Towards a Secure Behavior Modelling for IoT Networks using Blockchain

- **Jawad Ali**
- **Dr. Ahmad Shahrafidz Khalid**
- **Prof. Dr. Shahrulniza Musa**

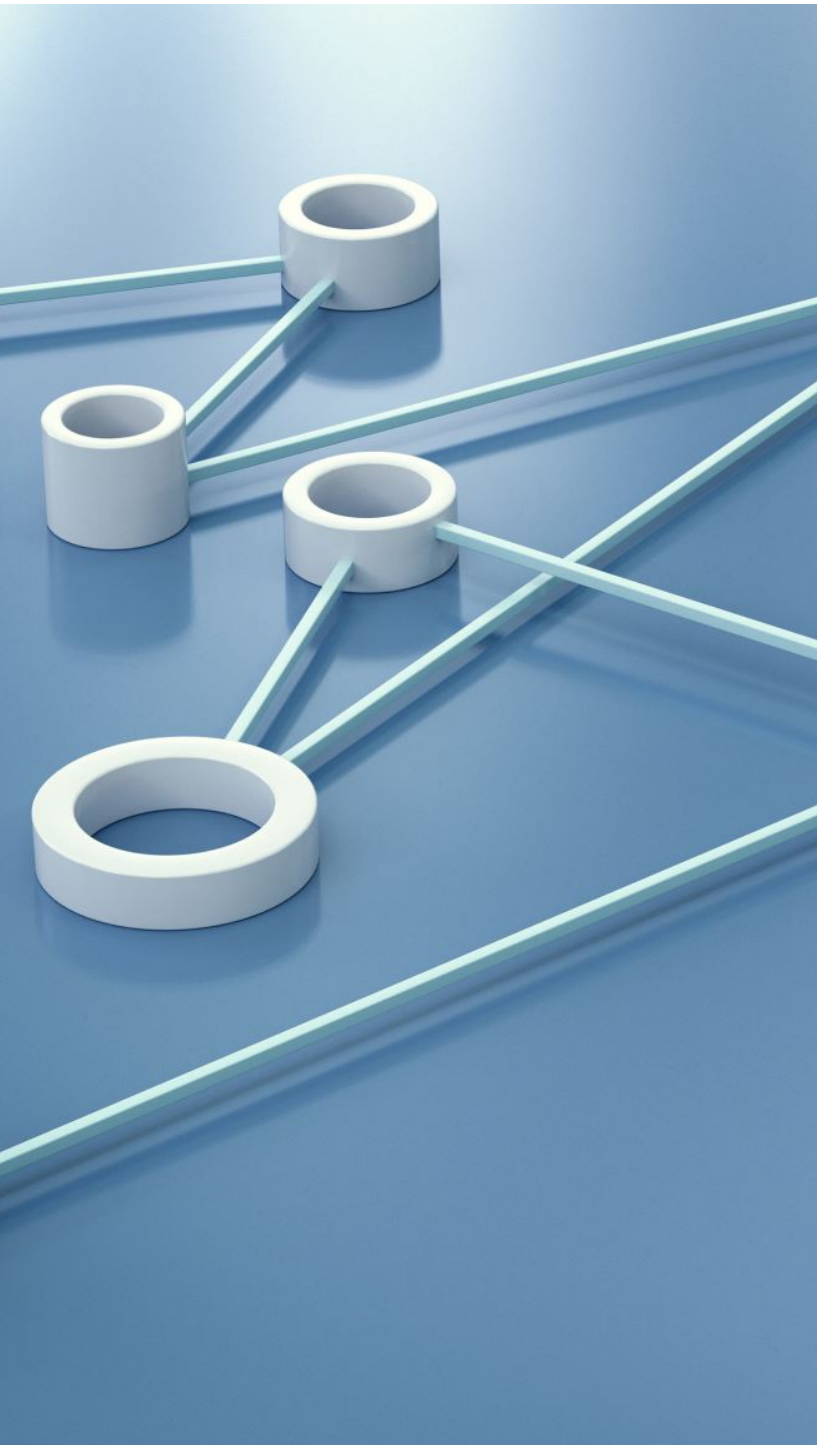
Contents

Introduction

- IoT is a widespread technology and will inclined to a huge number of devices in the near future.
- Numerous sensors are running in a distributed way and corporate really needs to monitor their own devices.
- Cyber attacks are very serious and even bring harms to human lives.
- A recent DDOS attack *(mirai)* affect millions of IOT devices [6].

