Journal of Basrah Researches (Sciences) **50**(1), 223 (2024)
DOI: https://doi.org/10.56714/bjrs.50.1.19

Main Primitive and Cryptography Tools for Authentication in VANET Environment: Literature Review

Zahraa Sh. Alzaidi, Ali A. Yassin*, Zaid Ameen Abduljabbar

Department of Computer science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq.

ARTICLE INFO

Received 25 March 2024
Accepted 03 May 2024
Published 30 June 2024

Keywords:

VANET, Authentication, Security, Integrity, Blockchain, Fog Computing.

Citation: Zahraa S. A., et al., J. Basrah Res. (Sci.) **50**(1), 222 (2014).
DOI:https://doi.org/10.56714/bjrs.50.1.19

ABSTRACT

Vehicular ad hoc networks (VANETs) provide the potential to improve transportation efficiency by facilitating the sharing of traffic information among vehicles. Acceptance of VANET depends on communication speed and accuracy as well as privacy protection guaranteeing an individual's safety. Vehicle authentication is necessary to ensure message correctness. This necessitates the implementation of an effective privacy-preserving authentication scheme, as well as the need for both secrecy and timebound delivery of messages. Various privacy-preserving authentication schemes have been suggested to guarantee the integrity of messages in communications. However, most of the schemes are not able to solve issues related to computing costs, communication, security, privacy, threats, and vulnerabilities. In this review, we focus on cryptographic strategies that are suggested to accomplish privacy and authentication, such as identity-based, public key cryptography-based, pseudonym-based, and blockchain-based schemes. We provide a thorough analysis of schemes, including their categorizations, advantages, and drawbacks. The study demonstrates that the majority of current authentication techniques necessitate trusted authorities that lack transparency in their operations. Additionally, authentication process incurs substantial computational and communication overhead, leading to a considerable impact on the timely delivery of messages. More efforts are required to enhance the development of efficient authentication schemes in VANETs.

1. Introduction

The developments and improvements of intelligent transportation systems (ITS) have garnered a lot of attention lately from both corporate and academic organizations. ITS are important for improving traffic flow, offering entertainment services in vehicles, and increasing road safety [1].

***Corresponding author email :** ali.yassin@uobasrah.edu.iq

N: 1817-2695 (Print); 2411-524X (Online)
line at: https://jou.jobrs.edu.iq

The vehicle industry is aware that wireless communication technologies must be installed in vehicles in order to provide intra-vehicle and infrastructure communication. Such communications have the capacity to significantly improve traffic flow and safety [2]. Consequently, the use of embedded sensors has facilitated the exchange of traffic data among neighboring vehicles, including driving patterns, traffic flow measurements, and driving circumstances, via the establishment of networks known as VANETs.

VANET is a road-route-based version of Mobile Ad hoc Network, or MANET [3, 4], maintaining traffic safety, increasing traffic flow, and optimizing the entire driving experience are its primary objectives. Trusted authorities (TAs) are responsible for the registration and administration of roadside units (RSUs) and on-board units (OBUs) [5]. Each vehicle has OBUs built in to act as transmitters, enabling communication with other moving vehicles. In contrast, RSUs are positioned next to network equipment along the curbside, network equipment for dedicated short-range communications (DSRC) [6] are housed in RSUs, which are used to connect to infrastructure. VANETs are classified into two categories: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [7, 8]. Vehicles have the capability to create intercommunication via a V2V system in order to share data pertaining to traffic. The interchange of traffic data is facilitated by V2I technology, enabling direct interaction between cars and infrastructure. WAVE, which stands for wireless access in vehicle settings and enables wireless communication utilizing the IEEE 802.11p standard, is a common abbreviation for the DSRC protocol. At intervals of 100–300 ms, the vehicle sends out informative signals to nearby vehicles or RSUs. VANETs are limited to a communication range of one kilometer and a transmission speed of six to twenty-seven megabits per second (Mbps) according to the DSRC standard. Communications are divided into two groups: non-safety communications and safety messaging. Through the use of V2V communication, the vehicle processes, exchanges, transmits, or receives important signals about traffic conditions from other Vehicles. Using Infrastructure-to-Vehicle (I2V) and V2I communication protocols, vehicles and RSUs establish contact. RSUs provide drivers access to real-time services including internet browsing, live accident streaming, and navigation [9].

The broadcast of safety signals from one vehicle to another that is far away is made possible by an in-range vehicle. If the message cannot be sent by an intermediate vehicle, the sender may choose to use a different vehicle to relay the message. Because VANET has the energy and storage capacity to support all vehicles, it can transmit information about accidents, emergencies, and traffic congestion to neighboring components more easily [10, 11]. vehicles are equipped to convey important information about road conditions in addition to safety alarms. This makes it possible for the recipient to move toward safer methods to reduce accidents or handle input from other individuals [12, 13]. An attacker is able to intercept, change, copy, or remove communications while they are being sent over an open wireless channel. To injure drivers of vehicles, for example, a criminal may alter safety-related messages to ones that cause accidents. Moreover, it may create an illusion of traffic congestion, which might interfere with the network's ability to operate normally [14]. In order to effectively counter the threats that the attacker may pose, VANET must have an appropriate mechanism and communication protocols. Prior to using VANET, the aforementioned security obstacles such as authentication and privacy concerns need to be addressed.

Researchers have taken attention of VANETs' top-notch ability in ITS control. When it comes to node mobility, community structure, and channel unreliability, the implementation techniques for ITS, VANETs, and MANETs differ from one another. Because of their intense mobility and instability, VANETs are vulnerable to attacks from each internal and external attacks. Security, privacy, and authentication are just a few of the challenges that the aforementioned assaults offer to the creation of steady VANETs [15].

VANETs face a number of privacies, and authentication-related security issues. Furthermore, the existence of dubious vehicles leads to additional security and communication problems. Because of its open access communication environment, VANETs are vulnerable to several types of attacks. As a result, a malevolent person may modify, intercept, add, and delete messages. For example, bad people may get access to traffic communications, which are used to direct vehicles on the road. These messages may be altered by an attacker, making it possible for false information to be sent on the road and leading to accidents, gridlock, and other hazards [16].

This study's main goal is to analyze, assess, and draw attention to the limitations of some authentication and privacy-preserving strategies that have been proposed recently. This study investigates basic requirements in the field of VANET security in more detail. The following is a brief summary of the main contributions of the present study:

- We presented a thorough analysis of the existing privacy-preserving and secure authentication systems on VANETs. This paper provides a description of their schemes and strategies to help understand both their advantages and weaknesses.
- We have also presented the overview of basic architecture and properties of VANET along with the types of Attack and security requirement.
- Inclusion of tools and programs like Scyther, Ganache, and MetaMask for assessing system effectiveness.
- This study seeks to clarify the many tools used in this field as well as cryptographic methods, such as hash functions and Elliptic Curve Cryptography (ECC) technologies.
- We have provided a comprehensive survey on the existing secure authentication and privacy-preserving schemes in VANETs. This article also describes their methods and strengths briefly to understand their achievements as well as weaknesses.
- We have classified the existing schemes into different categories based on the cryptographic techniques applied to achieve security and privacy. It helps to interpret their mechanisms and benefits in the VANET environment.
- We have given brief information about the existing surveys based on authentication and privacy-preserving schemes. We have also given a comparison of the present survey with the existing surveys considering the security mechanisms used.
- In the end, we have provided a summary of cryptographic methods used in VANETs along with their key features and drawbacks.

This paper is structured as follows: Section 1 presents the study's introduction. Section 2 discusses the primitive tools utilized in VANETs. Section 3 elaborates on various threat models, while Section 4 explores security requirements in depth. In Section 5, the system architecture is detailed, encompassing aspects such as the system model, integration of blockchain, and fog computing. Section 6 examines related surveys on security and privacy in VANET schemas. Lastly, Section 7 concludes the paper.

2. Primitive tools

2.1. Elliptic Curve Cryptography ECC

ECC is a widely adopted public-key cryptosystem that leverages the mathematical properties of elliptic curves to ensure the security of digital communications and transactions, offering distinct advantages over conventional asymmetric encryption algorithms like RSA or DSA. It stands as a cornerstone of contemporary cryptography, exhibiting numerous benefits over traditional asymmetric encryption methods such as RSA or DSA.

ECC relies on the algebraic structure of finite fields' elliptic curves, utilizing points on these curves for cryptographic operations. Its security hinges on the complexity of the elliptic curve discrete logarithm problem, which involves deriving a specific point Q from another point P and the outcome of multiplying P by a secret integer d. The ECC representation can be succinctly expressed through the congruence equation: E： $y^2 = x^3 + ax + b \pmod p$, where the constants a and b belong to the finite field $\mathbb{F}p$, ensuring the non-singularity of the elliptic curve, as indicated by the property $4a^3 + 27b^2 \neq 0$. Additionally, there exists a unique point denoted as O, recognized as the point at infinity (or zero point). The Ep (a,b) establishes an abelian or commutative group through addition modulo p.

Key operations within ECC include point addition, point doubling, and scalar multiplication, all of which demonstrate computational efficiency. One of ECC's notable advantages over RSA is the utilization of smaller key sizes for equivalent security levels. This characteristic leads to faster

computation times and reduced storage and bandwidth requirements in ECC compared to RSA [17]. Fig. 1. illustrates the addition of points on the Elliptic Curve.

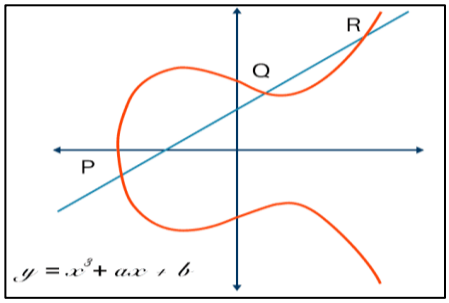


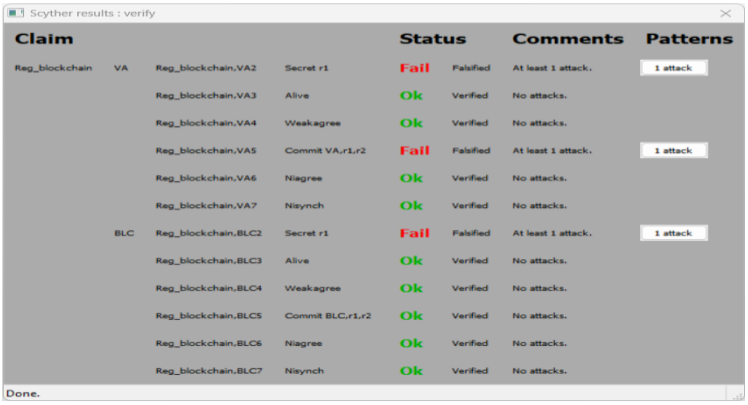
Fig. 1. Combining points on the elliptic curve[17].

