BTV2P: Blockchain-based Trust Model for Secure Vehicles and Pedestrians Networks

Massinissa Chelghoum *, Gueltoum Bendiab†, Mohamed Benmohammed *,
Stavros Shiaeles ‡, Emanuele Bellini §
*LIRE Laboratory, University of Constantine 2- Abdelhamid Mehri, Ali Mendjeli Campus, 25000 Constantine, Algeria,
massinissa.chelghoum@univ-constantine2.dz, mohamed.benmohammed@univ-constantine2.dz
†Department of Electronics, University of Frères Mentouri, LIRE Laboratory, Constantine 25000, Algeria,
bendiab.kelthoum@umc.edu.dz
‡Centre for Cybercrime and Economic Crime, University of Portsmouth, PO1 2UP, Portsmouth, UK
sshiaeles@ieee.org
§DH Lab, university of Roma Tre, Rome, Italy
emanuele.bellini@uniroma3.it

***Abstract*—With the arrival of connected and autonomous vehicles, Vehicle-to-Pedestrian (V2P) communications are promising to facilitate efficient future of mobility on the road by ensuring maximum protection and safety for both drivers and pedestrians. However, this new technology poses new security and privacy challenges that should be taken into account. For instance, a probable malicious node claiming to be a legitimate pedestrian or vehicle within the network can impact the traffic flow, or even cause serious congestion and traffic accidents by broadcasting fake observations or phenomena on the roads. Therefore, it is crucial to identify legitimate vehicles and road users against adversaries pretending to be one. The aim of this paper is to address these issues, by proposing a distributed trust management scheme that relies on blockchain technology and a trust computation approach for efficient and secure management of trust relationships between pedestrians and vehicles in Vehicle-to-Pedestrian (V2P) networks.**

***Index Terms*—Blockchain, V2P, Connected and autonomous vehicles, Pedestrians, Trust, Security**

I. Introduction

Recently, increasing attention has been provided to research Vehicle-to-Pedestrian (V2P) communication systems [1], [2]. These wireless-based networking paradigms promise to significantly improve pedestrian safety and reduce road fatalities and injuries by exchanging safety/warning messages related to dangerous road conditions, impending collisions and dangerous turns for both Connected Autonomous Vehicles (CAVs) and pedestrians [1], [3]–[5]. V2P network enables direct communication between CAVs, ranging from cars to trucks and buses to trains, and a wide range of road users, including walkers, wheelchair users, passengers boarding and disembarking from buses and trains, and cyclists [2]. According to recent studies, this technology could help prevent more than 80% of vehicle-pedestrian crashes that typically occur in the real world [3]. For instance, in the European Union, it is reported that over 16,000 vulnerable road users (VRUs, e.g., pedestrians and bicyclists) were killed on EU roads in 2021 [6]. However, V2P communications have many security and privacy challenges that can prevent the adoption of this technology, especially in security-critical applications [7], [8]. In particular, broadcasting false/fake warning messages by malicious entities can cause fatal accidents that directly threaten human life, whether on the side of pedestrians or CAVs [7], [8]. Further, location trailing attacks can exploit the location information to profile, predict, and possibly manipulate the behaviour of both CAV drivers and road users [7]. Attackers can also take advantage of insecure communications in V2P networks to steal sensitive information and use it to launch further attacks, which hinder the safety of pedestrians and undermine trust in the V2P system [7]–[9]. To prevent such attacks, it is essential that the receiver verifies the authenticity of the message as well as the credibility of the sender.

The aim of this paper is to address this particular issue by proposing BTV2P, a new distributed trust model that relies on blockchain technology for maintaining trust relationships between pedestrians and vehicles in the V2P system. Recently, blockchain technology has captured the attention of academia and industry as an effective solution for assessing the trustworthiness of unknown entities and exchanging trusted information in distributed environments [7], [9]. Blockchain-based trust management can provide tamper-proof data, enable a more reliable trust information integrity verification, and help to enhance its privacy and availability during sharing and storage [10], [11]. In addition, the distributed nature of blockchain helps to solve many problems of centralised trust models, which are vulnerable to cyberattacks and their failures would paralyse the operation of the network [7].

