Summary of Changes

Contents

1 Response to Associate Editor **2**
Comment 1 2

2 Response to Reviewer #1 **2**
Comment 1 2
Comment 2 3
Comment 3 4
Comment 4 4
Comment 5 5

3 Response to Reviewer #2 **7**
Comment 1 7
Comment 2 8
Comment 3 8
Comment 4 9
Comment 5 10

4 Response to Reviewer #3 **10**
Comment 1 10

General response

We would like to express our deep gratitude to the editor and the reviewers for their constructive comments on our paper titled **"Tittle"**, ID: **id**, sub-mitted to IEEE Transactions on Intelligent Transportation Systems. We have revised our manuscript according to the feedback, and please find our responses below.

In this revised version, we accept all reviewers' suggestions and comments to improve the paper, and fix the grammatical and sentence construction errors carefully to make the paper read more smoothly. All the questions, concerns, and comments have been addressed and incorporated into our revision and response letter. We have thoroughly considered the comments of each reviewer point by point. For convenience, modifications are made and highlighted in the revised manuscript. We hope the reviewers are satisfied with the changes we made and wish our paper to be reconsidered for further arrangements.

The followings are the comments of the reviewers and our replies.

1 Response to Associate Editor

Comment 1

The authors are requested to revise the paper carefully in the light of the reviewers' suggestions, especially focusing on the main technical contribution of the paper, the formal analysis of the security of the proposed method, etc.

Response: Thanks for your comments. In the revision, we have carefully addressed all raised concerns regarding

2 Response to Reviewer #1

The authors focused on a homomorphic blockchain scheme for intelligent transport services and designed a solution to address the challenges of security, processing costs, and communication delays. They also developed a simulator (MOTEL) to evaluate the effectiveness of the proposed scheme.

Comment 1

In the abstract, the authors describe the background, ignoring the core contributions and innovation of the proposed algorithm. It is recommended to rewrite the abstract in detail and highlight the contributions and innovation of the work.

Response: Thanks for your valuable time and efforts on our paper. In the revised version of the manuscript, we described the core contributions and innovations of the proposed algorithm. We rewrite the entire abstract from start to end.

Modern smart city services necessitate complex technological infrastructure with heterogeneous compute servers, networks, and communication protocols. However, there are many research issues in heterogeneous computing infrastructure for Intelligent transport systems (ITS) when using the services in the network. Therefore, the main objective of this paper is to intelligent transportation services and their underlying infrastructure, built on an amalgamation of the Internet of Things (IoT), cloud and fog computing, and associated technologies. Specifically, this paper investigates the challenging issues of security, processing costs, and communication delays that frequently occur during the communication of data and messages. We propose novel, secure, and cost-effective schemes based on blockchain-assisted homomorphic encryption techniques. A Secure, Cost-Optimal Workload Assignment (SCWA) algorithm and a blockchain scheme made possible by Partially Hashing Homomorphic Encryption and Decryption (PHHE/D) are designed to distribute workload efficiently. We developed a simulator, MOTEL, that simulates the different functions of the proposed schemes and all the necessary components. Using MOTEL and data sets from real

transport companies, the proposed approach is tested and evaluated using various experiments. The results demonstrate that, compared to existing solutions, the proposed approach significantly reduces processing costs and delays while maintaining an appropriate level of security in transport services.

The changes are highlighted in the abstract.

Comment 2

How does the proposed PHHE/D method contribute or impact to the PoW validation process?

Response: Thanks for your valuable time and efforts on our paper. In the revised version of the manuscript, we added the detail of the PHHE/D method with the contribution and defined why PHHE/D is more optimal than PoW.

Figure 1: PoW Scheme with Homomorphic Encryption.

In our system, we consider the heterogeneous computing nodes such as local transport, wireless and edge cloud nodes. Therefore, when we apply blockchain technology on nodes, there are resource constraints issues in nodes. The main contribution of the PHHE/D method is to compute encryption and decryption on the resource-efficient nodes, and on the resource constraint, it computes the validation on the ciphertext instead of reprocessing the encryption and decryption. In this way, we can keep the balance between resource-constraint devices and rich resource nodes and maintain blockchain security among different nodes. Whereas existing PoW schemes perform the computation on all nodes with the same strategy that

each node validates the data based on hashing and then starts the encryption and decryption for the next node, which is more time and resource consuming and resource constraints nodes can not support this scenario for intelligent transport applications. Therefore, we devise Partially Hashing Homomorphic Encryption/Decryption (PHHE/D) based on advanced standard encryption (AES).

