Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

A comprehensive survey on authentication and privacy-preserving schemes in VANETs

Pravin Mundhe [*], Shekhar Verma, S. Venkatesan

Indian Institute of Information Technology, Allahabad, U.P., 211015, India

ARTICLE INFO

Article history:
Received 18 September 2020
Received in revised form 19 May 2021
Accepted 27 May 2021
Available online xxxx

Keywords:
VANETs
Security
Privacy
Authentication

ABSTRACT

Vehicular ad hoc networks (VANETs) promise to enhance transport efficiency, passenger safety, and comfort through the exchange of traffic and infotainment information to vehicles. The acceptance of VANET hinges on the correctness and timeliness of messages and assurance of an individual's safety through privacy protection. The message accuracy requires the authentication of vehicles. This translates into the requirement of an efficient privacy-preserving authentication mechanism along with the need for privacy and time-bound delivery of messages. The security and privacy issues must be addressed primarily in the communication protocol's design. Different privacy-preserving authentication schemes have been proposed to ensure the correctness of messages during vehicular communications. However, most of the schemes do not entirely solve the issues related to security and privacy, threats and vulnerabilities, communication, and computation costs. In this survey, we focus on cryptographic techniques proposed to achieve authentication, privacy, and other security features required in VANETs like symmetric key cryptography-based schemes, public key cryptography-based schemes, identity-based cryptography schemes, pseudonym-based schemes, group and ring signature-based schemes, and blockchain-based schemes. We provide a comprehensive study of schemes with their classifications, strengths, and weaknesses. The study reveals that most of the existing authentication schemes require trusted authorities that are opaque in their functioning, certificate revocation requires heavy computation and storage along with a large amount of lookup time. The computation and communication overhead required for authentication is significant, which drastically affects the timely delivery of messages. More work is needed for the development of lightweight and efficient privacy-preserving authentication schemes in VANETs.

Contents

1. Introduction 2
  1.1. Comparison with existing surveys 2
  1.2. Main contributions of the present survey 2
2. Background of VANET 4
  2.1. System model 4
  2.2. Properties of VANETs 4
  2.3. Types of standards in VANETs 4
  2.4. Messages in VANETs 4
3. Security requirements in VANETs 4
  3.1. Authentication in VANETs 5
  3.2. Privacy in VANETs 5
4. Classification of authentication and privacy-preserving schemes 6
  4.1. Symmetric key cryptography-based schemes 6
  4.2. Public key cryptography-based (PKC) Schemes 6
  4.3. Identity-based cryptography (IBC) schemes 7
  4.4. Certificateless signature-based schemes 9
  4.5. Pseudonym-based schemes 10

[*] Corresponding author.
E-mail addresses: pcl2014001@iiita.ac.in (P. Mundhe), sverma@iiita.ac.in (S. Verma), venkat@iiita.ac.in (S. Venkatesan).

https://doi.org/10.1016/j.cosrev.2021.100411
1574-0137/

4.6. Group signature and Ring signature-based schemes 11
4.7. Blockchain-based Schemes 13
5. Discussion 15
6. Conclusion 15
Declaration of competing interest 16
References 16

1. Introduction

VANET is a wireless network with vehicles (*e.g.*, cars, buses, trucks) and adjacent roadside infrastructure [1]. Each vehicle is equipped with a transmission device that enables the vehicles to communicate with nearby vehicles and infrastructure [2]. A VANET consists of the on-board unit (OBU) on vehicles, the roadside unit (RSU), and trusted authority (TA). The TA is a third-party device that registers RSUs, authenticates vehicles, and monitors the entire network with the help of RSUs [3]. The RSU is a stationary wireless device (*e.g.*, WiFi, WiMAX) located along the roadside that works as a mediator between TA and vehicle's OBU and passes safety instructions to vehicles within the range [4]. The OBU is a storage device fixed on a vehicle to receive or transmit important messages to other adjacent vehicles.

The communication in VANETs is carried out using the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I/I2V) communication mode, as shown in Fig. 1. Both the V2V and V2I communications use the dedicated short-range communication (DSRC) protocol [5]. Later, the DSRC protocol is referred to as WAVE, *i.e.*, wireless access in vehicular environments that uses the IEEE 802.11p standard for wireless communication [6]. A vehicle broadcasts informative messages every 100–300 ms to RSUs or nearby vehicles. As per the DSRC standard, the maximum communication range in VANETs can be up to 1 km, and the transmission speed varies from 6 to 27 Mbps. Messages are categorized as safety and non-safety messages. The vehicle processes, exchanges, transmits, or receives important messages about traffic situations to or from other vehicles using V2V communication. Similarly, vehicles and RSUs communicate with each other using V2I/I2V communication, and RSU provides real-time services such as navigation, internet connectivity, and live streaming of accidents to respective drivers [7,8].

