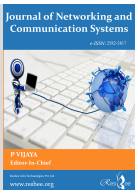
Vol.5 No.4 Oct 2022

Journal of Networking and Communication Systems

Received 10 August, Revised 25 September, Accepted 11 October



A Brief Survey on Security Issues in Vehicular Networks

Sesham Anand
Professor in CSE
Maturi Venkata Subba Rao Engineering College, Hyderabad, Telangana, India.

Abstract: With the growth of Internet of Things and wireless communication systems, vehicular ad hoc networks (VANETs) have attained much consideration recently. VANETs act as a paradigm for vehicular management and communication and thereby, it requires the assurance of efficiency and security for the unreliable and resource constrained networks. This survey makes a critical analysis on about 65 papers regarding security issues in VANET. More particularly, varied performance measures and different types of systems that are contributed in different papers are analyzed. In addition, a comprehensive study is made regarding the signatures models in each contribution. Moreover, analytical review is made concerning various adopted tools and furthermore, the chronological review of the contributed works is examined. Finally, the survey extends with the determination of various research issues and gaps that might be useful for the researchers to promote improved future works on VANET systems.

Keywords: VANET, Security, Signature Models, Centralization, Communication, Wormhole Attack.

Nomenclature

Abbreviations	Descriptions
ART	Attack- Resistant Trust Management Scheme
BARS	Block chain-Oriented Anonymous Reputation System
BTMS-FDD	Beacon Trust Management System and Fake Data Detection
CRVANETs	Cognitive Radio VANET
CPS	Cyber Physical Systems
CL-AS	Certificate Less Aggregate Signature
CPPA	Conditional Privacy-Preserving Authentication
CHs	Cluster Heads
DREAMS	Distributed Reputation Management System
DSRC	Dedicated Short-Range Communication
ESAC	Efficient And Secure Access Control
ECDSA	Elliptic Curve Digital Signature Algorithm
e2e	End to End
FPR	False Positive Rate
IPFS	Inter Planetary File system
IDS	Intrusion Detection System
MANET	mobile ad hoc network
NLOS	None Line of Sight
PPREM	Privacy Preserving Revocation Mechanism
PAACP	Privacy-Preserving Authentication and Access Control Protocol
PDR	Packet Delivery ratio
RSUs	Road Side Units
SDN	Software-defined networking
SPBAC	Security And Privacy Based Access Control
T-CLAIDS	Trust aware Collaborative Learning Automata based IDS
TBRS	Trust-Based Recommendation Scheme
TMR	Trust-Based Multicast Routing protocol
TEAM	Trust-Extended Authentication Mechanism
T-CLAIDS	Trust aware Collaborative Learning Automata based IDS
V-NDN	Vehicular Named Data Networking
VANET	Vehicular Ad Hoc Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
VSRP	Vehicular Security via Reputation and Plausibility checks
VEC	Vehicular Edge Computing
WAVE	Wireless Access In Vehicular Environment

© Resbee Info Technologies Pvt Ltd
https://doi.org/10.46253/jnacs.v5i4.a3

1. Introduction

VANETs are a kind of MANET that could offer the communication among the infrastructures and vehicles [25] [26]. They are modelled to offer road safety, develop driving experiences, and enhance the overall traffic efficiency by passing information amongst varied units in the network. Generally, the exchange of information in VANET occurs among a roadside equipment and vehicle node or between vehicle nodes. A message in VANET [56] [57] [58] consist of traffic condition, traffic managing instructions, vehicle speed, vehicle position, and other service- related information that are exploited to find alternative routes, and to find nearby service location and so on. Nevertheless, owing to its open, dynamic, and distributed nature, recently VANETs are subjected to various "network security attacks".

Mainly, security risks like message forging, wormhole attack, black hole attack, and privacy invasion are most common in VANETs [36] [37] [28]. As secure communication is the base of numerous appliances in VANETs, "how to assess and provide data integrity and the trustworthiness of nodes among vehicles" has developed into a significant issue. Several solutions were implemented to aid secured communication in VANETs [39] [50], which come under 2classes: trust scheme and cryptographic technology. The later is proficient to provide security in VANETs [51] [52], though it includes additional power consumption and time delay, thus restraining its appliances in dynamic environments mainly under limited energy.

Accordingly, these issues can be handles using diverse trust approaches that are categorized into three kinds: "(1) vehicle node-based; (2) message-based; and (3) hybrid" [13] [14]. In an intricate VANET system, the trust model is an essential measure to assess the security of network. In recent times, merging the "trust management with the mobile model" was extensively deployed. Conventional trust model of VANET was categorized into 2types, the "direct trust model and cooperative computing-based trust model". The direct model takes decision concerning the signals and as a result it leads to decision error, whereas the latter cooperate with other nodes and evaluates their trust values [15] [16].

The main contribution of the paper is as follows.

1. Carried out a review associated with security issues in VANET by analysing 65 research papers.
2. Presents a comprehensive review on various performance metrics and types of systems adopted in each reviewed articles.
3. Makes evaluation on signatures, chronological review and adopted tools in each reviewed papers.

This paper is organized as: Section 2 illustrates the related works based on secure VANET systems. The comprehensive review on performance metrics and types of systems are preferred in section 3. The evaluation on signatures, chronological review and adopted tools in adopted works is represented in Section 4. Furthermore, Section 5 organized the research gaps and challenges and the conclusion is portrayed in Section 6.

2. Literature Review

2.1 Related Works

In 2020, Ruhulet al. [1] have presented a novel robust protocol, which guaranteed security at high-level than the conventional protocols and moreover, it protected all associated doable attacks. Numerical analysis has revealed the significance of the presented scheme in terms of security. In 2020, Cui et al.[2] have proposed a privacy preserved authentication model that lessened the overhead and computing issues in VANETs. It also focused on diminishing the side-channel attacks. At the end, simulations were held and the outcomes have demonstrated the efficacy and minimal cost of this method. In 2019, He et al.[3] have established a trust management scheme that improved the security for spectrum sensing and data transmission processes in CR-VANETs. In the end, analysis outcomes have revealed the betterment of the adopted scheme in terms of efficacy.

