VDMF: VANETs Detection Mechanism Using Fog Computing for Collusion and Sybil Attacks

Asif Khan, Qazi Ejaz Ali*

Department of Computer Science, University of Peshawar, Pakistan.

***Correspondence:** qaziejazali@uop.edu.pk

Citation | Khan. A, Ali. Q. E, “VDMF: VANETs Detection Mechanism Using Fog Computing for Collusion and Sybil Attacks”, IJIST, Vol. 06 Issue. 03 pp 1554-1567, Sep 2024

DOI | https://doi.org/10.33411/ijist/20246315541567

Received | Aug 23, 2024 **Revised |** Sep 25, 2024 **Accepted |** Sep 26, 2024 **Published |** Sep 30, 2024.

Vehicular Ad Hoc Networks (VANETs) have evolved as a key component of the intelligent transportation system, enhancing road safety and traffic efficiency. It is crucial to secure sensitive information, and detection of incident response, whenever malicious activity is observed. Key components of VANETs include vehicles, Roadside Units (RSUs), and Fog servers (FS). Despite this, the open and evolving nature of VANETs introduces substantial security challenges, including exposure to malicious attacks like Sybil and collusion attacks. The proposed technique addresses the crucial security vulnerabilities in VANETs by developing a robust and efficient fog computing-based mechanism for detecting and mitigating Sybil and collusion attacks. The proposed approach emphasizes minimizing computational and communication overheads while ensuring timely and accurate detection and response to malicious activities. The results show that the proposed technique provides less communication and computational overheads in sparse and dense scenarios with enhanced security.

Keywords: VANETs, Fog Computing, Incident Response, Sybil Attack, Collusion Attack.

Introduction:

Vehicular Ad hoc Networks (VANETs) are disseminated networks where devices such as Road Side Units (RSUs) the Central Management System (CMS) and users/vehicles connect through wireless medium. The technology known as Dedicated Short-Range Communication (DSRC) Wireless Access in Vehicular Environment (WAVE) or IEEE 802.11P is used for communication in VANETs [1]. VANETs play a vital part in the Intelligent Transport System (ITS), paying to decrease traffic congestion, and accidents, and improving traffic efficiency. Each vehicle is furnished with an onboard unit (OBU) that allows communication between vehicles (V2V) and with infrastructure (V2I), such as RSUs [1][2]. As a complex technology, VANETs require slight delays for distribution, getting, and handling applications [3]. ITS meaningfully donates to a country's economy by decreasing fuel consumption and efficiently managing a person's time [4].

Fog computing, which is a dispersed procedure, covers cloud services to the edge/user layer, donating minor latency and power consumption. Fog computing is near to the edge/user and more secure than the traditional system by managing the data/information of VANET users in a controlled way. The specific advantages, that fog computing offers are proximity to a data source, real-time processing, reduced network congestion, and enhanced quality of service. This makes it mainly effective for applications demanding low latency, location alertness, and movement. Fundamentally, fog computing is similar to traditional systems but operates closer to the edge/operator layer. Fog computing provides security and privacy to data over other systems as all data processing is done near the edge layer [5]. Fog computing in VANETs can achieve the speedily increasing number of smart and Internet of Things (IoT) devices, which generate large dimensions of data making it suitable for the accommodation of large numbers of users overwhelming the restrictions of other systems, such as continuous services and position alertness [6].

In [3] the researchers inspected event response using the 4G/5G/6G cellular network to improve latency and interval performance in fog computing for smart city accident avoidance. However, this mechanism required encryption approaches between VANET and fog servers. In [7] Lourenço et al. planned a traffic management approach built on V2I communication, where RSUs gather vehicle data and provide substitute ways throughout traffic jams or accidents. Despite decreasing travel time, the scheme is vulnerable to sole points of failure at the RSU. In [8] Li et al. presented an instinctive incident detection system called WARDEN by the Microsoft Azure-based Incident Management (IcM) platform. However, handling incident alerts by many on-call engineers augmented the risk of unauthorized access. In [9] Almaiah et al. argued a risk intelligence method to protect fog computing edge devices from security attacks, exploiting the Travelling Salesman approach (TSP) to identify the shortest route for the first confronted node response. However, attackers could gain access through dropper-attached worms before the TSP analysis.

In [10] the authors examined early incident response in Traffic Monitoring Centers (TMCs) but couldn’t report the related limitations. In [11] Olugbade et al. discovered artificial intelligence and machine learning applications in road transport incident detection, however, their use of open-area cameras with tracking algorithms made them vulnerable to invaders. In [12] the authors suggested a fog-based incident managing scheme called Emergency that minimized response and rescue times through a mobile application using sensors and GPS for location. However, GPS faced issues with signal interference and inadequate reflectiveness, particularly in unclear circumstances. In [13] Chavhan et al. introduced a context-aware vehicle incident route provision for ITS, but their model dependence on accurate data collection led to possible failures if there were interruptions. Moreover, data switched among vehicles and RSUs required security, and their cloud-built incident response faced possible inaccessibility.

In [14] Hsiung et al. planned a fog computing technique using the Anubis algorithm to avoid security threats but at a high computational cost. In [15] Zhang et al. presented a certificate-less aggregate sign-crypto scheme to defend fog computing and VANETs from collusion attacks, but this approach has high communication overheads. In [16] Borah et al. developed a fog computing-based technique, FSDV-H, to detect Sybil attacks in VANETs by Beam forming for highway scenarios, though it had a single point of failure and was vulnerable to colluding Sybil attacks. In [17] Chen et al. used multi-source data fusion detection for Sybil attacks with machine learning arrangement, but the technique practiced high delays and overhead in tightly occupied areas.

