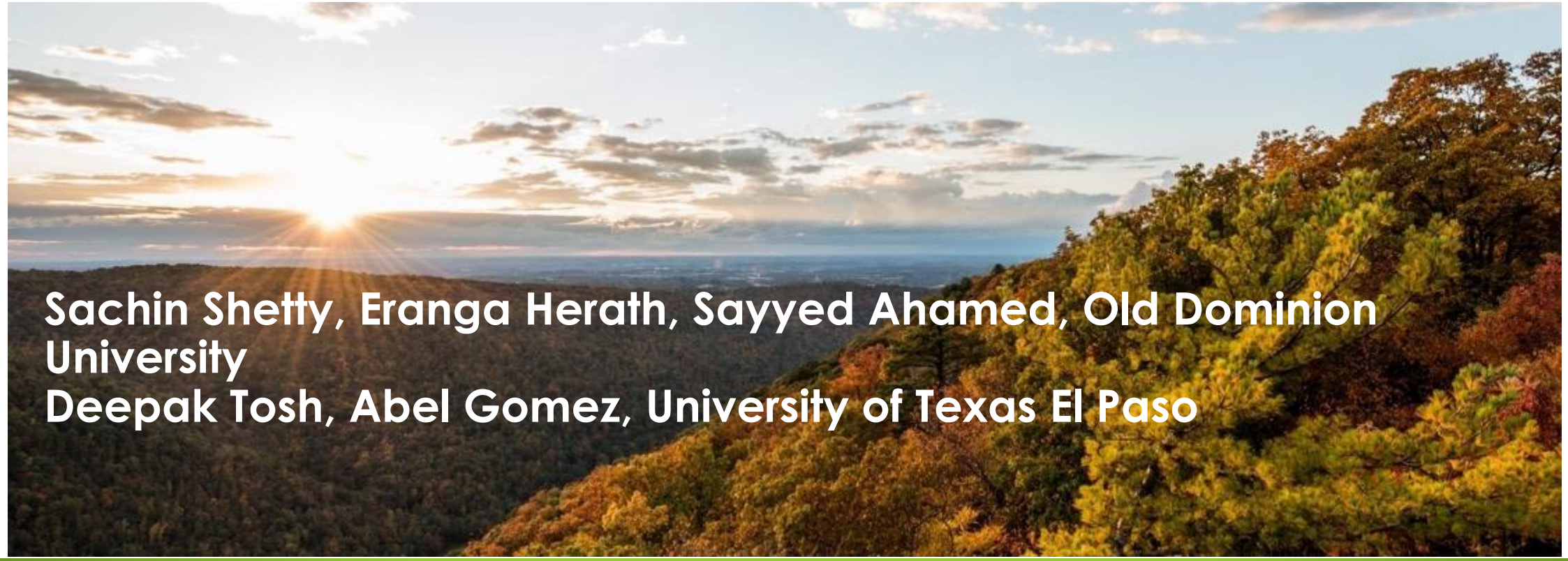
Blockchain Empowered Provenance Framework for Sensor Identity Management and Data Flow Security in Fossil-Based Power Plants



Sachin Shetty, Eranga Herath, Sayyed Ahamed, Old Dominion University
Deepak Tosh, Abel Gomez, University of Texas El Paso

Project Description

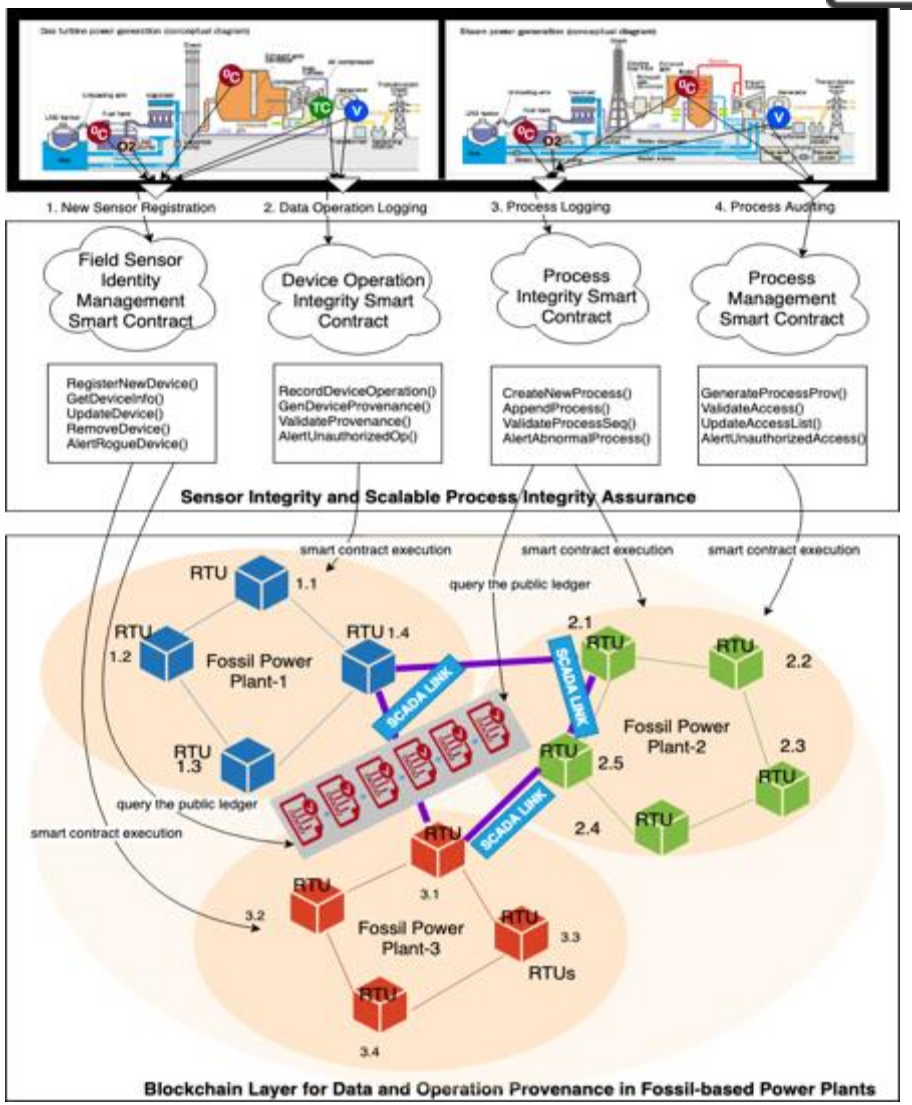
- **Project Goal** - Blockchain empowered provenance platform for identity management and process integrity for sensors in *Fossil-based Power Plants (**FPP**)*.
- **Strategic alignment with DOE -** Improving electric grid reliability, resilience and availability
- **DOE-NETL** –Dr. Sydni Credle and 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