In 2019, Liang et al. [4] have introduced a TBRS for guarantying real-time security and data transmission in a VANETCPS network. Finally, the simulated outcomes have demonstrated the efficacy of the presented model. In 2019, Fan and Chase [5] have implemented an integrated security technique that aided the nodes in VANETs for recognizing the authenticity of messages for enhanced decision making. At the end, the outcomes have exposed that the presented approach was competent of attaining superior reliability and delivery rate. In 2019, Lai et al.[6] have implemented a new privacy preserving for VANET based on query processing model. Here, the query deliverance proportion was higher than the conventional approaches and the privacy was also sustained at an enhanced rate.

In 2019, Kamil and Sunday [7] have established a big data anonymous batch verification method depending on CL-AS algorithm. Finally, the superiority of the implemented technique was proved with

respect to efficiency. In 2019, Habib et al. [8] have modelled a novel SPBAC method, where the communication took place by means of the onboard unit sensory devices. The examination outcomes have revealed that the presented technique presented private, secured communication when distinguished over the traditional schemes. In 2019, Xia et al.[9] have examined the trust properties and constructed a new trust inference approach, which incorporated recommendation trust and subjective trust that quantify the level of trust for a specific vehicle. The simulation analysis has revealed the betterment of the adopted scheme over the other compared schemes in attack resistance.

In 2019, Gulenget al. [10] have suggested a decentralized trust management model for VANETS. In this model, a trust calculation was carried out based on fuzzy logic for evaluating the direct trust of node. At the end, simulations were held that prove the effectiveness of the introduced scheme. In 2019, Yang et al. [11] have presented a decentralized trust management model in VANETS on the basis of block chain method. Here, the received messages were validated from adjacent vehicles via "Bayesian Inference Model" and it has offered effective trust values. In 2019, Arshad et al. [12] have modeled BTMS-FDD approach, wherein the density and speed data were utilized for establishing a relationship with neighbourhood vehicles. The investigational analysis has demonstrated that the presented model capably detected the malevolent nodes with minimal overhead.

In 2019, Chen et al.[13] have introduced a security model, which exploited "evidence combination technique" for merging the local data with external evidence. The experimentation have illustrated that the presented method offered enhanced outcomes in terms of better precision and recall. In 2018, Sarah et al.[14] has presented a novel technique that elected the CHs depending on the trust and stability factors. Furthermore, the analysis validated the improvement of the developed scheme in terms of stability and data sharing. In 2018, Pham and Chai [15] have implemented a flexible and secure approach for VANETs that managed both trust and privacy. It further authorized the nodes in computing the trustworthiness of received events by concerning the privacy of the senders. On carrying out a widespread analysis by means of the adopted model, precise decisions were taken in a flexible way.

In 2018, Kalaiarasy and Sreenath [16] have developed an enhanced pseudonym approach and one-way hash function for assessing the vehicular incentives that facilitated the privacy security. In addition, the security of developed method was analysed over extant schemes for illustrating its betterment. In 2018, Li et al.[17] have presented a secured CPPA approach for VANETs. Consequently, the offered solution has offered both privacy and security required for VANET appliances. At the end, minimal overhead and cost was attained by the adopted system over the conventional models. In 2018, Ahmad et al.[18] have dealt with a new TEAM model that served as a characteristic prototype for the valuation, design, and management of trust models. Moreover, the efficiency of the model was established against diverse attacks.

In 2017, Muhammad et al.[19] have developed the game theory oriented secure approach for VANETs. The developed method depends on defender and attacker security game that identified and removed the malevolent nodes. The benefit of the presented method was demonstrated over the state-of-the-art schemes in terms of throughput. In 2017, Chakeret al. [20] deployed a scheme that prevents the DDoS attacks and misbehaving nodes in distributed and instantaneous manner. Moreover, a trusted routing model was deployed that delivered data in a most reliable manner. In 2017, Huang et al.[21] have established a technique called DREAMS, where VEC servers were used for performing reputation management tasks for VANET. At last, investigational outcomes have presented greater advantages in detecting the mischievous vehicles.

In 2016, David et al.[22] have presented a new framework called PUCA, which defended in opposition to the attacks, hence offering enhanced privacy for diverse users. Also, several numerical illustrations were offered for analyzing the confidentiality of the presented model. In 2016, Li and Song [23] have developed ART model for VANETs, which detected and resisted the malevolent attacks. It further computed the trustiness of both data and mobile nodes in VANETs. In addition, traffic security and mobility were improved by the designed model. In 2015, Hichem and Sidi [24] have adopted a lightweight and precise intrusion detecting model called AECFV that secluded the network against a variety of risky attacks. Here, the outcomes have exposed improved attack detection capability with high scalability.

In 2015, Ltifiet al. [25] have developed a novel approach for distributing the warnings amongst vehicles without utilizing the road base. Accordingly, a novel "Active vehicle concept" was offered that combined the ambient intelligence with VANET mechanisms. In 2015, Zhang et al.[26] have introduced a privacy and secure oriented model for value-added appliances in VANET. In the end, the performance of the developed scheme was assessed in terms of security and malevolent recognition. In 2014, Gañánet al.[27] have established PPREM model that presented explicit, concise and authenticated data concerning the revocation status, when maintaining the privacy of users. Hence, the sensitive information could be protected from malevolent risks and attacks.

In 2014, Kumar and Naveen [28] have established a novel T-CLAIDS method for VANETs. Furthermore, a novel classifier was modelled for recognizing the malevolent attacks in VANETs. In 2012, Mármol and Gregorio [29] have implemented trust and reputation management that was regarded as an accurate and new technique for dealing with the uncertain risks. In addition, the examination outcomes have exposed the effectiveness and superiority of the offered scheme. In 2011, Yeh et al.[30] have established a novel Portable PAACP model that was employed for non-safety VANET appliances. Further, experimentations were held for exposing the scalability and effectiveness of the presented approach.