In BTV2P, blockchain technology is used to securely store sensitive information related to the rating of communications between CAVs and pedestrians in V2P networks. Due to the limited processing power of CAVs and the smartphones of pedestrians, the blockchain network is composed of Road Side Units (RSU) nodes, which are responsible for all core activities of the blockchain including reading data, verification, transaction execution, mining and block generation. The trust management system uses the mechanism of a time-sliding

window to produce a trust value for each entity (CAV or Pedestrian) based on the rating of its past history, enabling the vehicles and pedestrians to perform action whether the incoming messages are trusted or not. The sliding window mechanism, inspired from [12], is mainly used to reflect the timeliness of transaction evidence. Initial testing of BTV2P is carried out in a simulation environment based on a private Ethereum blockchain environment with a single node under Linux Ubuntu. Experimental results proved the feasibility of BTV2P and its performance.

The rest of the paper is structured as follows. Section 2 provides a summary of the relevant publications on the topic of trust management in connected vehicles and Pedestrians Networks (V2P). Next, Section 3 introduces the design and conception of the proposed trust scheme using blockchain technology. It also provides a detailed description of the trust computation approach. After that, Section 4 presents a prototype that implements and validates the proposed scheme with a discussion of the obtained results. Finally, Section 5 highlights research gaps and recommendations for future work directions with proposals and a conclusion.

II. Related work

Since trust is a vital component of vehicular networks, numerous trust models have been proposed in the literature to manage trust in these smart networks. In this context, several approaches for managing trust in V2P networks have used movement or location verification schemes to verify the trustworthiness of the messages received from pedestrians such as [13], [14] and [8]. For instance, authors in [8] proposed a trust management scheme to ensure that only legitimate mobile pedestrians can be admitted to the P2V networks consisting of trustworthy vehicles and pedestrians. Based on the assumption that adversaries are likely to launch attacks remotely via static malicious devices, the authors used the round-trip time (RTT) of the wireless signal between vehicle and pedestrian's devices, only moving (mobile) ones, to track and verify that the movement pattern of the sender matches that of a pedestrian. The main problem with this kind of solution is that it can be applied in limited scenarios. Further, they need specialised hardware that is costly to deploy and manage.

Recently, blockchain technology has gained extensive attention as a solution that can solve the limitations of centralised trust models for securing communications in smart vehicular networks [7], [15]. In particular, many studies have used this technology for storing and sharing reputation information and for mitigating adversary attacks [7], [16], [17]. For instance, authors in [16] used a consortium blockchain to store transactional updates through a reputation score. Entities with a score level higher than a predefined threshold are allowed to communicate messages in the Vehicle-to-Everything (V2X) network. V2X technology enables vehicles to exchange information at any time, from any place to any network. This includes V2P, V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) networks. In another work [18], blockchain technology is used for managing trust between the SDN controllers forming Software-defined Internet of Vehicles (SD-IoV) networks. These large-scale system networks are mainly used to exchange information between connected vehicles and people (including pedestrians), vehicles and roads, and vehicles and the Internet. In this work, smart contracts have been used to implement and run a trust scheme to determine whether an SDN controller should accept a modification request from a third-party application or not.

In a similar study [15], authors exploited blockchain to manage trust between vehicles in V2V networks by evaluating the credibility of Basis Safety Messages (BSMs) messages received from neighbouring vehicles. The authors used a joint Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanism to enable all RSU nodes to participate in computing and updating the trust scores of vehicles in a decentralized manner. In the same context, the IOTA (https://www.iota.org/) Tangle distributed ledger has been exploited in [19] to implement TangleCV, a blockchain-based distributed trust and reputation model. The TangleCV trust model focuses on a specific class of attacks in V2X networks, namely tampering attacks. Message tempering is a critical issue that has been reported from the early days of V2X communications, where many successful message tampering attacks have been reported, especially those related to traffic safety [7].

