iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50453

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

SE-VFC: A Secure Framework for Computation Outsourcing in Vehicular Fog Computing Environments

Bhavya Vaishnavi[1], Dr. Praveen Kumar K V[2]
[1]*Student,* [2]*Professor, Dept. of Computer Science Engineering, Sapthagiri Engineering College*

Abstract: ***SE-VFC is a proposed computing scheme that addresses the challenge of providing secure and efficient outsourcing computing in vehicular fog computing. Vehicular fog computing is a paradigm that involves the utilization of computing resources in vehicles to provide various computing services to end- users. However, since fog vehicles may be untrusted, there is a potential for malicious operations that can cause serious accidents.***
To address this challenge, SE-VFC proposes the use of a secure and efficient outsourcing computing scheme that involves fog vehicles with computing resources. The scheme utilizes lightweight Boneh-Lynn-Shacham (BLS) signature and group signature for batch anonymous authentication of fog vehicles while preserving their privacy in multiple outsourcing tasks. This means that fog vehicles are authenticated and verified without revealing their identities, which helps to protect their privacy.
Additionally, SE-VFC ensures the correctness of the computing results by verifying them. This helps to ensure that the results produced are accurate and reliable. Compared to existing schemes, SE-VFC has relatively low communication and computation overhead, making it efficient for batch authentication in multiple computing tasks. The effectiveness and practicality of the proposed scheme have been verified through extensive simulation results.
Overall, SE-VFC is an important contribution to the field of vehicular fog computing, as it addresses the challenge of providing secure and efficient outsourcing computing while also ensuring the privacy and correctness of the computing results.
Index Terms: Outsourcing computing; vehicular fog computing; Boneh-Lynn-Shacham (BLS) signature; attribute-based encryption (ABE)

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) have evolved from providing simple internet services to advanced applications like video streaming, augmented and virtual reality. However, ensuring the secure and reliable delivery of data in VANETs poses challenges due to privacy and security concerns. Attribute- based encryption (ABE) has been proposed to provide secure information dissemination in highly dynamic vehicular communication environments. Nonetheless, the decryption time of ABE increases with the number of attributes, limiting its practical application in VANETs. As an alternative, vehicular fog computing has been proposed to enhance the performance of latency-critical applications. This paradigm employs end-users like vehicles and mobile devices as infrastructures, utilizing their communication and computational resources. However, fog vehicles may forge identities, leading to malicious activities. To address these issues, we propose a secure and efficient outsourcing computing scheme in vehicular fog computing (SE- VFC), which allows the source vehicle to outsource complex ciphertext policy ABE decryption operation to fog vehicles whileensuring secure and efficient real-time information services.
The proposed scheme employs a lightweight Boneh-Lynn- Shacham (BLS) signature and group signature algorithm to achieve batch anonymous authentication of fog vehicles while ensuring their privacy in multiple outsourcing tasks. The scheme also employs verifiable outsourcing CP-ABE algorithm to prevent malicious fog vehicles from performing incorrect outsourcing computing.
The passage discusses the challenges of security and privacy in vehicular ad-hoc networks (VANETs) and proposes a solution called Secure and Efficient Outsourcing Computing Scheme in Vehicular Fog Computing (SE-VFC). VANETs are becoming increasingly complex, with applications ranging from simple email services to video streaming and augmented/virtual reality.

However, ensuring the secure and reliable delivery of data is challenging due to the highly dynamic vehicular communication environment. Attribute-based encryption (ABE) has been proposed to provide secure information dissemination, but its decryption time increases as the number of attributes increases, limiting its practical application. Therefore, SE-VFC proposes todelegate part of the complex decryption to fog vehicles, which are vehicles that voluntarily join and leave the vehicular fog computing network. The proposed scheme uses a lightweight Boneh-Lynn-Shacham (BLS) signature and group signature algorithm to achieve batch anonymous authentication of fog vehicles while protecting their privacy. The fog vehicles' integrity is verified using verifiable outsourcing CP-ABE algorithm to prevent malicious fog vehicles from stealing or tampering with information. The proposed solution aims to ensure the secure and efficient delivery of real-time information services in VANETs.