In 2018, Lu et al.[31] have portrayed BARS that detached the link ability amongst public keys and real identities for conserving privacy. In the end, the outcomes have shown the betterment of the developed model in contributing enhanced security for VANET systems. In 2018, Lu et al.[32] have developed BARS for setting up a trusted privacy-conserving model for VANETs. At last, investigation was performed that established the betterment of the developed model in terms of robustness and efficiency. In 2018, Steichen et al.[33] have initiated a novel approach that presented a simplified version of IPFS, which employed Ethereum smart contracts for offering file sharing in a controlled way. In the end, investigational results have exposed the improvements made by the adopted method.

In 2018, Seyedet al. [34] have presented a novel authentication model that presented secured communications in VANET. In this work, a secured and fast communicational link was created amongst TA and RSUs. The numerical evaluations and experimentation have exposed the effectiveness of the presented scheme in terms of security. In 2012, Omar et al. [35] have adopted a decentralized security oriented reputation model that facilitated the users in providing feedback in a private and uninhibited way. In the end, numerical experimentations have established the effectiveness of the presented system in raising the security. In 2019, Shrestha et al.[36] have established a new block chain model that solved noteworthy message distribution issues in the VANET. This work mostly focused on public block chain that guaranteed the trust for safe transmission of messages. In 2013, Hasan et al. [37] have introduced a novel privacy preserving model for the “malicious adversarial model”. This technique do not needed “centralized entities, trusted third parties, or specialized platforms, such as anonymous networks and trusted hardware”. At last, the experimentations have confirmed the efficiency of the developed scheme.

In 2018, Shrestha et al. [38] have adopted a new type of block chain for resolving the critical message distribution in VANET, for which a local block chain design was created. From the outcomes, the presented scheme has presented enhanced trustiness over the distinguished schemes. In 2018, Kaur et al.[39] have established a novel approach, wherein a range of security issues were recognized for VANET and viable security techniques were offered for mitigating those attacks. Moreover, defence mechanisms were categorized and examined on the basis of performance metrics. In 2020, Ankitet al. [40] have developed a secured AODV routing protocol for detecting the black hole attacks. The adopted scheme has proved secured network than existing protocols.

In 2018, Laurent [41] have presented a new technique that relied on the employment of smart auditable agreements in blockchain system. Furthermore, the effectiveness of the introduced authentication method was established in realistic scenario. In 2019, Kang et al.[42] have established a proficient “smart contract and consortium block chain mechanism” for attaining safe sharing of data in VANETS. The outcomes have established the betterment of presented model regarding security and data sharing. In 2019, Di et al. [43] have developed a new method depending on block chain mechanism for introducing the policies that certified the distributed transmission of right amid users. Moreover, several arithmetic outcomes were offered that represented the development of the executed method.

In 2020, Kaiet al. [44] have presented a verifiable and secure technique data sharing model for solving the credibility issues. Moreover, an effective model was proposed for certificating the computing abilities of vehicular users. In 2015, Yang and Wang [45] have presented a social network model for examining the secure sharing of data in VANETs. At the end, the simulated outcomes have demonstrated the enhancement of the offered method in terms of security. In 2020, Jiaqi et al. [46] have presented a new framework of 5G SDN and proposed an efficient and secured privacy conserving authentication system for VANETs. In 2010, Tajeddineet al. [47] have introduced a trust-oriented preservation model for VANETs. In addition, simulated outcomes have revealed the betterment of the offered model in terms of accurateness and reliability.

In 2020, Jiang [48] have deployed an ESAC approach for delivering contents in V-NDN. In particular, proxy re-encryption technique was constructed for attaining data confidentiality and access control. At last, the outcomes had demonstrated the efficacy of the presented approach in terms of minimal overhead. In 2015, Li et al. [49] have developed the announcement model for VANETs that permitted the evaluation of message reliability based on reputation system. In addition, the investigational outcomes have exposed the development of the adopted method in terms of security and fault tolerance. In 2013, Yang [50] has introduced a novel trust and reputation management model for VANETs. Moreover, a

similarity mining technique was exploited for identifying the identical messages or vehicles. Therefore, a trustworthy message was identified by the offered technique. In 2014, Zhen et al.[51] have presented several issues concerning the current trust techniques in VANETs and the ways to solve them was also discussed. Further, the designed method has presented enhanced "voting accuracy" over the distinguished techniques.

In 2016, Diep and Yeo [52] have established a safer approach for managing both trust and privacy in vehicles in a better manner. At last, the analysis results have aided the nodes in safeguarding the privacy along with enhanced decision making ability. In 2010, Jie et al.[53] have presented aninnovative trust-oriented approach for message transmission and assessment in VANETS. Here, the peers shared data by considering road or safety conditions. Furthermore, the effectiveness of developed model was demonstrated from the investigational outcomes. In 2014, Chuang and Lee [54] have modelled TEAM for performing communiqué in VANETs. Furthermore, the simulated analysis exposed enhanced authentication and it resolved different attacks.

In 2010, Ding et al.[55] have implemented a reputation management approach that prevented the distribution of fake messages. At last, the experimentations have demonstrated the development of the developed model in terms of false message filtration. In 2016, Wang et al. [56] have established a reputation oriented approach, which deployed both service reputation and feedback reputation. In addition, for avoiding the strategic attacks, a feedback reputation model was offered that identified the false feedbacks. In 2010, Dhurandheret al. [57] have developed a robust model known as VSRP for deploying security in VANETs. Furthermore, the presented method has dealt with the issues concerning the data aggregation and data dropping.

