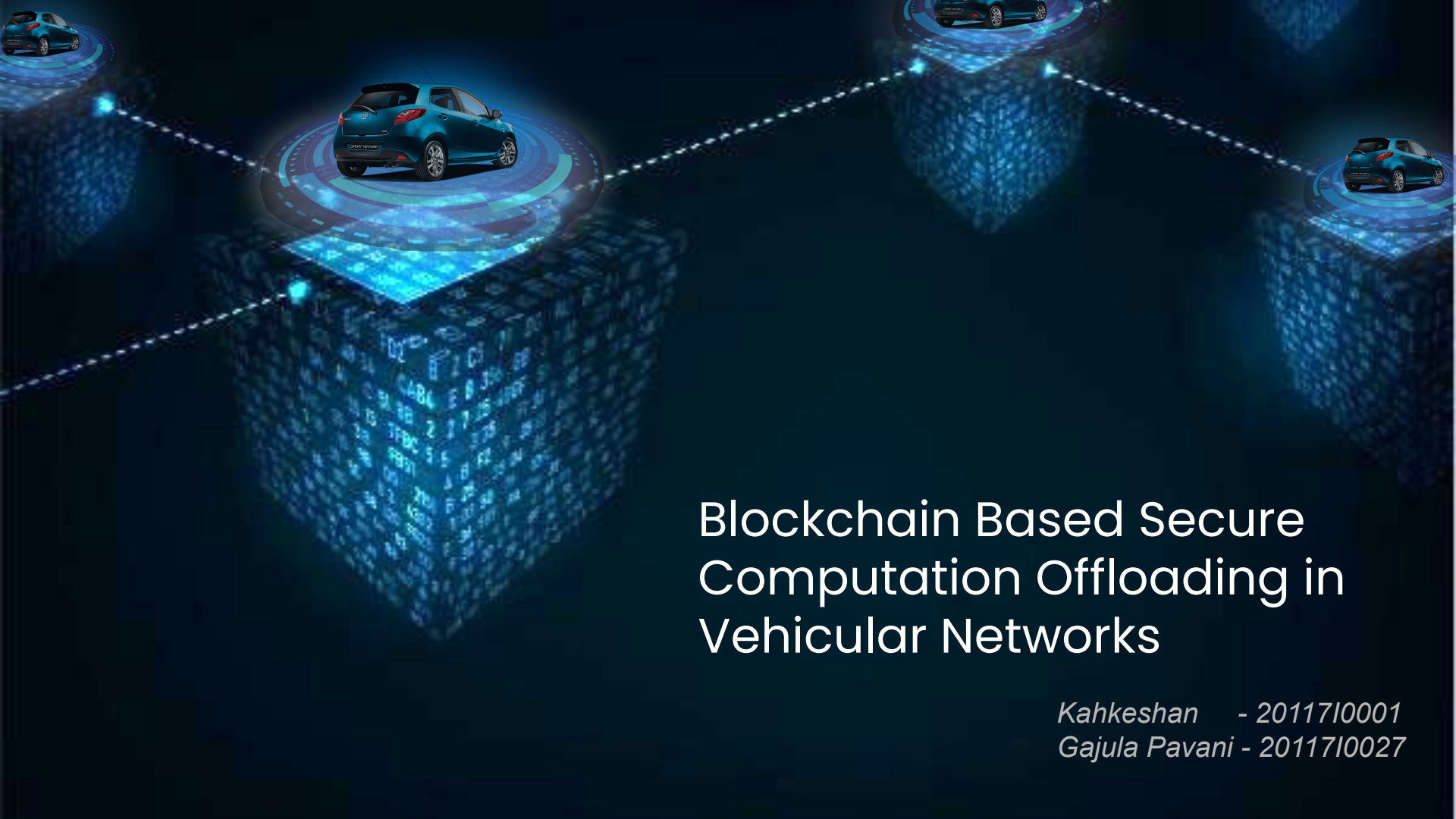


Blockchain Based Secure Computation Offloading in Vehicular Networks

Kahkeshan - 20117I0001
Gajula Pavani - 20117I0027

INTRODUCTION

- Vehicle Ad Hoc Network (VANET) is used for communication among vehicles & between vehicles and roadside infrastructure.
- VANET is a mobile ad hoc network (MANET) for vehicle environments in smart cities.
- Mobile applications that do not require latency will be offloaded to a resource-rich cloud server, while other time-sensitive applications will perform on edge servers to meet the rapid response service.
- Attackers can receive mobile data by threatening computing resources on cloud servers, which can cause privacy issues for VANET applications.
- To ensure the safety of mobile offloading, blockchain can be considered as a third-party system that does not require centralized trust management.
- The design of a peer-to-peer network is the core of the blockchain, where transaction information exists between multiple nodes and is not controlled by any single centralized entity.