Ideas

- There are many researches related to authentication, authorization, access control and trust of IoT devices
- From review, some improvement can be done:-
  - The behavior of the IoT devices are to be monitored
  - Need to use decentralized approach of access control instead of centralised approach for IoT devices
  - Need to have device level trust



Problem statements

- *Current centralized and decentralized security mechanisms for IoT ensure the authorization of end-nodes but still there is no mechanism regarding device behavior whether it is normal or malicious.*

- *This research proposed a mechanism that record the dynamic behavior of IoT device and verify it for normal or malicious*

Objectives

- To design a custom behavior monitor framework in IoT-Blockchain setup that can store data, monitor and classify IoT device behavior
- To apply filter on sensor-level that can stabilise output – faulty or malicious sensors will be rejected
- To implement Trusted Execution Environment (TEE) on a local blockchain IoT zone that ensure integrity and confidentiality of sensitive application code and data

Literature study - Blockchain and IOT

- Transactive IoT Blockchain applications [1]
- Blockchain solution for smart-home [2]
- Decentralized authentication mechanisms for IoT [3]
- Access control systems in IoT [4]

Behavioral Profiling of IoT devices

Selected Literature Study

- Fingerprinting IoT device: Features extraction from network traffic. [7]

  Machine Learning on Network Packets (i.e. TCP window size)

  [IoTSense: Behavioral Fingerprinting of IoT Device]

- Classification of Device Behavior in Internet of Things [8]

  Variable: Traffic feature analysis (IP-source & destination, TCP Port etc)

  [Classification of Device Behavior in Internet of Things Infrastructures: Towards Distinguishing the Abnormal From Security Threats]

- Context Extraction: Sensor data correlation in baseline data (bit level) [9]
- Learning of Packet frequency and size, of IoT device

Methodology

Studying security mechanisms for IoT network:

Choosing the best option for IoT security:

Studied Blockchain based security solutions in IoT:

Identifying the efficient blockchain type for IoT use-case:

Deploying a private blockchain and setting up the environment:

Design of the proposed framework:

Proof-of-Concept (POC) implementation for the proposed framework:

Setup of Testbed environment:

Results and Analysis:

Why Choosing Fabric BC for IoT

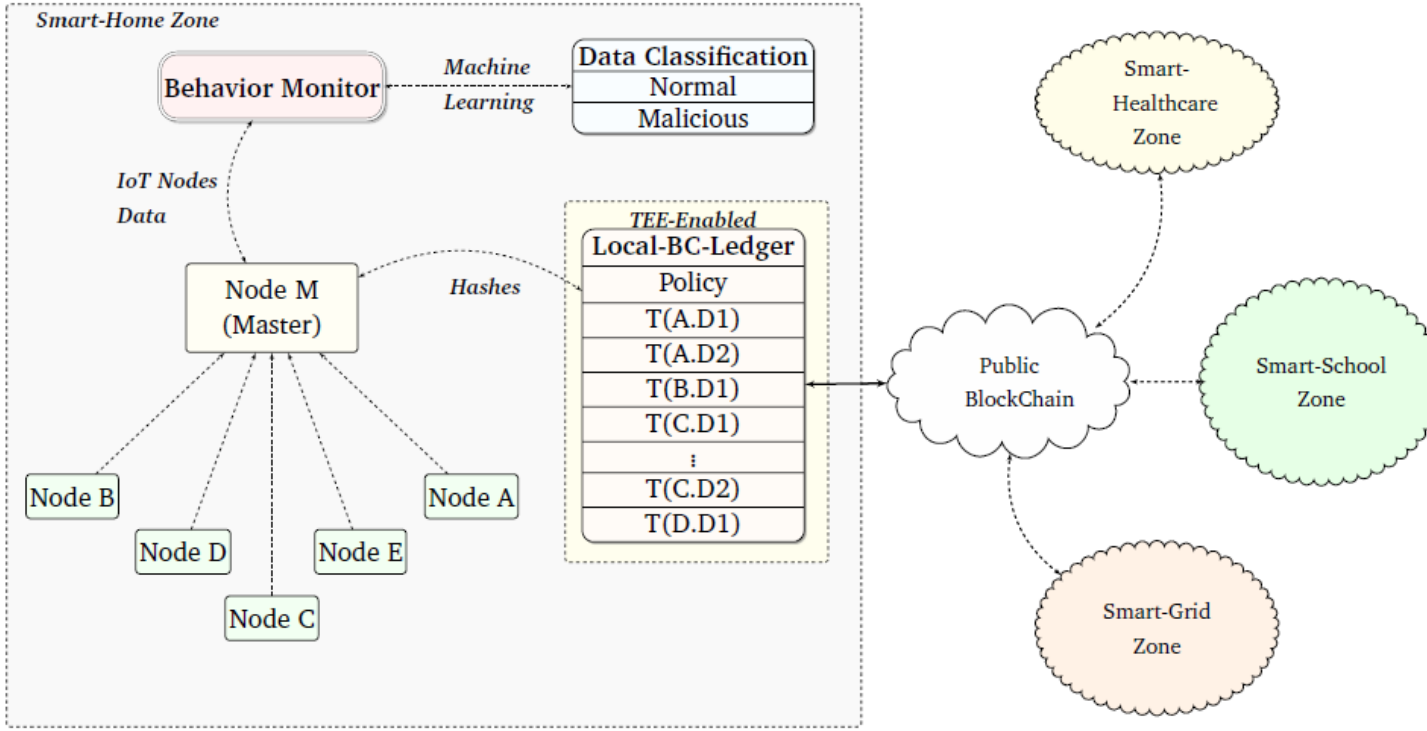
- To provide standardize BC solution for IoT.
- Permissioned BC
- Execute-order architecture which will results in efficiency.
- Pluggable consensus algorithm.

Design Goals

- Efficiency: Performance on the master node
- Accuracy: Algorithm used for optimal accuracy
- Pluggable: Design should be pluggable to other use-cases
- Updated and fresh information: Regularly updated information could well represent the device and the network
- Trustworthy mechanism
- Scalability

Entities in Proposed Framework

- Smart-Home Network
- Master node
- Blockchain



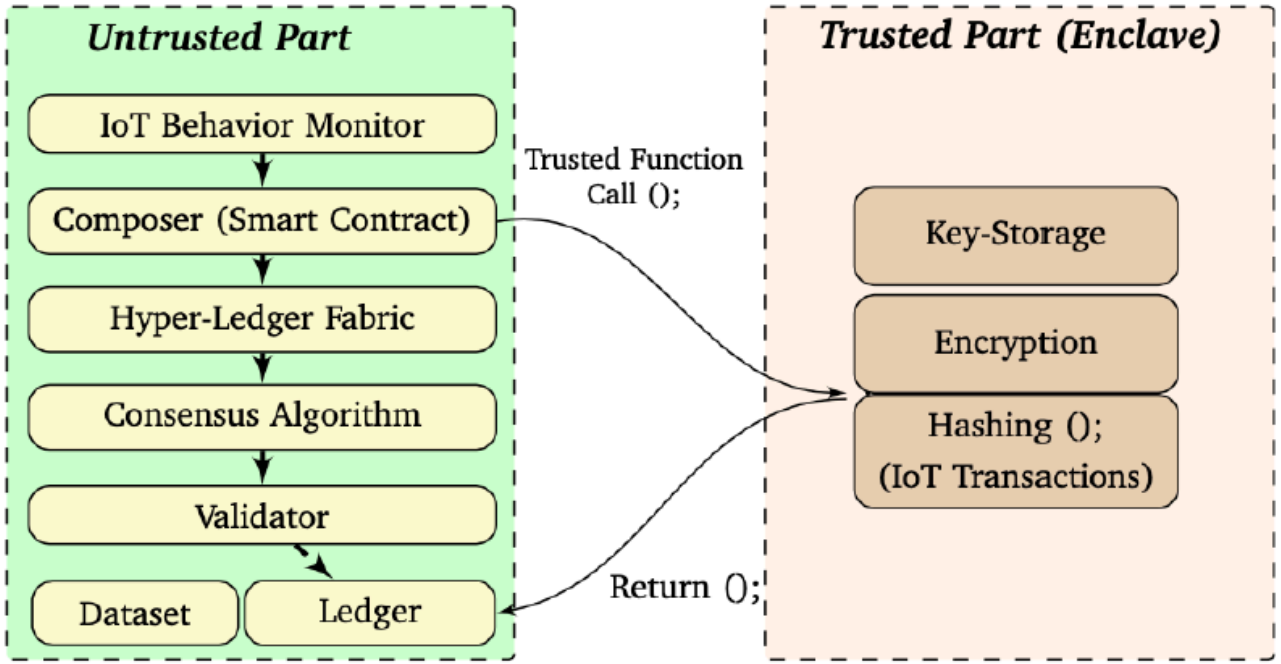
Proposed Framework (Cont)

- Transactions: i.e. Communication between devices
- Initialization and System functioning: selection of master node
- Local BC setup: Hyperledger Fabric implementation
- Behavior Monitor: To record the behavior of each node and calculate the trust-level of each zone.

Behavior Monitor

- The snapshots contains *sourceIP, DestIP, MAC-address and port Number.*
- Feature Extraction: Behavior snapshots of data arrived from IoT devices i.e. protocols and host related data.
- Training Model: Deep autoencoders is used to train the model, because of its complex correlation and better accuracy.
- Continuous Monitoring: The model is continuously monitored the incoming data and label each instance.
- Compromised node should be mark i.e. such as if someone spoof IP.

IoT secure behavior capturing and storage environment using TEE



Proof of Concept Implementation

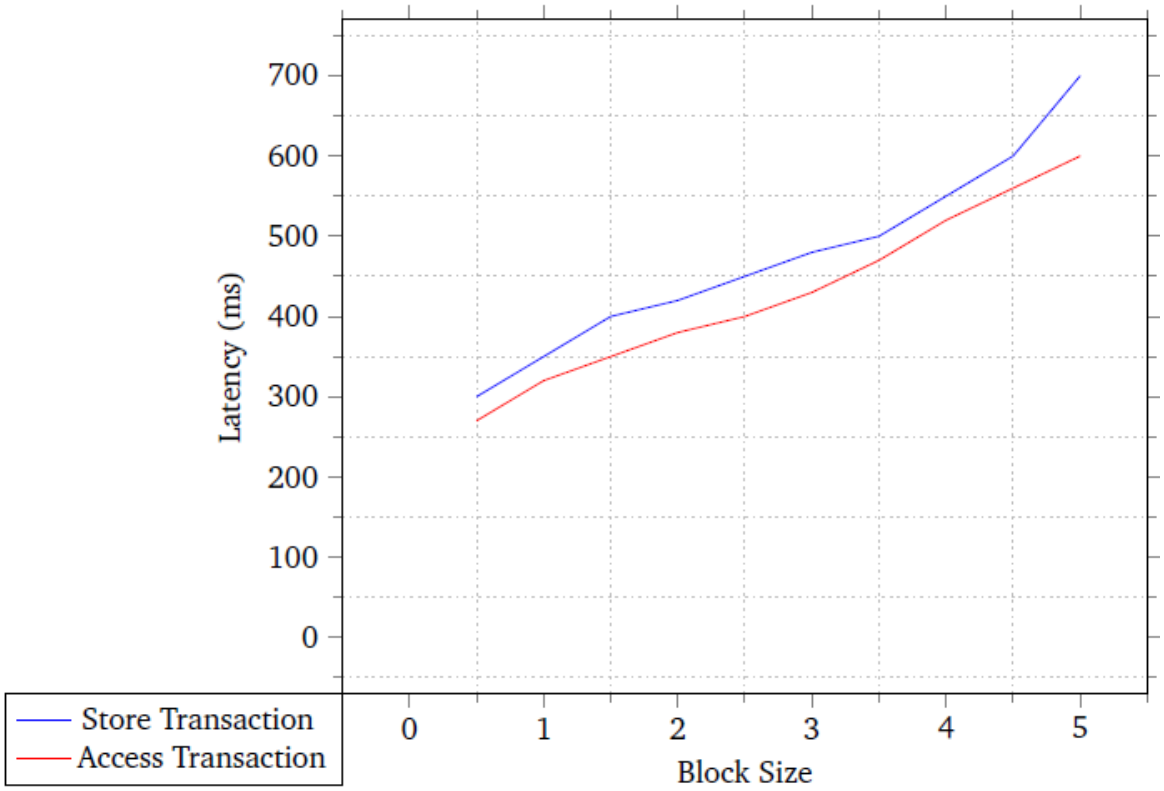
- IoT Network Setup : Raspberry pi-3 devices were used.
- BC implementation: Fabric implementation in UBUNTU
- Behavior monitor placement: Python, Keras and TensorFlow libs.
- Dataset from University of California, Irvine (UCI Machine Learning Repository) of smarthome IoT was used for training

