Software-Defined Vehicular Networks (SDVN)

Zeyad Ghaleb Al-Mekhlafi[1†]

Department of Information and Computer Science, College of Computer Science and Engineering,
University of Ha'il, Ha'il 81481, Saudi Arabia

Summary
In order for the Vehicular Ad Hoc Networks (VANETs) environments to be able to provide such useful road services, large amounts of data are generated and exchanged among the various communicated entities wirelessly via open channels in these vehicular networks. This attracts adversaries and threatens the network with a variety of potential types of security attacks. In this paper, we focus on blockchain-based security schemes while demonstrating the effectiveness of blockchains in the VANET context. Following a thorough introduction to VANET and blockchain, a comprehensive list of security needs, difficulties, and potential threats in vehicle networks is presented. Then, with a thorough comparative assessment of the method- ologies utilized, network models, evaluation tools, and attacks mitigated, a more in-depth review of modern blockchain-based authentication systems in VANETs is offered. Finally, several potential issues with VANET security are presented that will need to be resolved in future studies.

Keywords:
Terms—Vehicular Ad-hoc Network (VANET), Blockchain, Security Schemes, Privacy, Security Attacks.

1. Introduction

There are more accidents and traffic congestion problems today due to the vast growth in the number of vehicles on the road [1-3]. This highlights the necessity of making serious plans to guarantee traffic flow and road safety. One technology that has been introduced to maintain safer and more expedient driving on routes is Vehicular Ad-hoc Networks (VANETs), that enable cars to exchange data about their velocity, position, and other road-related data to increase smart of surrounding road conditions and aid in decision-making [4–7]. Avoidance of congestion, management of traffic, routing, transfer of data, and control of traffic signal are a few examples of the former [9], [10].

VANET has emerged with an important chance to provide various applications and support many benefits to the road environment such as recording fatal occurrences [8], effectiveness of cost, efficiency of time, road safety [9], dynamic warning systems [10-12], autonomous driving alarms [13-16], and evolution of smart cities [17], [18], as well as traffic management [19-21]. The VANET system will need to generate and share vast volumes of data with the various IoV entities, such as vehicles, pedestrians, and roadside infrastructure, in order to be able to secure such services.

Due to the open-channel nature of the wireless network used for this information exchange, the transmitted messages are susceptible to a number of security breaches that could compromise the confidentiality and privacy of the communicating parties' data through eavesdropping or even compromise the integrity of the transmitted messages by tampering with them before they reach their intended recipient [22-24].

On the other hand, industry and academia have recently become interested in the efficient features of blockchain technology. Decentralization, immutability, consensus, fault tolerance, and enhanced security are some of these traits [25–30]. Blockchain was initially recognized as the supporting technology for cryptocurrencies like Bitcoin. Although some of these surveys may have included a few blockchain- based authentication schemes in IoV, they did so in passing as a minor aspect of the larger subject of IoV security, and none of them offered a thorough survey that was solely focused on these schemes. The main contribution of this paper is: (I) By showcasing a variety of blockchain-based authentication techniques that have been put out in recent literature, we can emphasize the importance of blockchain technology in VANETs; (II) We talked about blockchain-based solutions while taking into account several aspects of VANET security, including application administration, key and certificate management, authenticity, control of access, and manage certificate and key; (III) We have identified a number of unresolved problems and challenges that need to be addressed in the context of blockchain-enabled VANET research initiatives.

The remainder of this paper is organized as follows. Section II introduces the background of this paper. Section III reviews blockchain based on security schemes. Section IV discusses the future direction of research. Ultimately, we discuss this work in Section V.

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.33

2. BACKGROUND

2.1 Vehicular Ad Hoc Network (VANET)

VANET is a group of vehicles that are connected by a wireless network and can be either moving or stationary [31]. VANETs were created with the goal of providing comfort and safety to drivers of moving cars [32]. This viewpoint is evolving since VANETs are increasingly regarded as the foundation of smart transportation systems that enable autonomous vehicles and any activity needing an Internet connection in the context of a smart city setting [33]. Additionally, VANETs make it possible for mobile computing cloud resources to run on computers inside of stationary cars, like those in airport parking lots, with the least amount of assistance from the Internet infrastructure. The stuff created and consumed by cars only has local application in terms of time, place, and the people who produce and consume it [34].

1) VANET Architecture: Figure 1 depicts the Trusted Authority (TA), Roadside Unit (RSU), and On-Board Unit (OBU) as the three main elements of the VANET architecture.

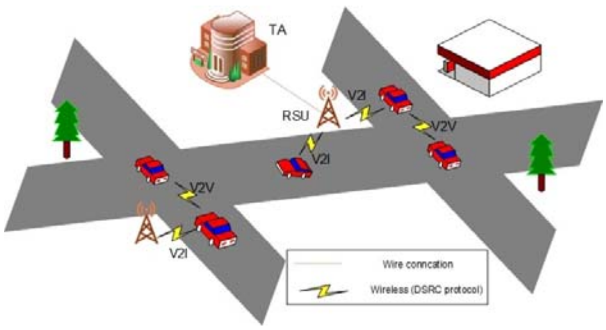

Fig. 1 Architecture in OMNeT++. [35], [36]

- TA: a dependable, competent third party in charge of registering other VANET components. It can safely connect to the RSUs over wired networks as well. All RSUs and vehicles must be registered with the TA before they can join a network [37], [38].
- RSU: Vehicle management device that is used on the side of the road and has a communication range. RSUs that send messages to the TA or local cars can check the veracity and authenticity of the message that was received [39], [40].
- OBU: The DSRC Protocol can be used by a vehicle with an OBU to communicate with other vehicles or RSUs. To prevent information from being exposed or leaked, each OBU has a tamper-proof device (TPD) [41].