Most of the above-mentioned systems trust malicious activity detection mechanisms but scrap with security and privacy encounters. Meanwhile, fog computing security and privacy are serious research zones, precise and timely detection of hateful activity, as well as suitable replies, are essential. Therefore, a necessity occurs for a detection mechanism that remarkably safeguards VANET nodes and provides effective responses to malicious activities. This study suggests a VANET detection mechanism using fog computing for collusion and Sybil attacks, intended by resourcefully addressing detection and response.

The detached of this paper is to develop a VANET detection mechanism using fog computing for collusion and Sybil attacks, with the following key objectives:

- To detect and respond to malicious events quickly while reducing computational and communication costs.
- To deliver effective defense alongside collusion and Sybil attacks.
- To compare the designed technique with current state-of-the-art mechanisms.

The rest of the paper is organized as; Section 2 consists of the literature review, Section 3 presents the network model, Section 4 presents results and discussion, and Section 5 shows the conclusion and future work.

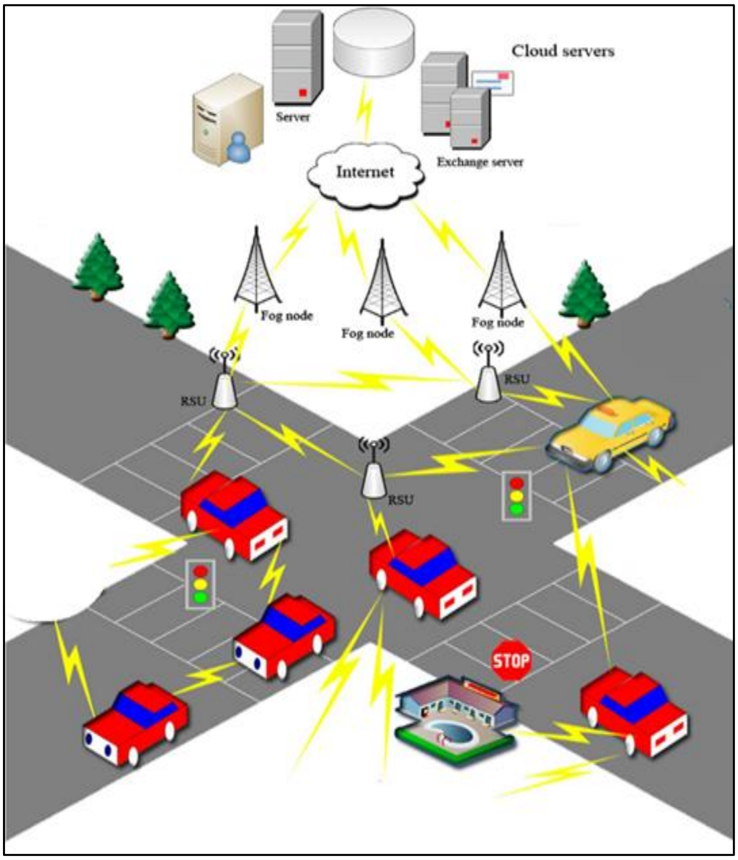

Figure 1. System Model

Literature Review:

This section covers the literature review and the purpose of the proposed technique. VANETs are a promptly growing research area. For all their benefits, VANETs face security attacks that make them vulnerable. Vehicles in ad hoc networks are easy targets for attackers because of their decentralized nature. Additionally, they are not suitable for scenarios involving multiple vehicles and large amounts of data, primarily important interruption or disruption. To address these issues, various studies have focused on research. Using hash and signature technology, verification and authentication in VANETs can be achieved by generating keys and hash methods. The hash and signature method file can be created and secured using strong encryption, intelligent protocols, and other advanced technologies.

Fog Based Techniques:

In [3] Farooqi et al. the researchers inspected event response using the 5G cellular network to improve latency and interval performance in fog computing for smart city accident avoidance. However, this mechanism required encryption approaches between VANET and fog servers. In [7] Lourenço et al. planned a traffic management approach built on V2I communication, where RSUs gather vehicle data and provide substitute ways throughout traffic jams or accidents. Despite decreasing travel time, the scheme is vulnerable to sole points of failure at the RSU.

In [12] Dar et al. the authors suggested a fog-based incident managing scheme that minimized response and rescue times through a mobile application using sensors and GPS for location. However, GPS faced issues with signal interference and inadequate reflectiveness, particularly in unclear circumstances. In [13] Chavhan et al. introduced a context-aware vehicle incident route provision for ITS, but their model dependence on accurate data collection led to possible failures if there were interruptions. Moreover, data switched among vehicles and RSUs required security, and their cloud-built incident response faced possible inaccessibility. In [18] Firdhous et al. discussed that fog computing is a distributed platform that can be extended to the edge layer due to less delay as compared with the cloud. Therefore, researchers tried their best to use fog computing instead of the cloud directly.

Darabkh et al. [19] introduced the Innovative Cluster-Based Dual-Phase Routing Protocol (ICDRP-F-SDVN), which utilizes fog computing and software-defined networks (SDN) to enhance network performance, scalability, and flexibility. By implementing clustering techniques and efficient control overhead reduction mechanisms, the protocol minimizes communication overhead and improves routing efficiency. However, the scheme has security and privacy issues.

In [20] Dong et al. presented a scheme, in which they combine vehicular fog computing and vehicle-to-vehicle communication to improve ITS functionality, additionally, they proposed a new energy-efficient pre-emptive imitation mechanism to ensure the system remains reliable. However direct communication of vehicles can cause security and privacy issues. Real-time synchronization can cause latency problems.