In summary, the application of blockchain technology to manage trust in vehicle networks is currently the most popular research topic because it offers the best way to detect and respond to potential threats in real-time [7], [20]. However, it is still in a nascent phase. Actually, most of the proposed solutions are theoretical frameworks that have been tested in a simulation environment. Moreover, only few studies focused on V2P networks, which have their own specific security threats that should be taken into account in the trust model.

III. Proposed approach

In this section, we proved a detailed description of BTV2P architecture as well as the proposed approach for evaluating the trustworthiness of CAVs and pedestrians in V2P networks.

A. Model Architecture

BTV2P is a decentralized trust model that uses blockchain technology and fuzzy logic to evaluate the trustworthiness of CAVs and pedestrians over time based on their behaviour. As shown in Fig. 1, the architecture of the proposed trust model incorporates the blockchain network, where the primary nodes are Road Side Units (RSUs). RSU nodes are used for mining, new block generation, and data authentication and verification. These units have the computing power for the blockchain system and are assumed to be secure units compared to CAVs and pedestrians' smartphones. Actually, even if an RSU is controlled by an attacker, security management by network operators in real-time makes this control very limited, and thus the attacker loses control of the RSU quickly [15].

The blockchain is mainly used to store and manage sensitive information related to the rating of communications between CAVs and pedestrians to prevent it from being

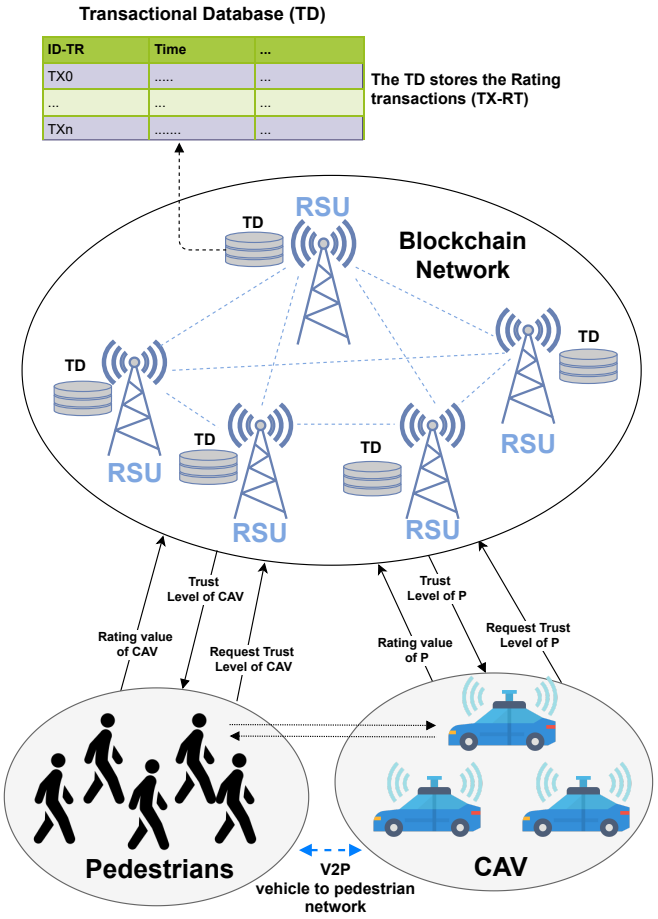

Fig. 1. High-level architecture of the proposed system

tampered with illegally. Thus significantly increasing the security level of exchanged messages between CAVs and pedestrians. This information is used by the trust model to evaluate the trustworthiness of entities in the V2P network, which allows CAVs and pedestrians to check the credibility of each other and decide whether to accept or deny a received message. In particular, CAVs and pedestrians rate each other after each communication. This rating is stored as evidence information in the blockchain by using rating transactions (noted as TX-RT) whose structure is represented as follows

$$\text{TX-RT} = \{ID_{\text{RT}}, time, ID_{\text{receiver}}, ID_{\text{sender}}, Rat_{\text{sender}}\}$$

where ID_{RT} is the identifier of the transaction and $time$ is the time of the transaction, whereas ID_{receiver} and ID_{sender} are respectively the identifiers of the receiver and the sender of a message. It could be a CAV or a pedestrian. Rat_{sender} is the rating value assigned by the receiver to the sender after a V2P communication between the two entities.