2) Security Schemes Issues: Major security issues that a security scheme for VANET must address include the following:

- Key Management: Keys are required for the crypto-graphic algorithms used in VANET security. In such a dynamic environment, it is preferred to properly establish, maintain, and distribute keys.
- Latency Control: Every VANET application is delay-sensitive. For these real-time applications, security algorithms need to be quicker and more effective.
- Error Tolerance: Because VANET uses quick to receive and response times, security systems should be fault resilient.
- High Mobility: Although node of VANET has the similarity computational power and ability offer as wired communication devices, due to their rapid security, movement protocols must be executed more quickly to provide the same throughput.
- Data Consistency: Life-threatening circumstances could arise if a rogue node forges vital information. Therefore, a system should be developed to prevent any malicious activity that could lead to data inconsistency between authenticated and unauthenticated nodes.

3) Blockchain Technology: The VANET's adoption of blockchain technology must incorporate these methods.

- Proof-of-capacity (PoC): Instead of competing on the speed of PoW calculation, miners in this mechanism compete on the size of information saved by each of them.
- Proof-of-importance (PoI): The value of a user is determined by the quantity of money and the number of transactions that the user has completed.
- Proof-of-authority (PoA): That approach relies on authorized accounts verifying all blocks and transactions.
- Proof-of-work (PoW): During this phase, communication devices vie with one another to insert their block to the blockchain by solving a computationally challenging challenge. Applications of the PoW consensus algorithm includes Bitcoin, Litecoin, and Ethereum.
- Proof-of-stake (PoS): With this method, users receive mining privileges according to the number of cryptocurrencies they have stored on the blockchain network. Examples of PoS applications include PeerCoin, NXT, and Ethereum.

- Leased proof-of-stake (LPoS): A register can increase his profit by moving his balance to mining nodes that are being leased or rented.
- Delegated proof-of-stake (DPoS): The register with the highest funds can select their friends and authorize them for signing blocks in the system in this PoS version. It implies that the one who has the largest scales can use the votes of their patterns to their advantage.

4) Blockchain in VANET: The VANET is a sizable and heterogeneous network that consists of a sizable number of linked vehicles, roadside infrastructure, mobile personal de- vices, central and distributed storage, and computation servers in the event of combining cloud and edge computing plat- forms. This leaves the VANET network open to a variety of security attacks that could endanger the VANET applications like navigation, accident detection and notification, dynamic alternative routing, route optimization, and congestion management, all of which put drivers and passengers on the road in danger. This is in addition to the public Internet access and the open-channel wireless communication model, which constitute most of the communication.

Blockchain technology, on the other hand, has lately become popular as a decentralized storage mechanism in a variety of industrial applications due to its high capabilities in terms of distributed storage as well as privacy, performance, automation, security, and lower computing costs. Recently, blockchain has also been integrated into the VANET paradigm for a variety of uses, including forensic applications, resource trading, resource sharing, ridesharing, and data management. Blockchain technology has been incorporated into the IoV because of the many capabilities it can offer, which has encouraged industry and research to do so. The following are a few of these characteristics:

- Security and privacy: Blockchain’s adoption of crypto-graphic hash functions and digital signatures can guarantee the security of transaction data and the privacy of users who participate in VANET.
- Immutability: It is nearly hard to alter or tamper with the blockchain since fresh blocks of transactions must first be created and validated by all or most of the peers using various consensus processes before being added to it.
- Decentralization: In contrast to centralized storage platforms, where data storage and maintenance are handled by a reliable central node, blockchain technology exhibits a decentralized nature in which data records are maintained and managed by all participating entities.
- Traceability: Each transaction record is saved in the blockchain and given a timestamp to be added to the public ledger.
- Automation: Smart contracts are software scripts that can be run automatically in response to an event or when a predefined set of conditions is met, and blockchain technology promotes their adoption.

2.2 Challenges and Issues

In this section, we discuss some challenges and issues that need attention during implementing blockchin-based security schemes in VANET as follows.

- Mobility: Driving on the highways are autonomous auto- mobiles and autonomous driver-controlled vehicles. De- spite having considerable communication and processing capabilities, dependable communication is very challenging with vehicles because of their high mobility.
- Complexity: Several wireless technologies exist side by side. For V2V and V2I modes, DSRC is employed, while LTE/4G/5G is used to connect RSUs to one another.
- Decentralized consensus: Only a portion of each node’s surroundings is known to it. In a VANET environment that is this complicated, reaching a consensus is challenging.
- Storage Capability: For automotive communication systems to advance, massive data exchange and storage are necessary. The sophistication of the data supplied by automobiles is growing, which puts more pressure on data transmission. Due to a lack of resources, vehicles cannot achieve these requirements.
- Consensus Delay: The majority of system services require latency-sensitive functionality with short to average broadcast far. Services based emergencies and safeties in system are anticipated to need little transmission time, allowing for the avoidance of unforeseen circumstances.
- Propagation of blocks: Blockchain requires block propagation over the whole network in order to come to a consensus. To emphasize the dissemination of ledgers to all devices, there should be effective block propagation, taking VANET’s peculiarities into account.
- Transaction Throughput: The transaction rate is the number of transactions that are recorded on a blockchain every second. Due to the complexity of the consensus method, blockchain networks based on

Bitcoin may support seven transactions per second with a maximum one-hour time delay.