Security Based Techniques:

Ullah et al. [21] proposed an emergency message dissemination scheme which is designed for congestion avoidance in VANETs using fog computing. However, the research focused mainly on congestion avoidance and message dissemination while highly addressing other particular factors such as security, privacy, and long-term scalability. Ogundoyin et al. [22] proposed an efficient privacy-preserving certificate-less authentication approach in fog-assisted VANET using blockchain technology and neuro-fuzzy machine learning techniques. However, their analysis of security threats was limited, specifically, VANETs are considered real-time scenarios.

Paranjothi et al. [23] introduced a new approach known as fog-based rogue nodes detection (F-Round) to improve the detection of rogue nodes in VANETs by utilizing OBU using fog computing. However, their model has scalability and security issues. Al-Otaibi et al. [24] proposed a privacy-preserving scheme for identifying rogue vehicles using fog computing, their approach improves vehicle privacy and communication by restricting communication to roadside units (RSUs). However, they did not fully explore the security of RSUs and did not address possible security threats.

Zhang et al. [25] proposed a traffic route management scheme for fog-based vehicular ad hoc networks that gives priority to security and privacy. The scheme utilizes homomorphic encryption to protect the confidentiality of individual vehicle routes while exploiting blockchain for secure public key management. However, the models depend on a centralized Traffic Management Center (TMC) could probably point to a single point of failure. In [14] Hsiung et al. the authors suggested a fog-based computing technique and Anubis algorithm to prevent security threats but have high computational costs. Wang et al. [26] proposed a privacy-preserving framework for Collaborative Intrusion Detection Networks (CIDNs) using fog computing. The Rabin fingerprint algorithm has been used in the model to detect Intrusions. However, the model has not discussed any specific mechanism so that the data remains secure during the transmission and processing of fog devices.

Sybil Attack Detection Techniques:

In [17] Chen et al. used multi-source data fusion detection for Sybil attacks with machine learning arrangement, but the technique practiced high delays and overhead in tightly occupied areas. In [27] Eddine et al. proposed an efficient authentication scheme over blockchain (EASBF) for the Internet of vehicles using fog computing and blockchain technology. The scheme is designed to protect IoV systems from different cyber-attacks by utilizing elliptic curves and one-way hash functions, while also ensuring confidentiality, integrity, and privacy. However, their scheme may face scalability challenges under high traffic conditions, and it may be vulnerable to insider attacks.

In [16] Borah et al. developed a fog computing-based technique, FSDV-H, to detect Sybil attacks in VANETs by Beam forming for highway scenarios, though it had a single point of failure and was vulnerable to colluding Sybil attacks. Paranjothi et al. [28] proposed fog computing-based Sybil attack detection for VANETs (FSDV), which utilizes the capability of onboard units (OBU) in vehicles to dynamically form a fog network. This fog network is utilized to effectively identify rogue nodes responsible for Sybil attacks within the vehicular network. However, the model presents security and privacy issues, and the system lacks scalability.

Almazroi et al. [29] proposed a novel fog computing-based lightweight Sybil-resistant attack (FC-LSR) model for 5G-enabled vehicular networks. The FC-LSR scheme uses Modified Merkle Patricia Trie (MMPT) and Merkle Hash Tree (MHT) techniques to improve security and privacy. However, the model is vulnerable to Denial-of-Service Attacks (DOS) and may face scalability issues in more complex or large-scale environments. Benadla et al. [30] proposed a blockchain-based mechanism to detect Sybil attacks in vehicular fog networks using the Trajectory Comparison (TC) and the Received Signal Strength Indicator (RSSI) technique. However, the system has scalability issues and remains vulnerable to collusion and Denial of Service attacks.

Grover et al. [31] proposed a distributed security scheme to detect Sybil attacks in vehicular ad hoc networks (VANETs). The method utilized the differences in movement patterns between legitimate and Sybil nodes, in this model the RSUs are responsible for detection in the model. However, the approach has communication and computation overhead. Khalil et al. [32] proposed a lightweight protocol to prevent a model from Sybil attack in VANETs, the approach used symmetric key encryption and authentication methods to prove the unique identity of a vehicle in a network. These two methods are used in between the vehicles and Road Side Units (RSUs). However, collusion and Denial of Service (DOS) attacks are possible in the model. Hao et al. [33] proposed a protocol where the vehicles use Global

Positioning System (GPS) positions periodically broadcasted within the network to detect a Sybil attack. However, GPS spoofing may suffer from this technique.

Collusion Attack Detection Techniques:

In [15] the authors proposed a certificate-less scheme to protect fog computing and VANETs from collusion attacks. However, their model lacks due to high communication costs. Yaseen et al. [34] developed a model that utilizes Fog Computing infrastructure to adequately monitor IoT devices and detect collusion attacks. The model implements the fog computing layer to enable real-time monitoring and detection of collusion attacks within IoT domains. The authors also pointed out the potential for future work to improve the model by incorporating secure authentication systems, which would further reduce the risk of collusion by unauthorized users.

Cui et al. [35] introduced an efficient and secure road condition monitoring scheme known as the Certificateless Aggregate Signcryption Scheme (CLASC), integrated with a fog computing framework, making it highly suitable for the Internet of Vehicles. However, the scheme is vulnerable to collusion attacks. To remove the above shortcomings, there is a need to design an efficient secure technique.

Network Model:

This section includes the System model, Design Goals, and Methodology of the proposed research work.

System Model:

There are four main entities in the proposed technique, which are Fog Server (FS), Cloud Server (CS), Road Side Unit (RSU), and Vehicles (Vs). The FS, CS, and RSU are assumed to be entirely reliable, while among the vehicles some vehicles may be malicious. Each vehicle contains an onboard unit (OBU) with storage and processing capabilities that communicate with the Vs, RSUs, and FS. Furthermore, in VANETs, due to the wireless and ad hoc nature of VANETs, the attackers can access private data such as locations.