This paper presents the proposed scheme's contributions, which include secure and efficient outsourcing computing in vehicular fog computing, an efficient batch anonymous authentication scheme for fog vehicles, and the employment of verifiable outsourcing CP-ABE algorithm to ensure the correctness of outsourcing computing results. The paper is structured as follows: Section II presents literature survey on vehicular fog computing and attribute-based encryption in VANETs. Section III outlines the consolidated table. Section IV evaluates the acknowledgement, and Section V concludes the conclusion and future scope.

II. LITERATURE SURVEY

In this section, we review the vehicular fog computing and attribute-based encryption in VANETs, and analyze the security problems.

A. Vehicular Fog Computing in VANETs

Different from vehicular cloud computing, vehicular fog computing supports the mobility and location awareness of nearby vehicles and uses the idle computing and storage resources of vehicles located inside VANETs to generate fog instantly [8, 13]. In vehicular fog computing, many researcherspaid attention to task allocation [14–16], fog node selection [17] and secure data sharing [13, 18]. Task allocation approaches mainly focused on optimized task allocation for minimizing average service latency [15], dynamic task allocation solutions using reinforcement learning [14], reliable task offloading under information uncertainty [16] and an application-aware offloading policy by the semi markov decision process [19]. They adopted different methodsto make task allocation efficient and reliable. Security issues such as malicious fog vehicles are important issues that greatly affect the reliable of task allocation in vehicular fog computing. So we focus on authenticating the fog vehicles and verifying the correctness of the results in fog task computation. To attract the fog-capable vehicles to participate in the vehicular fog computing network, Wang et al. [20] designed a contract-based resource allocation framework to attract nearby vehicles to participate through an effective incentive mech anism. Hao et al. [17] proposed a vehicular fog computing architecture to implement cooperative sensing among multiple adjacent vehicles driving in the form of a platoon. However, fog vehicles sometimes may be untrusted, and results from themalicious operations will cause serious accidents. We identify the security research challenges that need to be addressed to select fog node and improve tasks' offloading performance.

B. Security Issues in Vehicular Fog Computing

Researchers proposed that fog server was aided and assisted in the secure cloud-based data sharing. Xue et al. [13] pro posed a fog-to-cloud-based architecture for data sharing, in which data cloud be offloaded to the fog vehicles in advance based on a user's mobility prediction. And the encryption task and decryption task were outsourced to semi-trusted fog servers and the cloud server, respectively. The scheme could provide verifiable auditing of fog servers' reports withthe assumption that there was no collusion between different providers for the cloud and fog servers. Yao et al.[18] explored a mechanism for provisioning client-vehicles with reliable and secure vehicular fog service provided by a group of server vehicles. They applied the existing public key algorithms in vehicular fog contruction and vehicular fog service access to achieve reliability and security, but did not address the security issues such as verification in vehicular fog service. Due to the openness and dynamic nature of vehicular fog computing, when malicious fog vehicles join the network, theymight send false reports [21], steal users privacy [13] or even perform incorrect computing. Therefore, under the influence ofmalicious mobile vehicles, fog computing is greatly threatened by security attacks. Zheng et al. [22] studied the security of offloading in multi-vehicle edge cloud system based on cloud blockchain, which used blockchain-based access control to protect the cloud from illegal offloading actions. Liao et al.

[23] developed a secure and intelligent task offloading framework, which exploited blockchain and smart contract to facilitate fair task offloading and mitigate various security attacks. The scheme considered the malicious behavior of fognodes and used signature based on asymmetric cryptosystem and smart contracts to authenticate fog nodes. Wei et al. [24] designed a secure and efficient outsourcing algorithm, which used identity-based signature to achieve unforgeability. How ever, the above schemes ignored the situation that malicious fog vehicles may perform incorrect outsourcing computing, which would cause the failure of the entire task offloading in vehicular fog computing.