2.2. SHA-256

A technique for reducing messages of different lengths into code of a fixed length is called a one-way hash function. It stands out for its unique features, which include creating output with a set duration and making it impossible to retrieve the original text. As such, it is a powerful tool that may be used to achieve security goals. 2001 saw the release of the Secure Hash Algorithm 2 (SHA-2) program and the National Security Agency. Six hash algorithms of the SHA-2 family are intended to produce digests (hash values) of 224, 256, 384, or 512 bits. Safe password hashing is one of the many popular security methods and applications that make extensive use of the SHA-2 hash algorithm. Integrity preservation is ensured by using SHA-2 [18].

2.3. Scyther

This tool is used for formal security analysis to evaluate the security and correctness of communication messages. The assurance given guarantees the implementation's security against known threats. The Security Protocol Description Language (SPDL), which defines the numerous roles, protocols, and the sending and receiving of messages between various entities, is the linguistic framework that is used in the current [19]. Additionally, it offers a computational framework for simulating key cryptographic operations, including encryption, decryption, hashing, and digital signatures, across both symmetric and asymmetric cryptosystems [20]. The graphical user interface of the Scyther is illustrated in Fig. 2. Two approaches are available for verifying schemes in Scyther, as outlined below [21]:


Scyther results : verify

Claim				Status		Comments	Patterns
Reg_blockchain	VA	Reg_blockchain,VA2	Secret r1	Fail	Falsified	At least 1 attack.	1 attack
		Reg_blockchain,VA3	Alive	Ok	Verified	No attacks.	
		Reg_blockchain,VA4	Weakagree	Ok	Verified	No attacks.	
		Reg_blockchain,VA5	Commit VA,r1,r2	Fail	Falsified	At least 1 attack.	1 attack
		Reg_blockchain,VA6	Niagree	Ok	Verified	No attacks.	
		Reg_blockchain,VA7	Nisynch	Ok	Verified	No attacks.	
	BLC	Reg_blockchain,BLC2	Secret r1	Fail	Falsified	At least 1 attack.	1 attack
		Reg_blockchain,BLC3	Alive	Ok	Verified	No attacks.	
		Reg_blockchain,BLC4	Weakagree	Ok	Verified	No attacks.	
		Reg_blockchain,BLC5	Commit BLC,r1,r2	Ok	Verified	No attacks.	
		Reg_blockchain,BLC6	Niagree	Ok	Verified	No attacks.	
		Reg_blockchain,BLC7	Nisynch	Ok	Verified	No attacks.	

Done.

Fig. 2. The parameters of Scyther.

- Verification Claim: Security attributes concerning claim events can be specified using Scyther's input language. Within a role definition, assertions may be made regarding the confidentiality (secrecy) of certain values or the expected qualities of communication partners (authentication). Scyther's functionality enables the confirmation or rejection of specific characteristics.

- Automatic Claim: In cases where a protocol specification lacks explicit security claims, Scyther can autonomously generate them. Verification claims are associated with each role, stipulating that the purported communication partners must adhere to the protocol as intended. All locally generated values and parameters are subject to confidentiality claims, which are also encompassed within the scope of the document. Scyther examines the expanded protocol definition akin to the aforementioned scenario, facilitating rapid analysis of a technique's strengths and weaknesses. This capability allows users to expediently investigate protocol properties using the Scyther utility.

Several parameters are used to evaluate the security of proposed protocols in Scyther:

- Non-Injective Synchronization (Nisynch): This parameter ensures that messages are sent and received according to the specifications of the protocol. It verifies that once the initiator (A) completes the protocol with the responder (B), and vice versa, all messages are received exactly as they were sent, adhering to the protocol's sequence.
- Non-injective agreement (Niagree): Suppose two entities want to communicate securely with one another. The Niagree option returns OK if sender A uses the protocol with recipient B and recipient B utilizes the protocol with sender A.
- Aliveness (Alive): An originator A can only be certain of an agent B's aliveness if A executes the protocol, most likely in cooperation with responder B, who has already done so.
- Weak agreement, also known as Weakagree, is a protocol feature that guarantees a weak agreement between an originator A and another agent B, given that A completes a protocol run successfully, most likely with responder B who has already completed the protocol run with A. It is important to emphasize that B's identity as the respondent is still unknown.

The metrics listed above serve as critical indicators of the security and effectiveness of the proposals, providing insightful information about how well they can resist and recover from various security threats and vulnerabilities.

2.4. Ganache

The Ganache platform is a robust and effective Ethereum blockchain answer designed for the cause of records storage and deployment. This platform permits developers and organizations to safely and customizable design, test, and install smart contracts and decentralized programs (dApps) over a private blockchain community. Ganache’s seamless integration with the Ethereum Virtual Machine (EVM) enables builders to take benefit of the whole variety of features offered via the Ethereum platform. This includes the use of Ethereum’s indigenous currency (Ether) as well as Ethereum-related smart contracts and decentralized applications (dApps) [22]. Fig. 3. shows the Ganache graphical user interface. Ganache has many features that make it ideally suited for data storage and application purposes. Using a local development network allows developers to test smart contracts and applications separately. Avoiding connections to the main Ethereum network reduces the risk of exposing sensitive data during the development process. Ganache can simulate network conditions such as latency and congestion, thereby helping developers analyze the performance and scalability of applications. In functional applications, efficient and secure data storage and retrieval is essential. The Ganache platform has a variety of built-in data protection features. A secure key management system allows developers to generate and manage account private keys, which are used to restrict access to blockchain data. Additionally, Ganache includes encryption and multifactor authentication mechanism to enhance data security.

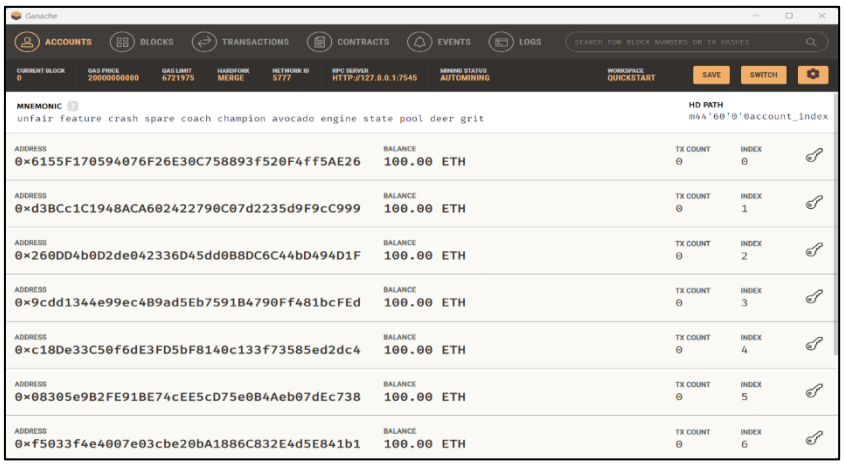


Fig. 3. Ganache Dashboard.

2.5. Truffle

When creating Ethereum smart contracts, the truffle is a crucial resource. Smart contracts are written in the solidity programming language. Truffle is considered by many to be an essential part in developing decentralized Ethereum blockchain applications. You may install it by using the command $npm install –g ruffle [23].

2.6. MetaMask

Google Chrome was designed to be compatible with the MetaMask browser plugin. As seen in Fig. 4., it is an essential prerequisite for interacting with the Ethereum network. The Ethereum blockchain cannot be used without a download from the Google Chrome Web Store, since current browsers do not allow blockchain connections by default. Setting up MetaMask makes it simpler to connect to blockchain networks by transforming the browser into a platform that can support blockchain technology [24]. Furthermore, on systems like Ganache, MetaMask is essential to project deployment and user account management. Furthermore, without requiring users to execute the whole Ethereum blockchain, MetaMask acts as a gateway to the distributed web, enabling them to instantly access Ethereum Decentralized Applications (DApps) in their browser [25]. One of the main features of MetaMask is its strong identity vault, which offers an easy-to-use interface for managing online identities and carrying out blockchain transactions. This feature-rich addon works with web browsers such as Chrome, Firefox, and Opera, ensuring wide accessibility and ease of usage.

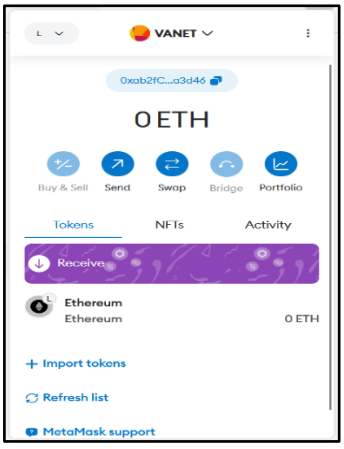


Fig. 4. GUI of the MetaMask.

3. Threat model

Adversaries in the context of VANETs may be broadly categorized as internal or external attackers. While external attackers operate destructively from outside the VANET framework, causing significant harm to the system, internal attackers participate in hostile actions inside the VANET system. Our main goal is to fortify the VANET system in order to shield it from internal and external assaults. Several attack modalities, illustrating the diversity and severity of potential threats, have been delineated, with particular emphasis on external assailants and their potentially far-reaching consequences. Notably, an internal attack considers a greater threat than an external one due to its origin from individuals with privileged access and an in-depth understanding of the system. Detection and mitigation of these types of attacks are inherently challenging. The closeness of internal attackers to important assets considerably increases the potential for injury and exploitation. This situation therefore emphasizes the need of having robust internal security measures [26-30]. The VANET attack categorization is shown in Fig. 5.

3.1. Confidentiality Threats and Attacks

- Eavesdropping: Unauthorized parties can intercept and listen to communication between vehicles or between vehicles and infrastructure, potentially gaining sensitive information, such as locations, routes, or personal data.
- Traffic analysis: is the process by which attackers analyze traffic patterns to infer sensitive information, such as travel patterns, that might be used for a variety of malicious purposes.
- Packet sniffing: To intercept and seize communication packets inside the VANET and gather private data, adversaries use technologies known as packet sniffing.
- Man-in-the-middle (MITM) attacks include the intentional placement of attackers between communication entities with the goal of intercepting and altering communications to allow for the desired modification or eavesdropping on of content.

3.2. Integrity Threats and Attacks

- Replay attacks: include the acquisition and rebroadcast of valid packets by attackers with the aim of tricking vehicles or RSUs, creating confusion or aiding illegal activities.
- Message tampering: the act of hostile actors interfering with or altering messages that are sent within a VANET with the intention of manipulating information or spreading false data, hence influencing decision-making processes.
- Sybil attacks: include the establishment of many false identities by malevolent actors with the goal of misleadingly presenting a false impression of consensus or agreement inside a network.
- Tampering: adversaries possess the capability to influence or alter communications sent between automobiles or between automobiles and infrastructure, leading to the propagation of inaccurate or misleading data.
- Attackers who purposefully introduce false or misleading information into a network are said to be engaging in false information injection. This might be accomplished by altering real messages or fabricating fake ones.

3.3. Authentication and Identification Threats and Attacks

- The act of attackers impersonating real vehicles or infrastructure parts in order to get illegal access to networks, record conversations, and obtain sensitive information is known as identity spoofing.
- Impersonation: Adversaries may pose as legitimate VANET infrastructure or vehicles in order to transmit misleading messages, disseminate incorrect information, or carry out illegal activities.
- The goal of sybil assaults is to overwhelm a network with false information or gain control and authority over the communication process by having attackers create many false identities.