To prevent attacks and improve the trustworthiness of VANETs, the proposed system model, which is shown in Figure 1 includes FS, RSUs, and Vs. Each vehicle communicates with other Vs, RSUs, and FS via DSRC. RSUs generate a hash from vehicle data and send it to Fog servers. Fog servers are responsible for overall secure communication.

Design Goals:

The following are the design goals of the proposed technique:

Improve Security:

The main goal of the paper is to enhance the security of VANETs to protect the system from various attackers, malicious users, and unauthorized access.

Send Incident Response:

One of the main goals of the research is to create an incident response mechanism that detects and mitigates malicious activities in VANETs. When unsure behavior, like Sybil or collusion attacks is detected, the system will automatically take predefined security actions such as Fog servers sending incident reports to all vehicles and RSUs.

Enhancing Communication and Computational Efficiency:

The primary goal of this research is to efficiently reduce communication and computational costs in VANETs.

Data Integrity:

The system guarantees the authenticity and integrity of vehicle data, protecting it from modifying, and unauthorized changes. By implementing robust and cryptographic techniques, the system ensures that the data remains correct, secure, and reliable all over the communications.

Methodology:

The proposed VDMF technique, which is illustrated in Figure 2, is implemented using MATLAB [36]. The implementation is carried out on a system equipped with a Core i5 processor and 8GB RAM. The VDMF technique involves the following steps:

- **Step 1:** VANET nodes that are vehicles and RSUs gather and transmit data such as ID, payload e speed, location, sensor readings, and a timestamp to fog servers.
- **Step 2:** Before communicating data, each VANET node computes a hash value over the payload using SHA-256 and produces a digital signature using its private key.
- **Step 3:** Fog Server 1 gets data from the VANET nodes and validates the digital signature by the resultant public key of each VANET node. Once certified, Server 1 stores the data in a hash table, including the ID, payload, and timestamp. Fog Server 1 then computes a hash using the ID, payload, and timestamp via SHA-256 to safeguard its counterparts from the established hash.

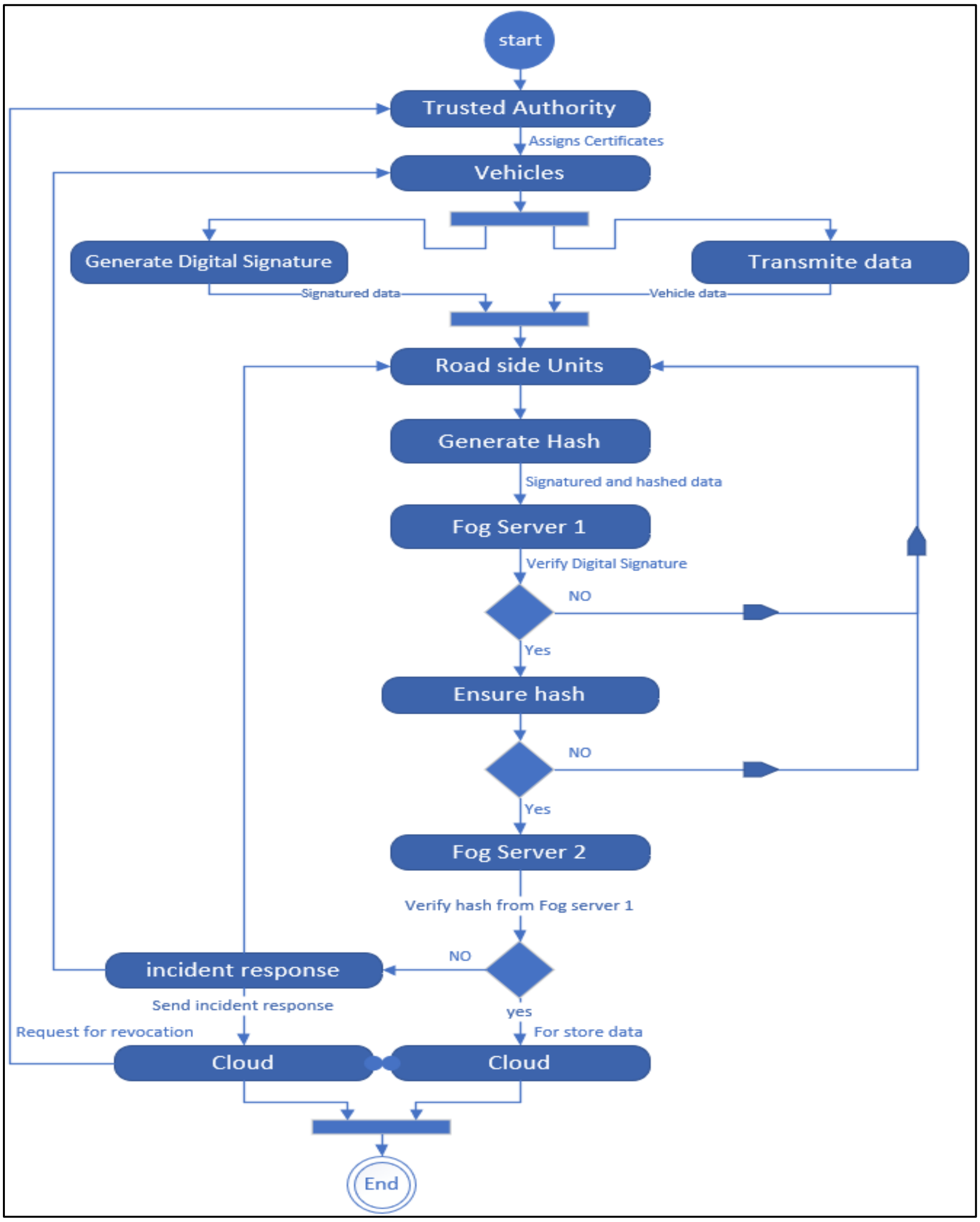

Figure 2. Proposed Methodology

- **Step 4:** Fog Server 2 acts as a secondary verifier and incident responder. It cross-checks the hash established from Fog Server 1 with the intended hash. If there is a divergence or any variances are noticed, an incident response is prompted to the VANET nodes and the cloud. Fog Server 2 employs a collaborative incident response method to efficiently send precise responses to the VANET nodes and the cloud.