The scheme is diagrammatically represented in Fig. 1. The scheme exploits the asymmetric security mechanism, where the public key is used for encryption, and the private key is used for the resultant decryption. In the proposed scheme, local devices can encrypt data and results. Other devices can only transfer and apply computation to the data.

The changes are highlighted in the manuscript on page number 7.

Comment 3

There are many notations for mathematical modeling. It is recommended that the authors use a table to list the variables and names used in this work.

Response: Thanks for your valuable time and efforts on our paper. In the current version of the manuscript, we added Table 1 of mathematical notations where we defined the list of variables with their description. The changes are highlighted in the manuscript on page number 5. Table 1 defines all mathematical notations with their description as defined above in the manuscript. Each variable is defined with their definition, we put all notations of the problem in Table 1.

Comment 4

In Eqs. (2) and (3), are the local execution time and local cost of requests during encryption and decryption equal to 1?

Response: Thanks for your valuable comment! In the current version of the manuscript, we provide the definition and purpose of setting 1 in Eqs. (2) and (3).

The proposed system makes the local encryption and decryption based on partial homomorphic and determines the time in the following way.

$$time_{LE} = \sum_{v_w=1}^{W} \sum_{v=1}^{V} \sum_{d=1}^{D} \frac{v_w}{\zeta_d} \times Enc + Dec \times x_{v,bs,k} = 1, \tag{1}$$

$$cost_{LE} = \sum_{v_w=1}^{W} \sum_{v=1}^{V} \sum_{d=1}^{w} \frac{v_w}{\zeta_d} \times Enc + Dec \times x_{v,bs,k} = 1. \tag{2}$$

Whereas Eqs. (2) and (3) determine the local execution time and local cost of requests during encryption and decryption. However, the local time and cost are calculated after assignment

Table 1: Mathematical Notation

Problem Notations	Notation Definitions
V	Number of vehicular applications
v	The particular vehicular application v
W	Total number of workloads
v_w	Workload of application v
R	Total number of requests of V
r_w	Particular request of workload v_w
v_d	Deadline of vehicular application
D	Number of vehicle devices
d	Particular vehicle device
ζ_d	Processing speed of device d
ϵ_d	Resource of device d
BS	Number of BSs
bs	particular BSs
ζ_{bs}	Processing speed of BSs
ϵ_{bs}	Resource of BSs
K	Number of fog nodes
k	Particular fog node
ϵ_k	Resources of node k
B	Set of blockchain blocks
b	Particular block
p, q	Random number
PK, PV	Primary key, Private key 256-bits
$L1, L2, L3$	Initial Location, Mobility Location, Destination

on nodes as shown with this expression, e.g., $x_{v,bs,k=1}$. The 1 shows the assignment of tasks on the nodes. Otherwise, it is equal to 0.

The changes are highlighted in the manuscript on pages 5 to 6.

Comment 5

More comparison experiments are suggested to compare the effectiveness of the proposed method and current encryption methods.

Response: Thanks for your valuable comment! In the current version of the manuscript, we added more result analysis as shown in Fig. 2 and Fig. 3.

Fig. 2 and Fig. 3 show the effectiveness of the proposed scheme PHHE/D compared to existing encryption techniques used in the blockchain for the validation of services of transport applications. Fig. 2 shows that PHHE/D has less processing time and cost in dollars than existing encryption methods. The main reason is that we perform the encryption compu-

tation on the rich resource node and do not repeat the encryption and decryption on each node for hashing, as the generally existing hashing and cryptography methods are done in blockchain technology. The partially homomorphic minimizes the time and cost and avoids re-encryption and decryption again and again on nodes and saves many resources consumption and service cost as shown in Fig. 3.

The changes are highlighted in the manuscript on pages 13 and 14.

Further, we conduct more experiments to compare our scheme with existing consumer electronics transport applications. The results are shown in Fig. 2. These show that the proposed homomorphic encryption and decryption have a lower delay and cost than SHA-256 and AES, which are implemented in the existing blockchain for consumer electronics transport applications.