- An attack known as a distributed denial of service (DDoS) attempts to stop a network, service, or website from operating normally by flooding it with excessive amounts of data. This kind of attack involves several hacked computers or devices working together to produce and route large amounts of traffic towards the target. When this happens, people trying to access the targeted system experience a denial of service, which is comparable to the disruptive features of Sybil attacks.
- GPS spoofing: involves transmitting false or manipulated GPS signals to deceive GPS receivers, making them believe they are in a different location from their actual position. Spoofers can provide inaccurate position, velocity, and time (PVT) information to the GPS receiver, leading to inaccurate navigation or location-based decisions.

3.4. Availability Threats and Attacks

- Denial of service (DoS): Attackers may flood the network with an excessive amount of traffic or malicious requests to disrupt normal communication, causing a significant degradation in network performance or rendering it unavailable.
- Jamming: Adversaries can use radio frequency interference to disrupt communication between vehicles and infrastructure, inhibiting the network's availability and functionality.
- Bulk SMS flooding: Sending a large number of spam messages via SMS or messaging apps to targeted users, causing congestion, delays, and potential disruption of communication services.

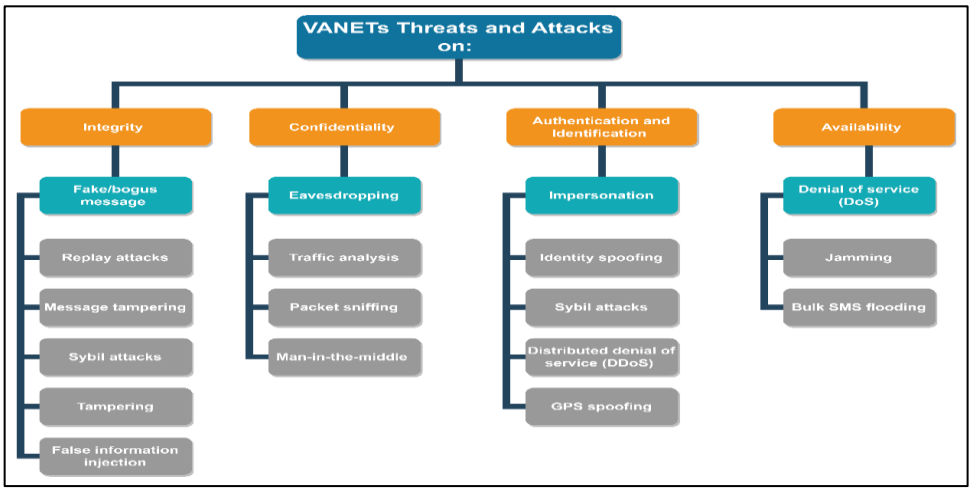


Fig. 5. Illustrates the categorization of attacks.

4. Security Requirement

Security measures are of paramount importance within the domain of VANETs to ensure reliable and secure communication among vehicles. The VANET system integrates a comprehensive array of security features to mitigate potential threats and enhance overall network resilience[29, 31, 32].

- Scalability refers to a system's ability to maintain optimal performance levels while efficiently handling growing user counts, rising transaction volumes, or growing data collections. When it comes to authentication systems, it is essential that the components that make up the system be able to change and grow dynamically in response to changes that take place in the surrounding environment.
- Anonymity is the process of concealing a legitimate user's personal information so that an unauthorized person cannot find it and the user's identity is kept secret.
- Unlinkability: When an opponent cannot distinguish among numerous entities interior a system, the attacker can neither compromise the machine nor misuse it.

- The unobservability refers to the potential to conceal movements or behaviors in a way that renders them undetectable or invisible to outdoor observers.
- Pseudonymity is the system of reflecting users' real identities the use of temporary identifiers or pseudonyms, striking a balance between protective privacy and permitting transactional or conversation.
- Identity management refers to the thorough and efficient administration of users' identities, including the procedures of identification, authorization, and access control.
- Prior to any data transmission, mutual authentication entails the identity verification of all parties involved in order to reduce the risk of adversaries or other threats.
- Forward secrecy is a characteristic that ensures the confidentiality of session keys set before to an attack, even in the event of long-term keying material attacks.
- Backward secrecy: Specifically, it is crucial that the compromise of a long-term key does not provide an attacker with the capacity to decode previous messages or gain unauthorized access to ongoing or future communications.
- Authentication and Authorization: Vehicles and infrastructure nodes must authenticate each other to verify their identities and authorize communication. Strong authentication mechanisms are essential to prevent unauthorized access.
- Data Integrity: By avoiding any tampering during transmission, this measure ensures the correctness and dependability of the information sent and received within the VANET.

5. System model

A. Trusted Authority (TA)

The TA is the highest-level entity inside the VANET system. This organization's main duty is to manage the whole VANET system, which includes duties like RSU and OBU registration as well as assigning unique registration IDs to vehicle users. It aims to manage and maintain the integrity of the database and software information. The vehicle user must satisfy all conditions to register in TA. As a result, TA has all the information about RSUs and OBUs as well as some personal information about the vehicle user. TA is fully responsible for providing secure transmission of information between different entities in the VANET system. Furthermore, it plays a pivotal part in revoking the malicious vehicle drivers from the VANET system grounded on a conditional tracking mechanism. All the RSUs in the TA area are connected to TA utilizing wired media in accordance with the system architecture. Wired cables are used for communication between RSUs and TA. TA is responsible for the creation of the private and public keys [33]. Fig. 6. illustrates the structure of our proposed system.

B. Roadside Unit (RSU)

RSU is an apparatus positioned strategically on roadsides or highways to enable data exchange and communication with motor vehicles. ITS, traffic management, and safety warnings are among its main duties. Each RSU has a unique and authenticated real identity (RIDR), which is essential for guaranteeing secure communication amongst units and enhancing the network's overall dependability. RSUs and OBUs establish contact using the DSRC protocol, which guarantees an efficient wireless connection. In addition to being connected wirelessly to the vehicle user, every RSU has wired connections to the TA, other RSUs. Moreover, it offers verifiable location-based data about vehicles. The TA gives RSU the required credentials [33].

C. On-Board Unit (OBU)

In the context of ITS and services, a vehicle incorporates an OBU to provide communication, data processing, and interaction with other vehicles or the RSU infrastructure. Each vehicle has an OBU, which VANETs use to facilitate intelligent communication. Specialized hardware equips the OBU to efficiently carry out its assigned functions. Within VANETs, OBUs play a critical role in enabling inter-vehicle communication. OBUs, equipped with GPS technology, provide precise latitude, longitude, and time-related data for each vehicle. These gadgets have data recorders built in,

like black boxes in aircraft, which are meant to collect accident data from vehicles in an organized manner for research and oversight [33].

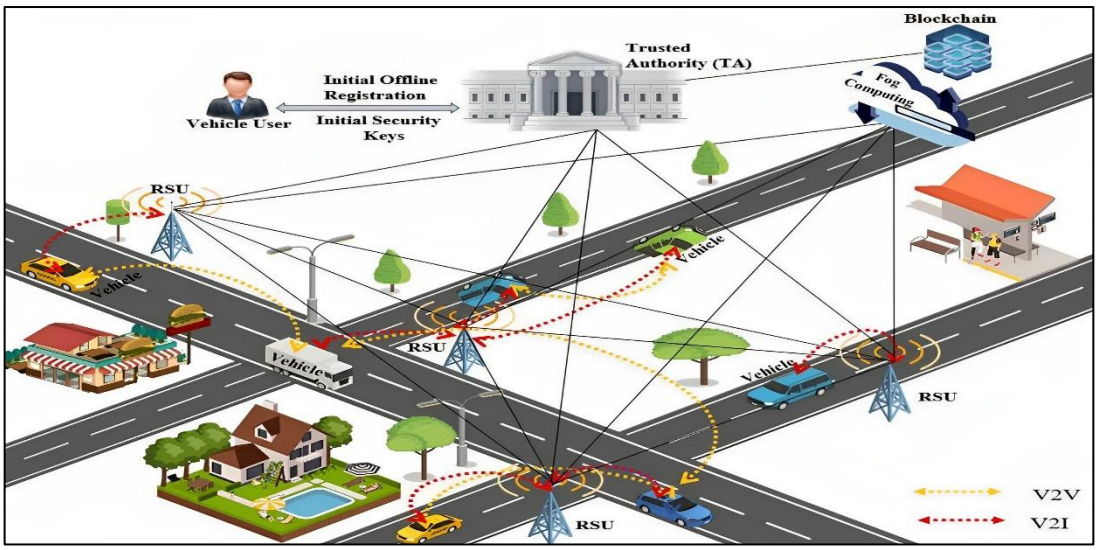


Fig. 6. Proposed system model for VANET.

D. Blockchain

A blockchain serves as a distributed ledger facilitating inter-node communication within a peer-to-peer network protocol structure while also validating new blocks in the system [34, 35] . Defined as an "open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way," the blockchain architecture comprises multiple blocks storing processed data records, all linked together through cryptography. Each block contains a cryptographic hash of the preceding block and includes timestamps and a Merkle tree to display transaction data. A key advantage of the blockchain approach is its immutable nature, as records saved in blocks cannot be altered without necessitating a complete change in all subsequent blocks. This inherent resistance to data tampering provides security to the entire blockchain, rendering it tamper-proof. Moreover, blockchain technology can detect any changes within the system [36, 37].

Three primary types of blockchains exist: public, private, and consortium. Public blockchains enable all participants to manage the entire blockchain network, exemplified by Bitcoin. In contrast, private blockchains are controlled and typically managed by organizations, restricting access to authenticated users, such as employees within the organization (e.g., Hyperledger Framework). Consortium blockchains involve a group of organizations collaborating to manage the blockchain in a decentralized manner [38, 39]. The Blockchain architecture is presented in Fig. 7.

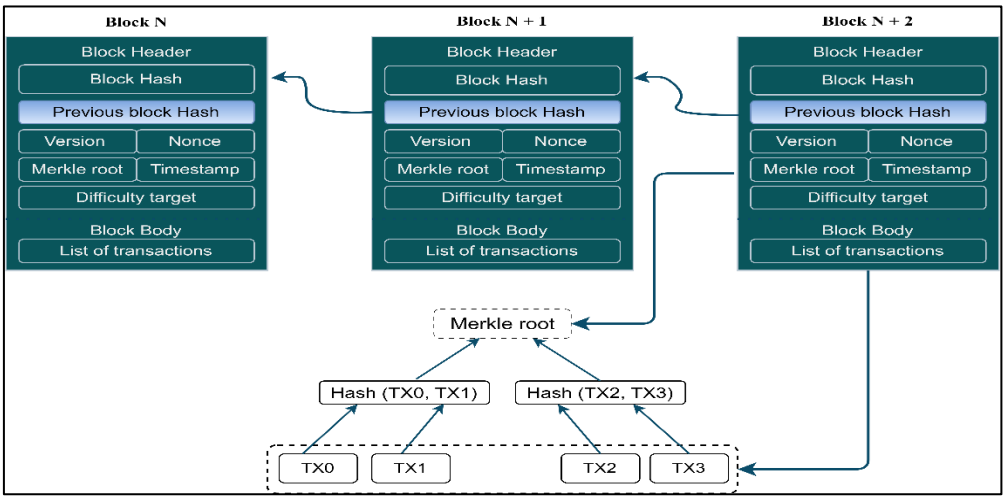


Fig. 7. Architecture of Blockchain.