In 2011, Abumansooret al. [58] have deployed a trust evaluation model based on location verification and information in a NLOS condition. From the arithmetic analysis, the offered method has resulted in enhanced success rates in message deliverance. In 2016, Umar et al.[59] have established a novel composite trust model that integrated majority oriented trust, role oriented trust and experience oriented trust, by which the count of received reports were restricted. In 2020, Jianet al. [60] have developed a secured "real-time traffic data aggregation model" in VANETs. Here, the signature validity of vehicles was authenticated, and the original traffic information was retrieved from signatures. Finally, the arithmetical experimentation had demonstrated the efficacy of the presented approach in terms of reduced cost and communication.

In 2020, Jian et al.[61] have adopted a data-sharing model, in which both dynamic and key updating property of VANET were maintained. Furthermore, the investigational outcomes were offered that confirmed the efficiency and high security of the presented algorithm. In 2018, Xia et al.[62] have suggested a TMR for opposing the diverse attacks and furthermore, the routing efficiency was enhanced. Accordingly, the effectiveness of developed scheme was revealed via overhead and e2e delay. In 2020, Chenet al.[63] have established an optimum decision model, which maximized the probability of taking correct decisions regarding message contents. In 2018, Ltifiet al.[64] have introduced a secured communication model amongst active vehicles for distributing alerts. Using this new approach, traffic accidental alerts were established depending on the trust ranges of the sender. In 2016, Bahuguna et al. [65] have presented a novel method for safeguarding the privacy of vehicles in opposition to external eavesdroppers. At last, the development of the adopted method was established in terms of superior decision making.

In 2023, M. R. Dey et al. [66] have introduced an LTE vehicular network including mobile network components for real-time identification and localizing of DoS assaults. This method executed three components: the machine learning algorithms, the average Packet Delivery Ratio (PDR), and the data packet counter (DPC). Initially, PDR and data packet counter were used for effective attack detection. Secondly, ML algorithms were added to detect more vigorous and reliable attacks. The Data Packet Counter (DPC) was finally introduced to measure and report on both purposeful and unintended DoS assaults. This method outperformed this experiment.

In 2022, Mahmood et al. [67] have executed a data-sharing plan for 5G-enabled mobility networks. This process had six steps: initialization of TA (TA Setup), production of pseudonym identities (PIDGen), generation of keys (KeyGen), generation of messages (MsgSign), generation of single and batch signatures (BSigVerify), and message signing. Initially, the TA Setup Phase generated pseudonyms for vehicles to protect their privacy. Then it moved to the PIDGen phase, where a unique identity was created for the communication process. Next came the key generation phase, which communicated the generated key securely between two communicating parties using public cryptography techniques. Further, it had gone to the Signing Phase, which allows signing messages between parties. Finally, signature verification verified the signed messages at the receiving end. This method was a cost-effective and safe data-sharing method for 5G networks that did not require RSU.

In 2023, Boya Liu et al. [68] have applied deep reinforcement learning (DRL) to improve the performance of vehicular ad hoc networks (VANET). Initially, this method designed a state and action space that matched the vehicular Network environment. In addition to this, they created a reward system to guide effective training of the DQN system. The included information was obtained from current nodes with complexity O(12N), where N was the next hop node available for selection by the current node. After the above process, an adaptive routing scheme was selected based on complex state spaces to provide secure message services for users through VANETs. This resulted in fast convergence, strong generalization capacity, excellent transmission security, and minimal network delay with rich patterns for VANET message services.

In 2023, Vita Santa Barletta et al. [69] have enforced a vehicle-security operation center (V-SOC4AS) to enhance vehicular security through the identification, reply, and protection from hackers on vehicle communication networks such as CAN, LIN, FlexRay, etc. V-SOC4AS used Event Management and Security Information technology to track messages sent between ECUs in real time. This monitoring happened within the vehicle or from external sources like the infotainment/telematics system or vehicular ports. While monitoring, it also automated the threat detection processes, which resulted in reduced response times. When malicious intent was detected, the SOC analysts were notified using payloads containing CAN frames and attack notifications. The output helped to work on the threat, attack vector, and risk associated with a specific vehicle component and improved the detection, response, support, and prevention of cyber-attacks. It also identified their type and pattern.

In 2022, Men et al. [70] have rendered the Additive Increase Multiplicative Decrease method (AIMD) and blockchain technology to compute the reputation scores of vehicles. Initially, vehicles broadcast events to other vehicles and RSUs (roadside units). Then, the RSU received opinions from its neighbors about this message. Based on the opinions and decisions of the neighbor, the accuracy score was calculated. If the affirmative score exceeded a certain threshold, a reputation score was assigned and the vehicle was rewarded; if it fell below a certain level, they were penalized for their actions. The output stated a lower time delay with higher accuracy.

In 2023, JUNQIN HUANG et al. [71] have concentrated on blockchain technology and Zero-Knowledge Proof (ZKP) technology using privacy-preserving vehicular data-sharing frameworks for tamper-proof, traceability, and decentralization. Initially, vehicular data was shared and encrypted with a master public key. Next, using the relevant vehicle's public key, an Auth primitive produced a Zero-Knowledge Proof (ZKP). Finally, cipher text and ZKP were sent for sharing, which protected and preserved the audit ability of their data. This method strengthened system security, protected data privacy, and reduced communication complexity compared to existing sharing protocols.

In 2023, Xu et al. [72] have tried a secured blockchain technology in data trading systems for VCS. This was called BTT. To guarantee the accuracy of sensing data and safeguard user privacy, the technique initially entailed fusing a lightweight truth discovery algorithm with a blockchain-based data trading process. In addition to this, it also included a gas optimization mechanism and distributed judgment mechanisms to minimize costs incurred by users and also regulate all participants during the process. Finally, the Ethereum test network was carried out for demonstration purposes through extensive simulations. This method produced high precision at a low cost.

In 2023, Shangle Li et al. [73] have introduced a solid excludability authentication strategy for VANETs that protects privacy. Initially, using a double-key approach, two keys were assigned to each vehicle: one for authentication purposes (public) and another for encryption/decryption operations (private). Then vehicles updated their private keys online using short group signatures that were to be verified by TA or RSUs. Once authentication was verified, trusted communication was established. This provided complete authentication, anonymity, traceability, and strong excludability.