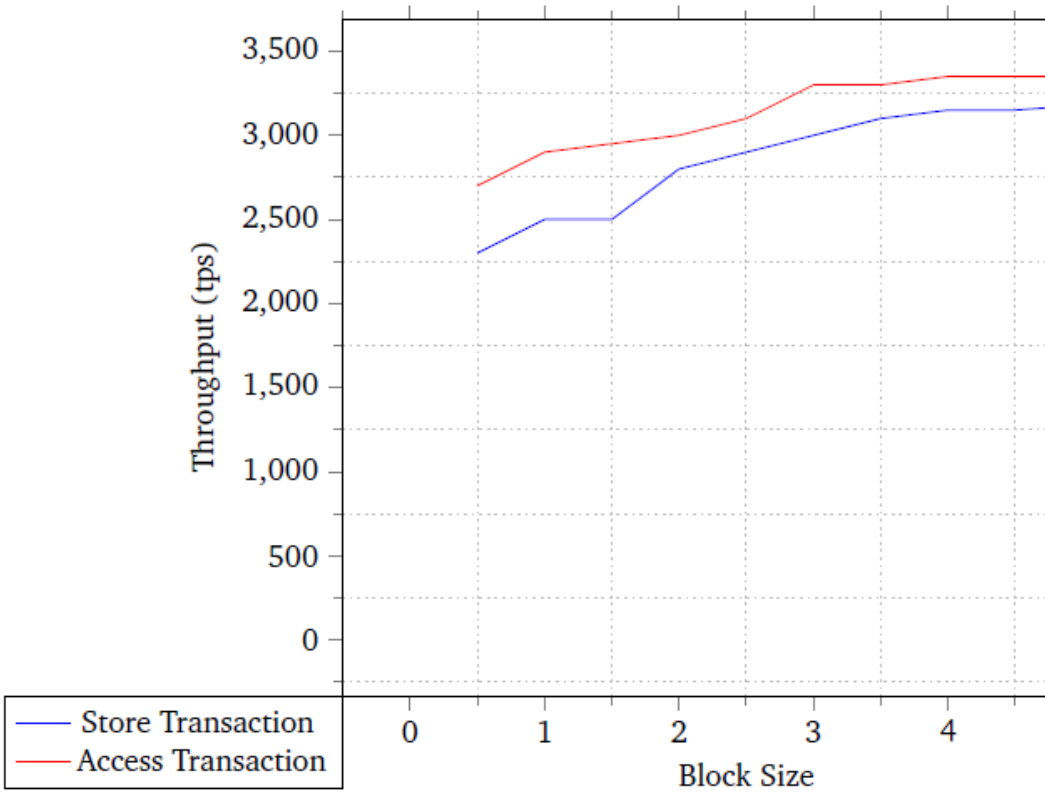
Testing

- Apply mirai DDOS attack
- Compare with other ML algorithm – SVM (Support vector machine, Isolation forest and LOF (local outlier factor)
- Compare the detection time and accuracy

Results

- Throughput and latency in terms of block size





Result (cont)

- Latency with variable transaction Size in comparison
- Transaction Payload size analysis

Payload Size in (KB)	Proposed BC	Quoram BC [ ]
1	0.225	0.325
10	0.280	0.383
20	0.320	0.384
30	0.330	0.407

- The results show that the latencies increases with the increment of 10KB in payload size. The total increase

in transaction latency in QUORAM **25.23%,** while in our technique the value is approximately **22.45%.**