C. Attribute-based Encryption in VANETs

Ciphertext policy attribute-based encryption (CP-ABE) was first proposed by Waters et al. [25] and considered to be a promising encryption mechanism for access control of en crypted data. CP-ABE schemes have been extensively studied in VANETs. Safi et al. [4] proposed a cloud-based security andprivacy-aware information dissemination scheme to achieve fine-grained information sharing between vehicle nodes and cloud systems. Pan et al. [26] proposed a scheme for sharing data between different domains, which used ABE and ellip tic curve cryptography to ensure information confidentiality. Many researchers have proposed lots of variants of ABE scheme in different environments [27, 28], including non monotonic access structure, attribute revocation and so on. In summary, the CP-ABE algorithms have been widely used in VANET's applications such as information sharingand information storage, but the computation costs in the decryption increase with the number of attributes in the access formula, which required many parings in most of existing traditional CP-ABE schemes. Green et al. [29] introduced the outsourcing decryption of the ABE ciphertext. Zhou et al proposed to outsource some encryption and decryption computing to the cloud. The method based on outsourcing computing could effectively solve the problem of efficiency, butit introduces security problems that need to be solved urgently. Zuo et al. [31] proposed a concrete chosen-ciphertext security (CCA) ABE scheme with outsourcing decryption. A CP-ABE system with outsourcing computing should ensure that an adversary (including a malicious cloud or fog) would not be ableto learn anything about the encrypted message and guarantee thecorrectness of the computation done by them [32, 33].

III. CONSOLIDATED TABLE

Sl.No.	Title of thepaper	Description	Advantage	Limitation
1.	"Secure task offloading in vehicular fog computing" by Liuet al. (2018)	This paper proposed a secure task offloading scheme for VFC that uses attribute-based encryption (ABE) to ensure data privacy and integrity. The scheme allows vehicles to offload computation tasks to fog nodes while ensuring that only authorized fog nodes can access the data.	The paper proposes a novelsecure task offloading scheme that uses homomorphic encryption toprotect the privacy of data and computation during theoffloading process. The scheme takes into account the dynamic and unreliable nature of vehicular networks and considers factors such as mobility, location, and trustworthiness of fog nodesto ensure secure and efficient task offloading. The authors evaluate the proposed scheme through simulation experiments, andthe results show that it outperforms existing schemes in terms of security, privacy, and efficiency.	The proposed scheme relies heavily on homomorphic encryption, which can be computationally expensive and may not be practical for resource-constrained devices and networks. The paper assumes that all fog nodes and vehicles are honest and trustworthy, which may not be realistic in real-world scenarios. More research is needed toaddress the issue of trust in vehicular fogcomputing. The simulation experiments are based on a specific set of assumptions and parameters, andthe results may not be generalizable to other scenarios or network conditions.Further studies

				are needed to validate the proposed scheme in real-world environments.
2.	"Efficient and secure data sharingin vehicular networks using blockchain" by Wang et al. (2019)	This paper proposed a blockchain-based scheme for secure and efficient data sharing in VFC. The scheme uses smart contracts to enforce access control and data privacy policies and allows vehicles to offload computation tasks to fog nodes securely.	The paper proposes a novel blockchain-based data sharing scheme that can ensure data privacy, integrity, and availability invehicular networks, where data are transmitted amongvehicles and roadside units. The proposed scheme employs lightweight consensus mechanisms and smart contracts to achieve fast and secure data sharing,without relying on a centralized authority or a trusted third party. The authors evaluate the proposed scheme through simulation experiments, andthe results show that it outperforms existing data sharing schemes in terms of security, privacy, efficiency,and scalability.	The proposed scheme relies on blockchain technology, which can be computationally expensive and may not be practical for resource-constrained devices and networks. The paper assumes that all participating nodes in the vehicular network are honest and trustworthy, which may not be realistic in real-world scenarios. More research is needed toaddress the issue of trust in blockchain- based vehicular networks. The simulation experiments are based on a specific set of assumptions and parameters, andthe results may not be generalizable to other scenarios or network conditions. Further studies are needed to validate the proposed scheme in real-world environments.
3.	"Privacy- preserving data aggregation in vehicular fog computing" by Wu et al. (2019)	This paper proposed a privacy-preserving data aggregation scheme for VFC that allows fog nodes to aggregate data from vehicles without revealing sensitive information. The scheme uses homomorphic encryption and random masking to ensure data privacyand integrity.	The proposed scheme provides a practical solutionto protect the privacy of vehicular data while allowing fog nodes to aggregate it for analysis anddecision making. By using homomorphic encryption and random masking, the scheme ensuresthat data privacy and integrity are preserved while minimizing the communication and computation overhead.	The proposed scheme may still suffer from certain types of attacks, such as traffic analysis attacks or correlation attacks, which could compromise the privacy of vehiculardata. The implementationand deployment of the scheme may face challenges in terms