- Scalability: The price of constructing a standard blockchain public is highest since automobile networks are resource constrained. Network nodes only briefly communicate with one another. In addition, scalability is a crucial problem which should be solved in the systems-based public blockchain.

3. BLOCKCHAIN BASED ON SECURITY SCHEMES

This section studies how blockchain can be utilized to detect concerns according to the security of VANET in multiple aspects. The many components of security schemes enabled by the blockchain system are depicted in Figure 2.

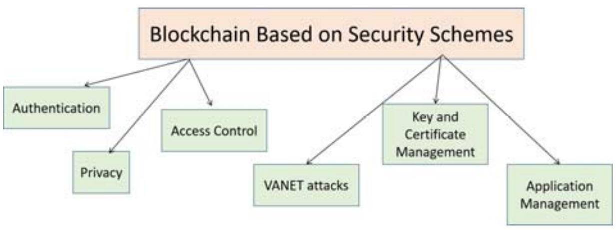

Fig. 2 Blockchain Based on Security Schemes.

3.1 Blockchain for Authentication in VANET

Vehicles use pseudonyms given by a centralized authority (CA) to connect with other communicative entities in a blockchain-based authentication system [42], [43]. This method safeguards vehicle identifying privacy while integrating a reliable communication environment across all internal misleading communications. However, because it does away with the requirement for a key authorization as in conventional methods, the distributed structure using blockchain technology is deemed safety and dependable.

RSUs serve as peer devices and create the blockchain system for identity authentication and revocation in the effective VANET [44]. The first RSU on the road receives an authentication request from a car as soon as it enters communication range. Table 1 provides a summary of authentication methods based on blockchain for VANET environments.

Table 1: AUTHENTICATION IN THE VANET ENVIRONMENT USING BLOCKCHAIN-BASED SCHEMES.

Authors	Main	Blockchain Data
Feng et al. [42]	VANET authentication mechanism with blockchain support	table of vehicle public keys
Lu et al. [43]	An authentication method that protects privacy	table of vehicle public keys
X. Feng et al. [44]	Authentication Mode that Protects Privacy	Certificates for vehicle pseudonyms

3.2 Blockchain for VANET attacks

This section presents numerous security options created with blockchain technology in the context of a VANET. All attacks in VANET have a Sybil attack as their primary source [45]. It's a type of forgery adversary in which a hacker creates a large number of bogus nodes in order to seize control of a network without authorization. As a result, the attacker is able to access the network simultaneously using all of the fake identities.

Over the past ten years, several specialists have worked to identify and prevent Sybil's assaults. However, as of yet, there is no surefire defense [46].

Blockchain technology can help VANET users resist replay assaults. In a blockchain-based VANET, each transaction has a distinct transaction identifier or txid. Consensus RSUs, therefore, disallow trans-actions involving the same identity [47].

A distributed public ledger that is updated by all network nodes functions as a secure means of message distribution that is given [48]. It is used to record the date of all cars' trust tops in addition to providing event notifications.

To ensure that blockchain features like scalability, timeliness of message dissemination, and trustworthiness of node and message passing are suitable for the VANET, the conventional blockchain can be modified by implementing a local blockchain with independent blockchains from different geographic regions [49].

3.3 Management of Vehicular Application

By exchanging traffic data over a VANET connection, such as information about road construction, traffic jam, trip adjustments owing to road congestion, etc., intelligent road management can be put into effect. Applications for the VANET must be implemented with regularly updated traffic data. For implementing these applications, the blockchain is one of the most promising technologies.

It is employed to protect the consensus mechanism from manipulation and to guarantee the accuracy of communications. In [50], a proof-of-event (PoE) for VANET is put out. This method uses RSUs to record traffic data, and after receiving the event alert, passing cars confirm the veracity of the message. PoW becomes problematic because correct modeling of block exchange is difficult. As a result, an analytical technique [51] is described that determines how mobility affects a blockchain-according to system's performance according to the like- lihood that a block will be added to the chain successfully and the quantity of blocks that are shared during a specific periodic frame.

Zhang et al. [52] tested the effect of movement on block broadcasting in a system with one-chain parameters. They investigated block propagation from a macro points before creating a related-form expression for one-block broadcasting date.

With the use of a novel technique called Proof of Driving (PoD) [53], blocks for blockchain-based VANET apps can now be effectively produced.

Tables 2 and 3 provide a summary of solutions for controlling automotive applications based on blockchain.

Table 2: SCHEMES BASED ON BLOCKCHAIN FOR MANAGING VEHICULAR APPLICATIONS.

Author	Type of Blockchain	Blockchain Data	Mining nodes	Consensus algorithm	Issue
Yu et al. [45]	Public	Messages of VANET	each car indepen- dently validating	PoW	Data authenticity, non- repudiation, and integrity
Mostafa et al. [46]	Public	data of ITS	RSUs	PoW	Data authenticity, non- repudiation, and integrity
Kang et al. [47]	Public	Messages of VANET	each node indepen- dently validating	PoW	Immutability attack
Shrestha et al. [48]	Public/Private	data of VANET	RSUs	Distributed consensus	DDoS attacks, data tampering, im- personation, replay attacks, and other security and privacy risks

Table 3: SCHEMES BASED ON BLOCKCHAIN FOR MANAGING VEHICULAR APPLICATIONS.

