논문 20-45-11-24 The Journal of Korean Institute of Communications and Information Sciences '20-11 Vol.45 No.11
https://doi.org/10.7840/kics.2020.45.11.2022

블록체인을 활용한 MEC 기반의 IoT CO_2 배출량 감소 방안

무하마드 마수두짜만◆, 아닉 이슬람*, 서 종 완**, 신 수 용°

A Blockchain-Enabled MEC-Assisted CO_2 Emission Reduction Scheme Using Internet of Things

MD Masuduzzaman◆, Anik Islam*, Jong Wan Seo**, Soo Young Shin°

요 약

현재 세계에서 큰 과제 중 하나는 온실효과를 줄이기 위해 이산화탄소(CO_2) 가스의 배출을 억제하는 것이다. 운송 부문에서 사용되는 차량은 대기 중 CO_2 농도를 높이는 원인이 된다. 개인 차량 사용자에게 사회에서 CO_2 가스의 사용을 제한할 수 있다. 사물인터넷(IoT) 장치는 센서를 사용하여 특정 사용자의 차량에서 나오는 CO_2 가스량을 수집할 수 있다. 또한, MEC(Mobile Edge Computing) 서버는 수집된 데이터를 처리하는 데 도움을 준다. 본 논문에서는 CO_2 가스가 환경에 미치는 영향에 대해 간략히 설명하고 CO_2 가스 배출률을 감소시키는 데 도움이 될 수 있는 최신 기술을 활용한 방안을 제안한다. 마지막으로, 블록체인 기술은 공격(즉, 사이버 위협과 데이터 무결성)과 제 3자의 상호작용으로부터 이를 보호하기 위한 시스템 구축을 위해 사용된다.

Key Words : Blockchain, Carbon-di-oxide, Internet of Things, Mobile Edge Computing, Sensor

ABSTRACT

One of the biggest challenge in the world right now is to control the emission of carbon-di-oxide (CO_2) gas to reduce the greenhouse effect. Vehicles that are used in the transport sector are responsible to increase the level of CO_2 in the atmosphere. Restriction can be applied for private vehicle users to limit the usage of CO_2 gas in the society. Internet of Things (IoT) devices specially different sensors can be used to collect the usage of CO_2 gas from the vehicles of a particular user. Additionally, Mobile edge computing (MEC) server can be helpful to process the collected data. This paper briefly explains the impact of increasing CO_2 gas in the environment and propose a secure scheme using recent technologies that can help to reduce the CO_2 gas emission rate. Finally, blockchain technology is endorsed to build a secure system to protect it against the attacks (i.e., cyber threats and data integrity) and any kind of third-party interaction.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2020-2020-0-01612)
◆ First Author : Kumoh National Institute of Technology, Masud.prince@kumoh.ac.kr, 학생회원
° Corresponding Author : Kumoh National Institute of Technology, wdragon@kumoh.ac.kr, 종신회원
* Kumoh National Institute of Technology, anik.islam@kumoh.ac.kr, 학생회원
** Kumoh National Institute of Technology, sayo94@kumoh.ac.kr, 학생회원
논문번호 : 202007-174-B-RE, Received July 29, 2020; Revised August 31, 2020; Accepted August 31, 2020

Ⅰ. Introduction

Because of the excessive use of carbon dioxide (CO_2) gas fossil fuel utilization in different sectors, the temperature of the world is heating up gradually day by day[1]. As a result, the world is facing the most disastrous period in the history of mind kind for the last couple of decades. Therefore, it's high time to create awareness as well as taking the necessary step to reduce CO_2 gas emission in the atmosphere. Atmospheric CO_2 gas levels have been increased over 40% since the starting time of the industrial revolution[2]. If global warming is not checked under a certain level, it will be responsible for certain climate change, sea-level rise, and extreme weather changing and other natural disasters, warned by the researchers.

In recent times, humans are ignoring the facts of using excessive CO_2 gas in different manmade sectors like transportation, industrialization, building material and constriction etc. Vehicles in the transportation sector are now considered as one of the major origins of producing CO_2 gas in the atmosphere. European Union (EU) warned that the emission rate of CO_2 gases needs to be decreased near about 15-20% before 2020 so that the global temperature will be adjusted and rising below 2%[3]. If the government can fix/restrict the usage of CO_2 gas using a personal vehicle, the produce of CO_2 gas can be scaled down. Not only that, if any user crosses his/her limit of using CO_2 gas, then he/she needs to pay extra money every month to the government for excessive usage of the vehicle. However, collecting data and develop any system to control the usage of CO_2 gas omission is very challenging.