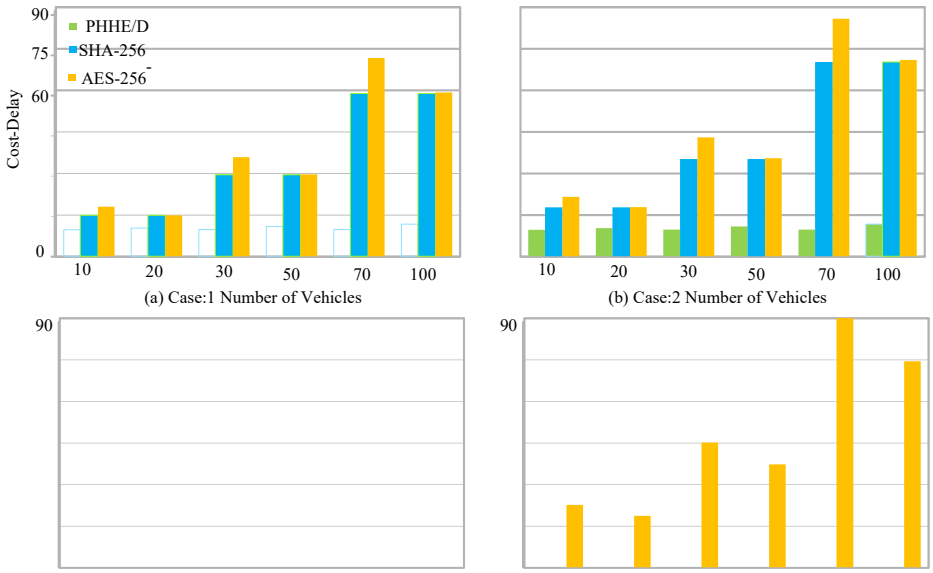

Figure 2: Processing Cost and Delay of Hashing and Blockchain Validation for Vehicles Applications.

We implemented different encryption methods, such as generic cryptography and hashing techniques, which are widely used in blockchain technology to validate transport data with different services.

Fig. 3 shows the effectiveness of the proposed scheme PHHE/D compared to existing encryption techniques used in the blockchain for the validation of services of transport applications. Fig. 3 shows that PHHE/D has less processing time and cost in dollars than existing encryption methods. The main reason is that we perform the encryption computation on the rich resource node and do not repeat the encryption and decryption on each node for hashing, as the generally existing hashing and cryptography methods are done in blockchain technology. The partially homomorphic minimizes the time and cost to avoid re-encryption and decryption again and again on nodes and saves many resources consumption and service costs as shown in Fig. 3.

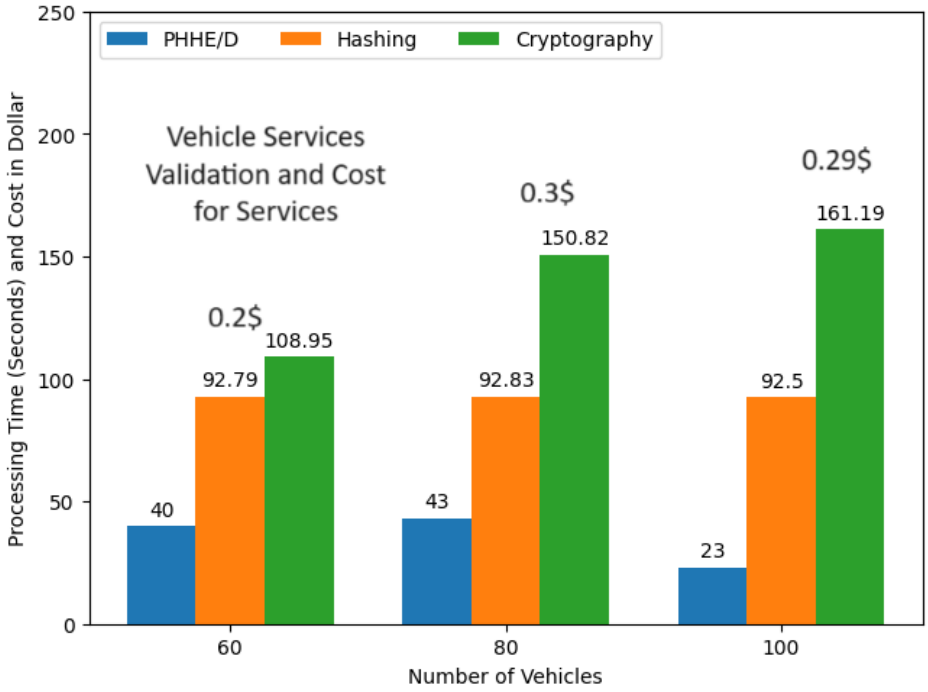

Figure 3: Processing Time and Cost Based on Encryption Methods for Vehicle Services.