Authors	Main	Blockchain Data
Yang et al. [50]	Concept for proof-of-event consensus	The roadside units are used to collect traffic statistics.
Kim et al. [51]	Mobility's Effect on Blockchain Performance in VANET	Applications data for VANET
Zhang et al. [52]	The blockchain-based VANET's block propagation	data of VANET
Kudva et al. [53]	a reliable and expand- able consensus mechanism	Applications data for VANET

3.4 Privacy

The message's signature is nameless and signing by a specific parameter pantry of RSUs thanks to a system suggested by Lu et al. [43], [54] preserves the privacy of car positions. A distributed trust management strategy was presented by Bouksani et al. [54] in blockchain-based VANETs to assess the acceptability of the fogging vehicle for work offloading.

Liu et al. [55] offered a privacy-preserving conditionally announcement approach and a blockchain-based trust management paradigm. RSUs compute message depend- ability according to the reputation amount which are maintained on the blockchain for each vehicle.

A blockchain-based privacy-preserving method for automo- bile social networks was created by Pu al. [56]. A pseudonym- according to method that conceals the identitication of cars allows for the anonymization of nodes. A technique of rewarding and punishing cars for providing accurate data is proposed.

Lu et al. [57] proposed a federated learning-based ar- chitecture to address providers' privacy concerns. A hybrid blockchain architecture combines the local Directed Acyclic Graph and the permissioned blockchain (DAG).

Using blockchain technology, Ren et al. [58] introduced a public key signing method that protects user privacy. This method uses the least amount of computation time for batch signature aggregation and verification.

Table 5 presents a summary of VANET privacy protection techniques based on blockchain.

Table 4: BLOCKCHAIN-BASED TRUST MANAGEMENT STRATEGIES FOR VANET

Authors	Main	blockchain Data	Consensus algorithm
Yang et al. [60]	Management of vehic- ular communication	Vehicles with high trust values	PoW
Li et al. [61]	Management of vehic- ular communication	messages relat- ing to roads	PoW
Yin et al. [62]	Collaboration- based IoV incentive mechanism	vehicle sensor information	PoT
Singh et al. [63]	Safe and distinct crypto ID (IVTP)	Intelligent vehi- cle trust point isa safe and dis- tinct crypto ID (IVTP)	PoT
Luo et al. [64]	A trust-based location privacy protection system powered by blockchain	vehicles location	PoT
Gao et al. [65]	For the VANET sys- tem to function well, blockchain and SDN are essential.	Vehicles with high trust values	PoW

Li et al. [66]	a system for managing local trust	Vehicles with high trust values	PoW
Liu et al. [67]	For VANET, behaviour analysis and trust management	messages of safety	PoT

Table 5: SCHEMES BASED ON BLOCKCHAIN TO PROTECT PRIVACY IN VANET.

Authors	Main	Blockchain Data
Liu et al. [55]	Model of trust management based on blockchain	Reputational values for automobiles are securely kept in the blockchain.
Pu al. [56]	Create a privacy-preserving, effective, and efficient system for mobile social networks.	Vehicle IDs with aliases
Lu et al. [57]	Internet of Vehicles: Federated Learning for Secure information exchange	Exchange of car information for various VANET servicess
Ren et al. [58]	batch verification signature technique that protects privacy	data of VANET

3.5 Trust Management in VANET

In a VANET scenario, malicious vehicles may spread false safety warnings, compromising traffic efficiency and safety. A trust management strategy is therefore necessary for such a distrusted workplace. It is unrealistic to create centralized trust management systems. For V2V communication networks, [59] provides a distributed (TEAM) mechanism.

For vehicle networks, Yang et al. [60] developed a decentralized trust management system based on blockchain. Based on the messages it has received, each car generates a trust value for its nearby vehicles, which it then transmits to the associated RSU.

In addition to managing the trust, cars are encouraged to communicate safety messages, as stated in [61]. A network for reward vehicle announcements based on the blockchain is called CreditCoin. A mechanism called Echo Announcement is suggested to ensure the authenticity of notifications. In addition, a blockchain-according to incentive system [62] is suggested to motivate cars to distribute safety alerts by accumulating a set number of reputation points known as Coins.

A secure environment for vehicular communication enabled by blockchain technology was presented by Singh et al. [63]. The intelligent transportation system does not disclose private information through this decentralized approach.

Location-based services could leak your location information. Luo et al. [64] described a blockchain-according to trust-based privacy preserving method. Based on the Dirichlet distribution, this trust strategic plan assumes that automobiles will only cooperate with other cars they trust. Similar to this, [65] suggests a trust-based system that is supported by blockchain and SDN, where reputation ratings are given to cars which send messages while taking into consideration the information on trustworthiness offered by the linked cars.

The VANET's trust protocols have a variety of vulnerabilities, including the instability of trust values between area and the creation of phony trusted amounts by collaborating malevolent devices. To address these issues, a local trust management system [66] based on blockchain is developed.

A HMM-based model was created by Liu et al. [67] while taking into account previous vehicle behavior. This approach can assess trust and identify malevolent driving behavior in automobiles. In addition, a trust management system according to an alliance chain that outperforms typical public chains in terms of throughput and efficiency is also suggested.

Table 4 provides a list of blockchain-according to resolve for types of system trusted authentication strategies.