EXISTING SYSTEM

- Mobile edge-cloud computation offloading (MECCO) has been regarded as a promising means to support delay-sensitive IoT applications.
- Offloading mobile tasks to the cloud is vulnerable to security risks due to malicious mobile devices (MDs).
- Unauthorized RBUs may achieve malicious access to utilize cloud services without central authorization.

DISADVANTAGES

- In the existing work, the system is not computation offloading, edge-cloud computing.
- This system is less performance in which the system focuses on the ECCO system with the concept of access control and offloading on the blockchain network.

PROPOSED SYSTEM

- This system combines blockchain and DRL for the ECCO system in the VANET network, and jointly investigate access control and computation offloading.
- The system has designed a hierarchical architecture of controllable programming derived from SDN, which implements the dynamic orchestration of VANET security to achieve the communication of connected vehicles.
- To improve offloading security, we propose a trustworthy access control using blockchain, which protects clouds against illegal offloading behaviors.
- The system has proposed a trusted access control mechanism that can use smart contracts on the blockchain to effectively detect and prevent illegal offloading of VANET devices.
- We develop a novel deep reinforcement learning (DRL) algorithm by using an advanced deep Q-network
- The extended offloading algorithm is based on DRL to attain the best offloading strategy for all vehicles, which should obey QoS requirements such as energy consumption and processing delay.