3. Comprehensive review on Performance metrics and Types of Systems

3.1 Analysis on Performance Measures

The performance measures considered in diverse contributions regarding the security in VANET is depicted in Table I.From Table I, it is observed that [1] and [60] made analysis on computational cost and [61] has made analysis on communication complexity. 3 papers have made a performance analysis under PDR and through put that have contributed about 4.62% of the reviewed works. Similarly, the execution time, detection ratio, reputation value and transmission range havebeen contributed about 24.62% (16 papers), 9.23% (6 papers), 6.15% (4 papers) and 9.23% (6 papers). Further, precision, recall and average delay have been adopted in 4.62% (3 papers), 3.08% (2 papers) and 3.08% (2 papers). Moreover, the transmission latency, Communication cost, e2e delay, packet loss and accuracy have contributed about 3.08% (2 papers), 4.62% (3 papers), 7.69% (5 papers), 6.15% (4 papers) and 3.08% (2 papers) of the entire

contribution respectively. In addition, communication overhead has contributed about 9.23% of the entire contribution. Over 1.54% of total contributions have analysed the measures like forwarding rate, awareness rate, anomaly ratio, query delay, packet reception probability, maximum velocity, event detection probability, energy utilization, error ratio, FPR, bit rate, block generation rate, % of incorrect decisions, average confidence value, relay effectiveness, frequency, RMSE, channel bandwidth and average distance correspondingly.

Table 1: Review on Different Performance Metricsin VANETs

Measures	Citations
Computational cost	[1] [60]
Communication complexity	[61]
Execution Time	[2] [7] [8] [9] [10] [12] [14] [17] [25] [26] [28] [30] [31] [32] [42] [62]
PDR	[14] [58] [62]
Throughput	[3] [5] [19]
Precision	[10] [13] [23]
Transmission Range	[4] [20] [34] [55] [64] [65]
Reputation Value	[21] [42] [47] [56]
Detection Ratio	[13] [18] [20] [24] [28] [42]
Average Delay	[25] [64]
Recall	[13] [23]
Communication Cost	[2] [6] [17]
Transmission Latency	[4] [11]
Packet Loss	[4] [40] [46] [48]
e2e Delay	[27] [62] [40] [46] [48]
Accuracy	[9] [29]
Communication overhead	[7] [15] [23] [31] [32] [61]
Miscellaneous measures	
Forwarding Rate	[5]
Awareness Rate	[58]
Anomaly Ratio	[18]
Query Delay	[6]
Maximum Velocity	[10]
FPR	[18]
Energy Utilization	[16]
Error Ratio	[20]
Packet Reception Probability	[10]
Event Detection Probability	[18]
% of Incorrect Decisions	[51]
Block Generation Rate	[36]
Bit Rate	[34]
RMSE	[55]
Frequency	[51]
Relay Effectiveness	[53]
Channel Bandwidth	[62]
Average Distance	[56]

3.2 Analysis on Type of Systems

This survey analyses the type of systems (centralized or decentralized) adopted in various reviewed works. Fig. 1 represents the percentage of contributions for the types of systems in bar chart format. From the surveyed report, 11 works have adopted the centralized systems, that is, 16.92% of the works have exploited the centralized systems. On the other hand, 18 works have contributed on decentralized systems, i.e. 27.69% of the works have exploited the decentralized systems.

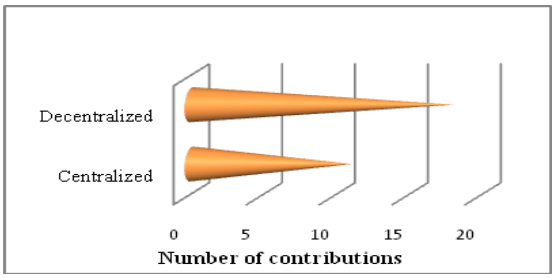


Fig.1. *Bar chart showing type of systems*

4. Evaluation on Signatures, Chronological review and adopted tools in adopted works

4.1 Analysis on Signatures

This section reviews diverse signature systems adopted in each work that is specified in a pie chart representation by Fig. 2. From the review, it was observed that aggregate signature was adopted by 2 works, i.e. [7], [53] and digital signature was adopted in 10 works, i.e. [1] [25] [32] [40] [42] [46] [55] [57] [58] [59]. In addition, ECDSA was adopted in [24] [27] [60] and group signature was adopted in [22] [26] [34] and [47] works respectively. Likewise, the signature concept has been adopted by 18 works.

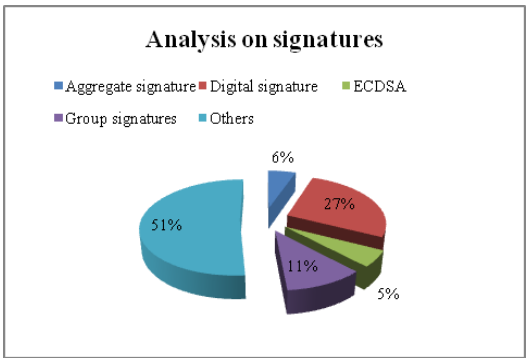


Fig. 2. *Analysis on the types of signatures*

4.2 Chronological Analysis

This study examines numerous papers published in different years. Fig. 3 shows the proportion of contributions for consequent years. Primarily, the papers established in 2020 to 2019 were found to be about 35.38% of total contribution. In the same way, 35.38% of the total reviewed works were established in 2018 to 2016. In addition, 20% of contributions on VANETs are taken from year 2015, 2014, 2013 and 2012. The count of works presented for VANETs security in the years 2011-2010 is 7.69% of the whole contributions.