			The scheme is scalable and can be adapted to different VFC scenarios with different requirements for data aggregation and privacyprotection.	of compatibility with existing VFCsystems and hardware constraints. The scheme may also add some additional latency and computational overhead to the dataaggregation process, which could affect the overall performance of the VFC system.
4.	"Secure and efficient computation outsourcing in vehicular networks" by Wang et al. (2017)	This paper proposed a secure and efficient computation outsourcing scheme for VFC that uses attribute-based encryption and homomorphic encryption to ensure data privacy and integrity. The scheme allows vehicles to offload computation tasks to fog nodes securely and efficiently.	The paper addresses an important issue in vehicularnetworks, which is the secure and efficient outsourcing of computationtasks. The proposed framework isbased on secure multi-partycomputation (MPC) and homomorphic encryption, which are well-established cryptographic techniques. The authors provide a detailed description of the proposed framework and its implementation, which makes it easy to replicate the results. The paper includes a comprehensive evaluation ofthe proposed framework using simulation experiments, which demonstrate its effectivenessand efficiency.	The proposed framework is evaluated only through simulation experiments, which may not reflect real-world conditions accurately. The paper assumes atrusted third party (TTP) to facilitate the secure multi-party computation (MPC), which may not be feasible in allsituations. The authors do not provide a detailed analysis of the scalability of the proposed framework, which could be a limitationin larger vehicular networks. The paper does notprovide a thoroughanalysis of the potential attack scenarios and theirimpact on the proposed framework's security.
5.	"Privacy-preserving deep learning in vehicular fog computing" by Huang et al. (2020)	This paper proposed a privacy-preserving deep learning scheme for VFC that uses secure multi-party computation (MPC) to enable vehicles to train machine learning models collaboratively without revealing sensitive information. The scheme allows vehicles to offload computation tasks to	The paper addresses an important issue in vehicularnetworks, which is the privacy-preserving deep learning in fog computing. The proposed approach is based on federated learning,which allows the model to be trained on decentralized data without compromisingthe data privacy of individual vehicles. The paper provides a detailed description of theproposed approach and its	The paper assumesthat all vehicles arehonest and follow the protocol, which may not be realisticin real-world scenarios. The proposed approach relies on atrusted fog node to coordinate the federated learning process, which may not be feasible in all situations.

		fog nodes while ensuring data privacy and inteKegrity.	implementation, which makes it easy to replicate theresults. The authors evaluate the proposed approach using both simulation experimentsand a real-world dataset, which demonstrates its effectiveness and efficiency. The paper provides a thorough analysis of the potential attack scenariosand their impact on the proposed approach's security.	The paper does notprovide a thoroughanalysis of the scalability of the proposed approach,which could be a limitation in larger vehicular networks. The proposed approach is evaluated only on a single task, and it is not clear how well itwould perform on other tasks or datasets.

