**Block chain-Based Secure Computation Offloading in Vehicular Networks**

**Abstract**

— Vehicular ad hoc networks (VANETs) has become an important part of modern intelligent transportation systems (ITS). However, under the influence of malicious mobile vehicles, offloading vehicle tasks to the cloud server is threatened by security attacks. Edge cloud offloading (ECCO) has considered a promising approach to enable latency-sensitive VANET. How to solve the complex computation offloading of vehicles while ensuring the high security of the cloud server is an issue that needs urgent research. In this paper, we studied the safety and offloading of multi-vehicle ECCO system based on cloud blockchain. First, to achieve consensus in the vehicular environment, we propose a distributed hierarchical software-defined VANET (SDVs) framework to establish a security architecture. Secondly, to improve the security of offloading, we propose to use blockchain-based access control, which protects the cloud from illegal offloading actions. Finally, to solve the intensive computing problem of authorized vehicles, we determine task offloading via jointly optimizing offloading decisions, consensus mechanism decisions, allocation of computation resources and channel bandwidth. The optimization method is designed to minimize long-term system of delays, energy consumption, and flow costs for all vehicles. To better resolve the proposed offloading method, we develop a new deep reinforcement learning (DRL) algorithm via utilizing extended deep Q-networks. We evaluate the performance of our framework on access control and offloading through numerical simulations, which have significant advantages over existing solutions.

**Existing System**

* The basic goal of MTD is to achieve the active defense to the external attacks based on unknown vulnerabilities and backdoors. To date, MTD has been studied in various contexts, including cloud computing and web applications.
* With the increasing amount of vehicles in VANET, the communication of different physical entities in a large-scale, high-mobility scenarios will product amount of real-time, high-speed, and continuous data flows. The result is that when offloading mobile tasks relies on untrusted MDs (here, roadside base units) of mobile vehicles in a dynamic environment, ECCO systems are prone to various types of threats. The result is that when offloading mobile tasks relies on untrusted MDs (here, roadside base units (RBU) of moving vehicles in a dynamic environment, ECCO is vulnerable to various types of threats. Unauthorized RBUs may achieve malicious access to utilize cloud services without central authorization. In addition, attackers can receive mobile data by threatening computing resources on cloud servers, which can cause privacy issues for VANET applications [9]. Therefore, how to ensure the safety of mobile offloading is crucial to any ECCO system

**Proposed System**

(1) We propose a new secure computation offloading framework for a blockchain-based VANET network, in which a mobile vehicle can offload its tasks to a cloud or edge server to perform computation under an access control mechanism.

(2) We have 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. The distributed SDN controller in the area control layer has the ability to gather vehicle consensus resource, and transmits the trust information it collects to the domain control layer.

(3) We have proposed a trusted access control mechanism that can use smart contracts on the blockchain to effectively detect and prevent illegal offloading of VANET devices. Its purpose is to verify vehicle identity, offloading tasks and manage offloading data to ensure the security and privacy of the ECCO system.

(4) We propose a dynamic offloading solution that considers offloading data size, available MEC computing power, throughput and bandwidth resources to offload its resource to the cloud or edge server. In particular, we propose an extended offloading algorithm based on DRL to attain the best offloading strategy for all vehicles, which should obey QoS requirements such as energy consumption and processing delay.

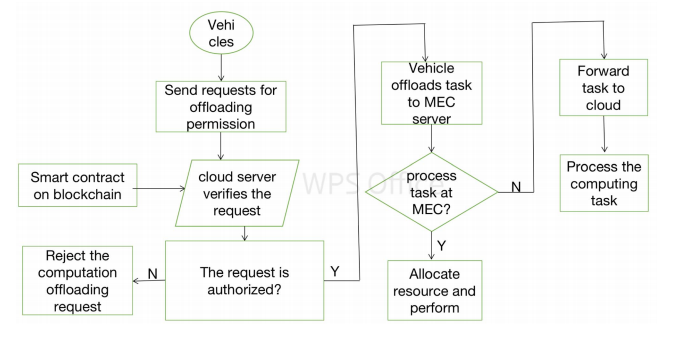
(5) We verify the proposed ECCO system via simulation experiments, and then investigate the access control and offloading performance.

**Advantages**

**Future work**

The proposed scheme can achieve the MTD features by the following procedures. First, a re-encryption process can be implemented on the outer NC layer of the scheme, so that the key and ciphertexts can be dynamically changed. Second, the key length can be actively extended, so that the scheme is adaptable to the rapid development of the computing power. Third, the parameters in the scheme can be flexibly chosen, so that there is a transition between efficiency and security.The security level of the proposed scheme will be tested in our future work.

**Architecture**

****

**Flowchart of ECCO system**

**Algorithm**

1. Multiple DES: The most classical multiple DES algorithm is the triple DES which we have discussed in Section Ⅴ. The complexity of multiple DES is several times larger than single DES and therefore much larger than our encryption scheme. Besides, as we said at the beginning, multiple DES cannot meet the dynamic security requirements of the intelligent information network.
2. Mutable S-box DES: This algorithm can change the content order of S-box based on the change of encryption key or directly change the content of S-box. Obviously, it can be used to resist differential cryptanalysis (DC) but has no contribution to enlarge the key space.
3. Sub key DES: This algorithm uses different sub key on every iteration during encryption in DES. Due to 48-bit key required in every iteration process, after 16 iterations, the key space of this improved DES is 768. This algorithm greatly increases the complexity of key space and has a good behavior to resist the exhaustive attack. However, its adaptability and extension with the rapid development of the computing power is even less than the multiple DES algorithm for the reason that its key space is strictly static.

**System Requirements**

# H/W System Configuration:-

# Processor : Intel (R) Pentium (R)

Speed : 1.1 Ghz

RAM : 2GB

Hard Disk : 57 GB

Key Board : Standard Windows Keyboard

Mouse : Two or Three Button Mouse

Monitor : SVGA

# S/W System Configuration

* Operating System : Windows 8/7/95/98/2000/XP
* Front End : AWT,SWINGS and Socket Programming.
* Database Connectivity : Mysql 5.1.44
* Java Version : jdk 1.8
* IDE Tool : Netbeans 8.1/8.2