- **Step 5:** Finally, Fog Server 2 communicates the data to the cloud server for backup. The main advantage of 2 servers is to avoid a single point of failure, improve scalability, and load balancing, increase reliability, and improve security and privacy.

In the event of malicious activity occurrence, fog server 2 will send an incident response to vehicles and RSUs. The RSUs will revoke the malicious vehicle from the VANETs. The proposed Hybrid scheme that uses signature and hash protocol as shown in Algorithm 1 is implemented in the VDMF technique. The notations of the suggested technique are given in Table 1.

Algorithm 1

```
Sig [V] ← Sig ($K_{private}$)
V→ RSU: [(Vid | | Vp | | LT1) | | Sig (V_D)]
RSU→ FogServer1: K [H (Vid, Vp, LT1) | | Sig (V_D)]
FogServer1→ FogServer2: K [H (Vid | | Vp | | LT1) | | H_C]
IF (MaliciousActivityDetected) {
    FogServer2→ Cloud: [I_R]
    FogServer2→ V: [I_R]
End IF
FogServer2→ Cloud: K [H (V_D)]
```

Table 1. Notations

<table>
<tr><th>Notation</th><th>Description</th></tr>
<tr><td>V</td><td>Vehicle</td></tr>
<tr><td>P_{rivate}</td><td>Vehicle Private Key</td></tr>
<tr><td>RSU</td><td>Road Side Unit</td></tr>
<tr><td>Vid</td><td>Vehicle Id</td></tr>
<tr><td>Vp</td><td>Vehicle Payload</td></tr>
<tr><td>LT1</td><td>Timestamp</td></tr>
<tr><td>Sig</td><td>Signature</td></tr>
<tr><td>V_D</td><td>Vehicle Data</td></tr>
<tr><td>K</td><td>Encryption</td></tr>
<tr><td>H</td><td>Hashed</td></tr>
<tr><td>H_C</td><td>Hash Calculated</td></tr>
<tr><td>I_R</td><td>Incident Response</td></tr>
<tr><td>| |</td><td>Concatenation</td></tr>
</table>

Results and Discussion:

In this section, the proposed technique is analyzed through overhead ratio, computational cost, and Attack model. The simulation parameters are given in Table 2.

Table 2. Simulation Parameters

Parameters	Description
No of Vehicles	10-100
No of RSUs	2
Simulator	MATLAB
No of Lanes	2
Road Length	1 Mile
Communication Protocol	DSRC
Technique Used	Fog Computing
Encryption Protocol	Digital Signature + Hash

Vehicle Speed	25-40 miles/ hr

Overhead Ratio:

The overhead ratio of the proposed technique and without security parameters is shown in Table 3. The results show no significant differences among the overhead ratio in sparse and dense scenarios, which indicates that the proposed technique works efficiently in all the scenarios.

Table 3. Overhead ratio with proposed security parameters and without security parameters

Number of Vehicles	With Signature + Hashed	Without Signature + Hashed
2	3.210ms	0.405ms
3	0.085ms	0.010ms
4	1.667ms	0.072ms
5	0.862ms	0.056ms
6	0.541ms	0.236ms
7	0.024ms	0.026ms
8	0.032ms	0.017ms
9	0.032ms	0.006ms
10	0.372ms	0.214ms
11	0.312ms	0.010ms
12	0.031ms	0.009ms
13	0.204ms	0.003ms
14	0.266ms	0.004ms
15	0.983ms	0.384ms
16	0.178ms	0.003ms
20	0.042ms	0.008ms
30	0.322ms	0.145ms
43	1.561ms	1.173ms

Computational Cost Analysis:

The computational cost is evaluated and specified in Figures 3, and 4 respectively, the message generation and verification time are low and there are no significant differences between the security parameters proposed and without security parameters. Therefore, the results make the proposed technique suitable for VANETs.

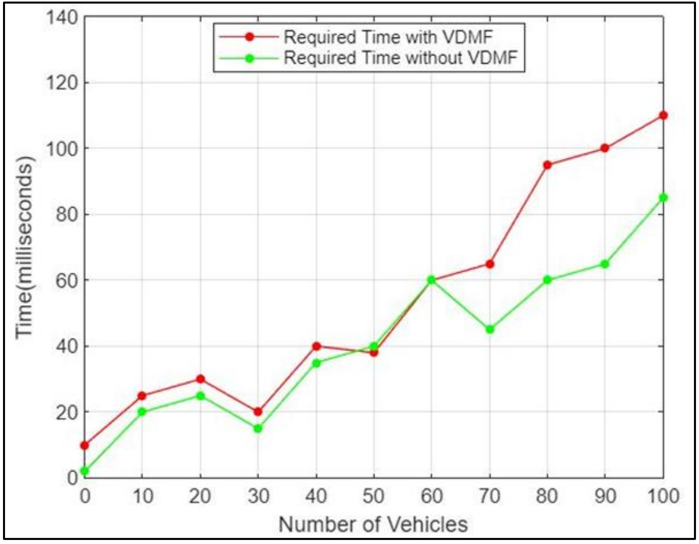

Figure 3. Time for V2V Communication

In Figure 5, the number of vehicles is shown on the X-axis, while the operational cost is shown on the Y-axis. In the sparse scenario, the operational cost is a little bit high, but in the dense scenario, it is low. However, there is no significant effect with and without the proposed technique.

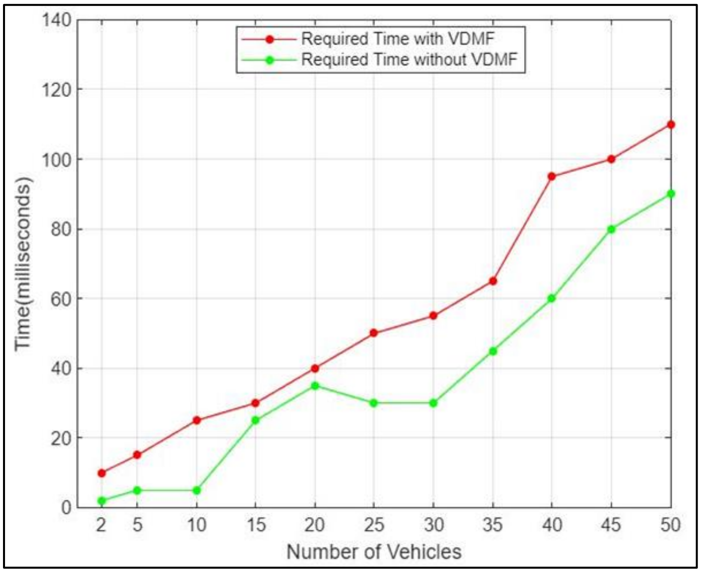

Figure 4. Time for Vehicle and RSU Communication

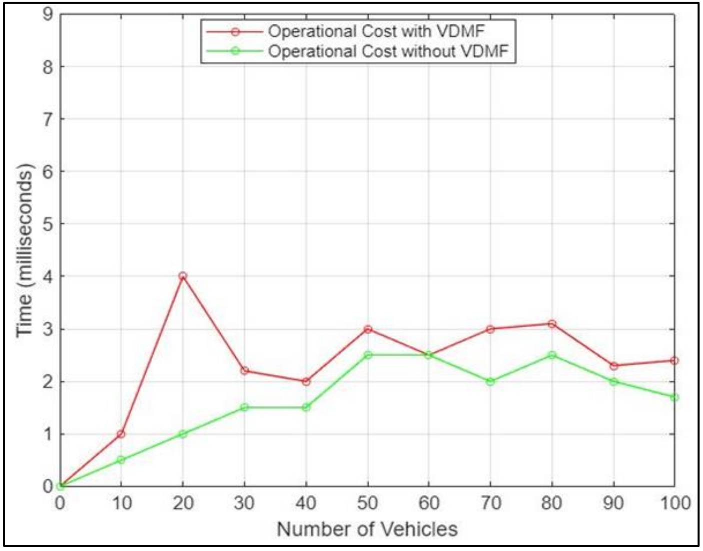

Figure 5. Operational Cost

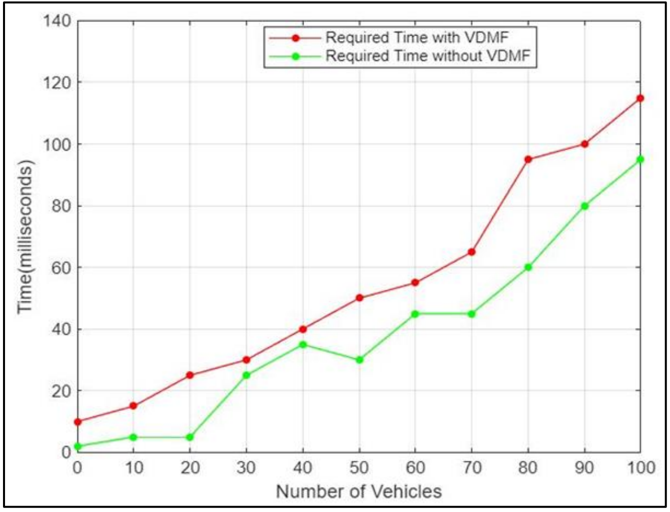

Figure 6. Communication cost comparison

The communication cost of the proposed scheme is a little bit higher than without security implementation as depicted in Figure 6, which is a tradeoff between security and without security considerations.

Attack Model:

To achieve controlled privacy and concealment, various risk scenarios are considered in the proposed model.

- Communication between V2V and V2I is Signature and Hashed protected. Therefore, it is difficult to modify the communication, which guarantees communication integrity.
- An attacker or malicious user cannot get the real identity of the vehicle during communication, as it is protected through pseudonyms.
- If any RSU is attacked, the attacker cannot get the actual information of the vehicle.
- The database of the Fog servers and Cloud server hold the encrypted materials therefore attacks on both these servers' databases reveal no beneficial evidence to any attacker.

When Sybil and collusion attacks are prevented, the Denial-of-Service attack is also prevented, because the fundamental security features that are confidentiality, integrity, and availability (CIA) are addressed. The comparison of the proposed scheme VDMF and existing literature is shown in Table 4.

