Used functional programming and acot actors based concurrent smart contract platform
- Smart contracts run with saas(smart actors as a service) architecture
- Tikiri-ca certificate authority and rule engine facilitates zero trust architecture based security and privacy for saas smart contract services

Tikiri - Lightweight and scalable blockchain

- Execute independent smart contracts on separate microservice
- Ensure smart contracts can execute transaction independently
- Multiple replicas of the smart contract service can be run parallelly
- Scalability and support high transaction throughput on tikiri blockchain





Tikiri –Proposed Zero Trust Architecture

- In saas smart contracts, tikiri blockchain supports zero trust architecture based security when communicating between smart contract services
- Certificates issued by tikiri-ca used to authenticate the requests between services
- Zero trust rules(authentication, authorization) of the smart contract services are stored in the rule engine
- Rules in smart contract services decides which requests to allow and reject

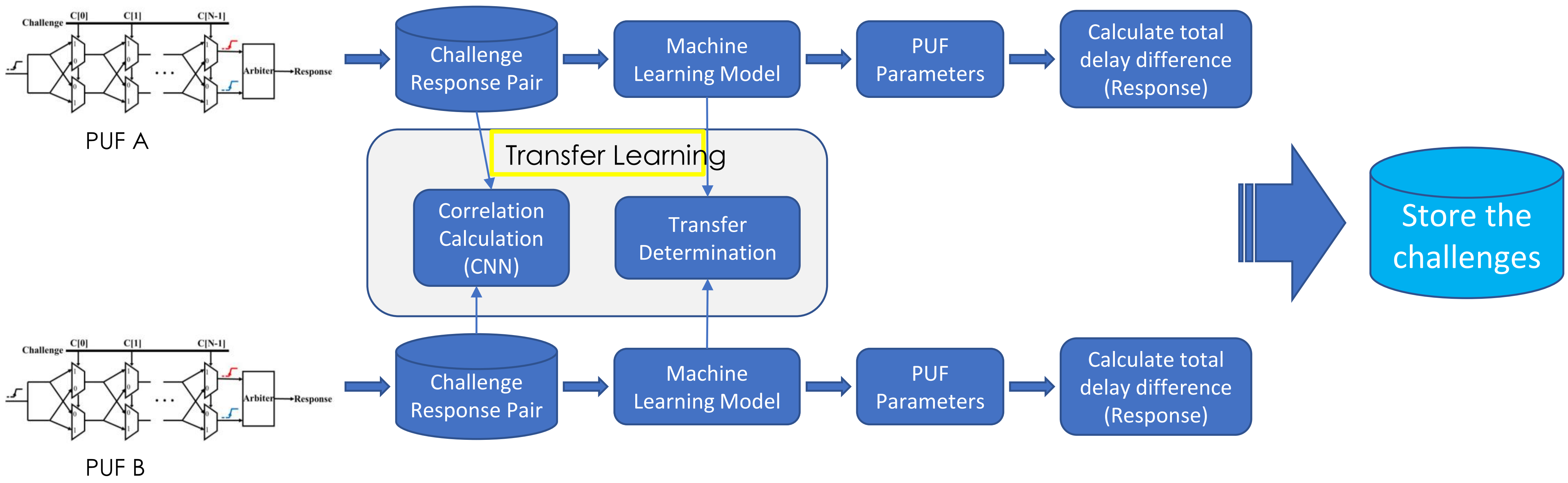
Collaboration with BLOSEM

- Discussions with BLOSEM resulting in following planned developments
- Improve resilience of continuous verification of devices using consensus
- Supporting Legacy devices who may not be compatible with SRAM based PUF
- Integrate with our Blockchain based supply chain design to allow onboarding of devices from vendors to the identity management system without severely compromising the minimum security threshold,
- Develop economic model for shared responsibility of smart contract execution cost.

Machine Learning Framework for Enhancing PUF Reliability-Collaboration with BLOSEM

- **Benchmark:** Machine Learning Technology for PUF Authentication
  - PUF parameter learning
    - Train a machine learning model using a subset of Challenge-Response pairs to model the PUF parameter
  - Challenge selection
    - Select challenges that can produce insensitive responses
- **Proposal:** Transfer Learning Technology for PUF Authentication
  - Capture the correlation between two sets of PUF's parameters and then control the level of transfer

Machine Learning Framework for Enhancing PUF Reliability-Collaboration with BLOSEM



Benefits and Other Research Areas

- Scalable data and process integrity assurance in FPP would help plant managers to better maintain the components
  - Reduce operational cost over long-run

- Establishment of overlay Blockchain for SCADA environment can also be applicable for achieving **access control and accountability**
  - Large and multi-site energy companies have many independent contractors, whose access to the infrastructure must be vetted

- **Supply-chain provenance** in energy delivery systems is critical and the proposed platform has potential to enable this service

Preparing Project for Next Steps

- **Market Benefits/Assessment**
  - The project addresses the need for an infrastructure based identity management and provenance solution that can provide early detection of rogue devices.
  - The proposed technology would realize a low cost security solution that would provide protection to large number of sensors in the power plant and lead to cost savings
- **Technology-to-Market Path**
  - The Blockchain platform will be integrated into state-of-practice security monitoring solutions
  - Ensuring the ability to provide desired benefits at lower cost
  - Integration with AI solutions to also provide trusted source of ground truth
  - Collaborating with Accenture, ReliabilityFirst, WoodPLC

Concluding Remarks

- The technology developed by the project will address the following specific challenges in fossil energy
  - Identity management and provenance that would enhance the infrastructure cybersecurity.
  - Increasing system reliability due to early detection of attacks
  - Optimize utility efficiency by identifying and isolating faults
  - Enhanced security of monitoring technology by improving resilience to cyber attacks

Thank You

Sachin Shetty, Ph.D.
Email – sshetty@odu.edu
Web – www.odu.edu/~sshetty