B. Trust Evaluation Model

As mentioned above, the transactions stored in the blockchain are used to evaluate the trustworthiness of each entity over time based on their behaviour. The entities involved in our system are CAVs and pedestrians (P). These entities exchange periodically messages related to road traffic status and safety. Each entity is identified in the system by a unique identifier noted as ID_{entity}. After each communication between a CAV and a pedestrian (P), the receiving entity rates the correctness of the received message from the sender. The rate assigned depends on the correctness of the message msg, which could be correct, incorrect or ambiguous. Thus, the rating value $Rat_{\text{sender}}(msg)$ is defined as follows:

$$Rat_{\text{sender}}(msg) = \begin{cases} -1, \text{if msg = "Incorrect"} \\ 0, \text{if msg = "Ambiguous"} \\ 1, \text{if msg = "Correct"} \end{cases} \quad (1)$$

This rating value is stored in the blockchain by using the TX-RT transactions described in the previous section. Based on the rating value, the TX-RT transactions are divided into three main categories: positive transactions (rating value =1), uncertain transactions (rating value =0) and negative transactions (rating value $=-1$).

With the assumption that in the real world, the importance of the rating information would decay decrease time, we have used a sliding window mechanism, inspired from [12], to express the timeliness of the rating information. For that, we have used three time windows with different sizes for the three categories of transactions as follows (see Fig. 2):

$$\begin{cases} SW_p = |t_c - t_p| \\ SW_u = |t_c - t_u| \\ SW_n = |t_c - t_n| \end{cases} \quad (2)$$

where SW_p, SW_u and SW_n respectively represent the size of the time window for positive transactions, uncertain transactions and negative transactions. t_c represents the current time when the system receives an evaluation request from an entity in the system. Whereas, t_p, t_u and t_n are respectively the critical times for the positive time window, uncertain time window and negative time window.

In addition, In the real world, negative feedback has a greater effect on the trust and trustworthiness of an entity because it shows changes in the entity's behaviour, which could be indicative of maliciousness. For that, we suppose that negative transitions will affect the trustworthiness of an entity for a longer time compared to positive transactions. In particular, the importance of negative transactions would decay more slowly than positive ones. For that, the size of the negative time window SW_n should be bigger than it of the positive time window SW_p. ($SW_p < SW_u < SW_n$).

As shown in Fig. 2, at the time t_c, only transactions inside the time windows are used for computing the trust value of an entity at that time (valid transactions). Thus, by querying the Transnational Database (TD) (see Fig. 2) of the blockchain, the system could count the number of transactions in each time sliding window. We define N_p to be the number of positive

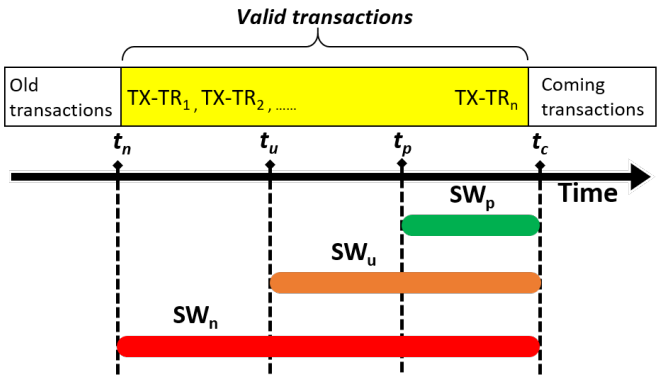

Fig. 2. The sliding window mechanism

transactions in SW_p, N_u the number of uncertain transactions in SW_u and N_n the number of negative transactions in SW_n.