Your location may be compromised by location-based services. A blockchain-according to trusted-base privacy preserving method was described by Luo et al. [64]. This trust strategy plan bases its assumption that vehicles will only cooperate with other vehicles they trust on the Dirichlet distribution. In a manner similar to this, [65] proposes a trust-based system supported by blockchain and SDN, where reputation ratings are granted to vehicles that deliver messages while taking into account the information on trustworthiness provided by the linked cars.

A thorough access control mechanism is proposed [69] to satisfy the requirements for vehicle data security and dependability. In order to increase reliability, the system uses a simple load distribution module to cut down on the number of packets lost at RSUs during the penetration phase.

The categories of regulation server, service providers, blockchain, and automobiles make up the list of four essential components that are required for authentication. Combining these four elements results in a three-phase system with the enrolment step, authenticity step, and authorisation step. By utilising a intelligent contract, the Remix tool's authenticity procedure can use blockchain to safeguard the method's privacy and security.

3.6 Key and Certificate Management

For averting keys and credential reputation in systems, it is advised to adopt an identity-based key establishment [70]. This approach makes use of self-generated PKC-based pseudo IDs. In KGC creates the private partial keys (CL-

PKC). This architecture encourages the utilization of certificate-lessness cryptographies to avert key issues.

As demonstrated in Figure 3, Lei et al. [71] established a framework for safe key management on heterogeneous networks, including VANETs. In this architecture, SMs capture each vehicle's departure information and add management keys into the block by rekeying to the cars. In order to reduce the time it takes to transfer keys during vehicle handover, distributed key management using blockchain must first be developed.

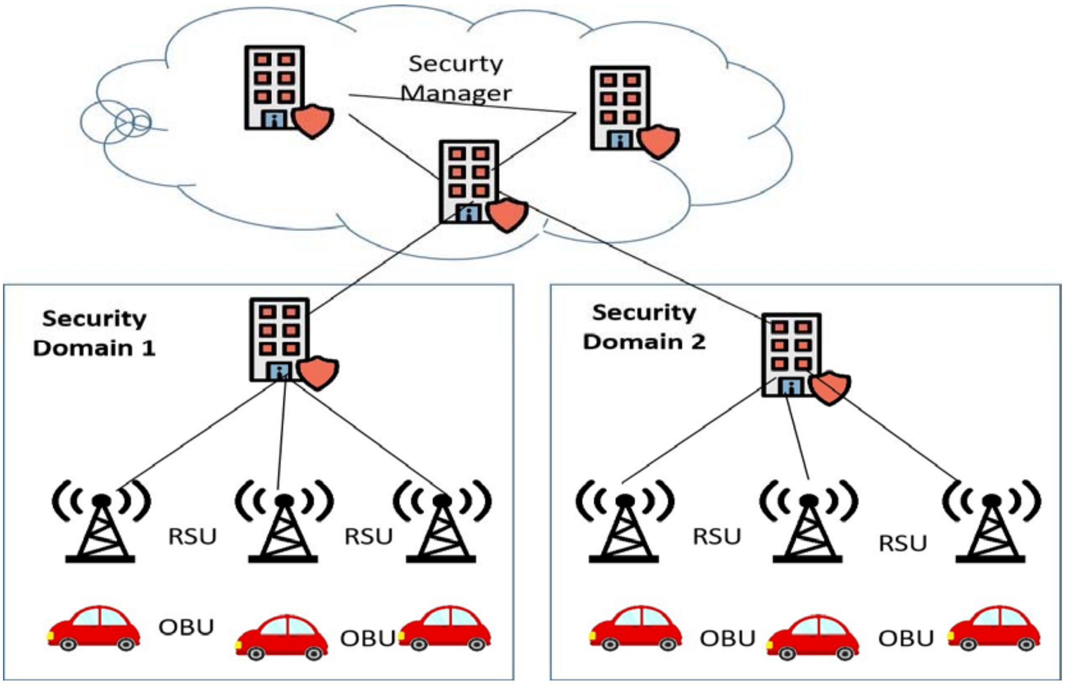

Fig. 3 A dynamic key management system based on blockchain.

4. FUTURE DIRECTION OF RESEARCH

This section discusses some research findings that came from an analysis of state-of-the-art and a survey of blockchain- based security schemes in VANET as follows.

- Application Aspect: VANET offers a wide variety of ap- plications. Based on these applications' traits and various quality of service (QoS) criteria, they can be distinguished from one another.
- Distributed Intelligence Aspect: A GPS, generate, save, and linked nodes are installed in every vehicle in the VANET. Due to the restricted resources available at each car, increased computation performance and reduced delay can be obtained by forming an alliance with other adjacent moving vehicles or immobile parked vehicles.
- Privacy Aspect: The network's transaction history is essential for reaching a consensus. However, it raises privacy issues because all transaction information is avail- able to authorized nodes, which increases the risk of a node's true identity being revealed.
- Reliability Aspect: Reliability considerations may have a negative impact on the performance of security algorithms. To address the reliability issues, new forms of dis- tributed architectures could be created using blockchain technology
- Integration Aspect: A hybrid vehicular architecture that uses blockchain technology as well as other technologies like 5G, SDN, and fog computing is possible. A significant obstacle to integrating different technologies in VANET is designing a secure and privacy-enabled

solution. Blockchain is an immutable, transparent technology that can be used as a security scheme.