Internet of Things (IoT) has been developed to collect information from different sources and can transfer the data from one end to another without any human interaction[4]. Therefore, IoT devices can be used not only to monitor the usage of CO_2 gas emission in the atmosphere but also to collect the information of individual user about their CO_2 emission record. However, due to the limited hardware issues, processing any computational task inside the IoT device is burdensome.

Mobile edge computing (MEC) server can be used to offload the task of IoT devices as MEC provides the support of fast data processing at the edge of the cellular network[5]. However, security issues while data transferring from IoT devices to MEC server needs to be considered as there are the possibilities of breaking the system and swipe the information by the hacker.

At the present state-of-the-art, researchers are proposing different approaches to reduce CO_2 gas in different sectors. Masud et al.[6] proposed an energy efficiency routing technique which decreases the usage of energy in the link-state routing protocol. Albreem et al.[7] have discussed green networking where IoT devices can be used to gain energy efficiency in any system and suggested to use IoT in the different sectors to gain improved performances and result. Rafeeq et al.[8] discussed green IoT where authors recommended an emphasis on the security issues of IoT. However, no other researchers have published any work on monitoring CO_2 gas emission from the vehicles using IoT devices. However, tracking the footprint of the vehicles are very crucial to control it from the user side. Additionally, proofing the authentication is also very important for any data that are stored in a server.

Blockchain is a distributed immutable ledger where no user is allowed to modify the data without the permission of others in the network. It can provide an extreme level of security to prevent third-party modification as well as different kinds of attacks. Many researchers are working to implement blockchain for storing the data securely both in academy and industry[9-12]. Blockchain can be a useful answer for different kinds of security threats[13]. In this paper, a blockchain-enabled MEC server assisted CO_2 emission reduction scheme has been proposed using IoT. The contribution of the paper is listed below :

A unique IoT based and MEC server assisted scheme has been proposed to monitor and control the emission rate of CO_2 gas.

Blockchain technology has been introduced to store the CO_2 gas usage information of private

vehicle owner as it will prevent illegal data modification from the third party.

Digital Wallet based automated payment system is proposed using digital mobile app.

Result analysis has been conducted to find out the throughput and delay while transferring the data inside the network using secure public key cryptography.

Ⅱ. Proposed Methodology

System model is described in Fig. 1 to explain the whole architecture of the proposed scheme. Firstly, the user registers themselves in the system with their personal vehicles registration number and information. Information like owners name, voter ID/ alien ID card number, vehicle license number, car mileage information and contact number need to be provided by the owner to register themselves in the system.

Debit card information is also necessary as the mobile application also supports the option of digital payment using the digital wallet of an individual user.

The basic functionalities of the proposed system are explained in Fig. 2. After registering in the system by the user, it is detected the usage of CO_2 gas in his/her vehicle. It is challenging to detect the usage of CO_2 gas by a vehicle. Therefore, different IoT devices like gas detector sensor can be used which detects the presence and usage of gases[14]. More specifically, the electrochemical sensor is used to check the usage of CO_2 gas emission from a vehicle. A raspberry pi board and the