We define *Trust-val*$_t(entity)$ to be the trust value of an entity in the system at time t. It is in the range $[0, 1]$ and depends on the three following states $\{Trsut(T), Uncertain(U), Distrust(D)\}$. The trust state (T) represents the average value of the valid positive transactions. It is computed as follows

$$T = \frac{N_p}{N_p + N_u + N_n} \tag{3}$$

The Distrust state (D) represents the average value of the valid negative transactions. It is computed as follows

$$D = \frac{N_n}{N_p + N_u + N_n} \tag{4}$$

The uncertain state (U) represents the average value of the valid uncertain transactions. It is computed as follows

$$U = 1 - (T + D) \tag{5}$$

Based on the values of the three stats T, D and U, the trust value *Trust-val*$_t(entity)$ of an entity in the system at time t is computed as follows

$$\textit{Trust-val}_t(entity) = w_1 * T + w_2 * U + w_3 * D \tag{6}$$

where w_1, w_1 and w_3 are the weights given to the stats T, U and D respectively. Their values are in the range $[0, 1]$. The obtained trust value is used by the receiver to decide whether to accept or reject a received message. In order to send a clear and accurate answer to the receiver, we have used an assessment of the obtained values of *Trust-val*$_t(entity)$ according to the following rule

$$A(x) = \begin{cases} \textit{Untrusted}, & \text{if } 0 \leq x \leq 0.5 \\ \textit{Moderate Trust}, & \text{if } 0.5 < x < 0.7 \\ \textit{Trusted}, & \text{if } 0.7 \leq x \leq 1 \end{cases} \tag{7}$$

The "Trusted" criterion means the behaviour of the evaluated entity to a certain extent is normal or positive, which makes it more trustworthy. The "Moderate Trust" criterion means that the evaluated entity could be trusted, but this can be risky because it has some abnormal actions in its history. While in the cases of "Untrusted", most or all of the transactions of the evaluated entity are negative which makes this entity untrustworthy. Because there is no unified security perspective that can be followed by all systems, the proposed criteria can be modified according to each system's security policies.

IV. Proof-of-concept experements and results

In this section, we describe and analyse the proof-of-concept experiments carried out on the proposed trust model in order to demonstrate its effectiveness and feasibility. The simulation experiments were performed on a physical machine running Intel ® Core (TM) i5-10300H CPU @2.5GHz, with 16 GB memory and a Hard disk of 1000 GB SSD. A prototype of the proposed evaluation approach is implemented. Due to performance constraints, the experiments were carried out in a private Ethereum blockchain environment with two nodes under Linux Ubuntu by using the packages NodeJS, NPM, Geth (go-Ethereum) and Truffle. The interaction with the smart contract is ensured via a front-end web application. Table I presents the parameters used in the experiments.

TABLE I
Parameters used in simulation experiments

Parameter	Description	value
w_1	Weight factor of positive transactions	0.9
w_2	Weight factor of uncertain transactions	0.5
w_3	Weight factor of negative transactions	0.3
SW_p	Size of SW of positive transactions	700
SW_u	Size of SW of uncertain transactions	750
SW_n	Size of SW of negative transactions	800
R	Number of transactions	1000

In the group of tests, we have one entity with an initial trust value of 0 because the entity is unknown for the trust model at the first transaction. Then, the entity will conduct 1000 transactions with other entities (1000 entities) in the system. In each test, we change the rates of positive, uncertain and negative transactions in order to evaluate the accuracy of the system decision to trust or not trust this entity. A summary of the results obtained in this test is presented in Table II.

