Secure Hierarchical Edge Service Framework for IoT Devices

Nishar Miya, Sajan Poudel Advisor: Rasib Khan, Ph.D.

Problem Area

Overview

This research introduces a hierarchical secure edge service framework to address IoT challenges, encompassing security, data management, and provenance. By integrating an IDS, hierarchical structure, and blockchain, the study advances edge IoT systems comprehensively.

Security Issues

•Data Provenance Concerns
•Distributed Challenges
•Unauthorized Access.
•Real-time Anomaly ID

Solutions

The proposed framework optimizes communication through a hierarchical structure, reducing congestion. Blockchain integration establishes an immutable ledger, ensuring data integrity. This approach improves security, efficient data flow, and reliable record-keeping.

Research Gap

Existing research focuses narrowly on specific IoT security aspects, leaving a lack of comprehensive solutions. A cohesive approach that integrates security, efficiency, and data provenance within a hierarchical edge service framework is missing. This research addresses this gap by presenting a holistic framework that enhances security, optimizes data management, and establishes robust data provenance mechanisms, contributing to the evolution of secure and efficient IoT-based edge services.

Edge Devices Architecture

This architecture comprises multiple nodes interconnected with dedicated edge servers, and these edge servers are further linked to a central edge monitor. The communication flow is structured in a way that optimizes data transmission and processing efficiency.

•Data collected from individual nodes is seamlessly transmitted to their respective edge servers which minimizes data congestion and facilitates rapid processing at the edge server level.
•The data from various edge servers is then relayed to the central edge monitor that allows for coherent data processing, storage, and subsequent actions, enhancing the overall system's effectiveness.
•meticulous records are created for each data, capturing the origin of each data point.
•The communication architecture is designed to accommodate new nodes seamlessly.
•Designed to support bidirectional data transmission. Not only from nodes to edge servers and further to the edge monitor, but also from the edge monitor to specific nodes when required.

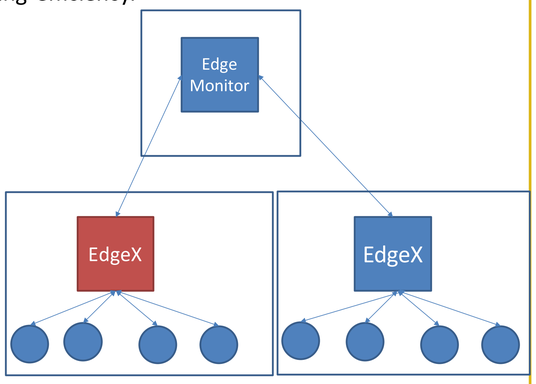

Figure 1: Network Architecture of Nodes, edge server and edge monitor

Network Intrusion Detection System

The research includes a robust Intrusion Detection System (IDS) integrated within the central edge monitor. This IDS employs the Snort network intrusion detection model to systematically analyze incoming data, network traffic, and various network attributes against a predefined set of rules.

• Network-Centric Threat Model for assessing network vulnerabilities.
• Facilitated by Snort, a well-established intrusion detection framework.
• The set of rules used by the Snort IDS, adapted to the network's unique configuration and characteristics.
•Data monitoring as it traverses the network, consistently assessing for any indications of intrusion or compromise.
•Propagation of alert throughout the network if intrusion id detected
• Pinpoints the source of the intrusion due to the meticulously recorded provenance data.

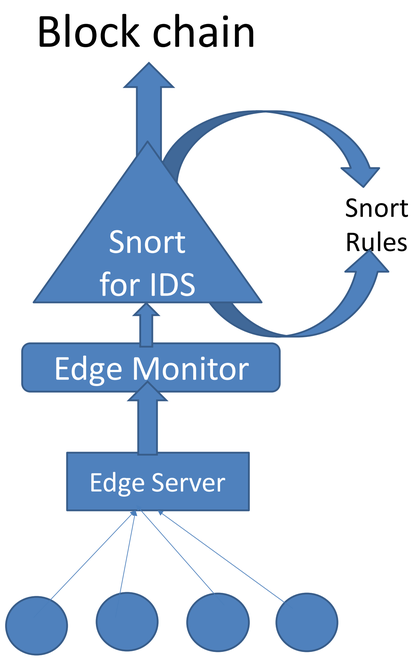

Fig 2: Intrusion Detection System

Blockchain for Data Storage

We explore the use of blockchain for data storage due to following reasons:

- Data sourced from the edge monitor is stored using a decentralized approach, leveraging the Ethereum Virtual Machine (EVM).
- The deployment and exhaustive testing of Ethereum contracts are efficiently streamlined by making use of Ganache, a versatile local blockchain development environment.
- Smart contracts written in Solidity are developed to facilitate the storage of vital node profile data and data-associated information.
- An emphasis on capturing and retaining provenance data ensures the integrity of data by maintaining a comprehensive record of its origin and modification history.
- The interaction between the architectural components and the Ethereum blockchain is facilitated through the integration of the Web3j library.

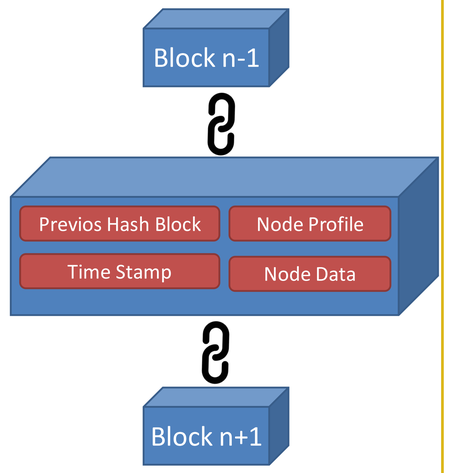

Figure 2: Representation of a block in blockchain

Design Analysis

Advantages

• Optimized data flow due to hierarchical edge infrastructure.
• Efficient and reliable data collection due to implementation of EdgeX Foundry, an advanced edge computing technology
• Enhanced data analysis and application due to central edge monitor
• Traceability of data due to focus on provenance
• Efficient addition of new nodes without significant disruption or resource bottleneck
• Flexibility and versatility due to bidirectional data transmission

Disadvantages

• Centralized point of failure for Edge Monitor, despite delocalization of EdgeX servers

• Latency due to communication with other EdgeX servers via the central Edge Monitor

• Intrusion detection rule set management

Key References

1. *Ethereum Development Documentation*. ethereum.org. (n.d.). https://ethereum.org/en/developers/docs/
2. Johanson, M. (n.d.). *EdgeX Foundry Documentation*. Introduction - EdgeX Foundry Documentation. https://docs.edgexfoundry.org/2.3/
3. Jonas. (2020, August 28). *Edgex Foundry Hands-on tutorial*. jonamiki.com. https://jonamiki.com/2020/08/26/edgex-foundry-hands-on-tutorial/
4. *Network Intrusion Detection & Prevention System*. Snort. (n.d.). https://www.snort.org/#documents