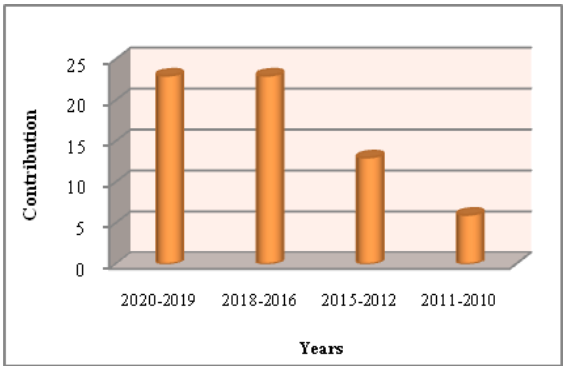


Fig. 3. *Bar chart representing chronological review*

4.3 Review on Adopted Tools

The simulations of the adopted works are executed in different simulators namely, C++, NS-2 simulator, NS-3 simulator, MobiSim, One simulator, OMNeT++ and so on. The bar chart representation of the adopted tools in the reviewed works is given by Fig. 4. Accordingly, MobiSim was adopted in 1 paperthat have offered about 1.54% of the total contribution, andC++ was used in 3 papers that had offered about 4.62% of the entire contribution. Similarly, the NS-2 simulator has been adopted by 10 papers and java has been adopted in 4 papers, which has provided about 15.38% and 6.15% of the total contribution. Moreover, NS-3 simulator has been exploited by 3 papers that contribute about 4.62% of the entire contribution. Accordingly, One simulator was adopted by 3 papers that offer about 4.62% of the whole contribution.

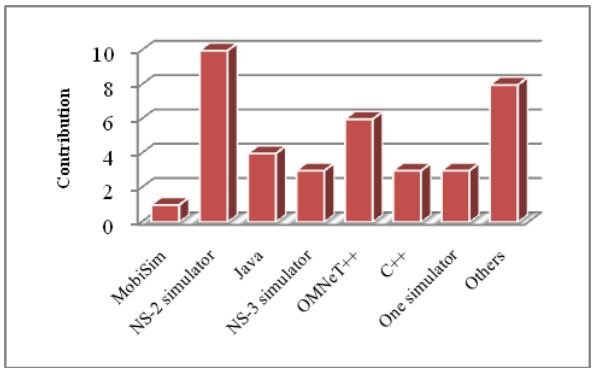


Fig. 4. *Analysis on adopted tools in reviewed works*

5. Research Gaps and Challenges

For the previous two decades, industrials and research academies have concerned their concentration on VANETs for providing assistance and safety appliances, for improving the driving experiences, and controlling the road traffics [44] [68]. In order to achieve this objective, numerous protocols have been introduced namely, WAVE, DSRC and other protocols, which runs as overlie on WAVE / DSRC instead of the IP protocol. In vehicular surroundings, massive quantity of data are switched under diverse kinds of communication namely; V2V, V2I, and so on [59] [61].

Nevertheless, sharing information and exchanging data in VANET under the usage of IP protocol is found to be a challenging one. This is because, the characteristics of the network often varies under the usage of poor-quality wireless links that made it more complicated in terms of security, mobility, and routing. In addition, owing to the reality that vehicles might exchange sensitive and personal data, it is indispensable to secure the content and communication of users while preserving data privacy [40] [1]. Thus, VANET communications should assure diverse security needs together with no repudiation, integrity, privacy, and confidentiality. Several conventional works have examined the security efforts; however, there was no enough consideration on nature of VANET communiqué and attacks in their analysis.

6. Conclusion

This paper has offered a comprehensive review on security in VANET systems. Diverse works were reviewed and their performances were portrayed. Moreover, this survey analyzes the varied features related to the VANET systems. In conclusion,

- This work has reviewed about 65 research papers and declared the noteworthy analysis on the types of systems (decentralized or centralized).
- The review has analysed different performance measures and signature models exploited in each works.
- Further, the chronological review and adopted tools in each works were also analysed and represented in brief.
- Finally, this paper has depicted varied research issues that could be helpful for the researchers to do additional research on VANET security systems.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

Reference

[1] Ruhul AminParas LohaniSatyanarayana Vollala, “An enhanced anonymity resilience security protocol for vehicular ad-hoc network with Scyther simulation”, Computers & Electrical Engineering, vol. 82 (Cover date: March 2020)Article 106554, 25 January 2020.

[2] Jie Cui, Wenyu Xu, Yibo Han, Jing Zhang, Hong Zhong, ”Secure mutual authentication with privacy preservation in vehicular ad hoc networks”, Vehicular Communications, vol. 21, January 2020, Article 100200.

[3] Ying He, F. Richard Yu, Zhexiong Wei, Victor Leung, “Trust management for secure cognitive radio vehicular ad hoc networks”, Ad Hoc Networks, vol. 86, pp. 154-165, 1 April 2019.

[4] Wei Liang, Jing Long, Tien-Hsiung Weng, Xuhui Chen, Albert Y. Zomaya, "TBRS: A trust based recommendation scheme for vehicular CPS network", Future Generation Computer Systems, vol. 92, pp. 383-398, March 2019.

[5] Na Fan, Chase Q. Wu, "On trust models for communication security in vehicular ad-hoc networks", Ad Hoc Networks, vol. 90, July 2019, Article 101740.

[6] Yongxuan Lai, Yifan Xu, Fan Yang, Wei Lu, Quan Yu, "Privacy-aware query processing in vehicular ad-hoc networks", Ad Hoc Networks, vol. 91, August 2019, Article 101876.

[7] Ismaila Adeniyi Kamil, Sunday Oyinlola Ogundoyin,"A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5G smart grid slice", Sustainable Energy, Grids and Networks, vol. 20, December 2019, Article 100260.

[8] Muhammad Asif Habib, Mudassar Ahmad, Sohail Jabbar, Shehzad Khalid, Muhammad Sayim Khalil ,"Security and privacy based access control model for internet of connected vehicles", Future Generation Computer Systems, vol. 97, pp. 687-696, August 2019.