Table 4. VDMF Comparison with other related literature

Research Paper	Sybil Attack	Collusion Attack	Dos Attack
[3]	Yes	Yes	Yes
[7]	Yes	No	Yes
[8]	No	Yes	Yes
[9]	Yes	No	Yes
[12]	No	Yes	No
[13]	No	Yes	No
[14]	Yes	No	No
[15]	Yes	No	Yes
[16]	No	Yes	Yes
VDMF	No	No	No

Conclusion and Future Work:

In VANETs, the experiments of infrequent connectivity and dynamic topology increase critical warnings about security and privacy. The proposed scheme efficiently detects and reduces malicious activities such as Sybil and collusion attacks, which ensures the integrity and authenticity of data exchanged between vehicles and Road Side Units. This paper integrated the Secure Hash Algorithm which is SHA-256 and Digital Signature Algorithm, which provides a strong cryptographic framework, protecting sensitive information from unauthorized access and tampering. The two fog server layouts enhanced security and reliability issues by introducing a secondary verification layer and facilitating timely incident response. The proposed scheme indicates its capability to minimize computational and communication overheads and provide a robust defense against attacks. The proposed solution addresses the unique security and privacy requirements of VANETs in the fog computing environment. In the future, the proposed scheme will be extended to the Internet of Vehicles environment by integrating into the cloud using a greater number of vehicles that will focus on the big data and further investigate more attacks.

References:

[1] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din, and G. Ali, "ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System," PLoS One, vol. 14, no. 8, p. e0221213, Aug. 2019, doi: 10.1371/JOURNAL.PONE.0221213.

[2] Deeksha, A. Kumar, and M. Bansal, “A review on VANET security attacks and their countermeasure,” 4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017, vol. 2017-January, pp. 580–585, Sep. 2017, doi: 10.1109/ISPCC.2017.8269745.

[3] J. Wu et al., “A Fog Computing Model for VANET to Reduce Latency and Delay Using 5G Network in Smart City Transportation,” Appl. Sci. 2022, Vol. 12, Page 2083, vol. 12, no. 4, p. 2083, Feb. 2022, doi: 10.3390/APP12042083.

[4] Q. E. Ali, N. Ahmad, A. H. Malik, G. Ali, and W. ur Rehman, “Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy,” Appl. Sci. 2018, Vol. 8, Page 1964, vol. 8, no. 10, p. 1964, Oct. 2018, doi: 10.3390/APP8101964.

[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” J. Netw. Comput. Appl., pp. 1–13, 2013, doi: 10.1016/j.jnca.2013.02.036.

[6] S.-U. Rehman, M. Khan, T. Zia, and L. Zheng, “Vehicular Ad-Hoc Networks (VANETs): An Overview and Challenges,” J. Wirel. Netw. Commun., vol. 3, no. 3, pp. 29–38, 2013, doi: 10.5923/j.jwnc.20130303.02.

[7] M. Lourenço, T. S. Gomides, F. S. H. De Souza, R. I. Meneguette, and D. L. Guidoni, “A traffic management service based on V2I communication for vehicular Ad-hoc networks,” LANC 2018 - Proc. 10th Lat. Am. Netw. Conf., pp. 25–31, Oct. 2018, doi: 10.1145/3277103.3277132.

[8] L. Li et al., Fighting the Fog of War: Automated Incident Detection for Cloud Systems. 2021. Accessed: Oct. 07, 2024. [Online]. Available: https://www.usenix.org/conference/atc21/presentation/li-liqun

[9] A. K. Al Hwaitat, S. Manaseer, R. M. H. Al-Sayyed, M. A. Almaiah, and O. Almomani, “AN INVESTIGATION OF DIGITAL FORENSICS FOR SHAMOON ATTACK BEHAVIOUR IN FOG COMPUTING AND THREAT INTELLIGENCE FOR INCIDENT RESPONSE,” J. Theor. Appl. Inf. Technol., vol. 15, p. 7, 2020, Accessed: Oct. 07, 2024. [Online]. Available: www.jatit.org

[10] M. M. Hamdi, L. Audah, S. A. Rashid, and M. A. Al-Shareeda, “Techniques of early incident detection and traffic monitoring center in VANETs: A review,” J. Commun., vol. 15, no. 12, pp. 896–904, Dec. 2020, doi: 10.12720/JCM.15.12.896-904.

[11] A. Editors et al., “A Review of Artificial Intelligence and Machine Learning for Incident Detectors in Road Transport Systems,” Math. Comput. Appl. 2022, Vol. 27, Page 77, vol. 27, no. 5, p. 77, Sep. 2022, doi: 10.3390/MCA27050077.

[12] B. K. Dar, M. A. Shah, S. U. Islam, C. Maple, S. Mussadiq, and S. Khan, “Delay-Aware Accident Detection and Response System Using Fog Computing,” IEEE Access, vol. 7, pp. 70975–70985, 2019, doi: 10.1109/ACCESS.2019.2910862.

[13] S. Chavhan, D. Gupta, C. Nagaraju, A. Rammohan, A. Khanna, and J. J. P. C. Rodrigues, “An Efficient Context-Aware Vehicle Incidents Route Service Management for Intelligent Transport System,” IEEE Syst. J., vol. 16, no. 1, pp. 487–498, Mar. 2022, doi: 10.1109/JSYST.2021.3066776.

[14] P. Y. Hsiung, C. H. Li, S. H. Chang, and B. C. Cheng, “A Fog-Based Collusion Detection System,” Adv. Intell. Syst. Comput., vol. 895, pp. 514–525, 2020, doi: 10.1007/978-3-030-16946-6_41.

[15] W. Zhang, S. Liu, Y. Liu, J. Cao, B. Fu, and Y. Du, “A Certificateless Online/Offline Aggregate Signcryption Scheme against Collusion Attacks Based on Fog Computing,” Electron. 2023, Vol. 12, Page 4747, vol. 12, no. 23, p. 4747, Nov. 2023, doi: 10.3390/ELECTRONICS12234747.

[16] A. Borah and A. Paranjothi, “Sybil Attack Detection in VANETs using Fog Computing and Beamforming,” 2023 IEEE 14th Annu. Ubiquitous Comput. Electron. Mob.

Commun. Conf. UEMCON 2023, pp. 626–631, 2023, doi: 10.1109/UEMCON59035.2023.10316102.