- Security Aspect: It is common knowledge that blockchain is more secure than traditional network systems due to its distributed structure. However, there is a chance of a 51 percent attack, which could have unexpected effects.
- Resource Management Aspect: As there are many transactions on each vehicle in the blockchain system, this uses up more energy, data storage, and transmission resources. Consensus techniques in blockchain systems need a lot of resources. For example, PoW needs a lot of mathematical calculations, but PoS and DPoS may use fewer resources but have security issues.
-

5. CONCLUSION

In this paper, security issues related to VANET and upcoming vehicular technology that has advanced ITS were reviewed. It also emphasized the power of the newly developed blockchain technology in general and in VANET particularly. Also discussed were various security requirements, difficulties, and potential security intrusions and threats in automotive networks. The discussion of a variety of contemporary blockchain-based authentication solutions in VANETs contexts was then given additional attention, and a thorough comparison between them was then given. Last but not least, some potential security issues and future research paths in VANETs were emphasized. We believe that adding more quantitative measurements to comparisons is one strategy that could be used and improved in upcoming surveys. We think this work will support the development of blockchain-according to security methods for system scenarios and will stimulate different elements of both blockchain and VANET security.

References

[1] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Ali A Yassin. Vppcs: Vanet-based privacy-preserving communica- tion scheme. IEEE Access, 8:150914–150928, 2020.

[2] Mahmood A Al-Shareeda, Mohammed Anbar, Iznan Husainy Hasbullah, Selvakumar Manickam, and Sabri M Hanshi. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. IEEE Access, 8:144957–144968, 2020.

[3] Mahmoud Al Shareeda, Ayman Khalil, and Walid Fahs. Realistic heterogeneous genetic-based rsu placement solution for v2i networks. Int. Arab J. Inf. Technol., 16(3A):540–547, 2019.

[4] Mahmood A Al-shareeda, Mohammed Anbar, Iznan H Hasbullah, Selvakumar Manickam, Nibras Abdullah, and Mustafa Maad Hamdi. Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets). In 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), pages 394–398. IEEE, 2020.

[5] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Review of prevention schemes for man-in- the-middle (mitm) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10, 2020.

[6] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Review of prevention schemes for modification attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10, 2020.

[7] Mustafa Maad Hamdi, Ahmed Shamil Mustafa, Hussain Falih Mahd, Mohammed Salah Abood, Chanakya Kumar, and Mahmood A Al- shareeda. Performance analysis of qos in manet based on ieee 802.11 b. In 2020 IEEE international conference for innovation in technology (INOCON), pages 1–5. IEEE, 2020.

[8] Rasheed Hussain, Donghyun Kim, Junggab Son, Jooyoung Lee, Chaker Abdelaziz Kerrache, Abderrahim Benslimane, and Heekuck Oh. Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds. IEEE Internet of Things Journal, 5(4):2441– 2448, 2018.

[9] Wan-Jung Chang, Liang-Bi Chen, and Ke-Yu Su. Deepcrash: a deep learning-based internet of vehicles system for head-on and single-vehicle

accident detection with emergency notification. IEEE Access, 7:148163– 148175, 2019.

[10] Gunasekaran Raja, Priyanka Dhanasekaran, Sudha Anbalagan, Aish- warya Ganapathisubramaniyan, and Ali Kashif Bashir. Sdn-enabled traffic alert system for iov in smart cities. In IEEE INFOCOM 2020- IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 1093–1098. IEEE, 2020.

[11] Rayan Nouh, Madhusudan Singh, and Dhananjay Singh. Safedrive: Hybrid recommendation system architecture for early safety predication using internet of vehicles. Sensors, 21(11):3893, 2021.

[12] Lien-Wu Chen and Hsien-Min Chen. Driver behavior monitoring and warning with dangerous driving detection based on the internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(11):7232–7241, 2020.

[13] Ali Hassan Sodhro, Joel JPC Rodrigues, Sandeep Pirbhulal, Noman Zahid, Antoˆnio Roberto L de Macedo, and Victor Hugo C de Albu- querque. Link optimization in software defined iov driven autonomous transportation system. IEEE Transactions on Intelligent Transportation Systems, 22(6):3511–3520, 2020.

[14] Cunqian Yu, Bin Lin, Ping Guo, Wei Zhang, Sen Li, and Rongxi He. Deployment and dimensioning of fog computing-based internet of vehicle infrastructure for autonomous driving. IEEE Internet of Things Journal, 6(1):149–160, 2018.

[15] Nishu Gupta, Arun Prakash, and Rajeev Tripathi. Internet of Vehicles and its Applications in Autonomous Driving. Springer, 2021.

[16] Hao Du, Supeng Leng, Fan Wu, Xiaosha Chen, and Sun Mao. A new vehicular fog computing architecture for cooperative sensing of autonomous driving. IEEE Access, 8:10997–11006, 2020.

[17] Li-Minn Ang, Kah Phooi Seng, Gerald K Ijemaru, and Adamu Murtala Zungeru. Deployment of iov for smart cities: Applications, architecture, and challenges. IEEE access, 7:6473–6492, 2018.

[18] Umar Zakir Abdul Hamid, Hairi Zamzuri, and Dilip Kumar Limbu. Internet of vehicle (iov) applications in expediting the implementation of smart highway of autonomous vehicle: A survey. In Performability in Internet of Things, pages 137–157. Springer, 2019.