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

- Devised a behavior-based Runtime State Verification (RSV) protocol that enables process integrity assurance
- Implemented the RSV in an emulated Fossil Power Plant
- Published BloSPAI paper in Cluster Computing Journal
- Submitted MBRSV protocol to IEEE Transactions on Smart Grid
- Published research results for Tikiri, a lightweight and scalable Blockchain platform at Future Generation Computer Systems Journal
- Reliable PUF capability within Tikiri

Achieving Runtime State Verification Assurance in Critical Cyber-Physical Infrastructures

NATIONAL ENERGY TECHNOLOGY LABORATORY

Problem Statement:

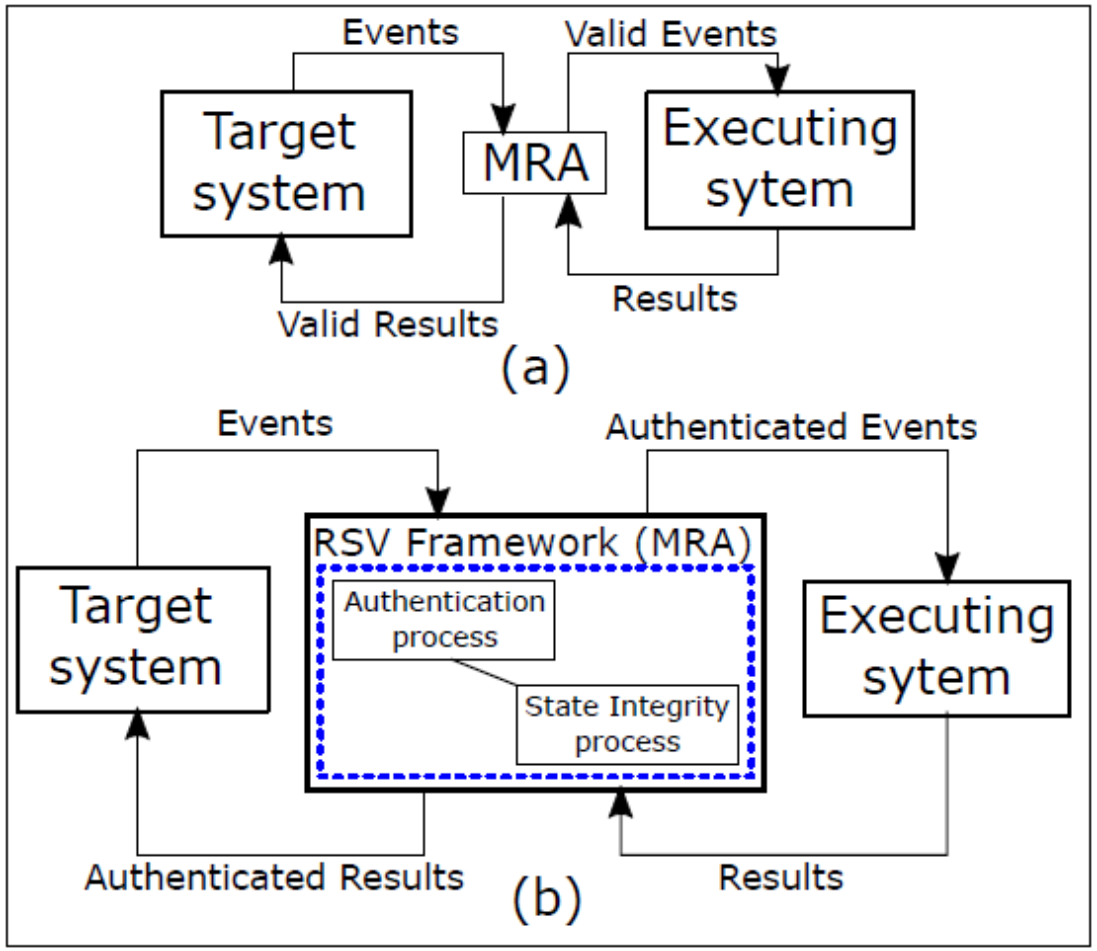
Traditional SCADA systems were not designed to monitor and record control process flow at the **granularity** associate with state-of-art **Intrusion Detection Systems** (IDS).

IDEA:

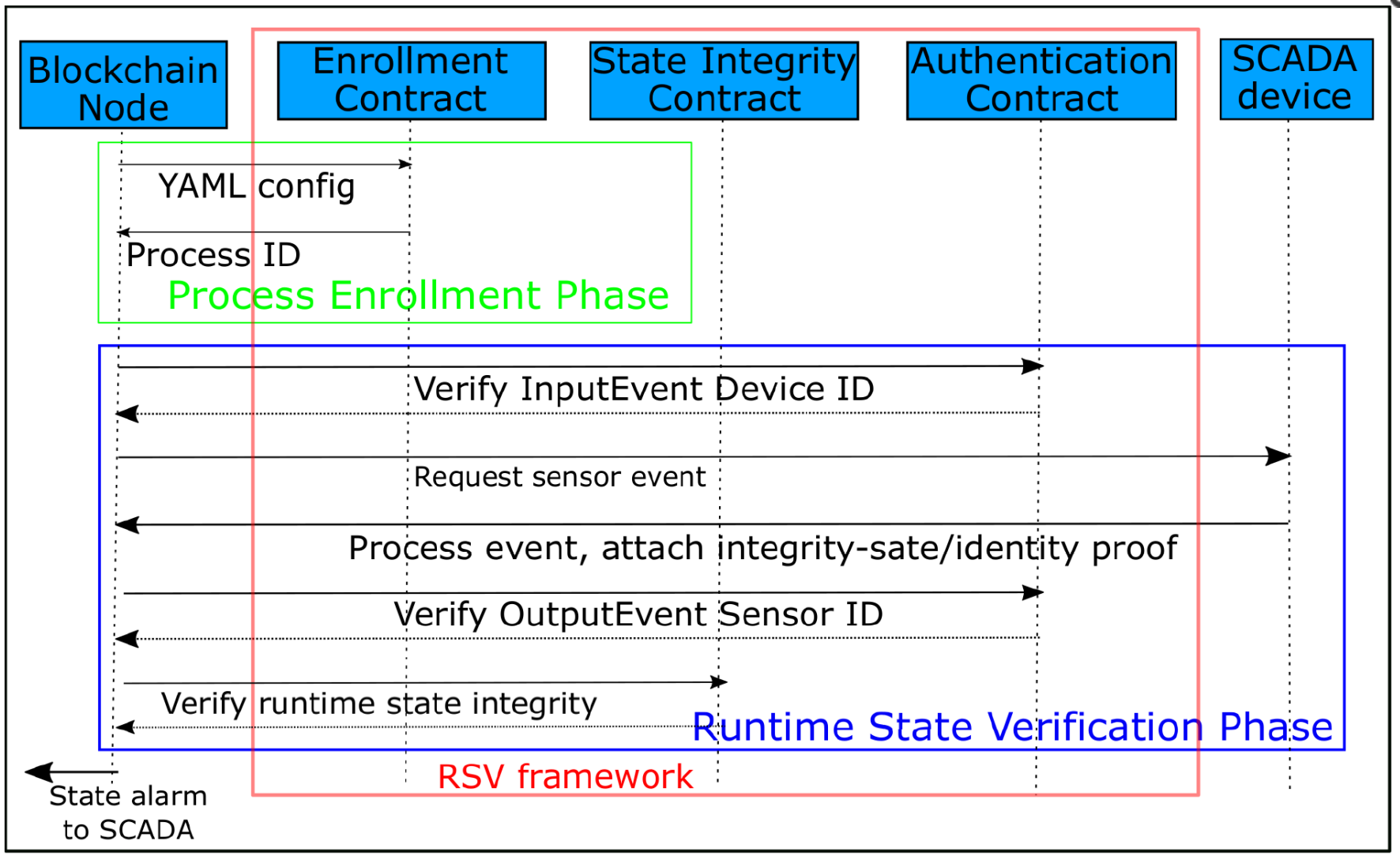
Our approach **leverages** the **pull-push** based communication protocol to extract device's behavior through **non-intrusive** monitoring services

