Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 8, pp. 2447–2460
DOI : 10.47974/JDMSC-2038

Scalable blockchain framework for trust management in the Internet of Vehicles for a secure intelligent transportation system

Nehad Albadri *
Department of Computer Sciences
College of Education for Pure Sciences
University of Thi-Qar
Thi-Qar
Iraq

Stijn Dekeyser †
School of Mathematics, Physics and Computing
University of Southern Queensland
Brisbane
Australia

Abstract

A vehicle connected to the Internet of Vehicles (IoV) communicates wirelessly with other vehicles, pedestrians, roadside units and sensors to improve driving comfort, traffic flow and road safety. The IoV poses significant security and privacy threats, posing a risk to human lives. Trust must be established among these potentially untrustworthy vehicles. In addition to scalability and single points of failure, current mechanisms face concerns such as sparsity, availability, consistency, robustness, privacy and efficiency. It is considered a promising solution to establish trust in IoV, because blockchain technology has already proven its success with cryptocurrencies and smart contracts. Decentralized trust management for vehicular networks is proposed in this paper using blockchains. We evaluate its efficiency against malicious vehicles and compare its performance with three hybrid trust models through extensive simulations. Our model achieves over 97% trust level, surpassing existing models that fall below 90% in networks with 25% malicious vehicles.

Subject Classification: *Primary 90B06, Secondary 91G20.*

Keywords: *Internet of Things, Internet of Vehicles, Security, Blockchain.*

* *E-mail:* **nihadghasab.comp@utq.edu.iq (Corresponding Author)**
† *E-mail:* **dekeyser@usq.edu.au**

1. Introduction

Blockchain originally emerged as the distributed ledger underpinning Bitcoin [1, 2, 3], designed to solve the double-spending issue in cryptocurrency transactions. Its pivotal feature lies in the immutability of this ledger, enabling parties to establish trust in a decentralized manner among initially untrusted entities. The widespread adoption of Bitcoin propelled blockchain into the spotlight, captivating the research community as a transformative technology. While initially serving as Bitcoin's foundation, blockchain has evolved into a decentralized system architecture that challenges traditional centralized paradigms. Implemented across numerous distributed nodes, each hosting a replica of cryptographically-linked transaction records (blocks), blockchain operates through consensus protocols. This setup ensures the ledger's immutability: once recorded, transactions cannot be altered without detection, enabling anyone to verify the entire transaction history. In essence, blockchain's decentralized and immutable nature enables the establishment of trust between untrusted things in a decentralized method, marking a paradigm shift in system architecture. Recent reports have highlighted instances where cybercriminals have successfully executed remote attacks on key functions of automotive vehicles (as shown in Fig. 1). These attacks, conducted through V2V or V2X communication, have included disabling the engine and brakes. Sensor networks can either be managed by centralized authorities or by distributed networks [4]. Centralized solutions, like the Kerberos authentication system [5, 6], are straightforward to implement but vulnerable to security and reliability issues. In contrast, distributed solutions are more resilient because participants can collaborate autonomously to withstand faults and complicate exploitation [7]. However, they often incur higher overhead due to increased message exchanges needed for nodes to assess each other's trustworthiness. Moreover, distributed solutions introduce unique security challenges not encountered in centralized setups, such as Denial-of-Service (DOS) attacks that flood reputation score requirements aimed at manipulating exchanged reputation scores.

2. Literature Review

The Authors Wasef and Shen in [8] employs bilinear pairing for identity verification and HMAC (Hashed Message Authentication Code) for message integrity. To verify message authenticity, all vehicles must