[19] Tej Tharang Dandala, Vallidevi Krishnamurthy, and Rajan Alwan. Inter- net of vehicles (iov) for traffic management. In 2017 International con- ference on computer, communication and signal processing (ICCCSP), pages 1–4. IEEE, 2017.

[20] V Vijayaraghavan and J Rian Leevinson. Intelligent traffic management systems for next generation iov in smart city scenario. In Connected vehicles in the Internet of Things, pages 123–141. Springer, 2020.

[21] Zahid Khan, Anis Koubaa, and Haleem Farman. Smart route: Internet- of-vehicles (iov)-based congestion detection and avoidance (iov-based cda) using rerouting planning. Applied Sciences, 10(13):4541, 2020.

[22] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, Iznan H Hasbullah, Nibras Abdullah, Mustafa Maad Hamdi, and Ahmed Shakir Al-Hiti. Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets). Appl. Math, 14(6):1–10, 2020.

[23] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. Sen- sors, 22(5):1696, 2022.

[24] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Se-cppa: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. Sensors, 21(24):8206, 2021.

[25] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah.

Password-guessing attack-aware authentication scheme based on chinese remainder theorem for 5g-enabled vehicular networks. Applied Sciences, 12(3):1383, 2022.

[26] Mahmood A Al-shareeda, Murtadha A Alazzawi, Mohammed Anbar, Selvakumar Manickam, and Ahmed K Al-Ani. A comprehensive survey on vehicular ad hoc networks (vanets). In 2021 International Conference on Advanced Computer Applications (ACA), pages 156–160. IEEE, 2021.

[27] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, Iznan H Hasbullah, Ayman Khalil, Murtadha A Alazzawi, and Ahmed Shakir Al-Hiti. Proposed efficient conditional privacy-preserving authentication scheme for v2v and v2i communications based on elliptic curve cryptography in vehicular ad hoc networks. In International Conference on Advances in Cyber Security, pages 588–603. Springer, 2020.

[28] Mahmood A Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J Alzahrani, Gharbi Alshammari, Amer A Sallam, and Khalil Almekhlafi. Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks. Applied Sciences, 12(12):5939, 2022.

[29] Mahmood A Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J Alzahrani, Gharbi Alshammari, Amer A Sallam, and Khalil Almekhlafi. Cm-cppa: Chaotic map-based conditional privacy-preserving authenti- cation scheme in 5g-enabled vehicular networks. Sensors, 22(13):5026, 2022.

[30] Mahmood A Al-Shareeda and Selvakumar Manickam. Security methods in internet of vehicles. arXiv preprint arXiv:2207.05269, 2022.

[31] MAASM Mahmood A Al-shareeda, Mohammed Anbar, Murtadha A Alazzawi, Selvakumar Manickam, and Iznan H Hasbullah. Security schemes based conditional privacy-preserving in vehicular ad hoc net- works. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), 2020.

[32] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, Ayman Khalil, and Iznan Husainy Hasbullah. Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. IEEE Access, 9:121522–121531, 2021.

[33] Mustafa Maad Hamdi, Lukman Audah, Sami Abduljabbar Rashid, and Mahmood Al Shareeda. Techniques of early incident detection and traffic monitoring centre in vanets: A review. J. Commun., 15(12):896–904, 2020.

[34] Mahmood A Al-Shareeda, Mohammed Anbar, Iznan Husainy Has- bullah, and Selvakumar Manickam. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal, 21(2):2422–2433, 2020.

[35] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehic- ular ad hoc network. Symmetry, 12(10):1687, 2020.

[36] Mahmood A Al-Shareeda, Mohammed Anbar, Murtadha A Alazzawi, Selvakumar Manickam, and Ahmed Shakir Al-Hiti. Lswbvm: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. IEEE Access, 8:170507–170518, 2020.

[37] Murtadha A Alazzawi, Hasanain AH Al-behadili, Mohsin N Srayyih Al- malki, Aqeel Luaibi Challoob, and Mahmood A Al-shareeda. Id-ppa: robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network. In International Conference on Advances in Cyber Security, pages 80–94. Springer, 2020.

[38] Mahmood A. Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J. Alzahrani, Gharbi Alshammari, Amer A. Sallam, and Khalil Almekhlafi. Provably secure with efficient data sharing scheme for fifth-

generation (5g)-enabled vehicular networks without road-side unit (rsu). Sustain- ability, 14(16):9961, 2022.

[39] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Access, 2021.

[40] Mahmoud Al Shareeda, Ayman Khalil, and Walid Fahs. Towards the optimization of road side unit placement using genetic algorithm. In 2018 International Arab Conference on Information Technology (ACIT), pages 1–5. IEEE, 2018.

[41] Yang Ming and Xiaoqin Shen. Pcpa: A practical certificateless con- ditional privacy preserving authentication scheme for vehicular ad hoc networks. Sensors, 18(5):1573, 2018.

[42] Qi Feng, Debiao He, Sherali Zeadally, and Kaitai Liang. Bpas: Blockchain-assisted privacy-preserving authentication system for vehic- ular ad hoc networks. IEEE Transactions on Industrial Informatics, 16(6):4146–4155, 2019.

[43] Zhaojun Lu, Qian Wang, Gang Qu, Haichun Zhang, and Zhenglin Liu. A blockchain-based privacy-preserving authentication scheme for vanets. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27(12):2792–2801, 2019.

[44] Xia Feng, Qichen Shi, Qingqing Xie, and Lu Liu. An efficient privacy- preserving authentication model based on blockchain for vanets. Journal of Systems Architecture, 117:102158, 2021.