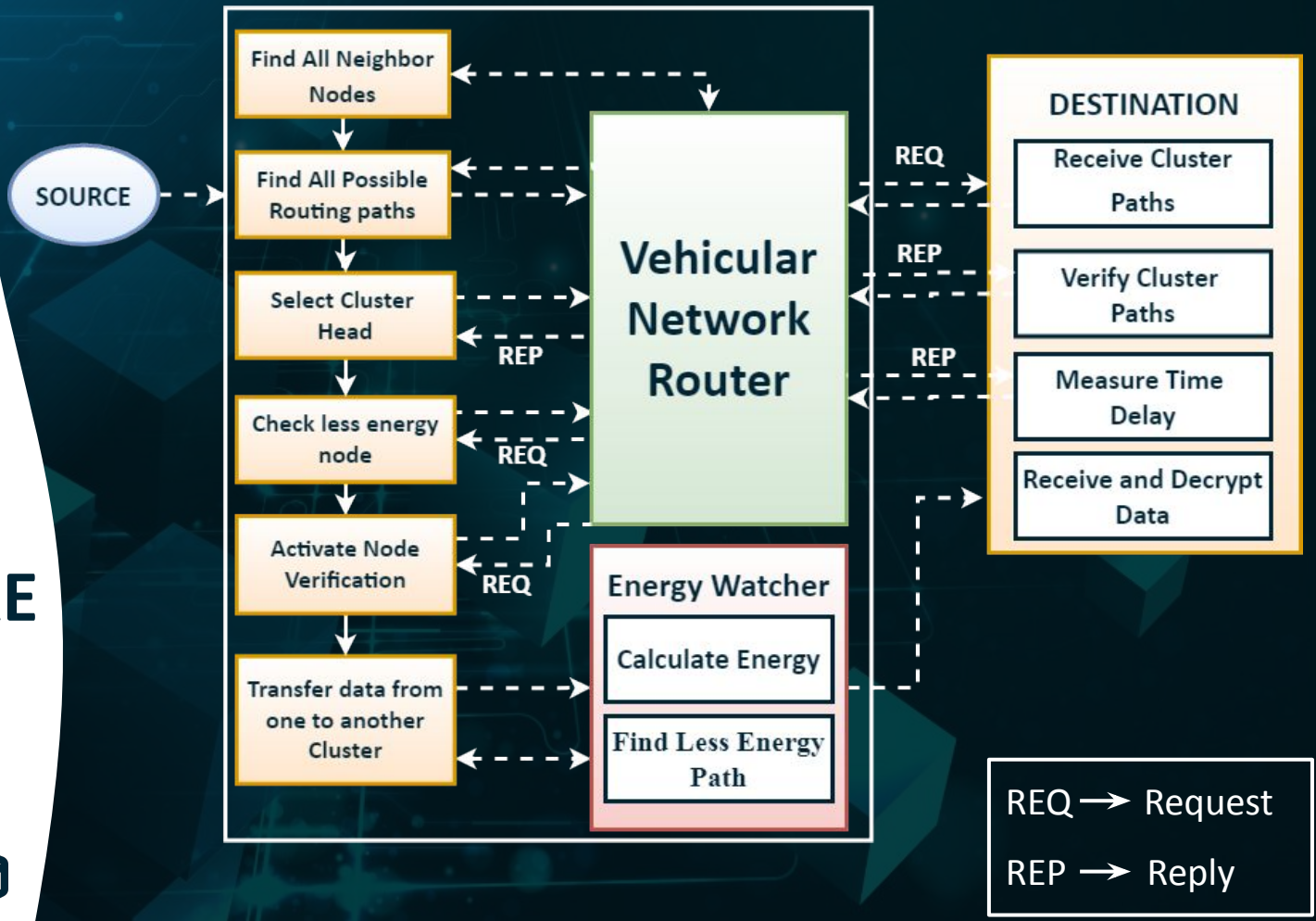
Hardware

- Processor : Pentium - IV
- Ram : 4GB (Min)
- Hard Disk : 20 GB
- Key Board : Standard Windows
- Mouse : 2 or 3 Button Mouse
- Monitor : SVGA

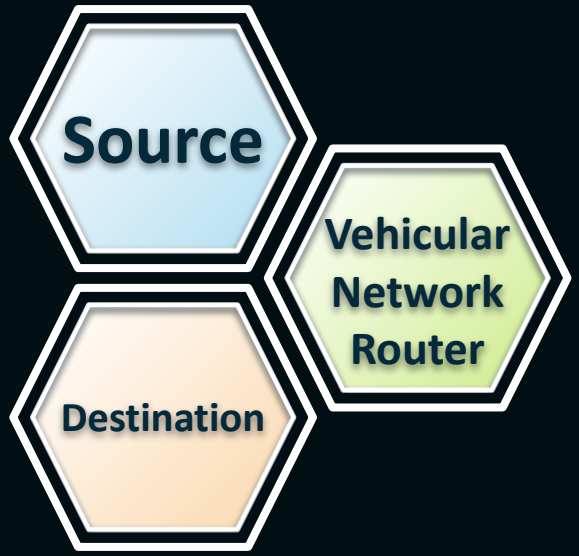
Software

- Operating System : Windows XP
- Coding Language : Java/J2EE (JSP, Servlet)
- Front End : J2EE
- Back End : MySql

SYSTEM ARCHITECTURE



IMPLEMENTATION

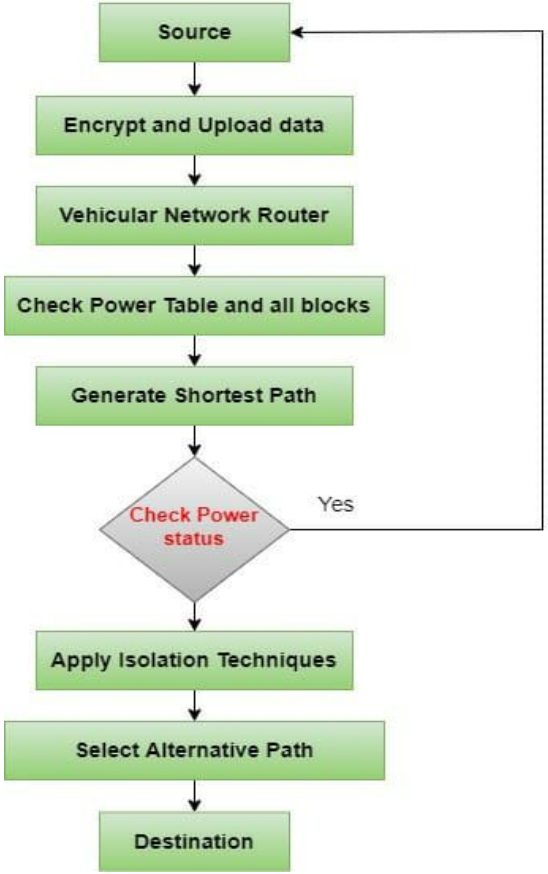


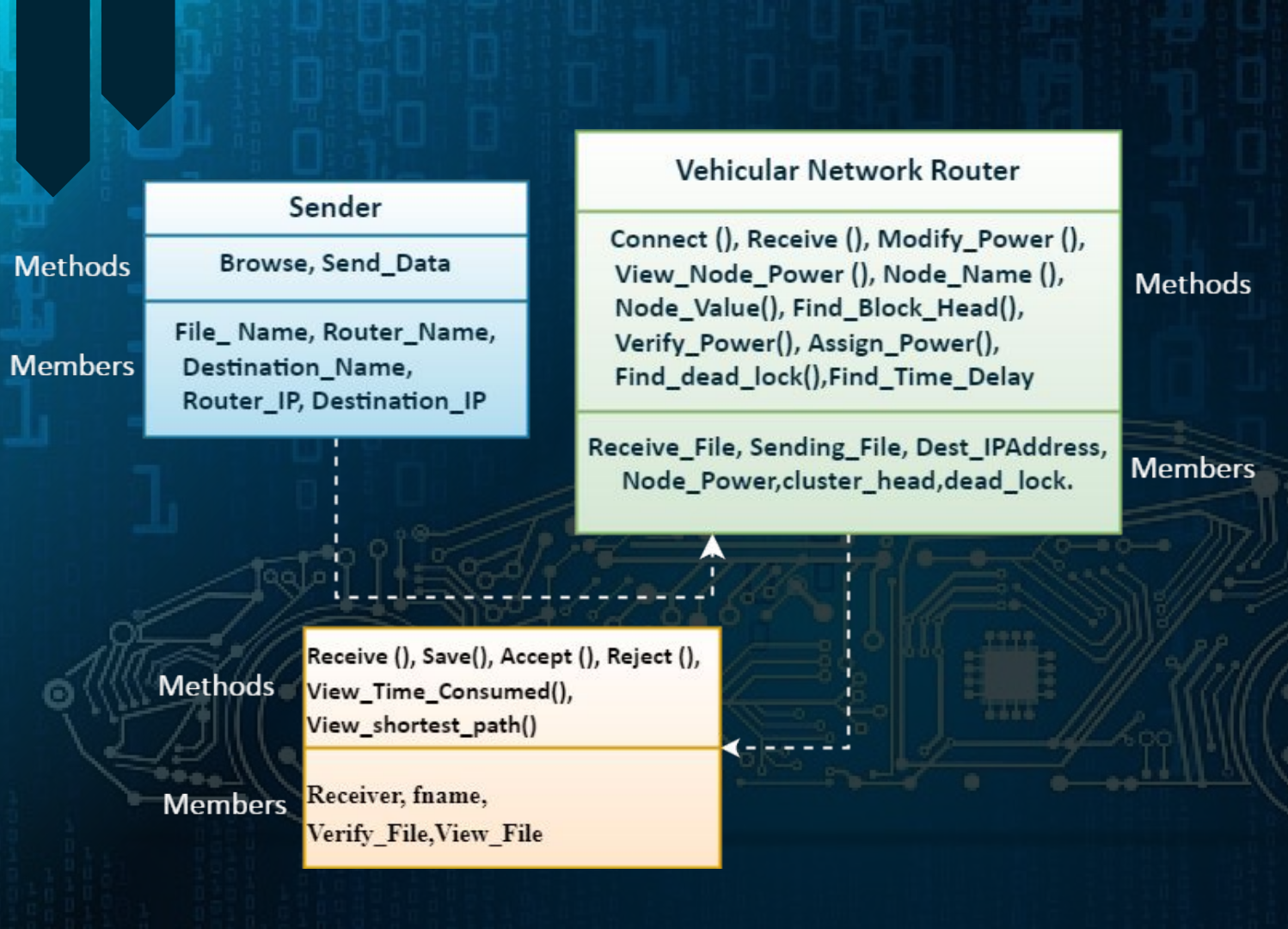
The Source browses the required file, initializes nodes with Power, and uploads to the destination via Vehicular Network Router

The Vehicular Network Router is responsible for forwarding the data file in the shortest distance to the destination. This the system can assign the power for the node and can view the node details with their power status and attack status.