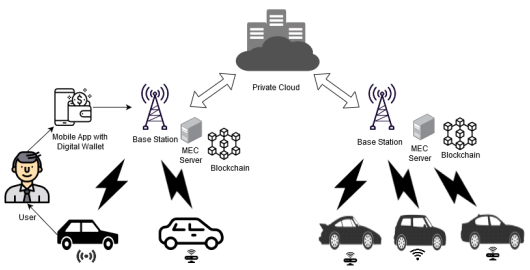

그림 1. 시스템 모델
Fig. 1. System model

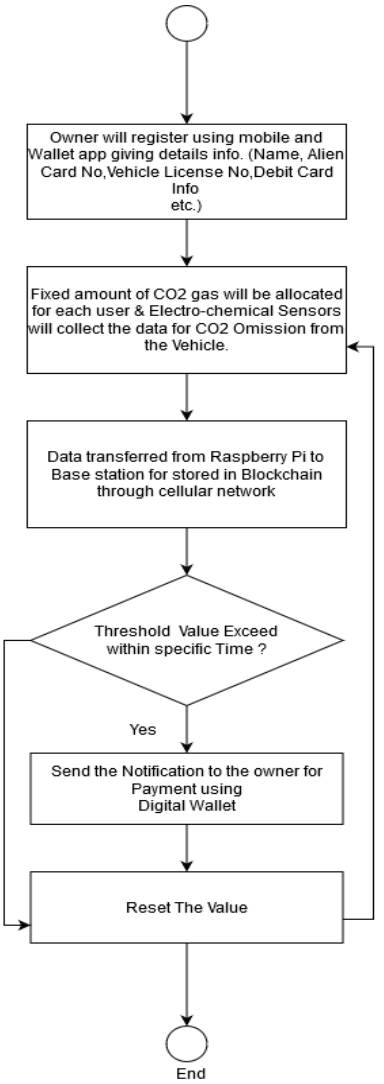

그림 2. 제안하는 기술 흐름도
Fig. 2. Flow Chart of the Proposed Scheme

electrochemical sensor is placed in every vehicle to monitor the usage of CO_2 gas for every user and the raspberry pi is represents as a personal user device. After collecting the data from the vehicle by the sensor, it is stored in the raspberry pi memory. Whenever the vehicle comes to the road, the raspberry pi transfers the stored data to the nearby MEC server. The MEC server checks the usage amount and stores the data in a private blockchain. Before storing the data in the blockchain, MEC server needs to verify the valid user information.

Public key cryptosystem can secure not only the

data transaction between IoT devices and MEC servers but also can verify the valid user identity. In public-key cryptosystem, every user has one private key and one public key. When the raspberry pi transfers the CO_2 usage data to the MEC server, it encrypts the information with the public key of the MEC server. The MEC server decrypts the information with the private key of itself. Additionally, to prove the identity of the user, the raspberry pi device encrypts the hash of the data with the private key of the user. The MEC server decrypts the hash using the public key of the user and matches the hash to verify the original data. Each user is assigned a fixed volume of CO_2 gas that he/she can spend in every month. If the user crosses the limit of the volume, the user has to pay extra money to the system before using it in the same month. Otherwise, the user needs to wait for the next month when the value will be reset again. After verify the user and collected the data from the raspberry pi, the MEC server stores the data in a blockchain to make it transparent and avoid any third-party interaction.

Blockchain make sure that the data is transparent and unauthorized user will not be able to modify any information. This paper proposed private blockchain instead of public blockchain because server can place restriction on who can participate in the network and in what transection [15]. When it crosses the limit, automated notification will be sent to the user to pay the fine to use his/her vehicle again in the specific time. Otherwise, in the next month, data usage limit will be automatically reset for every user. To make the system more user friendly, digital wallet payment system is added where user can payment using simplified payment verification (SPV) using Public key cryptosystem[16].

User registration details is described in Fig. 3 where user information will be also stored in the blockchain to match the hash whenever server collect any data from client to ensure the authenticity. Additionally, user can pay the extra charge if it crosses the volume of usage CO_2 gas through his digital wallet that is provided on the registration time by the user.

그림 3. 사용자 등록 과정
Fig. 3. User Registration Procedure

To check the gas usage volume of a vehicle, the electrochemical sensor is used in the proposed methodology. As the sensor collects the data in analog format, it needs to convert in the digital signal. Therefore, an analog to digital converter (ADC) is used to change it into a digital signal. As every vehicle contains a raspberry pi inside it, the usage volume data is transferred from the raspberry pi to the nearby MEC server. Figure 4 describes the data collection and processing workflow from the sensor to the MEC server via raspberry pi. As the cloud server needs more time to collect the data and delay is much higher than the MEC server, this is the reason for using a MEC server in the proposed system rather than a cloud server

The private key of the user is used by the raspberry pi inside the vehicle to transfer the CO_2 usage volume information while transferring it to the MEC server. The raspberry pi encrypts the information using the public key of the user and the MEC server decrypts the data using its private key. Alongside the data, the raspberry pi encrypts the hash of the data using the private key of the user and the MEC server matches the hash by decrypting it using the public key of the user. It proves the authentication of the user inside the network as well as non-repudiation.

After collecting the data, the MEC server checks the usage volume of CO_2 gas by a user that cross the max limit or not. When the usage surpass the limit, the server sends a notification to the user instantly as the contact information is given during the registration time by the user. The MEC server

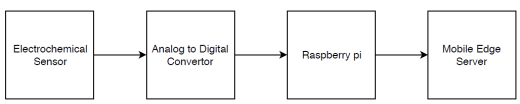

그림 4. 센서를 이용한 데이터 수집 및 전송 과정
Fig. 4. Data Collection & Transfer Process using Sensor

creates a block to store the data in the blockchain to prevent any kind of illegal modification by any third-party. It is considered that all the MEC server is connected via a backhaul network. Each MEC server is acting as a minor node. When any MEC server creates any block, it broadcast the data to verify by the other mining nodes. When the verification is done, only then the block is created. As the data is stored in the blockchain after verification by the mining nodes, no one can modify the previously stored data. Here, the blockchain provides data integrity in the network.