[45] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. Detecting sybil attacks in vanets. Journal of Parallel and Distributed Computing, 73(6):746–756, 2013.

[46] Ahmad Mostafa. Vanet blockchain: A general framework for detecting malicious vehicles. J. Commun., 14(5):356–362, 2019.

[47] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, and Jun Zhao. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3):2906–2920, 2019.

[48] Rakesh Shrestha, Rojeena Bajracharya, Anish P Shrestha, and Se- ung Yeob Nam. A new type of blockchain for secure message exchange in vanet. Digital communications and networks, 6(2):177–186, 2020.

[49] Adnan Shahid Khan, Kuhanraj Balan, Yasir Javed, Seleviawati Tarmizi, and Johari Abdullah. Secure trust-based blockchain architecture to prevent attacks in vanet. Sensors, 19(22):4954, 2019.

[50] Yao-Tsung Yang, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, and Chien-Chang Liu. Blockchain-based traffic event validation and trust verification for vanets. IEEE Access, 7:30868–30877, 2019.

[51] Seungmo Kim. Impacts of mobility on performance of blockchain in vanet. IEEE Access, 7:68646–68655, 2019.

[52] Xuefei Zhang, Wenbo Xia, Xiaochen Wang, Junjie Liu, Qimei Cui, Xiaofeng Tao, and Ren Ping Liu. The block propagation in blockchain-based vehicular networks. IEEE Internet of Things Journal, 9(11):8001– 8011, 2021.

[53] Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Albert Zomaya. Towards secure and practical consensus for blockchain based vanet. Information Sciences, 545:170–187, 2021.

[54] Walid Bouksani and Boucif Amar Bensaber. Rin: A dynamic pseudonym change system for privacy in vanet. Concurrency and computation: Practice and Experience, 31(24):e4719, 2019.

[55] Xingchen Liu, Haiping Huang, Fu Xiao, and Ziyang Ma. A blockchain- based trust management with conditional privacy-preserving announcement scheme for vanets. IEEE Internet of Things Journal, 7(5):4101– 4112, 2019.

[56] Yuwen Pu, Tao Xiang, Chunqiang Hu, Arwa Alrawais, and Hongyang Yan. An efficient blockchain-based privacy preserving scheme for

vehicular social networks. Information Sciences, 540:308–324, 2020.

[57] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology, 69(4):4298–4311, 2020.

[58] Yanli Ren, Xiangyu Li, Shi-Feng Sun, Xingliang Yuan, and Xinpeng Zhang. Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks. Journal of Information Security and Applications, 58:102698, 2021.

[59] Ming-Chin Chuang and Jeng-Farn Lee. Team: Trust-extended authenti- cation mechanism for vehicular ad hoc networks. IEEE systems journal, 8(3):749–758, 2013.

[60] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2):1495–1505, 2018.

[61] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xian- gliang Zhang, and Zonghua Zhang. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems, 19(7):2204–2220, 2018.

[62] Bo Yin, Yulei Wu, Tianshi Hu, Jiaqing Dong, and Zexun Jiang. An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains. IEEE Internet of Things Journal, 7(3):1582–1593, 2019.

[63] Madhusudan Singh and Shiho Kim. Branch based blockchain technology in intelligent vehicle. Computer Networks, 145:219–231, 2018.

[64] Bin Luo, Xinghua Li, Jian Weng, Jingjing Guo, and Jianfeng Ma. Blockchain enabled trust-based location privacy protection scheme in vanet. IEEE Transactions on Vehicular Technology, 69(2):2034–2048, 2019.

[65] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks. IEEE Internet of Things Journal, 7(5):4278–4291, 2019.

[66] Fuliang Li, Zhenbei Guo, Changsheng Zhang, Weichao Li, and Yi Wang. Atm: an active-detection trust mechanism for vanets based on blockchain. IEEE Transactions on Vehicular Technology, 70(5):4011– 4021, 2021.

[67] Han Liu, Dezhi Han, and Dun Li. Behavior analysis and blockchain based trust management in vanets. Journal of Parallel and Distributed Computing, 151:61–69, 2021.

[68] Hui Li, Lishuang Pei, Dan Liao, Song Chen, Ming Zhang, and Du Xu. Fadb: A fine-grained access control scheme for vanet data based on blockchain. IEEE Access, 8:85190–85203, 2020.

[69] Rohit Sharma and Suchetana Chakraborty. B2vdm: blockchain based vehicular data management. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 2337–2343. IEEE, 2018.

[70] Chengzhe Lai and Yuhan Ding. A secure blockchain-based group mobility management scheme in vanets. In 2019 IEEE/CIC International Conference on Communications in China (ICCC), pages 340–345. IEEE, 2019.

[71] Ao Lei, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P Anyigor Ogah, and Zhili Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6):1832–1843, 2017.

Zeyad Ghaleb Al-Mekhlafi received the B.Sc. degree in computer science from the University of Science and Technology, Yemen, in 2002, the M.Sc. degree in computer science from the Department of Communication Technology and Network, Universiti National Malaysia (UKM), in 2011, and the Ph.D. degree from the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in 2018. He is currently a Lecturer with the University of Ha'il, where he is also an Assistance Professor with the Faculty of Computer Science and Engineering. His current research interests include wireless sensor networks, energy management and control for wireless networks, time synchronization, bio-inspired mechanisms, and emerging wireless technologies standard.