[17] Y. Chen, Y. Lai, Z. Zhang, H. Li, and Y. Wang, "MDFD: A multi-source data fusion detection framework for Sybil attack detection in VANETs," Comput. Networks, vol. 224, p. 109608, Apr. 2023, doi: 10.1016/J.COMNET.2023.109608.

[18] "Fog Computing: Will it be the Future of Cloud Computing?" Accessed: Oct. 07, 2024. [Online]. Available: https://www.researchgate.net/publication/266477246_Fog_Computing_Will_it_be_the_Future_of_Cloud_Computing

[19] K. A. Darabkh and B. Z. Alkhader, "Fog Computing-and Software Defined Network-Based Routing Protocol for Vehicular Ad-hoc Network," Int. Conf. Inf. Netw., vol. 2022-January, pp. 502–506, 2022, doi: 10.1109/ICOIN53446.2022.9687147.

[20] L. Dong, Q. Ni, W. Wu, C. Huang, T. Znati, and D. Z. Du, "A Proactive Reliable Mechanism-Based Vehicular Fog Computing Network," IEEE Internet Things J., vol. 7, no. 12, pp. 11895–11907, Dec. 2020, doi: 10.1109/JIOT.2020.3007608.

[21] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency Message Dissemination Schemes Based on Congestion Avoidance in VANET and Vehicular FoG Computing," IEEE Access, vol. 7, pp. 1570–1585, 2019, doi: 10.1109/ACCESS.2018.2887075.

[22] S. O. Ogundoyin and I. A. Kamil, "An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy," Veh. Commun., vol. 31, p. 100384, Oct. 2021, doi: 10.1016/J.VEHCOM.2021.100384.

[23] A. Paranjothi, M. Atiquzzaman, and M. S. Khan, "F-RouND: Fog-based Rogue Nodes Detection in Vehicular Ad hoc Networks," Proc. - IEEE Glob. Commun. Conf. GLOBECOM, 2020, doi 10.1109/GLOBECOM42002.2020.9322131.

[24] B. Al-Otaibi, N. Al-Nabhan, and Y. Tian, "Privacy-Preserving Vehicular Rogue Node Detection Scheme for Fog Computing," Sensors 2019, Vol. 19, Page 965, vol. 19, no. 4, p. 965, Feb. 2019, doi: 10.3390/S19040965.

[25] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-Assisted Privacy-Preserving Traffic Route Management Scheme for Fog-Based Vehicular Ad-Hoc Networks," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 3, pp. 2854–2868, Sep. 2023, doi: 10.1109/TNSM.2023.3238307.

[26] Y. Wang, L. Xie, W. Li, W. Meng, and J. Li, "A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10581 LNCS, pp. 267–279, 2017, doi: 10.1007/978-3-319-69471-9_20.

[27] M. S. Eddine, M. A. Ferrag, O. Friha, and L. Maglaras, "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles," J. Inf. Secure. Appl., vol. 59, p. 102802, Jun. 2021, doi: 10.1016/J.JISA.2021.102802.

[28] A. Paranjothi and M. S. Khan, "Enhancing Security in VANETs with Sybil Attack Detection using Fog Computing," IEEE Veh. Technol. Conf., 2023, doi: 10.1109/VTC2023-FALL60731.2023.10333491.

[29] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, M. A. Alqarni, A. A. Almazroey, and T. Gaber, "FC-LSR: Fog Computing-Based Lightweight Sybil Resistant Scheme in 5G-Enabled Vehicular Networks," IEEE Access, vol. 12, pp. 30101–30112, 2024, doi: 10.1109/ACCESS.2024.3368393.

[30] S. Benadla, O. R. Merad-Boudia, S. M. Senouci, and M. Lehsaini, "Detecting Sybil Attacks in Vehicular Fog Networks Using RSSI and Blockchain," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 4, pp. 3919–3935, Dec. 2022, doi: 10.1109/TNSM.2022.3216073.

[31] J. Grover, M. S. Gaur, and V. Laxmi, “A novel defense mechanism against Sybil attacks in VANET,” SIN’10 - Proc. 3rd Int. Conf. Secure. Inf. Networks, pp. 249–255, 2010, doi: 10.1145/1854099.1854150.

[32] M. Khalil and M. A. Azer, “Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks,” IFIP Wirel. Days, vol. 2018-April, pp. 184–186, May 2018, doi: 10.1109/WD.2018.8361717.

[33] Y. Hao, J. Tang, and Y. Cheng, “Cooperative sybil attack detection for position based applications in privacy preserved VANETs,” GLOBECOM - IEEE Glob. Telecommun. Conf., 2011, doi 10.1109/GLOCOM.2011.6134242.

[34] Q. Yaseen, M. Aldwairi, Y. Jararweh, M. Al-Ayyoub, and B. Gupta, “Collusion attacks mitigation in the internet of things: a fog based model,” Multimed. Tools Appl., vol. 77, no. 14, pp. 18249–18268, Jul. 2018, doi: 10.1007/S11042-017-5288-3/METRICS.

[35] M. Cui, D. Han, and J. Wang, “An Efficient and Safe Road Condition Monitoring Authentication Scheme Based on Fog Computing,” IEEE Internet Things J., vol. 6, no. 5, pp. 9076–9084, Oct. 2019, doi: 10.1109/JIOT.2019.2927497.

[36] O. Akbarzadeh, M. R. Khosravi, and L. T. Alex, “Design and Matlab Simulation of Persian License Plate Recognition Using Neural Network and Image Filtering for Intelligent Transportation Systems,” ASP Trans. Pattern Recognit. Intell. Syst., vol. 2, no. 1, pp. 1–14, Feb. 2022, doi: 10.52810/TPRIS.2021.100098.