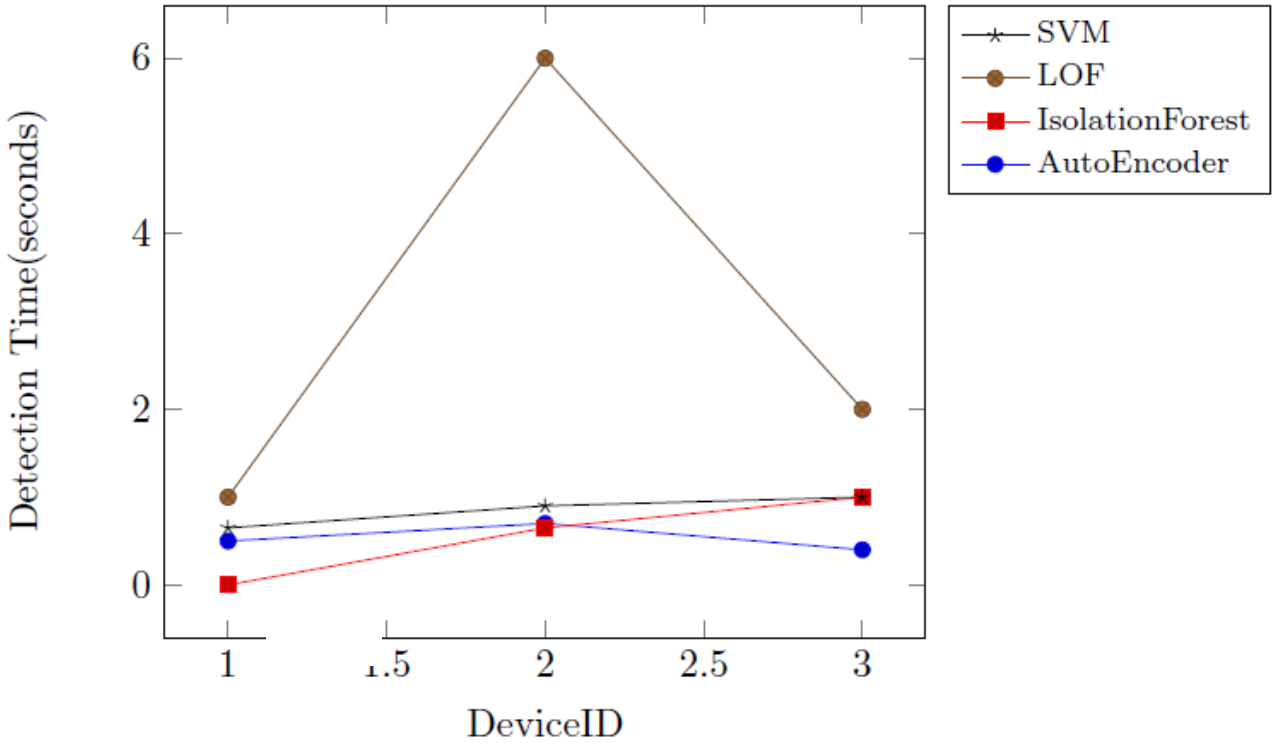
Results (Cont)

- Security Analysis

Security Requirements	Solution Provided
Confidentiality	Matching ID in Smart Contract
Integrity	Hashing Mechanism
Authorization	Endorsement Policy Checking

Result (cont)

- Accuracy – TPR : 99.2%
- Algorithm's Detection time



Future Work

- To investigate/comparative study of other ML – performance and accuracy
- To implement full scale POC with full verification mechanism in multiple zone

Publication Record in Scopus Count
Total Papers = **12** (2018-2021)

- Blockchain-based smart-IoT trust zone measurement architecture (Conference)
- Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure (Journal)
- Predicting IoT service adoption towards smart mobility in Malaysia: SEM-neural hybrid pilot study (Journal)
- Towards a secure behavior modeling for IoT networks using Blockchain (Conference)
- Structural Equation Modeling for Acceptance of Cloud Computing (Conference)
- Clustering based privacy preserving of big data using fuzzification and anonymization operation (Journal)
- Realizing Macro Based Technique for Behavioral Attestation on Remote Platform (Book Chapter)

Continue

- Providing Efficient, Scalable and Privacy Preserved Verification Mechanism in Remote Attestation (Conference)
- Efficient, scalable and privacy preserving application attestation in a multi stakeholder scenario (Book Chapter)
- User Behavior Assessment Towards Biometric Facial Recognition System: A SEM-Neural Network Approach (Book Chapter)
- Convergence of 5G with Internet of Things for Enhanced Privacy (Book Chapter)

Q&A