E. Fog computing

Fog computing has emerged as a pivotal component in distributed networks, offering cloud resources such as computation and storage at the network's edge. A typical fog network comprises a diverse array of interconnected devices dedicated to communication, computation, and storage, catering to latency-sensitive IoT applications, Fig. 8. illustrates the architecture of fog computing. This paradigmatic shift provides a practical platform, delivering local processing and networking services between data centers and end-users, a departure from early cloud computing technologies. Unlike centralized cloud systems, fog computing focuses on addressing the needs of latency-sensitive IoT applications, particularly in domains such as healthcare, industrial automation, and transportation. CISCO was among the first to emphasize fog computing's capability to support geographically distributed IoT applications, thereby alleviating the latency-energy trade-off inherent in sensitive and QoS-aware IoT applications [40].

Fog computing, also known as fogging or fog networking, entails a decentralized computing architecture positioned between end devices and cloud data servers. This elastic composition enables users to allocate resources, including applications and data generated by embedded devices or sensors, in relevant neighborhoods to enhance performance. Fog computing offers several distinct advantages over traditional cloud computing technology, notably in terms of security, agility, latency, and efficiency [41]. Key features of fog computing include:

- Geographical partitioning of different devices.
- End-device mobility.
- Collaborative processing of a vast number of user service requests.
- Support for heterogeneity in the number of IoT devices.
- Facilitation of real-time applications.
- Access to end devices and computing nodes via wireless communication [42, 43].

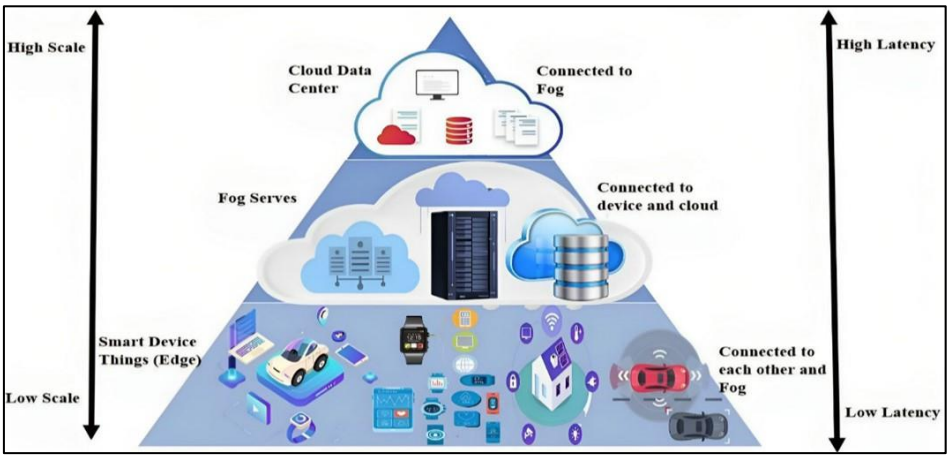


Fig. 8. Architecture of fog computing.

6. Related work

In efforts to enhance the security of VANETs, various approaches have been proposed. Numerous studies have examined security, authentication, and privacy solutions, with researchers conducting thorough surveys on these topics. Table 1 presents a qualitative evaluation of security characteristics in established authentication schemes. Table 2 presents the security and privacy requirements of VANETs across various schemes, outlining their respective characteristics and capabilities in addressing these needs.

In 2004, Hubaux et al.[44] proposed a PKI-based strategy where a vehicle's true identity is concealed through anonymous certificates, with each vehicle acquiring multiple certificates along with their respective key pairs during registration. However, this method necessitates a central

authority-controlled infrastructure, to enable specific security protocols, posing potential challenges in terms of cost, scalability, and coordination among various elements. Moreover, the implementation of these security mechanisms and smart vehicle technologies would demand considerable effort and investment. Consequently, only a limited subset of vehicles might adopt these features, potentially limiting the overall effectiveness of the proposed solutions.

In 2007, Raya and Hubaux introduced the PKI-based method for achieving Conditional Privacy-Preserving Authentication (CPPA) [45]. The solution results in substantial communication and storage restrictions since it necessitates preloading several anonymous public and private key pairs and their associated certificates into the vehicle's Trusted Platform Device (TPD). Furthermore, the process of canceling anonymous certificates involves lengthy steps, which adds to the overall complexity of the system.

In 2010, Wu et al. developed the message-linkable group anonymous digital signature technique and the one-time authentication system, which comprised the entire security architecture for V2V communications[46]. The proposed approach successfully integrates authentication methods while simultaneously addressing driver privacy concerns by detecting double-signed communications. But because bilinear pairing processes require a lot of resources, there are inefficiencies in the process of tracking down questionable communications. Within this design, the message linkable group signature (MLGS) system serves as a means to identify Sybil attacks, thereby establishing trust in a limited pool of anonymous automobiles whose number varies based on traffic conditions. In V2V communications, the use of license plates or public keys is required for message authentication. A reliable authority implements a revocability mechanism to guarantee privacy, safety, and trustworthiness. The goal of this strategy is to identify potential attackers.

In 2011 and for V2V and V2I communication, Zhang et al. [47] suggested an ID-based batch verification (IBV) system security technique with conditional privacy-preserving based on bilinear pairing. This scheme supports the batch verification process, which allows significant traffic-related messages to be verified simultaneously. In their scheme, they eliminated the use of certificate management and certificate revocation list (CRL) which reduced the amount of storage needed, as well as the overhead of the system. However, their approach still has significant drawbacks, such as the node's potential to fabricate an identity in order to circumvent the traceability function. Moreover, the impersonation assault fails to meet the non-repudiation condition and is vulnerable to replay and DoS attacks.

A MAC-based message authentication technique that is effective over VANET was presented by Rhim et al.[48] in 2012. The goal of this method is to address the problem of large-scale operations brought on by authentication techniques based on public keys. The suggested approach makes use of cryptography using secret keys. To guarantee integrity, the method computes hashes, or message digests, and sends them along with safety messages. Integrity is confirmed by computing hashes at the receiving end and comparing them with hashes delivered. However, the technique is vulnerable to side-channel, Sybil, and DoS attacks.

In 2013, Lozano et al.[49] introduced a warning message system aimed at preventing traffic accidents among vehicles by issuing timely alerts to drivers regarding current accident. The proposed system utilizes a distance-based flooding approach to disseminate warning messages effectively. The authors conducted calculations to determine the reaction time of vehicles following an accident to prevent subsequent collisions. Additionally, a scheme for disseminating low-priority warning messages was presented to optimize bandwidth utilization. The proposed routing scheme demonstrated superior dissemination of both high and low-priority messages, particularly in adverse weather conditions such as rain and sunlight. Moreover, the routing scheme exhibited reduced delay and efficient bandwidth utilization across varying traffic conditions. However, the routing scheme's limitations include its ineffectiveness in highly congested vehicular environments and the use of a simple flooding scheme for the highest priority messages, resulting in reduced decision-making time

for forwarding. Consequently, scalability issues arise in disseminating high-priority messages within the proposed scheme.

In 2015, He et al.[50] introduced the inaugural identity-based conditional privacy-preserving authentication scheme for VANETs. Their method boasts significantly reduced computation and communication costs compared to prior approaches, as it does not rely on bilinear pairing. Moreover, batch verification is facilitated to improve efficiency. Nonetheless, their scheme is vulnerable to modification attacks.

In 2016, Anirudh et al.[51] have introduced an effective message authentication protocol (Mavanet) utilizing QR encryption and decryption algorithms integrated with social network connections between senders and receivers. Within vehicular social networks, the dissemination of secure emergency messages is facilitated through QR code-based authentication, leveraging the topology derived from active social network users. Their evaluation involved various metrics, including message drop probability, packet delay upon reception, and the encryption/decryption time within the QR algorithm, all of which exhibit significant impacts with increasing user numbers. Furthermore, their proposal is susceptible to area security attacks and message modification attacks.

In 2016, Rajput et al. [52] proposed a method to mitigate authentication delays and prevent the exponential growth of Certificate Revocation Lists (CRLs) by dividing pseudonyms into two hierarchies for V2V and V2I communications. This approach involves the use of a Revocation Authority and a Law Enforcement Agency to manage primary pseudonyms provided by TAs for vehicle authentication by RSUs. Each RSU generates secondary pseudonyms with its signature for authenticated vehicles. Vehicles transmit messages with their secondary pseudonyms, and receivers verify messages by confirming the RSU's signature in the sender's second pseudonym. By employing long-term primary pseudonyms and short-term secondary pseudonyms, this scheme alleviates the burden of CRLs. Furthermore, the inclusion of the Revocation Authority and Law Enforcement Agency enhances network security by reducing reliance on TAs and RSUs in the event of compromised entities. However, this approach lacks guarantee of unlinkability and necessitates RSU or TA involvement to generate valid pseudonyms. Additionally, as most processing is handled by TAs, there is a risk of a single point of failure.

In 2016, Rabieh et al.[53] introduced a Privacy-Preserving Route Reporting mechanism for Traffic Management systems, aimed at providing route guidance to drivers to circumvent potential congestion and opt for alternative routes based on expected traffic conditions. However, this necessitates each vehicle to report its future locations, posing privacy risks and potential vulnerabilities to physical attacks and robbery by adversaries. Employing homomorphic encryption, the authors proposed encrypting all segments of a vehicle's future route within a single message, rather than encrypting each segment individually. Additionally, RSUs aggregate vehicle messages and transmit them to the Traffic Management Center (TMC), safeguarding individual vehicle routes from adversaries. However, it is imperative to acknowledge the potential vulnerability to collusion attacks, particularly as the volume of vehicles escalates significantly along a given route.

In 2018, Gao et al.[54] devised an authentication framework for VANET utilizing identity group signatures with edge computing, enabling authentication between vehicles (V2V) and vehicles-to-RSUs. The scheme incorporates an identification and revocation mechanism to identify and penalize malicious vehicles. However, it is susceptible to the key escrow problem, as the TA must issue secret keys for vehicles and RSUs, leading to high overhead due to numerous bilinear pairing operations. Furthermore, the scheme faces challenges including high computational complexity and vulnerability to tamper-proof device (TPD) compromise attacks. It lacks capabilities for achieving location privacy and resisting DoS attacks.

In 2018, Asghar et al.[55] devised a practical PKI-CPPA scheme aimed at streamlining request authentication with a linearly sized certificate revocation list (CRL), thereby augmenting the scalability of service acquisition by vehicles. However, the intrinsic challenges of PKI-based CPPA

strategies persist. First, the requirement to preload extensive private/public key pairs and their corresponding certificates onto vehicle OBUs imposes a substantial certificate management burden. Second, the constrained storage capacity within VANET vehicles becomes a concern due to the large preloaded key certificate sets. Third, the inclusion of certificates in message signatures amplifies computational and communication expenses because verifiers are tasked with validating these certificates alongside the message itself.