3 Response to Reviewer #2

In this work, the authors proposed a secure, and cost-effective schemes based on blockchain-enabled homomorphic encryption techniques. A Secure, Cost-Optimal Workload Assignment (SCWA) algorithm and a blockchain scheme made possible by Partially Hashing Homomorphic Encryption and Decryption (PHHE/D) are designed to distribute workload efficiently. Next, the authors developed a simulator, MOTEL, that simulates the different functions of the proposed schemes and all the necessary components. Using MOTEL and data sets from real transport companies, the proposed approach is tested and evaluated using various experiments.

Overall, the work is good in technical quality. The following suggestions need to be incorporated:

Comment 1

The motivation of the work should be more concise and concrete.

Response:

Thanks for your valuable time and efforts on our paper. In the current version of manuscript, we added the motivation of the paper with the novelty. We define the motivation and novelty of the work in the following way. Partial Homomorphic Enabled Blockchain for Complex Networks: The proposed scheme devises a blockchain-enabled secure complex network-aware framework in which data communication, offloading, and scheduling of requests are carried out securely and efficiently. It exploits the blockchain decentralized

mechanism to connect autonomous computing nodes (e.g., vehicular devices, base stations, IoT, cloud, and fog nodes), which take part in the processing of functionality of intelligent transport applications. The paper makes a novel contribution to the work. Heterogeneous Node Security Validation. The scheme introduces homomorphic encryption-enabled hashing and Pow validation schemes for transferring data among different nodes. It also devises a secure, delay-efficient, cost-optimal workload assignment (SCWA) algorithm. Partially Hashing Homomorphic Encryption/Decryption (PHHE/D) encrypts data and requests at local devices and then offloads them to the fog for execution via base stations. A novel and practical simulator called MOTEL-Transport. It contains consumer electronics data, complex network node services, applications, and information relevant to base stations, fog, and cloud layers. It contends that existing literature needs to design a novel, practical simulator for intelligent transport applications. The changes are highlighted in the manuscript on page 2.

Comment 2

A threat model should be provided.

Response: Thanks for your valuable time and efforts on our paper. In the current version of manuscript, we added the motivation of the paper with the novelty.

We define the motivation and novelty of the work in the following way. Partial Homomorphic Enabled Blockchain for Complex Networks: The proposed scheme devises a blockchain-enabled secure complex network-aware framework in which data communication, offloading, and scheduling of requests are carried out securely and efficiently. It exploits the blockchain decentralized mechanism to connect autonomous computing nodes (e.g., vehicular devices, base stations, IoT, cloud, and fog nodes), which take part in the processing of functionality of intelligent transport applications. The paper makes a novel contribution to the work. Heterogeneous Node Security Validation. The scheme introduces homomorphic encryption-enabled hashing and Pow validation schemes for transferring data among different nodes. It also devises a secure, delay-efficient, cost-optimal workload assignment (SCWA) algorithm. Partially Hashing Homomorphic Encryption/Decryption (PHHE/D) encrypts data and requests at local devices and then offloads them to the fog for execution via base stations. A novel and practical simulator called MOTEL-Transport. It contains consumer electronics data, complex network node services, applications, and information relevant to base stations, fog, and cloud layers. It contends that existing literature needs to design a novel, practical simulator for intelligent transport applications. The changes are highlighted in the manuscript on page 2.

Comment 3

A security analysis is needed based on the defined threat model.

Response: Thanks for your valuable time and efforts on our paper. In the current version of the manuscript, we analyzed the security analysis in the threat model.

For the security analysis, we match the hashing pattern in each blockchain block, which is available in the form of hashing. If the hashing pattern and offloaded hashed are matched, the system acknowledges it as authenticated and valid transactions. Otherwise, the transaction remains on hold until and unless the pattern is in its original form. Our system considers heterogeneous computing nodes such as local transport, wireless, and edge cloud nodes. Therefore, when we apply blockchain technology on nodes, there are resource constraints issues in nodes. The main contribution of the PHHE/D method is to compute encryption and decryption on the resource-efficient nodes, and the resource constraint computes the validation on the ciphertext instead of reprocessing the encryption and decryption. In this way, we can keep the balance between resource-constraint devices and rich resource nodes and maintain blockchain security among different nodes. Whereas existing PoW schemes perform the computation on all nodes with the same strategy that each node validates the data based on hashing and then starts the encryption and decryption for the next node, which is more time and resource consuming and resource constraints nodes can not support this scenario for intelligent transport applications.

The changes are highlighted in the manuscript on page number 7.