Proposed Approach

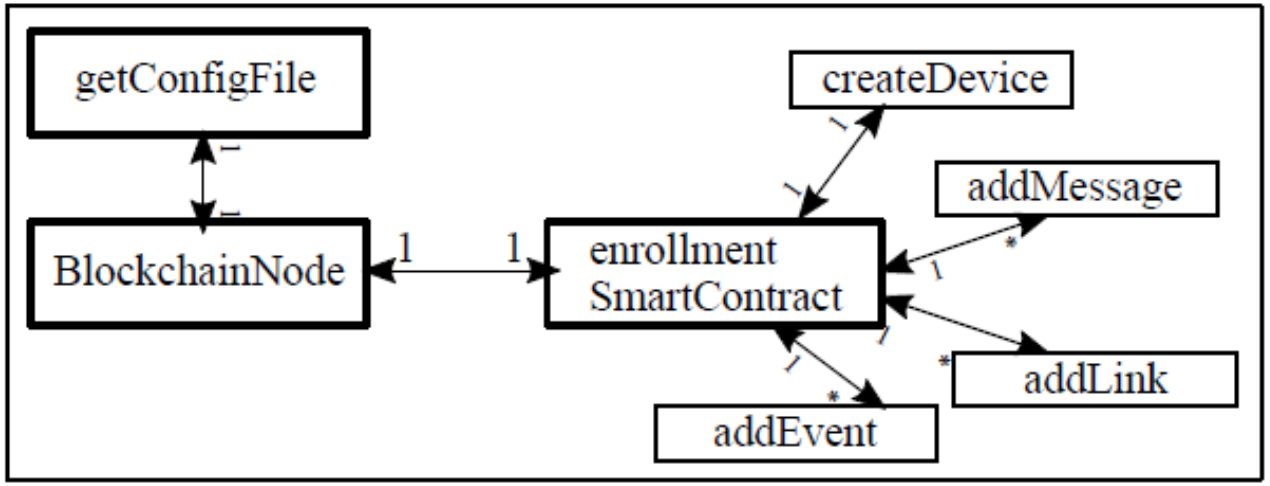
- Process integrity
- RSV protocol
- Mandatory Results Autonoma (MRAs)



Runtime State Verification (RSV) Protocol



Phase 1: Process Enrollment




```
{
    "processID": "CE",
    "device": [
        {
            "deviceID": "1501",
            "state": "00",
            "prvState": "00",
            "message": ["su", "cc", "du", "da", "pd", "ss"],
            "event": ["A1", "A2", "A3", "A4", "01", "03"]
        },
        {
            "deviceID": "1502",
            "state": "00",
            "prvState": "00",
            "message": ["su", "cc", "du", "da", "pd", "ss"],
            "event": ["B1", "B2", "B3", "B4", "01", "03"]
        },
        {
            "deviceID": "1503",
            "state": "00",
            "prvState": "00",
            "message": ["su", "cc", "du", "da", "pd", "ss"],
            "event": ["C1", "C2", "C3", "C4", "01"]
        }
    ],
    "message": ["su", "cc", "du", "da", "pd", "ss"],
    "dependency": [
        {
            "prvEvent": "00",
            "nxtEvent" : "03"
        },
        {
            "prvEvent": "03",
            "nxtEvent" : "A3"
        },
        {
            "prvEvent": "03",
            "nxtEvent" : "B3"
        },
        {
            "prvEvent": "E3",
            "nxtEvent" : "D4"
        },
        {
            "prvEvent": "03",
            "nxtEvent" : "D3"
        },
        {
            "prvEvent": "D3",
            "nxtEvent" : "D4"
        }
    ]
```

Phase 2: Runtime State Verification

Behavior-based Authentication Process:

Algorithm 1: authEvent

1 **Input:** eventRequest
2 **Output:** validEvent(bool)
Require: Access HLF network
1: $rq = readEventRequest()$
2: $hlfEventID = (rq.deviceID + rq.event) \oplus scrtkey$
3: **if** $rq.devicEventID! = hlfEventID$ **then**
4: $sendNotification()$
5: exit
6: **end if**
7: **return** $eventValid$

State Integrity Process:

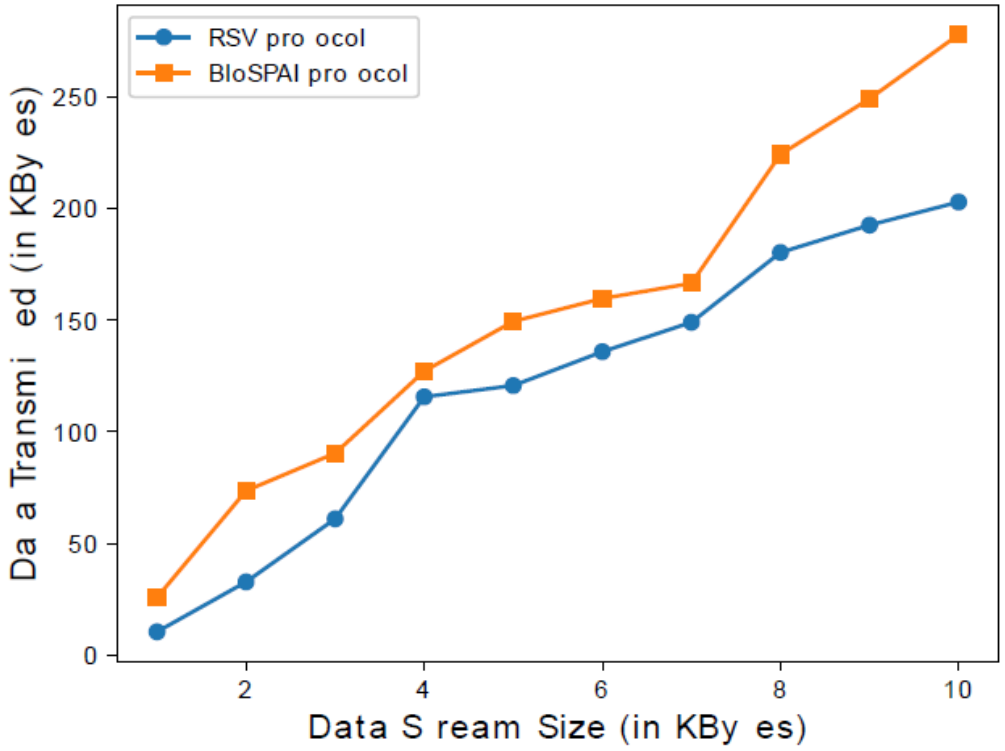
Algorithm 2: verifyState

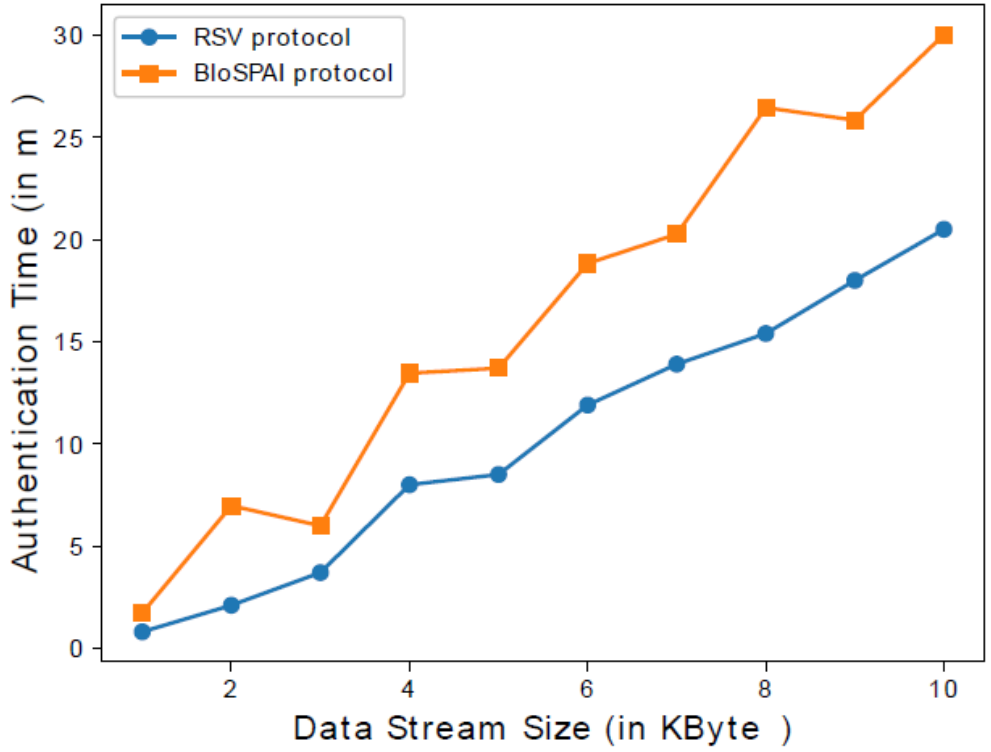
1 **Input:** ModbusPacket:event
2 **Output:** verifyEvent:bool
Require: Access to enrollment smart contract
1: $rq = readEventRequest()$
2: $deviceID = rq.deviceID$
3: $event = rq.event$
4: $D = event.getDepency()$ `// get dependencies from physical process`
5: $prevState = getPreviousState(deviceID)$
6: $currState = event$
7: **if** $!validEvent(event, deviceID)$ **then** `// is the event valid for the given device`
8: $verifyEvent = false$
9: $notifySCADA$
10: **end if**`// check that dependency is satisfied`
11: $dependency = D.find(currState)$
12: **if** $notEqual(dependency.nxtEvent, currState)$ **then**
13: $verifyEvent = false$
14: $notifySCADA$
15: **end if**
16: **if** $notEqual(dependency.prvEvent, prvState)$ **then** `// runtime state is out of sequence`
17: $verifyEvent = false$
18: $notifySCADA$
19: **end if**
20: **return** $verifyEvent$

Testbed setup

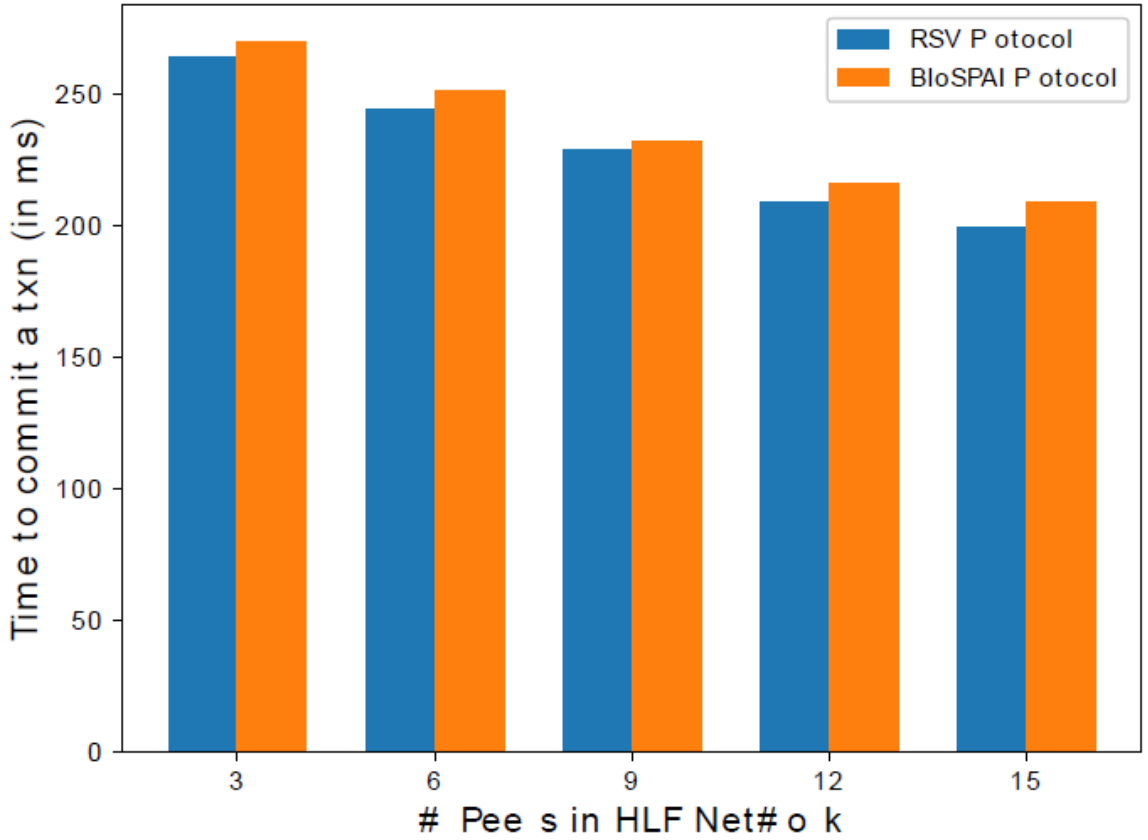
- Dell PowerEdge T440 Tower Server with a 28 cores Intel Xeon and 64GB of memory.
- Data stream size of 1Kb to 10Kb