In 2018, Tan et al.[56] introduced a novel pairing-based authentication and message transmission scheme within VANETs. The scheme relies on the assumption that a RSU is trusted and can acquire a vehicle's secret key from the TA, generating a partial secret key for the vehicle. However, the inherent vulnerability lies in the potential compromise of an RSU, posing significant risks to passenger and driver privacy and safety. Additionally, the scheme is susceptible to replay attacks and fails to achieve conditional privacy.

In 2018, Z. Lu et al.[57, 58], proposed a privacy-preserving architecture has been proposed, incorporating security mechanisms such as transparency, conditional secrecy, efficiency, and resilience. The authors adopt a dual blockchain approach, wherein the identities of certified and revoked vehicles are stored on separate blockchains. Additionally, a distinct blockchain is employed to record inter-vehicle communications. In 2018, X. Zhang et al.[59] contribute to the domain by introducing a blockchain-based system for storing crucial event information, such as traffic violations and accidents, to facilitate future inquiries. Notably, fog nodes are utilized to efficiently handle substantial computing loads, exhibiting minimal communication and computation overhead in comparison to pairing-based bilinear methods.

In 2019, Ali et al.[60] introduced a public key signature scheme utilizing blockchain technology for V2I Communication in VANETs. Their certificateless scheme, incorporating bilinear pairing for conditional privacy, aims at efficient revocation and traceability via blockchain. It guarantees the integrity and trustworthiness of vehicles, utilizing blockchain to store identities of authorized and other blockchain unauthorized/revoked vehicles separately. The use of batch signature and aggregate signature verification enhances verification speed while maintaining transparency in pseudo-identity revocation. Although the scheme ensures authentication and identity properties, its complexity is increased by the batch signature and aggregate verification process. Vulnerabilities include susceptibility to Sybil attacks and bogus information.

In 2019, Ming et al.[61] developed a certificateless Conditional Privacy-Preserving Authentication (CPPA) scheme, offering low transmission overhead and proven security under the random oracle model. Despite relatively low signing and verification costs, the scheme falls short in meeting the transmission overhead requirements for transmitting traffic emergency messages. However, the transmission overhead remains too high to meet the demands of the Internet of Vehicles (IoV). [61], two distinct certificateless authentication schemes for VANETs were proposed based on ECC. Despite meeting certain requirements, these schemes lack support for autonomy and fail to provide location privacy, as the linkability of a vehicle's pseudonym compromises its anonymity.

In 2019, Alazzawi et al. [62] proposed the robust pseudo-identity-based solution for V2V and V2I communications in VANET. With this method, the vehicle's real identify is replaced with a pseudonym used by the TA throughout the registration process. The vehicle transmits the pseudo-IDs PIDv1 and PIDv2, which it has derived, to the RSU in order to authenticate with the TA. As a part of the mutual authentication process, the RSU performs XOR operations to encrypt and send the signature key Sk of the vehicle's pseudo-IDs after verifying the validity of the vehicle. By using this specific approach, the signer may modify the verification time for the receiver by calculating the value of w.This method meets the requirements for protecting privacy, prohibiting non-repudiation, allowing tracing, simplifying revocation, and guaranteeing message integrity and authentication. It also offers conditional anonymity, which ensures that the true identity of an honest vehicle is maintained until harmful activity is identified. Man-in-the-middle (MITM) attacks, replay,

impersonation, and modification cannot affect this system. While bilinear pairing techniques are used in many modern systems, their complex processes result in significant processing costs, making this method ineffectual. As a result, substantial storage and transmission costs result from the lack of a revocation list.

In 2020, Gabay et al. [63] examined the potential for privacy breaches in electric vehicles (EVs) during the charging process. They introduced a privacy-aware authentication challenge using blockchain technology and zero-knowledge proofs. The decentralized consensus is enabled via the Ethereum distributed ledger, while privacy protection is provided by a zero-knowledge proof-based method. By using zero-knowledge proofs, an electric vehicle (EV) may anonymously authenticate its charging activities. The blockchain network, electric vehicles (EVs), and the company offering EV services are the system's constituent parts. Their plan overlooked the need for trusted authority's traceability even though it offered a robust privacy policy.

In 2020, Guo et al. [64] presented a trust management method that considers the context to evaluate the signals received by vehicles and guarantee responsible decision-making in terms of content integrity. A reinforcement learning model and a context-aware trust management model comprise the security architecture that this work describes. The first model was created to evaluate communication dependability. To ensure the highest level of accuracy in the evaluated results, the second model is used to choose the best assessment strategy. But the weakness is in the overstuffing of states, which results in a reduction in output.

Fog computing techniques provide the basis of the vehicle design that the Han et al. in 2020 [65] suggest. The vehicle layer, fog layer, and cloud computing layer are the three separate tiers of the architectural framework. The vehicle layer controls the data flow to the fog layer. RSUs, base stations, computing power, resource storage, and a local authority (LA) in the fog layer are all part of it. The LA assigned duty is to fabricate automobile certificates. Moreover, the authors assumed that the fog layer might be considered trustworthy. The Cloud computing layer is responsible for storing the data that is uploaded by the fog layer. Nevertheless, there is no consideration for the privacy and security of communication linkages between the fog and cloud layers.

In 2020, Shen et al. [66] have developed a decentralized and transparent cross-domain authentication system for industrial IoT devices spanning many domains, including factories, using blockchain technology. In their study, they use a consortium blockchain to build trust across several domains, and they utilize identity-based encryption (IBE) to authenticate devices. Furthermore, a proposed anonymous authentication system that may revoke identities is offered as a way to get around IBE's identity revocation constraint. Moreover, domain-specific data is moved to off-chain storage to relieve the blockchain system's storage limitations. The blockchain's poor throughput is the reason for the delayed response time.

In 2021 to improve the integration of scattered data in automobile safety applications, Liu et al. . [67] present the Lightweight Trust assessment and Privacy-Preserving (LPPTE) technique, which tries to strike a compromise between privacy preservation and trust evaluation. In addition to meeting the needs of efficient computing and communication overhead, privacy preservation, and authentication, the suggested system successfully assures the security of V2V communication. The suggested method exhibits robustness against replay, fake message, and message manipulation attacks. However, this specific approach is devoid of the necessary components of non-repudiation, unlinkability, traceability, and revocation of dangerous vehicles. It is also not flexible enough to handle the many scenarios that VANETs could face.

In 2021, fuzzy logic and blockchain are used by Inedjaren et al. [68] in their routing strategy to enhance the dependability of V2V communication by detecting rogue nodes. The researchers' strategy is based on the fuzzy logic trusted Optimized Link State Routing (FT-OLSR) protocol, which separates malicious vehicles using blockchain technology. This system is resistant to attacks that drop

messages. All of the security and privacy requirements of VANETs, including authentication, non-repudiation, privacy preservation, unlinkability, tampering, traceability, and revocation, are not met by it, and it is not flexible enough to adjust to various VANET scenarios. moreover, it is vulnerable to replay attacks, spoofing attacks, impersonation attacks, sybil attacks, DoS attacks, and firmware integrity issues.

Chukwuocha et al. [69] introduced a Bayesian trust inference model in 2021. The purpose of the model was to evaluate the reliability of vehicles and communications. It computed the beta distribution using messages derived from real-time event data. We further separate the road network into zones to reduce communication overhead and increase scalability, and place RSU in each zone. Together, these RSUs form a blockchain network, whereby vehicles communicate computed trust values to RSUs for blockchain archiving. The primary goal is to reduce the likelihood of bogus message attacks in order to improve the security of V2V communication. Nevertheless, even with its emphasis on security, the scheme falls short of meeting all security and privacy criteria, and its context-reading skills are limited.

Kalaria et al. devised the mutual authentication technique in 2021 [70], employing elliptic curve encryption, fog computing, and one-way hash functions. Their plan was to strengthen cybersecurity defenses and protect networked devices and organizations from cyberattacks. The fog computing environment successfully established mutual authentication, but immutability and inherited trust issues posed challenges for the technique. Furthermore, the network's persistent single point of failure created vulnerabilities that hostile actors could exploit.

Ghajar et al. [71] (2021) used blockchain technology in combination with a Bayesian trust management formula to create a robust system that ensures the reliability of received communications. Using this method, automobiles meticulously examine the accuracy of incoming signals and provide the sender vehicles with a confidence rating based on this evaluation. After calculation, RSUs receive the trust values for further processing. RSUs employ a shared consensus method to build trust values into blocks, allowing for secure and effective storage. While this specific method works well for storing trust values related to vehicles, it is not as context-sensitive as it might be. The current system also doesn't meet a number of basic requirements for VANETs, such as protecting privacy, being able to be disconnected, being able to be undeleted, being authentic, and not being able to be disputed.

In 2021, Pu [72] introduced a trust management system, Trust-Block MCDM, leveraging blockchain technology in VANETs. This model employs multicriteria decision making to assess the trustworthiness of received road safety messages and determine the credibility of their originators. The system computes trust values for message originators by aggregating opinions from neighboring validators, evaluating the message originator’s reputation, and considering its confidence in the event. These trust values are periodically transmitted to nearby RSUs to accommodate limited vehicle storage. RSUs, in turn, aggregate these values to calculate and store the message originators’ reputation in blockchain blocks to identify and eliminate spurious messages from the network. However, a notable drawback of this model arises from the susceptibility to unfair ratings sent to the RSUs by malicious vehicles, potentially compromising the integrity of the trust assessment process.

In 2021, Liu et al. [73] proposed the privacy-preserving trust management (PPTM) technique for emergency signal broadcasting in space-air-ground integrated vehicular networks. The suggested method minimizes communication overhead while enabling secure vehicle-to-vehicle (V2V) communication by combining strong conditional privacy preservation capabilities with trust management methods. However, no particular details on the behavior of this architecture under various VANET conditions were provided. Moreover, there is no way for the system to be revoked in the event that malicious vehicle are involved.

In 2022, Bhargava and Verma [74] provide a paradigm for trust management that ensures accuracy and security requirements. In order to improve accuracy, the writers account for the data's inherent uncertainty. It combines the direct and indirect trust related to the vehicles using Dempster-

Shafer theory (DST). The authors improve the accuracy of trust evaluation by using contextual information to distinguish the precise nature of the communications targeted by malicious vehicles. Lane Change Warning (LCW), Stopped Vehicle Warning (SVW), and Emergency Brake Warning (EBW) are among the messages that are being examined. The authors also use additional functions to boost the model's security and increase the trust assessment's correctness. The functions of rewarding, forgetting, punishing, and forgiving are used in this situation. However, it cannot provide privacy, scalability, or reactivity.