[9] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 7108-7120, July 2019.

[10] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga and Y. Ji, "Decentralized Trust Evaluation in Vehicular Internet of Things," IEEE Access, vol. 7, pp. 15980-15988, 2019.

[11] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, April 2019.

[12] M. Arshad et al., "Beacon trust management system and fake data detection in vehicular ad-hoc networks," IET Intelligent Transport Systems, vol. 13, no. 5, pp. 780-788, 5 2019.

[13] J. Chen, T. Li and J. Panneerselvam, "TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles," IEEE Access, vol. 7, pp. 148913-148922, 2019.

[14] Sarah Oubabas, Rachida Aoudjit, Joel J. P. C. Rodrigues, Said Talbi, "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme", Vehicular Communications, vol. 13, pp. 128-138, July 2018.

[15] Thi Ngoc Diep Pham, Chai Kiat Yeo, "Adaptive trust and privacy management framework for vehicular networks", Vehicular Communications, vol. 13, pp. 1-12, July 2018.

[16] C. Kalaiarasy, N. Sreenath, "An incentive-based co-operation motivating pseudonym changing strategy for privacy preservation in mixed zones in vehicular networks", Journal of King Saud University - Computer and Information Sciences, In press, corrected proof, Available online 12 September 2018.

[17] JiLiang Li, Kim-Kwang Raymond Choo, WeiGuo Zhang, Saru Kumari, Dieter Hogrefe, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks", Vehicular Communications, vol. 13, pp. 104-113, July 2018.

[18] F. Ahmad, V. N. L. Franqueira and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," IEEE Access, vol. 6, pp. 28643-28660, 2018.

[19] Muhammad Mohsin Mehdi, Imran Raza, Syed Asad Hussain,"A game theory based trust model for Vehicular Ad hoc Networks (VANETs)", Computer Networks, vol. 121, pp. 152-172, 5 July 2017.

[20] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T. Calafate, Abderrahmane Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs", Vehicular Communications, vol. 9, pp. 254-267, July 2017.

[21] X. Huang, R. Yu, J. Kang and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," IEEE Access, vol. 5, pp. 25408-25420, 2017.

[22] David Förster, Frank Kargl, Hans Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks", Ad Hoc Networks, vol. 37, Part 1, pp. 122-132, February 2016.

[23] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960-969, April 2016.

[24] Hichem Sedjelmaci, Sidi Mohammed Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks", Computers & Electrical Engineering, vol. 43, pp. 33-47, April 2015.

[25] Amel Ltifi, Ahmed Zouinkhi, Mohamed Salim Bouhlel, "Trust-based Scheme for Alert Spreading in VANET", Procedia Computer Science, vol. 73, pp. 282-289, 2015.

[26] Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Bao Liu,"Practical secure and privacy-preserving scheme for value-added applications in VANETs", Computer Communications, vol. 71, pp. 50-60, 1 November 2015.

[27] Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, Juanjo Alins, "PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks", Computer Standards & Interfaces, vol. 36, no. 3, pp. 513-523, March 2014.

[28] Neeraj Kumar, Naveen Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs", Computers & Electrical Engineering, vol. 40, no. 6, pp. 1981-1996, August 2014.

[29] Félix Gómez Mármol, Gregorio Martínez Pérez, “TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks”, Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941, May 2012.

[30] Lo-Yao Yeh, Yen-Cheng Chen, Jiun-Long Huang, “PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks”, Computer Communications, vol. 34, no. 3, pp. 447-456, 15 March 2011.

[31] Zhaojun Lu, Qian Wang, Gang Qu, Zhenglin Liu, "BARS: a Blockchain-based Anonymous Reputation System for Trust Management in VANETs",Cryptography and Security, 17 Jul 2018.

[32] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," in IEEE Access, vol. 6, pp. 45655-45664, 2018.

[33] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1499-1506, 2018.

[34] Seyed Morteza Pournaghi, Behnam Zahednejad, Majid Bayat, Yaghoub Farjami, “NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET”, Computer Networks, vol. 134, pp. 78-92, 7 April 2018.

[35] Omar Hasan, Lionel Brunie, Elisa Bertino, “Preserving privacy of feedback providers in decentralized reputation systems”, Computers & Security, vol. 31, no. 7, pp. 816-826, October 2012.

[36] Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Nam,”A new type of blockchain for secure message exchange in VANET”, Digital Communications and Networks, In press, corrected proof, Available online 26 April 2019.

[37] O. Hasan, L. Brunie, E. Bertino and N. Shang, "A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 949-962, June 2013.

[38] R. Shrestha, R. Bajracharya and S. Y. Nam, "Blockchain-based Message Dissemination in VANET," IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu, pp. 161-166, 2018.

[39] Rajdeep Kaur, Tejinder Pal Singh, Vinayak Khajuria, "Security Issues in Vehicular Ad-hoc Network(VANET)",Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, 2018.

[40] Ankit KumarVijayakumar VaradarajanKalyana C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm", Microprocessors and Microsystems, Available online, 21 October 2020, In press, corrected proof, Article 103352.

[41] M. Laurent, Nesrine Kaaniche, Mathieu Vander Plaetse, “An Access Control Scheme based on Blockchain Technology", Member of the Chair Values and Policies of Personal Information, 2018.

[42] J. Kang et al., "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019.

[43] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci, "Blockchain Based Access Control", Department of Computer Science, 2019.

[44] K. Fan et al., "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5826-5835, June 2020, doi: 10.1109/TVT.2020.2968094.

[45] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," in IEEE Communications Magazine, vol. 53, no. 8, pp. 42-47, August 2015.

[46] J. Huang, Y. Qian and R. Q. Hu, "Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8542-8554, Aug. 2020, doi: 10.1109/TVT.2020.2996574.

[47] Tajeddine, A. Kayssi and A. Chehab, "A Privacy-Preserving Trust Model for VANETs," 10th IEEE International Conference on Computer and Information Technology, Bradford, pp. 832-837, 2010.