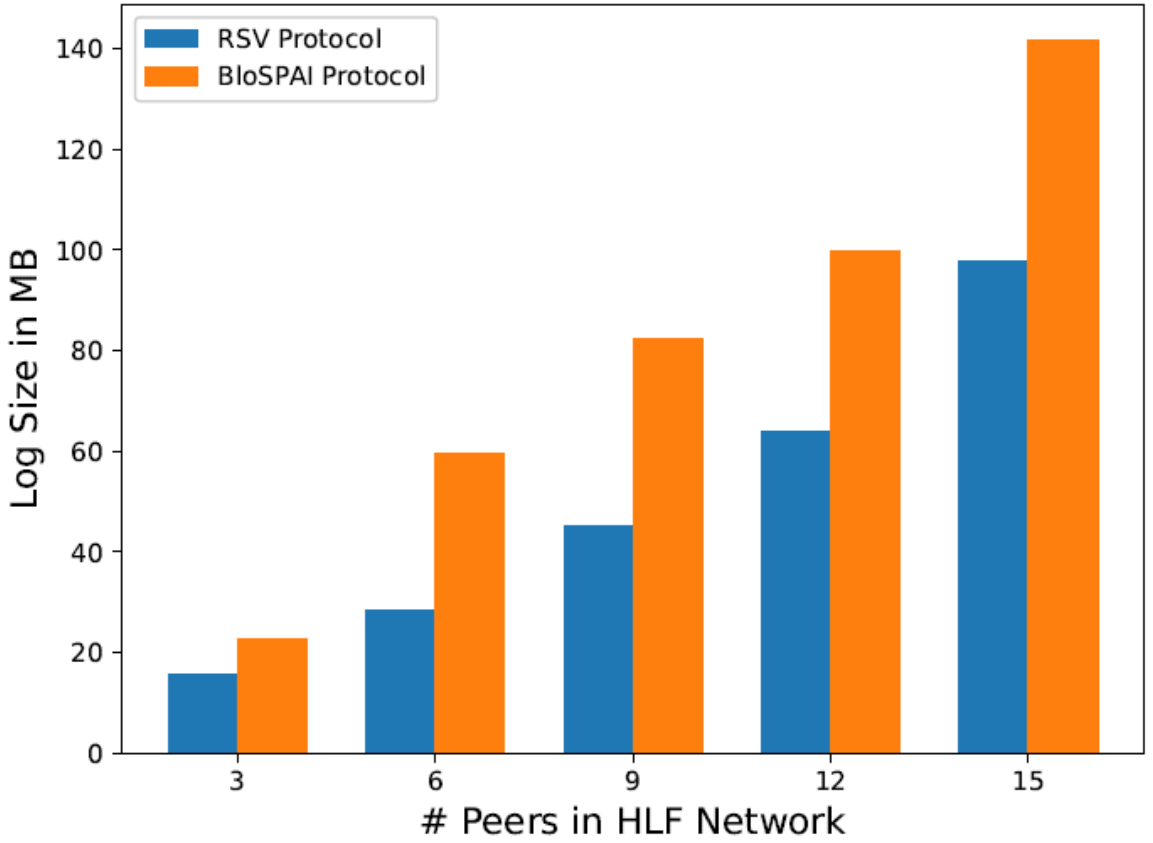
Evaluation RSV protocol





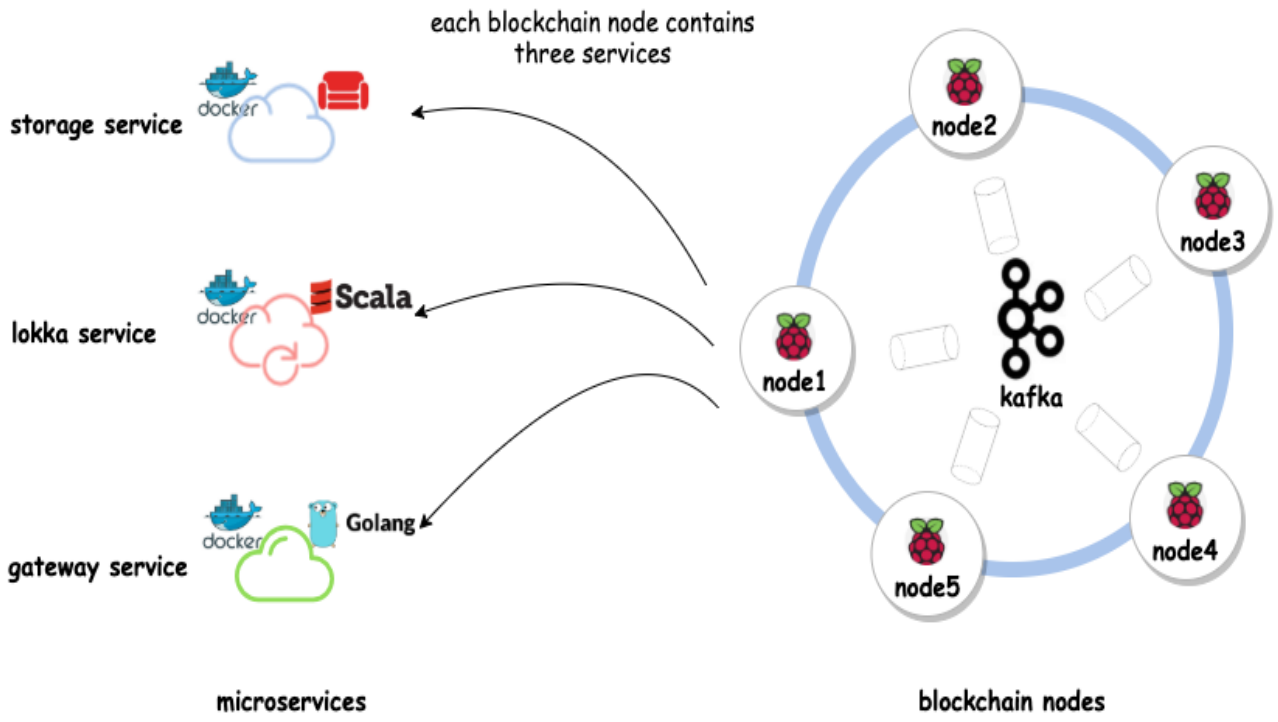
HLF Evaluation





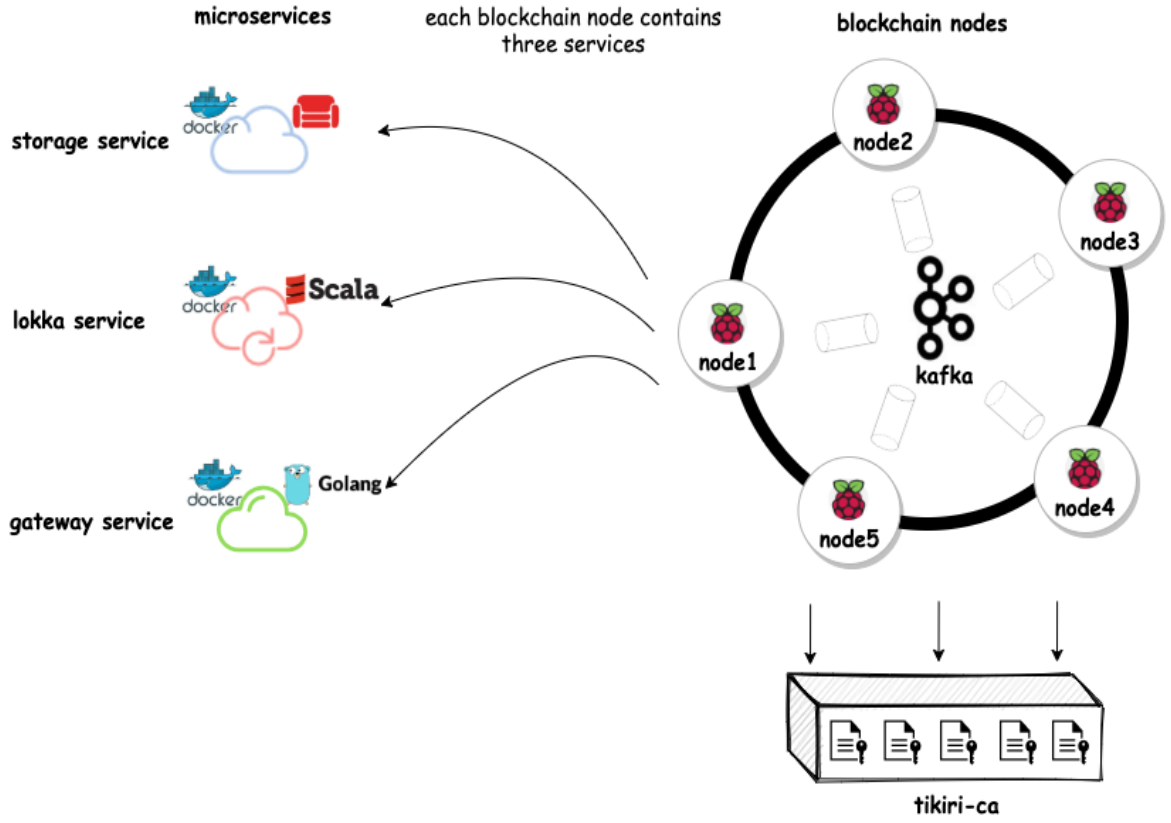
Tikiri - Lightweight and scalable blockchain