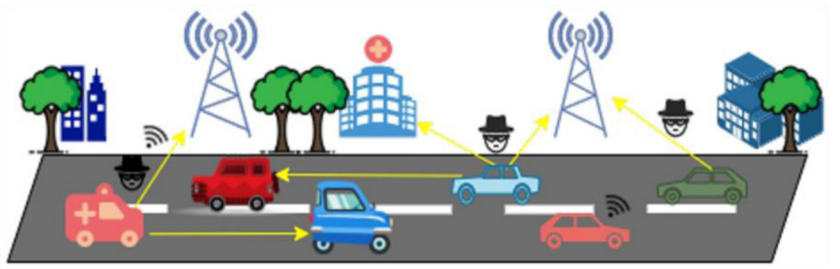

Figure 1

Intelligent transport system

maintain a record of each vehicle's HMAC. Author [9] utilizes a chameleon hashing scheme based on bilinear pairing, comparable to this study's approach. As a result of this study, users with the counterpart's ID are able to establish a shared secret key to communicate privately. Author [10] primarily procedures bilinear pairing for data authentication and supports batch authentication to decrease verification time. RSUs transmit self-authentication messages to IOV, which are then broadcast based on their emergency level or traffic status, constituting real-time data verification [10].

Author [11] proposes a trusted authority for maintaining vehicle privacy and verification. It introduces a dual authentication system allowing vehicles to verify themselves upon entry, employing distinct private keys for each group to safeguard vehicle confidentiality. Author [12] explores vehicles' use of multi-channel IEEE 802.11p MAC in VANETs, demonstrating promising experimental outcomes. In [13], cloud computing are associated with IOV services enhances traffic management while ensuring internet safety. Cloud-based analytics expand the utility of statistical data. In [14], lightweight Certificateless Negotiation for session key reduction focuses on reducing computational overhead and mitigating known malware attacks in web security.

Security stands out as a serious issue in the research focusing on future experiments in the Internet of Vehicles (IoV). The evolving IoV landscape has introduced a range of security concerns [15], making it a foremost challenge. Despite this, current approaches to trust evaluation and management in IoV have shown limited practical effectiveness [16, 17,18, 19].

Various trust assessment approaches have been designed for vehicle communications, predominantly rooted in VANETs/ITS frameworks, with a noticeable scarcity of recent advancements specific to IoV [20, 21,

22]. Recently, there have been preliminary discussions on IoV trust frameworks leveraging blockchain technology [[21, 23]. However, blockchain-based system face technical limitations such as high computational demands, proof of work requirements, scalability issues, and centralization concerns, which pose compatibility challenges for IoV integration. Trust measurement models can be categorized into data-centric, hybrid models, and entity-centric, representing the primary classifications employed in VANETs.

3. Proposed Model

A. *Network Model*

IoV integrates cellular communication technology with vehicles, enhancing user services through collaborative wireless communication among vehicles. It enables continuous monitoring and sharing of traffic as well as roads conditions. Similar to a vehicle cloud, the upper layer consists of a powerful server cluster capable of providing roadside communication services.

A virtual environment is created in the middle layer for trust valuation and lightweight communication with nearby RSUs. Meanwhile, the lower layer focuses on vehicle cooperation, enabling access to local networks and data transmission via multi-hop communication. Vehicles utilize shared resources in the middle layer to enhance resource utilization and service quality.

Currently, IEEE 802.11p is widely employed for vehicle-to-vehicle (V2V) as well as vehicle-to-roadside-unit (V2R) data transmission. Looking ahead, the advent of 5G promises faster data rates, lower latency, and heightened reliability, ushering in a new era of communication capabilities [24].

B. *Trust Model*

Trust in IoV represents a particular probability guiding node cooperation and potential actions against malicious vehicle when essential [25]. Each smart device can assess the trustworthiness of a subset of vehicles, leading to cascading trust relationships across the network. This propagation allows vehicles that have never interacted directly to establish mutual understanding and develop appropriate trust relationships.

Mutual trust evaluations among vehicles enable message filtering in IoV. The Trust Management and Evaluation Center (TMEC) comprise

several modules: (1) Calculating message trust, (2) Estimating global trust, and (3) Identifying malicious attacks. Vehicles aggregate traffic data to compute data trust, evaluating data dependability. Global trust values incorporate direct as well as indirect trust valuations. Subsequently, these calculated trust values update each vehicle's trust list autonomously.

C. *Attacker Model*

Transport entities are extremely vulnerable to a range of attacks, where vehicle and messages can be compromised at any time. Within the wireless communication range of devices, adversaries can eavesdrop, block, fake, modify, or discard information [26, 27]. Their objectives include intercepting normal data transmissions, forging or altering data, and submitting false advice to manipulate benign vehicle. Malicious vehicle disseminates negative remarks about benign nodes to tarnish their repute in the network. When trust and reputation management mechanisms are confused by this collusion, effective network paths can be disrupted. Here, malicious vehicle selectively provides false messages to some nodes while behaving correctly towards others. Such inconsistent behavior patterns create varying levels of trust among nodes, posing challenges for detection by trust management schemes. vehicle alter their behavior over time in this attack type. They may operate normally during certain periods but engage in unfair activities, such as providing biased ratings, at other times. These attacks underscore the need for robust security measures in transportation networks to safeguard against such threats.

D. *Trust Management using Blockchain*

Blockchain management consists of five stages: registration of entities, issuance of digital certificates for identity verification, secure data transfer between entities, computation of trust values based on interactions, and generation of new blocks to record verified transactions and maintain system integrity.

Step 1: Registration: A key, a default trust value (default value), and a default value are all provided by the Network Trust Authority (NTA), and a vehicle identity (V_{ID}, for example, a registration number). These vehicles actively engage in IoV, exchanging messages among themselves. All participating vehicles (V_i) have access to a proposed blockchain where parameters such as vehicle numbers, public key details, counts of

Communication Trust Authority (CTAs), Station Trust Authorities (STAs), and NTAs (N_s) (Network Trust Authorities), as well as the percentage of malicious messages (P_m), are stored. The protocol operates in two main phases: the Registration phase, where vehicles enroll and receive initial credentials, and the Data Transfer phase, where vehicles communicate securely using these credentials.

Step2: Certificate Issuance: As soon as credentials are issued and a certificate is issued, a vehicle is able to communicate with other nodes. Blockchain certificates ensure a vehicle's identity, protect its privacy, and reduce processing time.

After receiving credentials and a certificate, a vehicle can transfer data with other vehicles. Each vehicle's registration validity is confirmed using a blockchain record. When a vehicle registers, a Vehicle Certificate Triplet ($VCT(V_{ID}, Certificate, T_f)$) Noted by blockchain. An authentication code or hash is used to verify and authenticate the integrity of messages:

$$H\ (V_i, : msg; k_i, Z2) \tag{1}$$

A hash is generated, signed with a private key, and transmitted. Upon receiving an encrypted message from *Vi*, the system verifies the hash using *Vi* public key. If valid, *Vithe the* certificate is delivered.

Step 3: Data Transfer Phase: This is a schematic showing how the CTA and blockchain communicate with each other when a car uses it. A vehicle has to register with a valid certificate before it may send information. Using the addresses associated with their blockchain accounts, operations V: reg and V: del register and delete vehicles, respectively. The CL: registration blockchain ledger keeps track of cars that have certificates, and it also stores the full list of registered vehicles. Automobile certification is the purview of STA. Prior to issuing a new authentication certificate, the vehicle's certificate undergoes validation. Only after verification and issuance may a vehicle's certificate be granted. Vehicles that have expired certificates need to be re-registered and issued new ones by going through the setup procedure.

Step 4: Computation Value Trust: *Vi* in IoV calculates *TVj*Trust value by consider a the message of broadcast.

$$T_c = \left(\sum_{i=1}^{m} \delta_j d_j \right) \tag{2}$$

Tc takes into account the message types for transmission; when computing trust values, consider automobiles inside the transmission range. Based on the categorization supplied by the DSRC (the regulatory authority), trust value is calculated for connected vehicles *vj* where $j = 1, 2, .., n$. The sender will share feedback *dj*regarding messages received and based on its practice.

$$T_{V_j} = T_{V_j} + \left\{ {T_c}/{m} \right\} \tag{3}$$

For each data message authentication factor will be stored as a function $Res_{feedback}(V_{ID_i}, V_{ID_j}, \delta, d)$ From a set of m messages broadcast throughout the timeframe, this can help determine how many counterfeit messages were exchanged per answering vehicle Vj, where J=1. In this way, the trust value for each message will be calculated for the responding vehicle V_j, where $j = 1, 2, .., n$ and $j \neq i$ is the number of counterfeit messages exchanged from the set of m broadcasted messages during the time slot $m_{Counterfeit}$. For each vehicle, the blockchain will determine the initial trust.

Step 5: Block Generation: Using this approach, the CTA is responsible for storing and verifying security credentials, as well as sourcing messages. Within the system, all V_j vehicles continually update their nonce to maintain identity and compute trust values. The weight of a message depends on its category. Additionally, the proposed technique incorporates a reward and penalty system by considering the Accuracy of the message. The Evaluation Algorithm includes mechanisms for both rewarding and penalizing behaviors.

E. *Theoretical analysis*

Assume $\{V_1, V_2, \ldots, V_n\}$ represents a set of adjacent vehicles at a particular time interval $[t, t+\in]$. $\{CT\,A_1, CT\,A_2, \ldots, CTA_p\}$, represents the interacting CTAs calculating trust value based on vehicle responses R with response Matrix $R = [r_{ij}]n \times p$. Due to the weighted nature of the proposed trust calculation, we will minimize interactions with malicious vehicle by using the entropy weight method. As m indicates the number of data messages transmission among the vehicle, messages are distributed among them by using the position's distribution technique. Let P_{ij} signifies the probability of r_{ij} to be –1 and $P = [p_{ij}]_{n \times p}$ and deviation response σ as:

$$\sigma j = \frac{1}{n}\left(\left(\sum_{i=1}^{n} P_{ij} \sum_{j=1}^{P} (r_{iij} - \overline{r}_j)^2\right)\right)^{1/2} \tag{4}$$

V_j denotes the vehicle j with the highest response $\overline{r}_j$ d-factor. An objective function can be designed by minimizing the response deviation

$$\text{minimize } (\sigma^2) = \sum_{j=1}^{p}\sum_{i=1}^{n} P_{ij} \sum_{i=1}^{p}\left[\frac{1}{n}(r_{iij} - \overline{r}_j)\right]^2 \tag{5}$$

Since P_{ij} indicate the possibility of the response d-factors, the message entropy of j^{th} vehicle from i^{th} vehicle can be considered as

$$H = -P_{ij}\log(P_{ij}) \tag{6}$$

In this case, the matrix P has total message entropy of

$$H^* = -\sum_{j=1}^{p}\sum_{i=1}^{n}(P_{ij})\log(p_{ij}) \tag{7}$$

A method for optimizing overall message entropy is as follows:

$$\text{Minimize}(-\sigma^2) + \frac{1}{\gamma}\sum_{j=1i=1}^{p}\sum^{n} P_{ij}\log((P_{ij})) \tag{8}$$

$$\text{Subject to } \sum_{j=1}^{p} p_{ij} = 1 \tag{9}$$

Where γ is an symmetry factor based on prior experiences. The Lagrange Multiplier λ method can be used to obtain an optimal solution

$$L(p_{ij}, \lambda, \overline{r}_j) = (-\sigma^2) + \frac{1}{\gamma}\sum_{j=1i=1}^{p}\sum^{n} p_{ij}\log(p_{ij}) + \lambda\left|\sum_{j=1}^{p} p_{ij} - 1\right| \tag{10}$$

By solving this we get the minimum of $L(p_{ij}, \lambda, \overline{r}_j)$ is at

$$p_{ij} = \frac{E(-\gamma\sum_{i=1}^{n}))(r_{iij} - \overline{r}_j)^2}{\sum_{j=1}^{p} E(E(-\gamma\sum_{i=1}^{n}))(r_{iij} - \overline{r}_j)^2)} \tag{11}$$

Subsequently, where E represents the expectation, the analysis indicates that the proposed system's throughput can be maximized by minimizing the probability of interacting with a malicious node.

4. Result Analysis and Discussion

This section presents the performance analysis of the proposed model, where system configuration and algorithm directly influence its effectiveness. The system features an Intel(R) Core (TM) i7-CPU @ 3.20GHz processor, 16 GB of RAM, and a 1TB hard disk, running a 64-bit operating

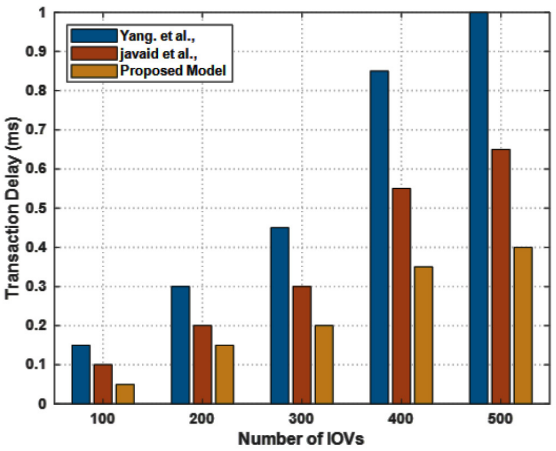

Figure 2

Transaction delay (ms) versus number of IOVs

system with an x64-based processor architecture. Each node is allocated 2GB of hard disk space, with a total of 500 nodes created.

In the Internet of Vehicles scenario, transactions are initiated and added to the blockchain after a specific duration known as transaction delay, which measures the time from initiation to blockchain inclusion. Comparative analysis with two other algorithms is illustrated in Figure 2, focusing on transaction response times. The average transaction delay is calculated relative to the increasing number of vehicles. This outcome underscores the reliance on acknowledgement broadcasts rather than block broadcasts, attributable to the absence of a commit phase in the proposed model. During the transmission phase, consistency checks are conducted across all Internet of Vehicles instances to maintain integrity.

Simulated mining produced blocks of 25 with varying numbers of transactions each. Fig. 3 illustrates the simulation results, where the number of transactions per block is correlated with computation time (measured in milliseconds). As the transaction count per block rises, computational time shows a linear increase. Evaluating the bandwidth and throughput of the proposed architecture involves assessing block size and miner count. Transaction volume is influenced by block size, regulated through the proposed methodology. However, larger blocks experience slower propagation across different zones. Fig.3 demonstrates that increasing block size from 1MB to 5MB escalates bandwidth consumption. Transaction dynamics are influenced by block size, a parameter governed by the proposed method.

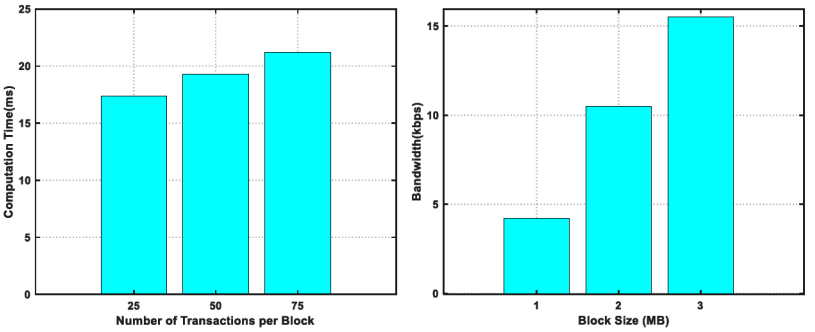

Figure 3

Performance analysis of computation time (ms) and block size (MB)

As depicted in Fig. 4, the throughput of the proposed method rises as block sizes increase from 1 MB to 5 MB, and the number of miners grows from 10 to 100. A greater number of miners accelerates consensus among controllers. Larger block sizes enable processing of more transactions per block, thereby enhancing throughput rates.

Figure 5 demonstrates the influence of the trust threshold on the overall packet detection rate within the network. Our proposed model consistently outperforms existing methods, achieving higher detection rates across different trust thresholds. Notably, as the trust threshold increases, existing methods tend to experience a decline in packet detection rates, whereas our approach maintains superior performance. Notably, while a higher trust threshold typically reduces overall detection rates due to stricter criteria for classifying messages as trustworthy, the proposed

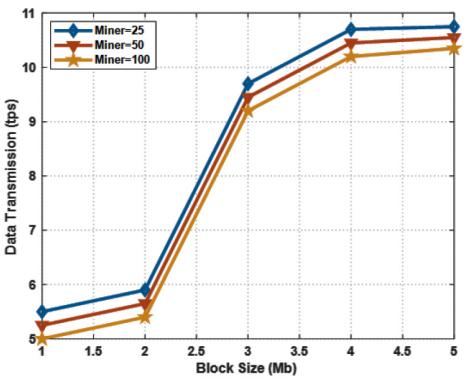

Figure 4

Data transmission (tps) versus block size (Mb).

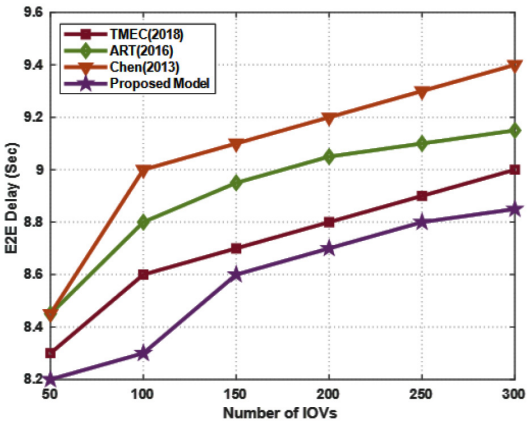

Figure 5

E2E Delay (sec) versus number of IOVs

model maintains superior performance. For instance, with a trust threshold of 0.7, our model detects approximately 97% of packets, whereas existing methods detect less than 90%.

In paper, we investigated the time parameter within vehicular networks by analyzing end-to-end (E2E) delay. The Figure 5 displays the overall E2E delay of our proposed model in comparison to existing trust models. The findings reveal that the current trust models experience significant E2E delays when malicious nodes are introduced into the network, particularly in scenarios with a high density of such nodes. In contrast, our proposed model consistently demonstrates lower E2E delays, even in environments with many malicious vehicles. This improved performance is attributed to the two-stage functioning of our trust model. When an entity is classified as malicious, its content is promptly removed from the network, allowing other vehicles to access accurate information with minimal delays.

5. Conclusion

The Internet of Vehicles (IoV) enhances travel safety, efficiency, energy savings, and comfort, but it also introduces significant security risks due to its openness. Trust management technology offers a simple and effective solution to these security issues, such as vehicles using their real identities while sending false information for personal gain. Analysing the characteristics of trust management in IoV, we propose a new trust model

specifically for IoV. This paper addresses the challenge of implementing trust management in IoV and introduces a blockchain-based protocol. The proposed protocol effectively differentiates between registered and malicious vehicles by maintaining a list of registered vehicles. Simulation results indicate that the proposed scheme significantly limits the impact of malicious vehicles and enhances the accuracy of event judgments based on received messages.

Acknowledgments

The researchers would like to acknowledge the University of Southern Queensland and the University of Thi-Qar. The first author expresses gratitude to her sponsor, the Ministry of Higher Education and Scientific Research (Iraqi Government), and the University of Southern Queensland, for accepting her for a one-year sabbatical leave.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, Accessed: Jun. 17 (2024). [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[2] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2084–2123 (2016), doi: 10.1109/COMST.2016.2535718.

[3] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3796–3838 (2019), doi: 10.1109/COMST.2019.2928178.

[4] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33 (2017), doi: 10.1109/MITP.2017.3680960.

[5] S. K. Jena, B. K. Tripathy, P. Gupta, and S. Das, "A Kerberos Based Secure Communication System in Smart (Internet of Things) Environment," *J. Comput. Theor. Nanosci.*, vol. 16, no. 5, pp. 2381–2388, May (2019), doi: 10.1166/jctn.2019.7904.

[6] N. Gregory Mankiw, Principles of microeconomics. Cengage Learning, (2014). A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "CoAP—Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Sup-

porting CoAP," in *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, and H. Jahankhani, Eds., in Internet of Things. , Cham: Springer International Publishing, pp. 151–175 (2020). doi: 10.1007/978-3-030-18732-3_9.

[7] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A Comprehensive Study on the Trust Management Techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. (2019), doi: 10.1109/JIOT.2019.2933518.

[8] A. Wasef and X. Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks," *IEEE Trans. Mob. Comput.*, vol. 12, no. 1, pp. 78–89, Jan. (2013), doi: 10.1109/TMC.2011.246.

[9] S. Guo, D. Zeng, and Y. Xiang, "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2794–2803, Nov. (2014), doi: 10.1109/TPDS.2013.277.

[10] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 148–161, Mar. (2018), doi: 10.1109/TSIPN.2018.2801622.

[11] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. (2016), doi: 10.1109/TITS.2015.2492981.

[12] P. Fazio, F. De Rango, and C. Sottile, "A Predictive Cross-Layered Interference Management in a Multichannel MAC with Reactive Routing in VANET," *IEEE Trans. Mob. Comput.*, vol. 15, no. 8, pp. 1850–1862, Aug. (2016), doi: 10.1109/TMC.2015.2465384.

[13] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks," *IEEE Wirel. Commun.,* vol. 22, no. 1, pp. 96–102, Feb. (2015), doi: 10.1109/MWC.2015.7054724.

[14] J. Song, C. He, L. Zhang, S. Tang, and H. Zhang, "Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs," *China Commun.*, vol. 11, no. 9, pp. 93–103, Sep. (2014), doi: 10.1109/CC.2014.6969774.

[15] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of Vehicles," *China Commun.*, vol. 11, no. 10, pp. 1–15, Oct. (2014), doi: 10.1109/CC.2014.6969789.

[16] S. Sumithra and R. Vadivel, "An Overview of Various Trust Models for VANET Security Establishment," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bangalore: IEEE, pp. 1–7, Jul. (2018). doi: 10.1109/ICCCNT.2018.8494009.

[17] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. (2017), doi: 10.1016/j.adhoc.2016.10.011.

[18] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolba, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things," *Comput. Netw.*, vol. 101, pp. 127–143, Jun. (2016), doi: 10.1016/j.comnet.2015.12.019.

[19] E. K. Duarte, L. A. L. F. Da Costa, M. Erneberg, E. P. De Freitas, B. Bellalta, and A. Vinel, "SafeSmart: A VANET System for Faster Responses and Increased Safety in Time-Critical Scenarios," *IEEE Access*, vol. 9, pp. 151590–151606 (2021), doi: 10.1109/ACCESS.2021.3126334.

[20] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, "Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem," in *2020 Global Internet of Things Summit (GIoTS)*, Dublin, Ireland: IEEE, pp. 1–6, Jun. (2020). doi: 10.1109/GIOTS49054.2020.9119623.

[21] U. Javaid, M. N. Aman, and B. Sikdar, "A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11815–11829, Dec. (2020), doi: 10.1109/JIOT.2020.3002711.

[22] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. (2021), doi: 10.1109/TITS.2020.3004041.

[23] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666 (2019), doi: 10.1109/ACCESS.2019.2913682.

[24] Abdulbaqi, Azmi Shawkat, Muslim, Israa Falih , Al-Ameer, Asraa A. Abd & Obaid, Ahmed J. Healthcare surveillance based on cloud computing utilizing mobile devices, *Journal of Discrete Mathematical Sciences and Cryptography* :, 1-8, DOI: 10.47974/JDMSC-1566.

Received June, 2024