IV. ACKNOWLEDGEMENT

Any achievement does not depend solely on the individual efforts but on the guidance, encouragement and co-operation of intellectuals, elders and friends. We extend our sincere thanksto Dr. Kamalakshi Naganna, Professor and Head, Department of Computer Science and Engineering, Sapthagiri College of Engineering, and Dr Praveen Kumar K V Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering, for constant support, advice and regular assistance throughout the work. Finally, we thank our parents and friends for their moral support.

V. CONCLUSION AND FUTURE SCOPE

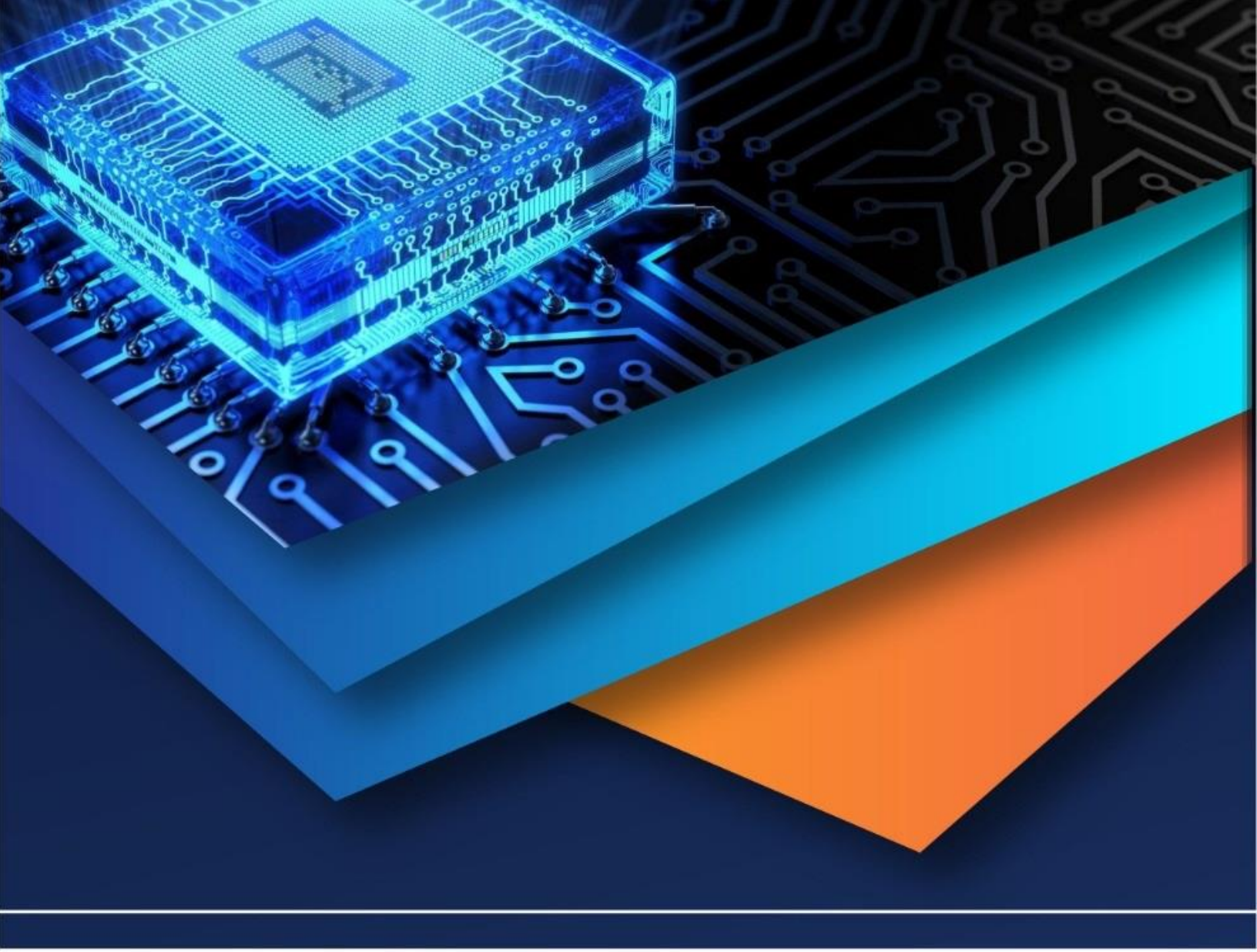
The paper proposes a secure and efficient framework for outsourcing computation tasks in vehicular fog computing (VFC) environments. The proposed framework uses secure multi-party computation (MPC) and homomorphic encryption to enable multiple vehicles to jointly perform computations on their data without revealing any sensitive information to each other or to the fog server. The framework also ensures data integrity and confidentiality by using digital signatures and secure communication protocols. The authors evaluate the proposed framework using simulation experiments and demonstrate its effectiveness and efficiency. Although the proposed framework is effective and efficient in addressing the secure outsourcing of computation tasks in vehicular fog computing environments, there is still room for improvement. Some future research directions are:

1) *Scalability:* The proposed framework needs to be evaluated for scalability to handle a larger number of vehicles and computation tasks.
2) *Robustness:* The proposed framework needs to be evaluated for robustness against various types of attacks, including attacks on communication channels andcomputation tasks.
3) *Real-World Experiments:* The proposed framework needsto be evaluated in real-world VFC environments to validate its performance and effectiveness.
4) *Privacy:* The proposed framework should be evaluated for its privacy guarantees, particularly in terms of the data privacy of individual vehicles.
5) *Comparison:* The proposed framework should be compared with other existing frameworks to evaluate its competitiveness and advantages.

REFERENCES

[1] Hani Sami, Azzam Mourad, and Wassim El-Hajj. Vehicular-obus-as-on-demand-fogs: Resource and con- text aware deployment of containerized micro-services. IEEE/ACM Transactions on Networking, 28(2):778– 790,2020.
[2] GG Md Nawaz Ali, Peter Han Joo Chong, Syeda Khairunnesa Samantha, and Edward Chan. Efficient data dissemination in cooperative multi-rsu vehicular ad hoc networks (vanets). Journal of Systems and Software, 117:508–527, 2016.
[3] Dijiang Huang and Mayank Verma. Aspe: Attribute- based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Networks, 7(8):1526–1535, 2009.
[4] Qamas Gul Khan Safi, Senlin Luo, Chao Wei, Limin Pan, and Guanglu Yan. Cloud-based security and privacy- aware information dissemination over ubiquitous vanets.Computer Standards & Interfaces, 56:107–115, 2018.
[5] Xuejiao Liu, Zhenyu Shan, Luming Zhang, Wei Ye, and Ruoyu Yan. An efficient message access qualitymodel in vehicular communication networks. Signal Processing,120:682–690, 2016.

[6] Mounia Bouabdellah, Faissal El Bouanani, and Hussain Ben-Azza. A secure cooperative transmissionmodel in vanet using attribute based encryption. In International Conference on Advanced Communication Systems and Information Security (ACOSIS), pages 1–6. IEEE, 2016.
[7] Yingjie Xia, Wenzhi Chen, Xuejiao Liu, Luming Zhang, Xuelong Li, and Yang Xiang. Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks. IEEE Transactions on Intelligent Transporta- tion Systems, 18(10):2629– 2641, 2017.
[8] Zhaolong Ning, Jun Huang, and Xiaojie Wang. Vehic-ular fog computing: Enabling real-time traffic manage- ment for smart cities. IEEE Wireless Communications, 26(1):87–93, 2019.
[9] Xueshi Hou, Yong Li, Min Chen, Di Wu, Depeng Jin,and Sheng Chen. Vehicular fog computing: Aviewpoint of vehicles as the infrastructures. IEEE Transactions on Vehicular Technology, 65(6):3860– 3873, 2016.
[10] Xuejiao Liu, Wei Chen, Yingjie Xia, Member, IEEE, Chenghan Yang. SE-VFC: Secure and efficient outsourcing computing in vehicular fog computing. IEEE Transactions on Network and Service Management, 18(3):3389-3399, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY