A Blockchain-based Home Edge Computing-aided Disaster Rehabilitation and Recovery Scheme using Unmanned Any Vehicle

Anik Islam¹, I Nyoman Apraz Ramatryana², Soo Young Shin³

¹Researcher, MERIT (Medical, Electronic, Robotic, IT) Convergence Innovative Talents Training Group for Smart Manufacturing Innovation,
²³Department of IT Convergence Engineering,
Kumoh National Institute of Technology (KIT), Gumi, South Korea
Email: {anik.islam, ramatryana, wdragon}@kumoh.ac.kr

Abstract

Natural disasters visited countries every year more or less and left devastating situations behind, which affect both the economy and health. However, instantaneous actions can lessen casualties in the affected areas. Unmanned any vehicle (UxV) is a concept where unmanned vehicles come together and perform missions cooperatively. UxV can assist in rehabilitating the affected area. Multi-access edge computing (MEC) can assist UxVs in real-time. However, disaster might jeopardize MEC structure. Home edge computing (HEC) is a paradigm that stays closer to the end devices and enables an offline computation environment. HEC can fill up the gap and assist in maintaining the mission. Besides, networks and data are surrounded by security and privacy issues. This paper introduces a blockchain-based HEC-assisted disaster rehabilitation and recovery scheme to restore everyday life using UxV. A proof of concept is considered for proving the feasibility.

I. Introduction

Natural disasters (e.g., floods) are very frequent in every country [1]. However, some of them are very devastating and harms both economic and human health. Nevertheless, after finishing the disaster, quick response in the affected areas can reduce the casualties and assist in bringing them back to their expected life. Unmanned any vehicle (UxV) is a concept in which unmanned vehicles (i.e., aerial, ground, surface, and underwater) are engaged altogether to perform a missing to bring efficiency [2]. However, these entities lack computation capabilities. Multi-access edge computing (MEC) is a paradigm that comes forward to provide services in real-time [3]. However, in disaster-affected areas, infrastructure might be compromised, and entities might not in contact with the MEC server. Home edge computing (HEC) is an emerging technology that brings computation closer to the user and enabled offline computation capabilities [4]. However, communication and data might be hampered by an attacker [5]. Blockchain is a revolutionary technology that introduces trust in the unknown environment and provides secure data and communication [6, 7]. After considering the aforementioned challenges, this paper presents an HEC-assisted disaster recovery scheme in which emergency services are provided in the disaster-affected areas using UxV and blockchain.

II. Proposed Disaster Recovery Scheme using UxV

This paper presents a disaster recovery and emergency services scheme (termed as "DRES") utilizing UxV through the facilitation of blockchain and HEC, as shown in Fig. 1. In DRES, HEC enables local cloud services to other entities (e.g., UAVs). MEC server (MECS) server provides real-time assistance to all of the entities. Cloud is the final destination for command and control. All the entities have performed various tasks (e.g., search and rescue). Satellite communication is considered for emergency data transmissions.

III. Communication in DRES

DRES maintains a hierarchy. Entities which is highly powered (e.g., computation) hold HES to assist other entities. HES controls a blockchain to manage data collected from other entities. If any request is not available in HES, the HES holder (HESH) requests the nearest MECS or cloud to maintain transparency. Each entity holds the public key of all the entities that are deployed in the mission. When an entity comes in contact with a HESH, it first establishes secure communication based on the public key of HESH with length $k$.

$$x = Enc_{pub_{HESH}} (pub_{REQ}.sig_{pri_{REQ}} (pub_{REQ}))$$
Upon receiving $x$, HESH verifies and generates a session key to enable fast and secure data transmission.

$$y = Dec_{pr_{HESH}}(x) | i$$

$$= filter (pub_{HESH}^k) \land ver (sig_{pr_{HESH}}(pub_{HESH}^k))$$

When the session key is ready, HESH returns it to the requester using the requester’s public key.

$$x' = Enc_{pub_{HESH}^k} (pub_{HESH}^k, sig_{pr_{HESH}}(pub_{HESH}^k))$$

When the requester receives $x'$, it decrypts and verifies.

$$y' = Dec_{pr_{HESH}}(x') | i$$

$$= filter (pub_{HESH}^k) \land ver (sig_{pr_{HESH}}(pub_{HESH}^k))$$

When an entity wants to transmit data, it first encrypts data using the session key and transfers it to HESH.

$$msg = Enc_{ses_k} (pub_{HESH}^k, data, sig_{pr_{HESH}}(data))$$

Upon receiving, HESH decrypts using the session key and verifies the requestor.

$$msg_{raw} = Dec_{ses_k}(msg) | i$$

$$= filter (pub_{HESH}^k) \land ver (sig_{pr_{HESH}}(pub_{HESH}^k)).$$

HES holds data for a certain amount of time in a lightweight blockchain within itself. When HESH comes in contact with a MECS, it offloads all the data. HESH maintains two chains, such as key chain and data chain. The key chain holds the public keys of entities, and the data chain contains the collected data temporarily. MEC and cloud act as a miner. Each miner maintains a transaction pool in which unattended data are stored. After a certain number of data, each miner creates a block based on these data and sends it to other miners for validation. When all the miners agree, the block is added to the blockchain.

**IV. Performance Analysis**

![Fig. 2. Throughput of the PoC.](image)

A proof of concept (PoC) is established in which a UAV and a UGV are engaged in the mission. A DJI Mavic pro 2 was considered as a UAV containing raspberry pi 3b+ as an onboard computer, and a ROSbot 2.0 was considered as a UGV. Ethereum was used as a blockchain platform containing 15 miners. Python is used for maintaining PoC.

Fig. 2 illustrates the throughput of DRES in the presence of filter techniques (i.e., bloom filter) in the network. With the elapsed time, throughput decreases due to the fading. However, due to using fast encryption technique, Fig. 2 represents promising data transmission rate.

**V. Concluding Remarks with Future Works**

A disaster recovery scheme was proposed in which emergency services are provided using UxV with the assistance of HEC. Furthermore, in the proposed scheme, data are securely stored in the nearest servers (MEC and cloud) with the assistance of blockchain. A proof of concept is discussed to prove the future applicability of the proposed scheme. The integration of artificial intelligence to enhance the efficiency of the mission is kept for the future extension of this paper.

**ACKNOWLEDGMENT**

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology” (2018R1A6A1A03024003).

**Reference**