When the user gets notification, user can send the money using the digital wallet in his mobile which is able transferred the money to the MEC server. The smart wallet transfers the money to the MEC server using the private key of the user to ensure the payment is authorized. Otherwise, the user needs to wait for the end of the monthly cycle when the user volume information will be reset in the next month.

Ⅲ. Result Analysis

As the raspberry pi needs to transfer the data to the MEC server regularly, it is important to calculate the throughput and delay time inside the network. Additionally, data needs to be encrypted using public-key cryptography. Therefore, a python code was written to observe and calculate the throughput of a network. Fig. 5 illustrates the throughput of the network. The throughput was calculated both for the secured channel and unsecured channel. The public key cryptographic technique was applied in the secured channel where no cryptographic technique is applied in the unsecured channel. From Fig. 5 it can be observed that throughput is higher in the unsecured channel than secured channel but it can be neglected as the secured channel provides more security while transferring data.

To calculate the delay of a network, it is needed to find out the starting time of data transferring of the raspberry pi and collecting time of data receiving by the MEC server. Network delay represents the performance and typical features of a network. It specifies how long time the data takes to

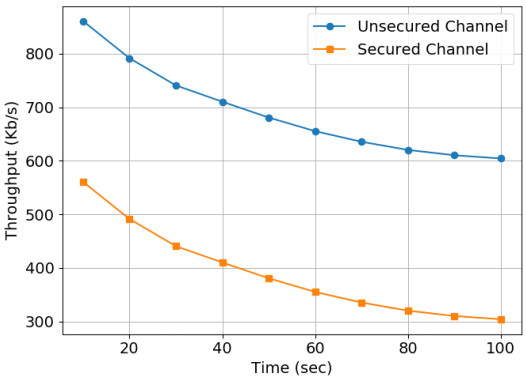

그림 5. 처리량 분석 실험
Fig. 5. Experiment for Throughput Analysis

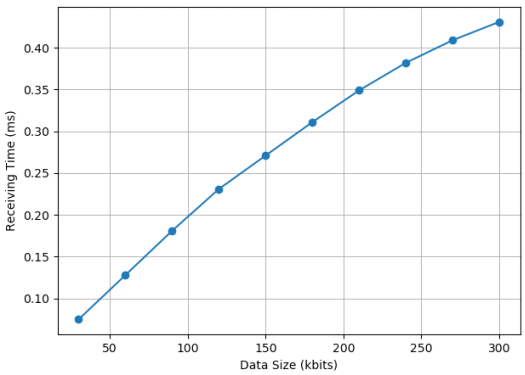

그림 6. 네트워크 지연 분석
Fig. 6. Delay Analysis of the Network

move across the network. Fig. 6 describes the delay time of the network.

Ⅳ. Conclusion and Future Work

This paper proposed an IoT based CO_2 emission reduction scheme using MEC server and with the assist of blockchain technology. Each personal vehicle user registers himself in the system providing his/her personal information. Fixed amount od volume is allocated for each user in a month. Whenever the vehicle runs in the road, the sensor collects the usage information and transfer it to the MEC server for further processing. The public key cryptographic technique is used to make the data transfer technique secure. After collecting the data, the MEC server checks the usage amount and if it crosses the limit it is notified the user. The

usage information is stored in a blockchain by the MEC server so that third-party won't be able to modify the data. User has to pay the penalty if it exceeds the limit using its digital wallet. When the monthly circle is finished, the user usage volume information is automatically reset by the system. Even after collecting the money from the user, authority can spend this money in other sectors to make the environment out of the greenhouse effect and reduce the emission rate of CO_2 gas. Finally, unregistered vehicle identification on the road that is responsible for unnecessary CO_2 gas emission, can be considered as the future work of this research.

References

[1] J. Li, Y. Liu, Z. Zhang, J. Ren, and N. Zhao, "Towards green IoT networking: Performance optimization of network coding based communication and reliable storage," in *IEEE Access*, vol. 5, pp. 8780-8791, 2017.

[2] M. Junxia, J. Linmin, X. Erfeng, and L. Dunnan, "Study on greenhouse gas emission source identification and emission calculation method for power grid enterprises," *2018 8th ICPES*, pp. 289-292, Colombo, Sri Lanka, 2018.

[3] C. Fang, F. R. Yu, T. Huang, J. Liu, and Y. Liu, "A survey of green information-centric networking: Research issues and challenges," in *IEEE Commun. Surv. & Tuts.*, vol. 17, no. 3, pp. 1455-1472, thirdquarter 2015.

[4] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," in *Computers & Electrical Eng.*, vol. 84, 2020, 106627, ISSN 0045-7906.

[5] A. Islam, K. Sadia, M. Masuduzzaman, and S. Y. Shin, "BUMAR: A blockchain-empowered uav-assisted smart surveillance architecture for marine areas," *2020 ICCA*, 2020.

[6] Md. Masuduzzaman, I. Ahmed, A. Arzoo, and T. Sharmin, "Energy efficiency analysis in wired networking by fine grained modification in link state routing protocol," *Int. J. Inf. Technol. and Comput. Sci.*, vol. 11, no. 3, Mar. 2019.

[7] M. A. M. Albreem, "Green internet of things (IoT): An overview," *2017 IEEE ICSIMA*, pp. 1-6, Putrajaya, 2017.

[8] R. Ahmad, M. A. Asim, S. Z. Khan, and B. Singh, "Green IoT—Issues and challenges," *ICACSE*, Available at SSRN 3350317, 2019.

[9] A. Islam and S. Y. Shin, "BUS a blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things," in *IEEE Access*, vol. 7, pp. 103231-103249, 2019.

[10] A. Islam and S. Y. Shin, "BUAV A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *in J. Commun. and Netw.*, vol. 21, no. 5, pp. 491-502, Oct. 2019.

[11] A. Islam and S. Y. Shin, "BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city," *2019 7th ICoICT*, pp. 1-6, Kuala Lumpur, Malaysia, 2019.

[12] A. Islam, M. B. Uddin, M. F. Kader, and S. Y. Shin, "Blockchain based secure data handover scheme in non-orthogonal multiple access," *2018 4th ICWT*, pp. 1-5, Nusa Dua, 2018.

[13] A. Islam, M. F. Kader, and S. Y. Shin, "BSSSQS: A blockchain-based smart and secured scheme for question sharing in the smart education system," *J. Inf. and Commun. Convergence Eng.*, vol. 17, no. 3, pp. 174-184, Sep. 2019.

[14] L. A. Ishaku, D. Hutson, and D. Gibson, "Temperature effects on photoacoustic carbon dioxide sensor developed using mid-IR LED," *2018 IEEE I2MTC*, pp. 1-6, Houston, TX, 2018.

[15] S. Liu, J. Wu, and C. Long, "IoT meets blockchain: Parallel distributed architecture for data storage and sharing," *2018 IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData*, pp. 1355-1360, Halifax, NS, Canada, 2018.

[16] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, and H. Jin, "SBLWT: A secure blockchain lightweight wallet based on trustzone," in *IEEE Access*, vol. 6, pp. 40638-40648, 2018.

무하마드 마수두짜만 (MD Masuduzzaman)

2014년 2월 : American International University-Bangladesh, computer science and engineering, B.Sc.

2016년 2월 : American International University-Bangladesh, computer science, M.Sc.

2019년 9월~현재 : Kumoh Na-tional Institute of Technology, IT convergence engineering, Studyi-ng Ph.D degree.

<관심분야> blockchain, internet of things, UAV, edge computing, machine learning, crytography, network security

[ORCID:0000-0001-8039-3673]

아닉 이슬람 (Anik Islam)

2014년 2월 : American International University-Bangladesh, software engineering, B.Sc.

2017년 2월 : American International University-Bangladesh, computer science, M.Sc.

2017년 9월~현재 : Kumoh National Institute of Technology, IT convergence engineering, Studyi-ng Ph.D degree.

<관심분야> 5G, cognitive radio networks, cooperat-ive communications, blockchain, internet of thi-ngs, wireless network, and distributed system.

[ORCID:0000-0002-6725-9805]

서 종 완 (Jong Wan Seo)

2019년 2월 : 국립금오공과대학교 전자 공학부 졸업

2019 3월~현재 : 국립금오공과대학교 IT융복합공학부 석사과정

<관심분야> 블록체인, 머신러닝 및 딥 러닝

[ORCID:0000-0002-5297-4486]

신 수 용 (Soo Young Shin)

1999년 2월 : 서울대학교 전기공학부 졸업

2001년 2월 : 서울대학교 전기공학부 석사

2006년 2월 : 서울대학교 전기공학부 박사

2010년~현재 : 국립금오공과 대학교 전자공학부 교수

<관심분야> 5G/B5G 무선 접속 기술, 드론 응용, 혼합 현실, 블록체인, 머신러닝 및 딥 러닝

[ORCID:0000-0002-2526-2395]