- 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).

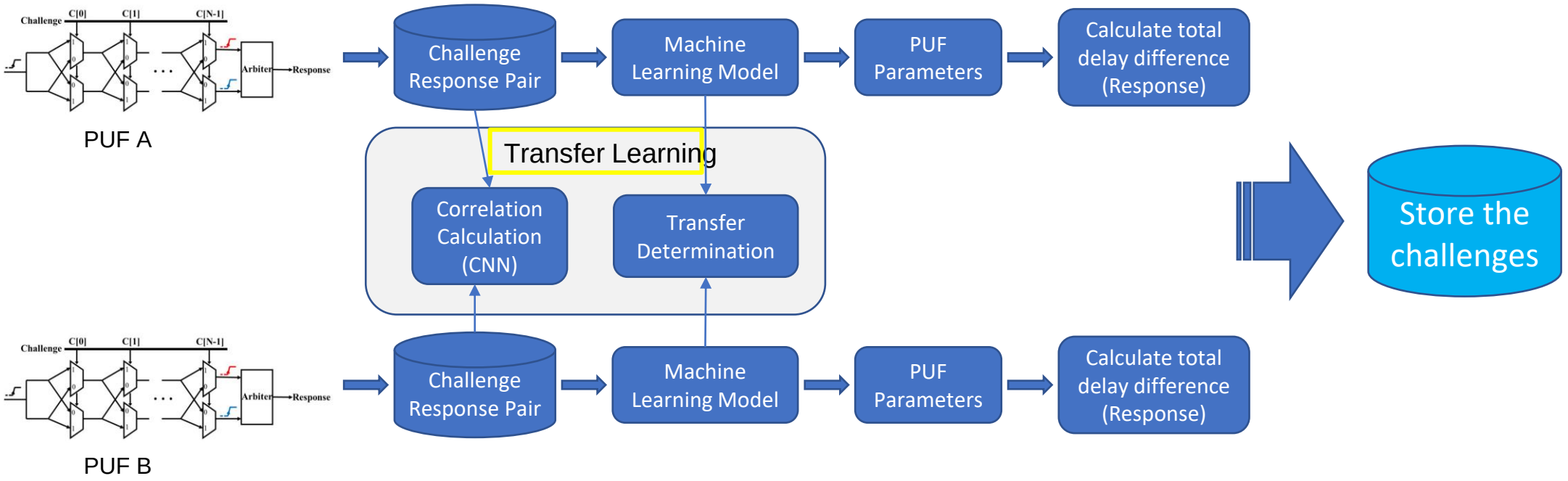
Collaboration with BLOSEM

- 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.