According to Rehman et al. [75] in 2022, a vehicle learns about its environment and creates contexts around events to choose which ones to believe. It creates a structure that connects a number of related concepts (such vehicle, evaluation, and event). The framework for assessing trust considers a number of variables, including role, opinion, and experience. Outlier detection is done using criteria related to time, speed, and distance. This technique evaluates the degree of confidence shown by the report in addition to the trust value assigned to each one. In this research, the framework is simulated in both urban and rural settings, and it is then compared to other frameworks already in use. However, malicious automobiles might evade the outlier-based detection process and send out signals that are erroneous but inside the permissible threshold set for this specific model.

In 2022, Bi et al. [76] established a unique identification method that makes use of a message and time transmission matrix. In order to accurately detect attack signals in real-time, the Electronic Control Unit (ECU) might benefit from the recommended Intrusion Detection System (IDS). Real-world automotive experiments revealed that their Intrusion Detection System (IDS) correctly recognized many threats with a lower computing resource consumption. The weakness is that the algorithm's weight exceeds the threshold, requiring more complex feature processing.

Table 1. Comparison of security features.

Scheme	Adopts Blockchain Technology (Efficient and Secure Data Storage)	Traceability of Malicious Vehicles and Their Revocation	Communication Situation		Efficiency (Communication Overhead and Computational Cost)	Resilience Against Attacks
			V2V	V2I		
Hasrouny et al.[77]	No	Yes	Yes	No	No	Malicious vehicles
Ahmad et al.[78]	No	No	Yes	No	No	Message-tampering attacks, message-delaying attacks
Ghaleb et al.[79]	No	No	Yes	No	No	False-message attacks
Liu et al.[67]	No	No	Yes	No	Efficient	replay attacks, message-tampering attack, false-message attacks,
Guo et al.[64]	No	No	Yes	No	No	False-message attacks

Inedjaren et al.[68]	Yes	No	Yes	No	No	Message-dropping attacks
Chukwuocha et al.[69]	Yes	No	Yes	No	No	False-message attacks
Ghaj ar et al.[71]	Yes	No	Yes	No	No	False-message attacks
Liu et al.[73]	No	It's possible to track malicious vehicles, but there's no ability to revocation.	Yes	No	Effective in terms of communication overhead, but without providing the computation cost.	Malicious vehicles
Bhargava and Verma [74]	No	No	Yes	No	No	False-message attacks, message-dropping attacks and message tampering attacks
Rehman et al.[75]	No	No	Yes	No	No	Malicious vehicles

In 2023, authentication schemes based on certificateless aggregate signatures (CLAS) are instrumental in enhancing computational efficiency, streamlining communication, and bolstering security by condensing multiple signatures into a unified aggregate signature. Nonetheless, numerous existing CLAS-based authentication schemes incorporating conditional privacy preservation (CPP) suffer from inadequate security measures or suboptimal performance. Recently, Zhu et al. [80] introduced a CLAS-based authentication scheme with CPP tailored specifically for VANETs, termed the Zhu-CLASA scheme, which demonstrates enhanced computational efficiency compared to its predecessors. However, our analysis reveals vulnerabilities in the Zhu-CLASA [80] scheme against coalition attacks orchestrated by malicious Road Side Units (RSUs) and vehicles, as well as being insecure against public-key replacement (PKR) attacks.

In 2023, Chen et al.[81] presented a privacy-preserving cross-domain authentication (PPCDA) system designed for VANETs, leveraging secure blockchain technology. This approach integrates both group signing and blockchain methodologies to accomplish its objectives, employing group signature techniques to offer some level of privacy protection and facilitate cross-domain vehicle verification. Their proposal introduces a secure blockchain-based solution aimed at preserving privacy during cross-domain authentication in VANETs. However, despite the incorporation of group signature techniques, the system's ability to ensure privacy protection remains limited, indicating deficiencies in its privacy provisions.

In 2023, Liu et al.[82] addressed the single point of failure issue by introducing a multi-layer location sharing system based on blockchain, which is adaptable to dynamic scenarios. They incorporated an accumulator to improve the efficiency of data refreshing and verification. However, this approach is associated with persistent communication overhead. The effectiveness of their

proposed system was evaluated through a formal security analysis using Real-Or-Random (ROR), and experimental results indicated its superiority over existing methods in terms of communication cost, computational overhead, and overall efficiency. Nevertheless, a limitation of the scheme is its inconsistency in achieving optimal efficiency.

In 2023, Prajapat et al.[83] propose a secure signature system tailored for efficient communication within VANET environments. Their approach, rooted in Identity-based cryptography, reduces the need for certificates. Leveraging lattice-based cryptography, the system is designed to withstand quantum attacks, demonstrating resilience under the quantum random oracle model. It fulfills various security requirements including mutual authentication, data integrity, identity privacy preservation, signature unforgeability, resistance to quantum attacks, and traceability. The utilization of aggregate signatures enhances the efficiency of the proposed scheme. Through rigorous security and performance analyses, the authors showcase the effectiveness and robustness of the lattice-based Identity-Based Aggregate Signature (IBAGS) scheme. Thus, the proposed lattice-based IBAGS emerges as a provably secure, efficient, and well-suited solution for VANET environments, making a valuable contribution to the related body of work in this domain.

In 2023, Yu et al.[84] employed ECC and certificateless aggregate signatures to alleviate the computational burden on OBUs. However, their scheme lacks support for dynamic groups. However, Wang el at[85], came up with a technique of conditionally saving privacy without using pseudonyms. However, the method includes operations on bilinear pairs which increases computational overheads and is poorly compatible with resource-constrained vehicles.

An advanced security and privacy solution for communication within VANETs was proposed by Namdev et al. in 2024 [86]. They combined biometric authentication with blockchain technology for this purpose. This integration helps to secure the vehicular network against malicious activities and unauthorized access because only authorized persons are allowed, while others are denied access. Through these measures, users are effectively authenticated based on their biometric attributes with the integrity of communication guaranteed by employing blockchain technology. The system meets required security standards as evaluated results show while maintaining efficient communications in VANETs.

In 2024, Su et al. [87] present a lightweight approach towards improved authentication and privacy coined towards reducing TAs dependence within VANET environments. Additionally, it focused on an improved “forgetful” transfer algorithm for the enhancement of privacy and authentication between nodes (vehicles) as well as TAs. Their mechanism would undoubtedly increase secrecy in the face of assaults since it has been shown that this may be accomplished by carefully analyzing security. In addition, they found out that their solution’s performance simulations necessitate limited computational resources and have low communication overheads.

The multisharding blockchain serves as the foundation for Huang et al.'s [88] (2024) proposed privacy-preserving vehicular data sharing architecture. The researchers create an auditable and anonymous data exchange system. They use Zero-Knowledge Proof (ZKP) to protect automobiles' identity privacy and provide conditional auditability. Furthermore, provide a multi-sharding blockchain system that is very effective and has less communication complexity than current sharding techniques. Particularly suitable for IoV-enabled systems is this protocol. The evaluation and analysis's findings show that the framework effectively enhances system security and safeguards user identification.

Table 2. Security and privacy requirements for various schemes.

Scheme	Confidentiality	Mutual authentication	User Anonymity	Data Integrity	Conditional Privacy	Non-repudiation	Replay attack
Hu et al.[89]	✓	✓	×	✓	×	✓	✓
Zhang et al.[90]	✓	✓	×	✓	×	✓	✓
Braeken et al. [91]	×	✓	✓	✓	✓	×	✓
Chim et al.[92]	✓	✓	×	✓	✓	✓	✓
Gayathri et al.[93]	×	✓	×	✓	×	✓	✓
Li et al.[94]	×	✓	×	✓	×	×	✓
Ming et al.[61]	×	✓	×	✓	×	✓	✓
Sutrala et al.[95]	×	✓	×	✓	×	✓	✓
Tan et al.[96]	×	✓	✓	✓	✓	✓	✓
Chen et al.[97]	×	×	✓	×	×	✓	×
Mahmood et al.[98]	✓	✓	×	✓	×	✓	×
Li et al.[99]	×	✓	×	✓	✓	×	×
Khan et al.[100]	×	✓	✓	✓	✓	✓	✓

7. Conclusion

This paper discusses the VANET design and implementation challenges. After that, an explanation of a basic authentication idea is given in connection with the communication between V2V, V2I and the RSU service. This study also provides an extensive comparison and analysis of authentication methods used in recent research, with an emphasis on how they rank in terms of security, privacy, scalability, low communication cost, and computational cost. The reliance on TA/CA, the need to maintain a CRL, the privacy issues of an electric vehicle while visiting charging stations often because of per charge constraints, and the restricted coverage in places with weak signals are only a few of the numerous flaws in the existing system that the authors have pointed out. To solve the aforementioned difficulties, a summary of 5G, fog computing, and Blockchain application for VANET authentication and privacy has been presented. Furthermore, in order to create a robust and scalable framework for the successful deployment of the VANET, researchers are likely to combine hybrid approaches like Fog-Blockchain with traditional encryption methods. In VANET, trust is an important topic that has to be carefully considered.

References

[1] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53-66, 2014, doi: https://doi.org/10.1016/j.vehcom.2014.05.001.

[2] A. Ali, M. M. Iqbal, S. Jabbar, M. N. Asghar, U. Raza, and F. Al-Turjman, "VABLOCK: A blockchain-based secure communication in V2V network using icn network support technology," Microprocessors and Microsystems, vol. 93, p. 104569, 2022, doi: https://doi.org/10.1016/j.micpro.2022.104569.

[3] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet," IEEE Access, vol. 8, pp. 91028-91047, 2020, doi: https://doi.org/10.1109/ACCESS.2020.2992580.

[4] I. M. Hassan and K. R. Hassan, "Vehicular social networks and vehicular ad-hoc networks, applications, modelling tools and challenges: A survey," International Journal of Computer Applications, vol. 975, p. 8887, 2020, doi: http://dx.doi.org/10.5120/ijca2020920224.

[5] S. Wang, Z. Fan, Y. Su, B. Zheng, Z. Liu, and Y. Dai, "A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks," Electronics, vol. 13, no. 8, p. 1418, 2024, doi: https://doi.org/10.3390/electronics13081418.

[6] M. A. A. Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks," IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14253-14266, 2024, doi: https://doi.org/10.1109/JIOT.2023.3340259.

[7] A. Guerna, S. Bitam, and C. T. Calafate, "Roadside unit deployment in internet of vehicles systems: A survey," Sensors, vol. 22, no. 9, p. 3190, 2022, doi: https://doi.org/10.3390/s22093190.

[8] I. A. Aljabry and G. A. Al-Suhail, "A survey on network simulators for vehicular ad-hoc networks (VANETS)," Int. J. Comput. Appl, vol. 174, no. 11, pp. 1-9, 2021, doi: http://dx.doi.org/10.5120/ijca2021920979

[9] Y .Lai, Y. Xu, F. Yang, W. Lu, and Q. Yu, "Privacy-aware query processing in vehicular ad-hoc networks," Ad Hoc Networks, vol. 91, p. 101876, 2019/08/01/ 2019, doi: https://doi.org/10.1016/j.adhoc.2019.101876.