Comment 4

The related work section should be more critical in analysis. There are some important work that need to be cited in the related work. Some of them are:
* "An Authentication and Key Management Framework for Secure and Intelligent Transportation of Internet of Space Things," in IEEE Transactions on Intelligent Transportation Systems, 2023, DOI: 10.1109/TITS.2023.3338274.
* "Blockchain-Based Efficient Access Control with Handover Policy in IoV-Enabled Intelligent Transportation System," in IEEE Transactions on Vehicular Technology, Vol. 73, No. 3, pp. 3009-3024, March 2024
* "Robust Authenticated Key Agreement Protocol for Internet of Vehicles-Envisioned Intelligent Transportation System," in Journal of Systems Architecture, Vol. 142, Article ID: 102937, pp. 1-12, September 2023
* "Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems using Blockchain and PUF," in IEEE Access, Vol. 11, pp. 60240-60253, 2023
* "A Provably Secure Mobile User Authentication Scheme for Big Data Collection in IoT-Enabled Maritime Intelligent Transportation System," in IEEE Transactions on Intelligent Transportation Systems, Vol. 24, No. 2, pp. 2411-2421, February 2023

Response: We are grateful for this suggestion. In the current version of the manuscript, we added the aforementioned references in the related work. The main objective of these studies is to allow one node to encrypt and decrypt in the blockchain-based network and offload workloads from one node to another. The homomorphic schemes have various types,

such as fully and partially homomorphic, with varying encryption schemes, such as ElGamal, Goldwasser-Micali, and Benaloh, to perform encryption on one node. The rest of the nodes perform computation on the encrypted data instead of plaintext, as done in previous AES and SHA-256 schemes. The main objective of these studies is to allow one node to encrypt and decrypt in the blockchain-based network and offload workloads from one node to another. These studies [1, 2, 3, 4, 5] suggested lightweight security protocols such as cryptography and hashing for intelligent transport system applications. These security analysis protocols validated the data transactions among different nodes. However, these studies could have avoided the higher cost of resources and processing time in blockchain-enabled transport services in mobile fog cloud networks.

Comment 5

Finally, the paper needs careful proof-reading for typos and grammatical mistakes.

Response:

We are grateful for this suggestion. In the current version of the manuscript, we revised the manuscript carefully and proofread it from abstract to conclusion. We tried our best level to remove the typo errors and grammatical mistakes and incomplete sentences from the entire contents of the manuscript.

4 Response to Reviewer #3

Comment 1

The paper presented trivial contribution and novelty, and the writing and organization were not suitable for this journal.

Response: Thank you for your valuable time and efforts on our paper. In this paper, we present the new homomorphic technique inside blockchain technology for data validation and perform all transactions in the immutable form. The main reason is that not all nodes have enough resources to perform transactions using blockchain technology. Therefore, we introduced the new novel homomorphic security threat model inside the blockchain for the intelligent transport vehicle to invoke the services efficiently and offload data in a secure form. This paper is designed according to the requirements of REUTER company OSLO, we collected and validated the data from the company. We designed the simulator MOET simulator based on their requirements, and in the simulation results, we have shown the optimal performances of the work. We have tried our best level to improve the writing and

organization of the paper according to journal standards.

References

[1] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty. An authentication and key management framework for secure and intelligent transportation of internet of space things. *IEEE Transactions on Intelligent Transportation Systems*, 25(6):5242–5257, 2024.

[2] Sandip Roy, Sourav Nandi, Raj Maheshwari, Sachin Shetty, Ashok Kumar Das, and Pascal Lorenz. Blockchain-based efficient access control with handover policy in iov-enabled intelligent transportation system. *IEEE Transactions on Vehicular Technology*, 73(3):3009–3024, 2024.

[3] Siddhant Thapliyal, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, and SK Hafizul Islam. Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system. *Journal of Systems Architecture*, 142:102937, 2023.

[4] Seunghwan Son, Deokkyu Kwon, Sangwoo Lee, Yongsung Jeon, Ashok Kumar Das, and Youngho Park. Design of secure and lightweight authentication scheme for uav-enabled intelligent transportation systems using blockchain and puf. *IEEE Access*, 11:60240–60253, 2023.

[5] Khalid Mahmood, Javed Ferzund, Muhammad Asad Saleem, Salman Shamshad, Ashok Kumar Das, and Youngho Park. A provably secure mobile user authentication scheme for big data collection in iot-enabled maritime intelligent transportation system. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2411–2421, 2022.