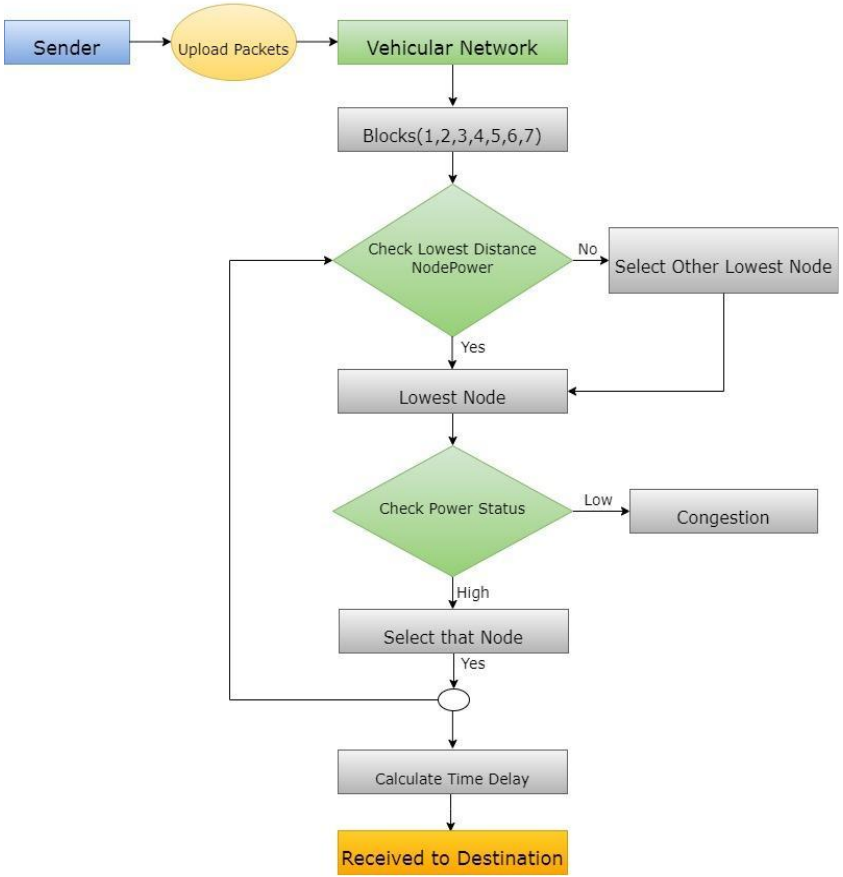
In this module, if a malicious or less power node is found in the Vehicular Network Router then it never forwards to the Destination to filter the content and adds to the attacker profile.

FLOW CHART


Source
Encrypt and Upload data
Vehicular Network Router
Check Power Table and all blocks
Generate Shortest Path
Check Power status
Yes
Apply Isolation Techniques
Select Alternative Path
Destination



CLASS DIAGRAM



DATA FLOW DIAGRAM

USE CASE DIAGRAM

CONCLUSION

We use the extended DQN algorithm to formulate task offloading decisions, consensus mechanism decisions, and edge resource as well as bandwidth allocation as joint optimization problems to minimize the total offloading cost of computation latency, throughput, and energy consumption. We conducted an experimental simulation to evaluate the effectiveness of the proposed scheme. The results show that, compared with other benchmark methods, our scheme provides high security for the ECCO system and achieves performance improvements with minimum offloading costs. Our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network(LAN).

LIMITATIONS

In the future, we will consider designing lightweight blockchains so that the access control architecture is devised and arrayed directly at the edge side. It will hopefully support time-sensitive network management services for offloaded systems.

THANK YOU