[10] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," Journal of Systems Architecture, vol. 103, p. 101692, 2020/02/01/ 2020, doi: https://doi.org/10.1016/j.sysarc.2019.101692.

[11] A. Alrawais, A .Alhothaily, B. Mei, T. Song, and X. Cheng, "An Efficient Revocation Scheme for Vehicular Ad-Hoc Networks," Procedia Computer Science, vol. 129, pp. 312-318, 2018/01/01/ 2018, doi: https://doi.org/10.1016/j.procs.2018.03.081.

[12] S.-J. Horng, S.-F. Tzeng ,P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," Information Sciences, vol. 317, pp. 48-66, 2015/10/01/ 2015, doi: https://doi.org/10.1016/j.ins.2015.04.033.

[13] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," Information Sciences, vol. 451-452, pp. 1-15, 2018/07/01/ 2018, doi: https://doi.org/1/0.1016j.ins.2018.03.060.

[14] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, p. 101842, 2019, doi: https://doi.org/10.1016/j.adhoc.2019.02.001.

[15] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K .Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Computers & Security, vol. 103, p. 102150, 2021/04/01/ 2021, doi: https://doi.org/10.1016/j.cose.2020.102150.

[16] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu" ,Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4757-4.2021 ,769, doi: https://doi.org/10.1109/TITS.2020.3041746.

[17] M. Bellés-Muñoz, B. Whitehat, J. Baylina, V. Daza, and J. L. Muñoz-Tapia, "Twisted Edwards Elliptic Curves for Zero-Knowledge Circuits," Mathematics, vol. 9, no. 23, p. 3022, 2021, doi: https://doi.org/10.3390/math9233022.

[18] S. H. L. Kanickam and L. Jayasimman, "Comparative analysis of hash authentication algorithms and ECC based security algorithms in cloud data," Asian J Comput Sci Technol, vol. 8, no. 1, pp. 53-61, 2019, doi: http://dx.doi.org/10.51983/ajcst-2019.8.1.2118.

[19] O. Siedlecka-Lamch, "Probabilistic and Timed Analysis of Security Protocols," in Computational Intelligence in Security for Information Systems, 2019, doi: https://doi.org/10.1007/978-3-030-57805-3_14.

[20] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper," in International conference on computer aided verification, 2008: Springer, pp. 414-418, doi: https://doi.org/10.1007/978-3-540-70545-1_38.

[21] N. El Madhoun and G. Pujolle, "A secure cloud-based NFC payment architecture for small traders," in 2016 3rd Smart Cloud Networks & Systems (SCNS), 2016: IEEE, pp. 1-6, doi: https://doi.org/10.1109/SCNS.2016.7870562.

[22] G. Mathur, "GANACHE: A Robust Framework for Efficient and Secure Storage of Data on Private Ethereum Blockchains," 2023, doi: https://doi.org/10.21203/rs.3.rs-3495549/v1.

[23] A. Dolgui, D. Ivanov, S. Potryasaev, B. Sokolov, M. Ivanova, and F. Werner, "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain," International Journal of Production Research, vol. 58, no. 7, pp. 2184-2199, 2020, doi: https://doi.org/10.1080/00207543.2019.1627439.

[24] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," The Review of Financial Studies, vol. 32, no. 5, pp. 1754-179.2019 ,7, doi: https://doi.org/10.1093/rfs/hhz007.

[25] A. Goñi, A. Burgos, L. Dranca, J. Rodríguez, A. Illarramendi, and J. Bermúdez, "Architecture, cost-model and customization of real-time monitoring systems based on mobile biological sensor data-streams," Computer methods and programs in biomedicine, vol. 96, no. 2, pp. 141-157, 2009, doi: https://doi.org/10.1016/j.cmpb.2009.04.010.

[26] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, "ABRIS: Anonymous blockchain based revocable and integrity preservation scheme for vehicle to grid network," Energy Reports, vol. 8 ,pp. 9331-9343, 2022, doi: https://doi.org/10.1016/j.egyr.2022.07.064.

[27] A. Giannaros et al., "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 493-543, 2023, doi: https://doi.org/10.3390/jcp3030025.

[28] E. Alalwany and I. Mahgoub, "Classification of Normal and Malicious Traffic Based on an Ensemble of Machine Learning for a Vehicle CAN-Network," Sensors, vol. 22, no. 23, p. 9195, 2022, doi: https://doi.org/10.3390/s22239195.

[29] X. He, X. Niu, Y. Wang, L. Xiong, Z. Jiang, and C. Gong, "A hierarchical blockchain-assisted conditional privacy-preserving authentication scheme for vehicular ad hoc networks," Sensors, vol. 22, no. 6, p. 2299, 2022, doi: https://doi.org/10.3390/s22062299.

[30] B. Akwirry, N. Bessis, H. Malik, and S. McHale, "A multi-tier trust-based security mechanism for vehicular ad-hoc network communications," Sensors, vol. 22, no. 21, p. 8285, 2022, doi: https://doi.org/10.3390/s22218285.
[31] K. N. Qureshi et al., "A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles," Applied Sciences, vol. 12, no. 1, p. 476, 2022, doi: https://doi.org/10.3390/app12010476.
[32] A. Verma, R. Saha, G. Kumar, and T.-h. Kim, "The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions," Applied Sciences, vol. 11, no. 10, p. 4682, 2021, doi: https://doi.org/10.3390/app11104682.
[33] B. Hou, Y. Xin ,H. Zhu, Y. Yang, and J. Yang, "VANET Secure Reputation Evaluation & Management Model Based on Double Layer Blockchain," Applied Sciences, vol. 13, no. 9, p. 5733, 2023, doi: https://doi.org/10.3390/app13095733.
[34] S. Umran, S. Lu, Z. Abduljabbar, J. Zhu, and J. Wu, "Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology," Applied Sciences, vol. 11, 07/09 2021, doi: https://doi.org/10.3390/app11146376.
[35] V. Singla, I. K. Malav, J. Kaur, and S. Kalra, "Develop leave application using blockchain smart contract," in 2011 19th International Conference on Communication Systems & Networks (COMSNETS), 2019: IEEE, pp. 547-54, doi: https://doi.org/10.1109/COMSNETS.2019.8711422.
[36] S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," Internet of Things, vol. 24, p. 100969, 2023/12/01/ 2023, doi: https://doi.org/10.1016/j.iot.2023.100969.
[37] Z. A. Hussien et al., "Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems," Applied Sciences, vol. 13, no. 2, p. 691, 2023, doi: https://doi.org/10.3390/app13020691.
[38] R. Banno and K. Shudo, "Simulating a blockchain network with simblock," in 2019 IEEE international conference on blockchain and cryptocurrency (ICBC), 2019: IEEE, pp. 3-4, doi: https://doi.org/10.1109/BLOC.2019.8751431.
[39] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, 2019, doi: https://doi.org/10.1109/TSMC.2019.2895123.
[40] A. M. Farooqi, S. I. Hassan, and M. A. Alam, "Sustainability and fog computing: applications, advantages and challenges," in 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 2 :019IEEE, pp. 18-23, doi: https://doi.org/10.1109/ICCCT2.2019.8824983.
[41] S. Misra, S. P. Rachuri, P. K. Deb, and A. Mukherjee, "Multiarmed-bandit-based decentralized computation offloading in fog-enabled IoT," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10010-10017, 2020, doi: https://doi.org/10.1109/JIOT.2020.3048365.
[42] A. Hazra, P .Choudhary, and O. Vivek, "An advance mobility management scheme in wireless network," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018: IEEE, pp. 1-5, doi: https://doi.org/10.1109/ICCCNT.2018.8493854.
[43] A. Hazra, M. Adhikari, T. Amgoth, and S .N. Srirama, "Joint computation offloading and scheduling optimization of IoT applications in fog networks," IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 3266-3278, 2020, doi: https://doi.org/10.1109/TNSE.2020.3021792.

[44] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security & Privacy, vol. 2, no. 3, pp. 49-55, 2004, doi: https://doi.org/10.1109/MSP.2004.26.
[45] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, no. 1, pp. 39-68, 2007, doi: https://doi.org/10.3233/JCS-2007-15103.
[46] Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," Vehicular Technology, IEEE Transactions on, vol. 59, pp. 559-573, 03/01 2010, doi: https://doi.org/10.1109/TVT.2009.2034669.
[47] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," Wireless Networks, vol. 17, pp. 1851-1865, 2011, doi: https://doi.org/10.1007/s11276-011-0383-2.
[48] J.-W. Rhim, "A Study on MAC-Based Efficient Message Authentication Scheme for VANET," Master's degree M.S. Thesis, Hanyang University, 2012 .
[49] E. Garcia-Lozano, C. T. Barba, M. A. Igartua, and C. Campo, "A distributed, bandwidth-efficient accident prevention system for interurban VANETs," in 2013 International Conference on Smart Communications in Network Technologies (SaCoNeT), 2013, vol. 1: IEEE, pp. 1-5, doi: https://doi.org/10.1109/SaCoNeT.2013.6654564.
[50] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security ,vol. 10, no. 12, pp. 2681-2691, 2015, doi: https://doi.org/10.1109/TIFS.2015.2473820.
[51] A. Paranjothi, M. S. Khan, M. Nijim, and R. Challoo, "MAvanet: Message authentication in VANET using social networks," in 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference)UEMCON), 20-22 Oct. 2016 2016, pp. 1-8, doi: https://doi.org/10.1109/UEMCON.2016.7777915 .
[52] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," Ieee Access, vol. 4, pp. 7770-7784, 2016, doi: https://doi.org/10.1109/ACCESS.2016.2620999.
[53] K. Rabieh, M .M. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2703-2713, 2016, doi: https://doi.org/10.1109/TVT.2016.2583466.
[54] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," International Journal of Distributed Sensor Networks, vol. 14, no. 2, p. 1550147718756581, 2018, doi: https://doi.org/10.1177/1550147718756581.
[55] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018: IEEE, pp. 1-3, doi: https://doi.org/10.1109/ATNAC.2018.8615224.
[56] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure certificateless authentication and road message dissemination protocol in VANETs," Wireless Communications and Mobile Computing, vol. 2018, 2018, doi: https://doi.org/10.1155/2018/7978027.
[57] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering

(TrustCom/BigDataSE), 2018: IEEE, pp. 98-103, doi: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00025.

[58] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," Ieee Access, vol. 6, pp. 45655-45664, 2018, doi: https://doi.org/10.1109/ACCESS.2018.2864189.

[59] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018: IEEE, pp. 258-259, doi: https://doi.org/10.1109/HOTICN.2018.8605952.

[60] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," Journal of Systems Architecture, vol. 99, p. 101636, 2019, doi: https://doi.org/10.1016/j.sysarc.2019.101636.

[61] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," Mobile Information Systems, vol. 2019, 2019, doi: https://doi.org/10.1155/2019/7593138.

[62] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen" ,Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network," IEEE Access, vol. 7, pp. 71424-71435, 2019, doi: https://doi.org/10.1109/TVT.2020.2977361.

[63] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5760-5772, 2020.