As shown in Table II, the evaluated entity achieved good trust values only when the number of positive transactions is very high (more than 70% of the messages are correct), which illustrates the accuracy of the obtained results because a good entity in the system is assumed to always send correct messages. Entities with random behaviour could have "Moderate Trust" if the number of positive transactions is more than 45% and the number of negative transactions is very low, otherwise, they will be classified as untrusted entities. But, they could never be classified as fully trusted entities. The entity becomes "untrusted" if the rate of negative transactions exceeds 40%, which reflects our assumption about bad entities.

Figure 3 illustrates the changes in the trust value over time in three scenarios of the test. In each scenario, the entity

TABLE II
THE RESULTS OF THE TEST

Test	PT%	UT%	NT%	Trust-V	Decision
1	95%	5%	0%	0.88	Trusted
2	90%	10%	0%	0.86	Trusted
3	80%	10%	10%	0.79	Trusted
4	72%	17%	11%	0.76	Trusted
5	60%	20%	20%	0.68	Moderate Trust
6	55%	20%	25%	0.65	Moderate Trust
7	45%	45%	10%	0.64	Moderate Trust
8	40%	40%	20%	0.61	Moderate Trust
9	30%	40%	30%	0.55	Moderate Trust
10	25%	30%	45%	0.50	Untrusted
11	15%	30%	55%	0.44	Untrusted
12	10%	5%	85%	0.37	Untrusted
13	5%	0%	95%	0.32	Untrusted
14	0%	10%	90%	0.32	Untrusted
15	0%	2%	98%	0.30	Untrusted

- PT%: rate of positive transactions
- UT%: rate of uncertain transactions
- NT%: rate of negative transactions
- Trust-V: final trust value

does 1000 transactions in the system (one transaction per second) in 16.14 minutes. In the first scenario, the entity is considered a trusted entity (good entity) (90% positive transactions, 10% uncertain transactions and 0% negative transactions). In the second scenario, The entity is an uncertain entity with "moderate trust" (30% positive transactions, 40% uncertain transactions and 30% negative transactions). in the last scenario, the entity is an untrusted or malicious entity (10% positive transactions, 5% uncertain transactions and 85% negative transactions). The results of the three tests are presented in Figure 3.

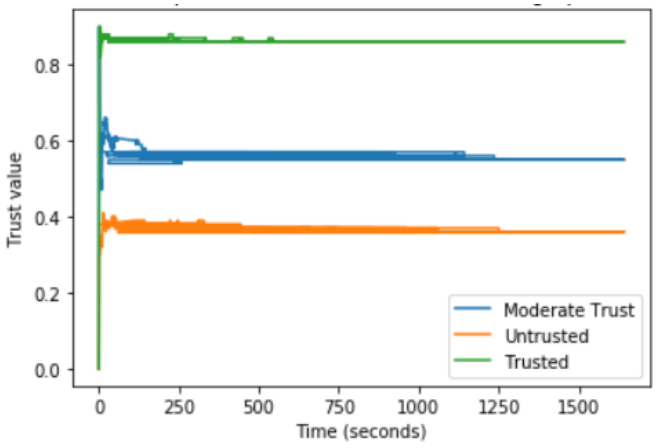

Fig. 3. Changes of the Trust value of good, uncertain and malicious entities over time

From the obtained results, we concluded that the trust value of the trusted entity continues to increase with the accumulation of positive transactions over time until achieving high values (0.8 - 0.9). For the random entities, the change in the behaviour results in a change in the trust value of the entity. The trust value of this entity decreases quickly after negative transactions as it has a greater effect on it and increases showily after positive transactions. Whereas, the trust value of the malicious entity (untrusted entity) continues to decrease until researching a certain value (minimal value is 0.3). In conclusion, the obtained results from the proof of concept experiments prove the feasibility of our trust system and show that it behaves correctly. Indeed, using this system, we can effectively identify malicious CAVs or pedestrians and prevent them from participating in the Blockchain network.