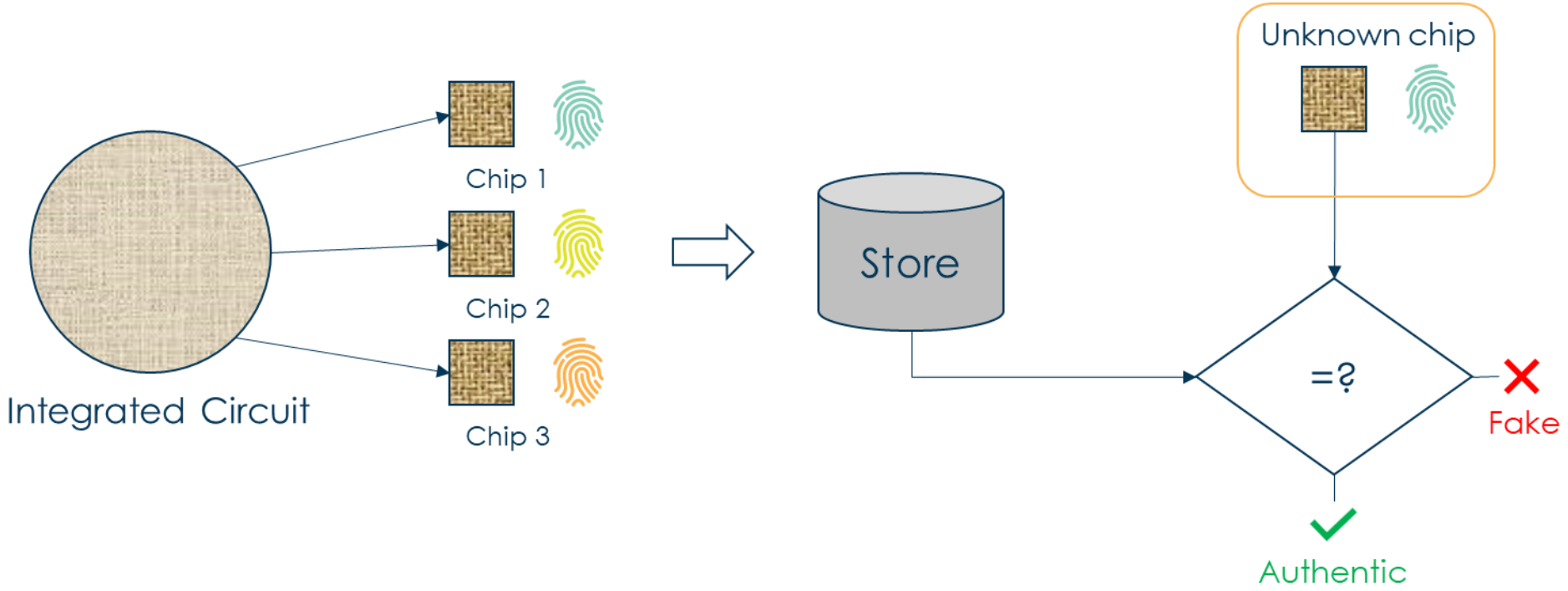
Machine Learning Framework for Enhancing PUF Reliability- Collaboration with BLOSEM

- **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



Physically Unclonable Functions (PUFs)



Objective

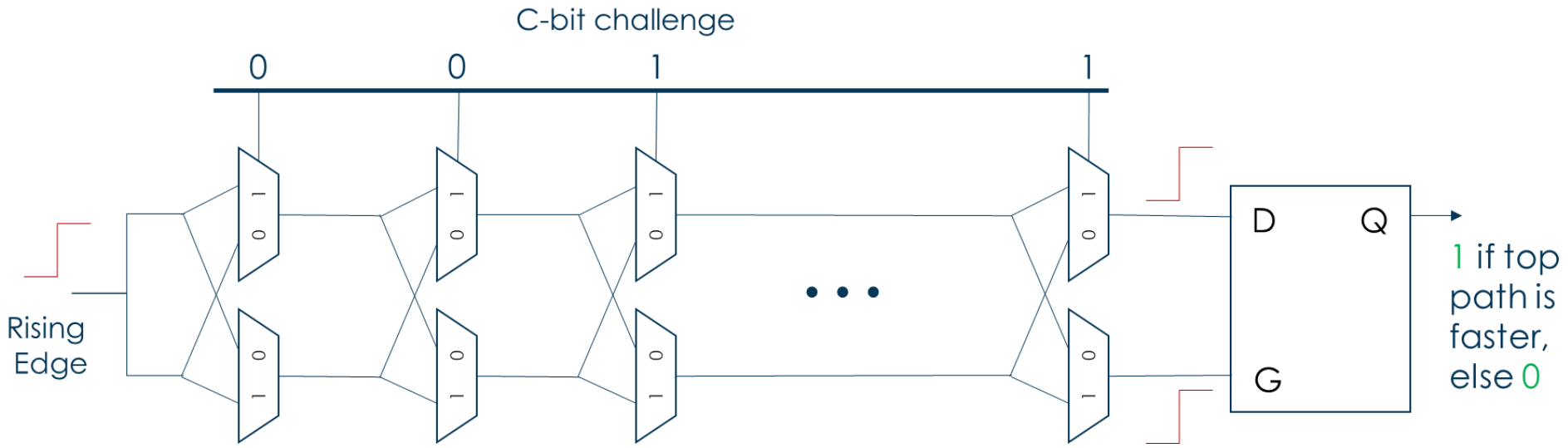
Problem Statement:

- Given PUFs challenge-response pairs (CRPs).
- Can we predict the future response for any incoming challenge and create transferability between PUFs for future prediction?