[64] J. Guo et al., "TROVE: A context-awareness trust model for VANETs using reinforcement learning," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6647-6662, 2020, doi: https://doi.org/10.1371/journal.pone.0228319.

[65] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," PLoS one, vol. 15, no. 2, p. e0228319, 2020.

[66] M. Shen et al., "Blockchain-assisted secure device authentication for cross-domain industrial IoT," IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942-954, 2020, doi: https://doi.org/10.1109/JSAC.2020.2980916.

[67] Z. Liu et al., "LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications," Information Fusion, vol. 73, pp. 144-156, 2021, doi: https://doi.org/10.1016/j.inffus.2021.03.003.

[68] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in VANET," Vehicular Communications, vol. 30, p. 100350, 2021, doi: https://doi.org/10.1016/j.vehcom.2021.100350.

[69] C. Chukwuocha, P. Thulasiraman, and R. K. Thulasiram, "Trust and scalable blockchain-based message exchanging scheme on VANET," Peer-to-Peer Networking and Applications, vol. 14, pp. 3092-3109, 2021, doi: https://doi.org/10.1007/s12083-021-01164-9.

[70] R. Kalaria ,A. Kayes, W. Rahayu, and E. Pardede, "A Secure Mutual authentication approach to fog computing environment," computers & security, vol. 111, p. 102483, 2021, doi: https://doi.org/10.1016/j.cose.2021.102483.

[71] F. Ghovanlooy Ghajar, J. Salimi Sratakhti, and A. Sikora, "Sbtms: Scalable blockchain trust management system for vanet," Applied Sciences, vol. 11, no. 24, p. 11947, 2021, doi: https://doi.org/10.3390/app112411947.

[72] C. Pu, "A novel blockchain-based trust management scheme for vehicular networks," in 2021 wireless telecommunications symposium (WTS), 2021: IEEE, pp. 1-6, doi: https://doi.org/10.1109/WTS51064.2021.9433711.
[73] Z. Liu et al., "PPTM: A privacy-preserving trust management scheme for emergency message dissemination in space–air–ground-integrated vehicular networks," IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5943-5956, 2021, doi: https://doi.org/10.1109/JIOT.2021.3060751.
[74] A. Bhargava and S. Verma, "DUEL :Dempster uncertainty-based enhanced-trust level scheme for VANET," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 15079-15090, 2022, doi: https://doi.org/10.1109/TITS.2021.3136548.
[75] A. Rehman et al., "CTMF: Context-aware trust management framework for internet of vehicles," IEEE Access, vol. 10, pp. 73685-73701, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3189349.
[76] Z. Bi, G. Xu, G. Xu, M. Tian, R. Jiang, and S. Zhang, "Intrusion detection method for in-vehicle can bus based on message and time transfer matrix," Security and Communication Networks, vol. 2022, 20.22, doi: https://doi.org/10.1155/2022/2554280.
[77] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "A security solution for V2V communication within VANETs," 2018 Wireless Days (WD), pp. 181-183, 2018, doi: https://doi.org/10.1109/WD.2018.8361716.
[78] 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, doi: https://doi.org/10.1109/ACCESS.2018.2837887.
[79] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-rimy, A. Alsaeedi, and W. Boulila, "Ensemble-based hybrid context-aware misbehavior detection model for vehicular ad hoc network," Remote Sensing, vol. 11, no. 23, p. 2852, 2019, doi: https://doi.org/10.3390/rs11232852.
[80] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, 2023, doi: https://doi.org/10.1109/TITS.2023.3275077.
[81] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, and K.-K. R. Choo, "BCGS: Blockchain-assisted privacy-preserving cross-domain authentication for VANETs," Vehicular Communications, vol. 41, p. 100602, 2023, doi: https://doi.org/10.1016/j.vehcom.2023.100602.
[82] H. Liu, H. Huang, Y. Zhou, and Q. Chen, "Improvement of blockchain-based multi-layer location data sharing scheme for Internet of Things," Computer Communications, vol. 201, pp. 131-142.2023 , doi: https://doi.org/10.1016/j.comcom.2023.02.005.
[83] S. Prajapat et al., "Secure Lattice-Based Aggregate Signature Scheme for Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, pp. 1-15, 2024, doi: https://doi.org/10.1109/TVT.2024.3383967.
[84] S. Yu et al., "Efficient ECC-based Conditional Privacy-preserving Aggregation Signature Scheme in V2V," IEEE Transactions on Vehicular Technology, 2023, doi: https://doi.org/10.1109/TVT.2023.3287989.
[85] Q. Wang, Y. Li, Z. Tan, N. Fan, and G. Yao, "Conditional privacy-preserving authentication scheme for V2V communication without pseudonyms," Journal of Information Security and Applications, vol. 78, p. 103616, 2023, doi: https://doi.org/10.1016/j.jisa.2023.103616.

[86] A. Namdev and H. Lohiya, "Design and Implementation of Biometric Blockchain Authentication for VANET Security," in 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2024: IEEE, pp. 1-8, doi: https://doi.org/10.1109/SCEECS61402.2024.10482007.

[87] H. Su, S. Dong, N. Wang, and T. Zhang, "An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs," Vehicular Communications, vol. 45, p. 100727, 2024, doi: https://doi.org/10.1016/j.vehcom.2024.100727.

[88] J. Huang et al., "Secure data sharing over vehicular networks based on multi-sharding blockchain," ACM Transactions on Sensor Networks, vol. 20, no. 2, pp. 1-23, 2024, doi: https://dl.acm.org/doi/10.1145/3579035.

[89] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body Area Network Security :A Fuzzy Attribute-Based Signcryption Scheme," Selected Areas in Communications, IEEE Journal on, vol. 31, pp. 37-46, 09/01 2013, doi: https://doi.org/10.1109/JSAC.2013.SUP.0513004.

[90] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," Vehicular Technology, IEEE Transactions on, vol. 59, pp. 1606-1617, 06/01 2010, doi: https://doi.org/10.1109/TVT.2009.2038222.

[91] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "EDAAAS: Efficient distributed anonymous authentication and access in smart homes," International Journal of Distributed Sensor Networks, vol. 12, 12/09 2016, doi: https://doi.org/10.1177/1550147716682037.

[92] T. W. Chim, S. Yiu, and V. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Networks, vol. 9, pp. 189-203, 03/01 2011, doi: https://doi.org/10.1016/j.adhoc.2010.05.005.

[93] N. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. U. Rahman, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," IEEE Access, vol. 6, pp. 31808-31819, 2018, doi: https://doi.org/10.1109/ACCESS.2018.2845464.

[94] J. Li, Y. Ji, K.-K. R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of Vehicles," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10332-10343, 2019, doi: https://doi.org/10.1109/JIOT.2019.2938008.

[95] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5535-5548, 2020, doi: https://doi.org/10.1109/TVT.2020.2981934

[96] H. Tan and I. Chung, "Secure Authentication and Key Management with Blockchain in VANETs," IEEE Access, vol. 8, pp. 2482-2498, 12/27 2019, doi: https://doi.org/10.1109/ACCESS.20.19.2962387

[97] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, "An Anonymous Authentication and Key Establish Scheme for Smart Grid: FAuth," Energies, vol. 10, no. 9, p. 1354, 2017, doi: https://doi.org/10.3390/en10091354.

[98] K. Mahmood, S. A. Chaudhry, S. H. A. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," Future Gener. Comput. Syst., vol. 81, pp. 557-565, 2018, doi: https://doi.org/10.1016/j.future.2017.05.002

[99] X. Li ,F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," Journal of Parallel and Distributed Computing, vol. 132, pp. 242-249, 2019/10/01/ 2019, doi: https://doi.org/10/1016.j.jpdc.2017.11.008.

[100] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: Password-based anonymous lightweight key agreement framework for smart grid," International Journal of Electrical Power & Energy Systems, vol. 121, p. 106121, 20 /20/10/01 ,2020, doi: https://doi.org/10.1016/j.ijepes.2020.106121.

Journal of Basrah Researches (Sciences) **50**(1), 223 (2024)
DOI: https://doi.org/10.56714/bjrs.50.1.19

أدوات التشفير والبرمجيات الرئيسية للمصادقة في بيئة شبكة المركبات المخصصة: مراجعة الأدبيات

زهراء شاكر الزيدي، علي عادل ياسين* ، زيد امين عبدالجبار

قسم علوم الحاسوب، كلية التربية للعلوم الصرفة، جامعة البصرة، البصرة، العراق.

معلومات البحث

الاستلام 25 اذار 2024
القبول 3 نيسان 2024
النشر 30 حزيران 2024

الكلمات المفتاحية

شبكة المركبات المخصصة، المصادقة، الأمن، النزاهة، البلوك تشين، حوسبة الضباب.

الملخص

توفر الشبكات المخصصة للمركبات (VANETs) إمكانية تحسين كفاءة النقل من خلال تسهيل مشاركة معلومات المرور بين المركبات. يتوقف قبول شبكات VANETعلى دقة الرسائل وتوقيتها وضمان سلامة الفرد من خلال حماية الخصوصية. وتتطلب دقة الرسائل المصادقة على المركبات. ويترجم هذا إلى متطلبات آلية مصادقة فعالة تحافظ على الخصوصية إلى جانب الحاجة إلى الخصوصية والتسليم المحدد زمنياً للرسائل. يجب معالجة قضايا الأمان والخصوصية بشكل أساسي في تصميم انظمة الاتصال. وقد تم اقتراح مخططات مصادقة مختلفة للحفاظ على الخصوصية لضمان صحة الرسائل أثناء اتصالات المركبات. ومع ذلك، فإن معظم المخططات لا تحل بشكل كامل المشكلات المتعلقة بالأمان والخصوصية والتهديدات ونقاط الضعف والاتصالات وتكاليف الحوسبة. نركز في هذه الدراسة على استراتيجيات التشفير المقترحة لتحقيق الخصوصية والمصادقة، مثل المخططات القائمة على الهوية، والقائمة على تشفير المفتاح العام، والقائمة على الأسماء المستعارة، والمخططات القائمة على تقنية blockchain . نقدم دراسة شاملة للمخططات مع تصنيفاتها ونقاط قوتها وضعفها. تكشف الدراسة أن معظم مخططات المصادقة الحالية تتطلب سلطات موثوقة غير شفافة في عملها، ويتطلب إبطال الشهادات عمليات حسابية وتخزين ثقيلة إلى جانب حاجتها الى وقت طويل للبحث. كما أن نفقات الحوسبة والاتصالات المطلوبة للمصادقة كبيرة، مما يؤثر بشكل كبير على تسليم الرسائل في الوقت المناسب. هناك حاجة إلى مزيد من العمل لتطوير مخططات مصادقة فعالة تحافظ على الخصوصية في الشبكات المخصصة للمركبات.

Citation: Zahraa S. A., et al., J. Basrah Res. (Sci.) **50**(1), 223 (2014).
DOI:https://doi.org/10.56714/bjrs.50.1.19

***Corresponding author email :** ali.yassin@uobasrah.edu.iq

N: 1817-2695 (Print); 2411-524X (Online)
line at: https://jou.jobrs.edu.iq