V. CONCLUSION

In this paper, we proposed BTV2P, a distributed trust model based on blockchain technology in order to maintain trust between entities in V2P networks. Therefore, CAVs and pedestrians could verify the trust value of each other in order to decide whether to accept or refuse the received message. The blockchain stores the rating of the communications between CAVs and pedestrians, where the rating value v is assigned based on the correctness of the received messages. This information is used by the trust model to compute the trustworthiness of an entity at time t. A prototype of BTV2P is implemented in order to demonstrate its feasibility in a simulated environment. The Proof of concept experiments proved the feasibility of the core idea of BTV2P. However, further research will still be required, especially, the aspects related to the security of the trust model and its.

For future work, we intend to conduct more experiments on the BTV2P in order to evaluate its scalability and robustness against different types of attacks. We propose to use some techniques like game-theory algorithms in order to try cracking our trust model to test its performances.We also intend to apply our solution in real-world scenarios in order to gather feedback and requirements.

ACKNOWLEDGMENT

This project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements 957406 and 101021936. The work reflects the authors' view and the Agency is not responsible for any use that could be made from the information it contains.

REFERENCES

[1] R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas, and A. Alamoody, "An overview on v2p communication system: Architecture and application," in *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*. IEEE, 2020, pp. 174–178.

[2] J. Walker, "Vehicle-to-pedestrian (v2p) communications for safety." [Online]. Available: https://www.its.dot.gov/research_archives/safety/v2p_comm_safety.htm

[3] R. D. Strickland, M. Yuan, S. Bai, D. W. Weber, and R. Miucic, "Vehicle to pedestrian communication system and method," Aug. 23 2016, uS Patent 9,421,909.

[4] P. Sewalkar and J. Seitz, "Vehicle-to-pedestrian communication for vulnerable road users: Survey, design considerations, and challenges," *Sensors*, vol. 19, no. 2, p. 358, 2019.

[5] A. Kabil, K. Rabieh, F. Kaleem, and M. A. Azer, "Vehicle to pedestrian systems: Survey, challenges and recent trends," *IEEE Access*, vol. 10, pp. 123 981–123 994, 2022.

[6] "Road safety: European commission rewards effective initiatives and publishes 2021 figures on road fatalities." [Online]. Available: shorturl.at/lotC1

[7] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[8] Y. Yang, K. Lee, Y. Kim, and K. Fawaz, "Pedro: Secure pedestrian mobility verification in v2p communication using commercial off-the-shelf mobile devices," in *Proceedings of the 2th Workshop on CPS&IoT Security and Privacy*, 2021, pp. 41–46.

[9] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, p. 108005, 2021.

[10] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, "Blockchain based trust management mechanism for iot," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–8.

[11] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the internet of vehicles," *Computer Networks*, vol. 203, p. 108558, 2022.

[12] X. Wu, R. Zhang, B. Zeng, and S. Zhou, "A trust evaluation model for cloud computing," *Procedia Computer Science*, vol. 17, pp. 1170–1177, 2013.

[13] M. Schäfer, P. Leu, V. Lenders, and J. Schmitt, "Secure motion verification using the doppler effect," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 135–145.

[14] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, 2008.

[15] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE internet of things journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[16] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, "6blocks: 6g-enabled trust management scheme for decentralized autonomous vehicles," *Computer Communications*, vol. 191, pp. 53–68, 2022.

[17] S. Abbes and S. Rekhis, "A blockchain-based solution for reputation management in iov," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2021, pp. 1129–1134.

[18] L. Mendiboure, M. A. Chalouf, and F. Krief, "Towards a blockchain-based sd-iov for applications authentication and trust management," in *Internet of Vehicles. Technologies and Services Towards Smart City: 5th International Conference, IOV 2018, Paris, France, November 20–22, 2018, Proceedings 5*. Springer, 2018, pp. 265–277.

[19] H. Rathore, A. Samant, and M. Jadliwala, "Tanglecv: A distributed ledger technique for secure message sharing in connected vehicles," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, pp. 1–25, 2020.

[20] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita, "Fcmdt: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management," *Computers Security*, vol. 86, pp. 270–290, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818312252