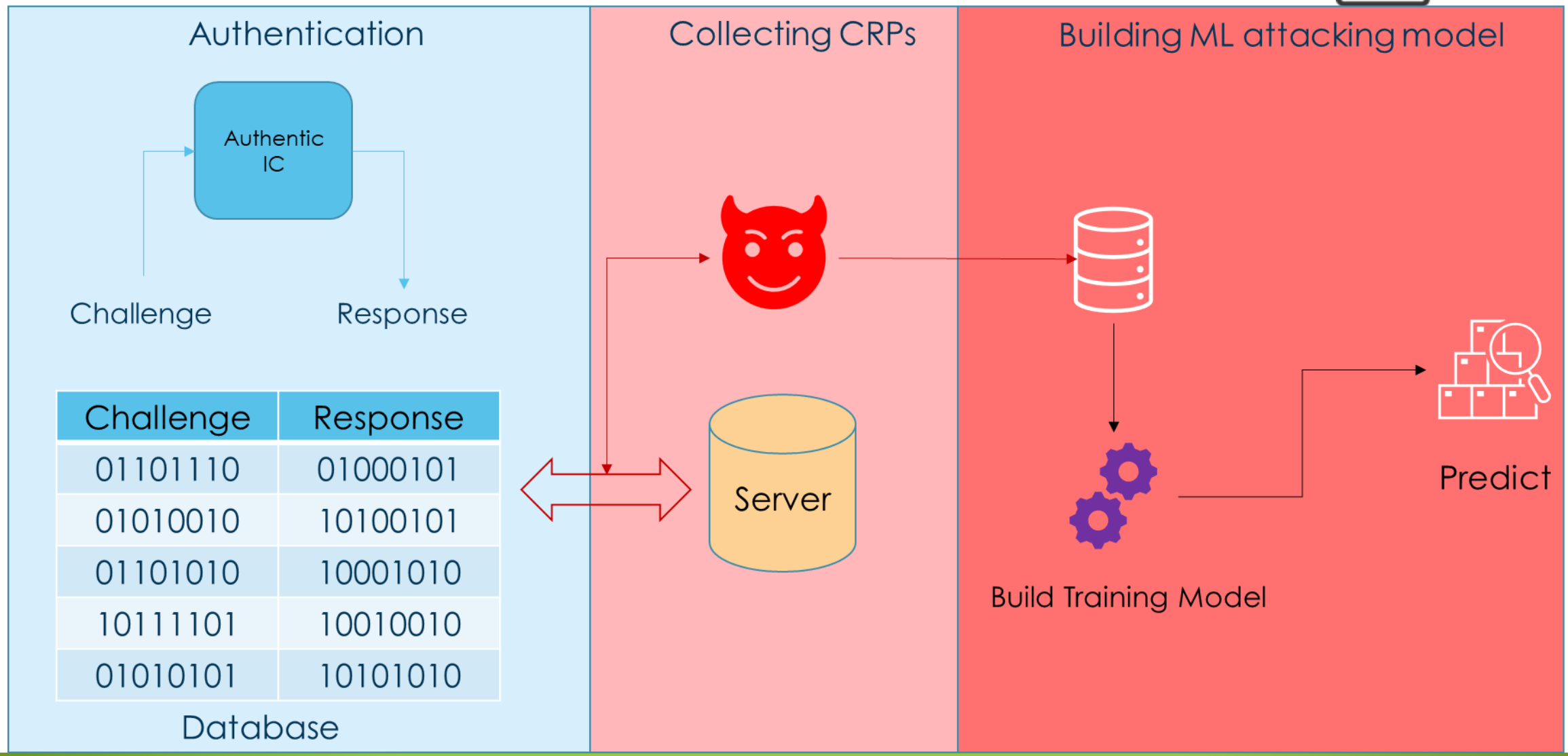
IDEA:

- Quantify the correlation between PUFs parameters and determine the transfer level.

Arbiter PUFs



Modeling Attack on PUFs



PUFs Modeling Attack Evaluation

PUF # A:

- Bit: 129
- Features: 128
- Response: 1/-1
- XOR: 5
- Training: 5 million
- Test: 1 million
- Optimizer: ADAM
- Accuracy:
  - Training: 92%
  - Validation: 89%

PUF # B:

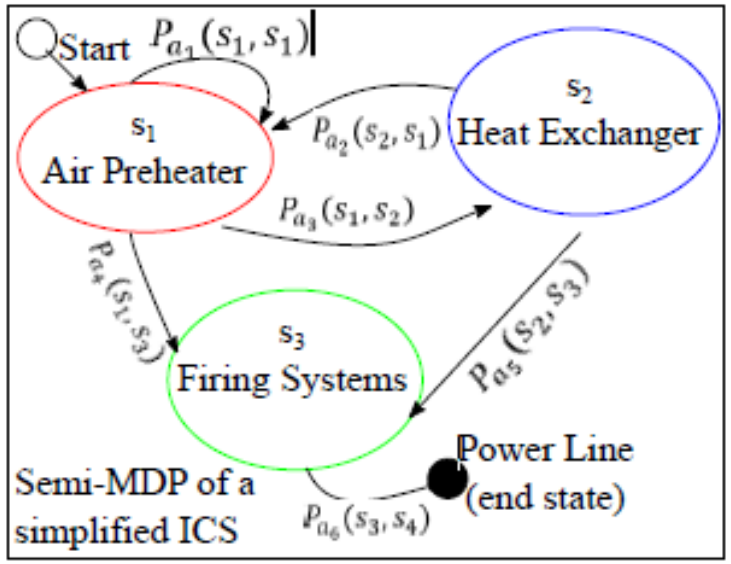
- Bit: 65
- Features: 64
- Response: 1/-1
- XOR: 6
- Training: 2 million
- Test: 400k
- Optimizer: ADAM
- Accuracy:
  - Training: 98%
  - Validation: 96%

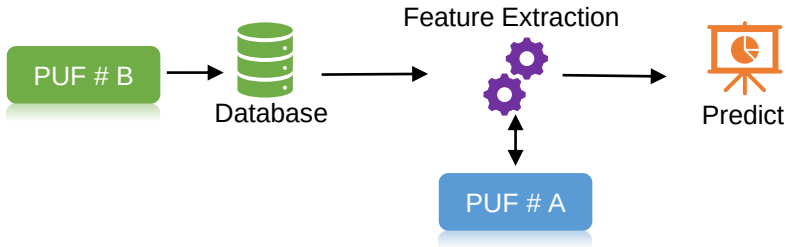
Concluding Remarks

- We proposed an RSV protocol that aims to provide continuous runtime state verification assurance of constrained field devices in traditional SCADA ecosystems.
- Besides achieving process integrity assurance in traditional SCADA ecosystems, the RSV protocol also addresses the shortcomings of the BIoSPAI protocol.
- The preliminary experiments demonstrated that the RSV protocol provides continuous runtime state verification and integrity assurance while achieving operational constraints in an emulated water-tube boiler.
- We aim to develop triage PUF authentication, where we improve the performances of training and prediction of PUF response. We focus on the reducing the computing delay, while still guaranteeing the accuracy performance.

Future Work

- Leverage reinforcement learning mechanisms to achieve autonomous control process integrity assurance
- We will employ transfer learning to measure the similarity between the source and target for the case of multi-group of PUFs.
- We use CNN to extract the silent features and compute the correlation coefficient as well as determine the exchanging level accordingly.





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