[48] S. Jiang, J. Liu, L. Wang, Y. Zhou and Y. Fang, "ESAC: An Efficient and Secure Access Control Scheme in Vehicular Named Data Networking," IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 10252-10263, Sept. 2020, doi: 10.1109/TVT.2020.3004459.

[49] Xiaoqing Li, Jicheng Liu, Xuejun Li, Hui Li, "A reputation-based secure scheme in vehicular ad hoc networks",International Journal of Grid and Utility Computing, vol.6, no.2, 13 May 2015.

[50] Nianhua Yang, "A Similarity based Trust and Reputation Management Framework for VANETs", International Journal of Future Generation Communication and Networking, vol. 6, no. 2, April, 2013.

[51] Zhen Huang, Sushmita Ruj,Marcos A. Cavenaghi, Milos Stojmenovic, Amiya Nayak, "A social network approach to trust management in VANETs", vol.7, no. 3, pp 229–242, September 2014.

[52] P. T. N. Diep and C. K. Yeo, "A trust-privacy framework in vehicular ad hoc networks (VANET)," Wireless Telecommunications Symposium (WTS), London, pp. 1-7, 2016.

[53] Jie Zhang, Chen Chen and Robin Cohen, "A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol.1, no. 4, pp. 3-15, December 2010.

[54] M. Chuang and J. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," IEEE Systems Journal, vol. 8, no. 3, pp. 749-758, Sept. 2014.

[55] Q. Ding, X. Li, M. Jiang and X. Zhou, "Reputation Management in Vehicular Ad Hoc Networks," 2010 International Conference on Multimedia Technology, Ningbo, pp. 1-5, 2010.

[56] Jin Wang, Yonghui Zhang, Youyuan Wang, Xiang Gu, "RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs", International Journal of Distributed Sensor Networks, March 6, 2016.

[57] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari and A. Tyagi, "Securing vehicular networks: A reputation and plausibility checks-based approach," IEEE Globecom Workshops, Miami, FL, pp. 1550-1554, 2010.

[58] Abumansoor, Osama & Boukerche, Azzedine, "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services", Global Telecommunications Conference (GLOBECOM 2011), IEEE. 1-5, 2011.

[59] Umar Farooq Minhas, Jie Zhang, Robin Cohen, "Towards Expanded Trust Management for Agents in Vehicular Ad-hoc Networks", -International Journal of Computational Intelligence Theory and Practice, vol. 2, no. 1, January-June, 2016.

[60] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar and P. Vijayakumar, "Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs," IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 807-817, Jan. 2020, doi: 10.1109/TVT.2019.2946935.

[61] J. Shen, T. Zhou, J. Lai, P. Li and S. Moh, "Secure and Efficient Data Sharing in Dynamic Vehicular Networks," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8208-8217, Sept. 2020, doi: 10.1109/JIOT.2020.2985324.

[62] Hui Xia, San-shun Zhang, Ben-xia Li, Li Li, and Xiang-guo Cheng, "Towards a Novel Trust-Based Multicast Routing for VANETs", Security and Communication Networks, vol. 2018, Article ID 7608198, 12 pages, 1 October 2018.

[63] J. Chen, G. Mao, C. Li and D. Zhang, "A Topological Approach to Secure Message Dissemination in Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 1, pp. 135-148, Jan. 2020, doi: 10.1109/TITS.2018.2889746.

[64] Amel Ltifi; Ahmed Zouinkhi; Med Salim Bouhlel, "Active vehicle: a new approach integrating AmI technology for trust management in VANET", International Journal of High Performance Computing and Networking, vol.11, no.4, 2018.

[65] Arti Bahuguna, Sunil Singh Bisht, Ajay Bahuguna, "A Social Network Approach to Privacy & Trust Management in (VANET)", International Journal of Computer Science and Mobile Computing, vol. 5, no.12, pg.111 – 123, December 2016.

[66] M. R. Dey, M. Patra, and P. Mishra, "Efficient Detection and Localization of DoS Attacks in Heterogeneous Vehicular Networks in IEEE Transactions on Vehicular Technology", 2023.

[67] Al-Shareeda, M.A., Manickam, S., Mohammed, B.A., Al-Mekhlafi, Z.G., Qtaish, A., Alzahrani, A.J., Alshammari, G., Sallam, A.A. and Almekhlafi, K., "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)", Sustainability, Vol. 14(16), pp.9961, 2022.

[68] Liu, B., Xu, G., Xu, G., Wang, C. and Zuo, P., "Deep Reinforcement Learning-Based Intelligent Security Forwarding Strategy for VANET", Sensors, Vol. 23(3), pp.1204, 2023.

[69] Barletta, V.S., Caivano, D., Vincentiis, M.D., Ragone, A., Scalera, M. and Martín, M.Á.S., "V-SOC4AS: A Vehicle-SOC for Improving Automotive Security", Algorithms, Vol. 16(2), pp.112, 2023.

[70] Men, R., Fan, X. and Yang, X., "Blockchain-Based Incentive-Compatible Reputation Management System in Vehicular Networks", Information Resources Management Journal (IRMJ), Vol. 35(2), pp.1-16, 2022.

[71] Huang, J., Kong, L., Wang, J., Chen, G., Gao, J., Huang, G. and Khan, M.K., "Secure Data Sharing over Vehicular Networks Based on Multi-Sharding Blockchain", ACM Transactions on Sensor Networks, 2023.

[72] Xu, H., Qi, S., Qi, Y., Wei, W, and Xiong, N., "Secure and Lightweight Blockchain-based Truthful Data Trading for Real-Time Vehicular Crowdsensing", ACM Transactions on Embedded Computing Systems, 2023.

[73] Li, S., Yang, R. and Chen, J., "A Privacy-Preserving Authentication Scheme for VANETs with Exculpability", Security and Communication Networks, 2023