A vehicle forwards safety messages to the remote vehicle using the services of a vehicle within the range. If any in-between vehicle fails to forward the message; the sender can still forward the message using other active vehicles. Hence, the VANET provides sufficient storage and power to all the vehicles for broadcasting information about accidents, emergencies, and traffic jams to adjacent members [9,10]. Apart from safety messages, vehicles can also transmit informative messages related to road conditions so that the receiver can drive to other safer roads to avoid accidents or responds to the information received from other members [11,12]. An attacker can eavesdrop, modify, repeat, or delete messages as they are transmitted using an open wireless channel. For example, the attacker may modify safety-related messages to accident-forming messages to harm vehicles' drivers. It may also create a false illusion of traffic jams to disturb the normal functioning of the network [13,14]. A suitable mechanism needs to in-build in VANET and communication protocol to address the challenge posed by an attacker. These security challenges manifest themselves as authentication and privacy issues that must be solved before deploying a VANET.

1.1. Comparison with existing surveys

Several surveys [15–20] have been proposed in the area of privacy-preserving authentication schemes in VANETs. Table 1 gives an overview of some of the existing surveys on authentication and privacy-preserving schemes in VANETs. These surveys thoroughly discuss routing protocols, security requirements, different threats and attacks, and authentication and privacy schemes. However, there are very few comprehensive surveys exist that cover all the properties of VANETs. Mejri et al. [21] provided basic architecture and security and privacy problems present in VANETs. It also categorized and grouped many studies and cryptographically compared them. Similarly, the study of security requirements and issues present in pseudonym-based schemes have been given by Petit et al. [15]. This study also provided a brief description of schemes based on symmetric key cryptography, public key cryptography, identity-based cryptography, and group signatures. Qu et al. [16] presented a survey that describes existing authentication schemes that solve various security issues leading to disturbances in VANET operations. It also describes privacy-preserving schemes that can achieve conditional privacy to remove malicious vehicles from the network.

Moreover, a study about pseudonym changing mechanisms and their classification is provided by Boualouache et al. [17]. Besides, it presented their comparison and different open challenges in VANETs. In [18], Lu et al. provided a survey of recent security, privacy, trust-based trends. It describes different types of security and privacy attacks, standards, transmission patterns, and characteristics of VANET. However, it does not provide any comparison with the existing surveys. Similarly, a survey of authentication and privacy schemes in VANETs is provided by Ali et al. [19]. It gives a classification of multiple privacy-preserving schemes and a comparison of security requirements achieved by them. But, it lacks a description of security attacks and privacy issues in VANETs. Manivannan et al. [20] presented a survey of secure authentication and privacy-preserving schemes. It also gives an overview of authentication, privacy, and message distribution problems in VANETs. This paper studies protocols that use public key cryptography, identity-based cryptography, pseudonyms, and group signature. Table 2 shows the comparison of the proposed survey with existing surveys based on the security mechanism applied.

1.2. Main contributions of the present survey

The main focus of the present survey is to analyze, review, and mention the limitations of different authentication and privacy-preserving schemes proposed in the last ten years. This article also studies basic requirements in the area of VANET security. The main contributions of the present survey can be summarized as follows:

1. In this paper, we have thoroughly provided the details about various security and privacy requirements in VANETs that are needed to establish efficient and reliable communication between the network members.
2. We have also presented the overview of basic architecture and properties of VANET along with the types of standards and messages used.

Table 1
Overview of existing surveys on VANETs.

Survey	Year	Journal	Major contribution	Limitation
Petit et al. [15]	2014	IEEE communications surveys & tutorials	Studies security requirements and issues present in pseudonym-based schemes in VANETs	Does not review schemes based on certificateless signatures
Qu et al. [16]	2015	IEEE Transactions on Intelligent Transportation Systems	Describes the existing privacy-preserving schemes which can achieve conditional privacy to remove malicious vehicles from the network	Does not consider mechanisms based on ring signatures
Boualouache et al. [17]	2017	IEEE Communications Surveys & Tutorials	Provides classification and comparison of pseudonym changing mechanisms in VANETs	Focuses only on pseudonym changing strategies for VANETs
Lu et al. [18]	2018	IEEE Transactions on Intelligent Transportation Systems	Studies recent security, privacy, trust-based trends in VANETs and describes different types of security attacks, transmission patterns, and characteristics	Does not provide any comparison with the existing surveys
Ali et al. [19]	2019	Vehicular Communications	Reviews authentication and privacy schemes in VANETs and gives classification of multiple privacy-preserving schemes and comparison of security requirements achieved by them	Lacks description about security attacks and privacy issues in VANETs
Manivannan et al. [20]	2020	Vehicular Communications	Describe various secure authentication and privacy-preserving schemes and presents overview of authentication, privacy, and message distribution problems	Fails to review techniques based on symmetric key cryptography, ring signature, and blockchain

Table 2
Comparison with similar existing surveys in view of security mechanisms.

Security mechanism	Petit et al. [15]	Qu et al. [16]	Boualouache et al. [17]	Lu et al. [18]	Ali et al. [19]	Manivannan et al. [20]	The proposed survey
Symmetric key cryptography	✓	✓	×	✓	×	×	✓
Public key cryptography	✓	✓	×	✓	✓	✓	✓
Identity-based cryptography	✓	✓	×	✓	✓	✓	✓
Certificateless signatures	×	×	×	✓	×	×	✓
Pseudonyms	✓	✓	✓	×	✓	✓	✓
Group signature	✓	✓	×	✓	✓	✓	✓
Ring signature	×	×	×	×	×	×	✓
Blockchain	×	×	×	×	×	×	✓

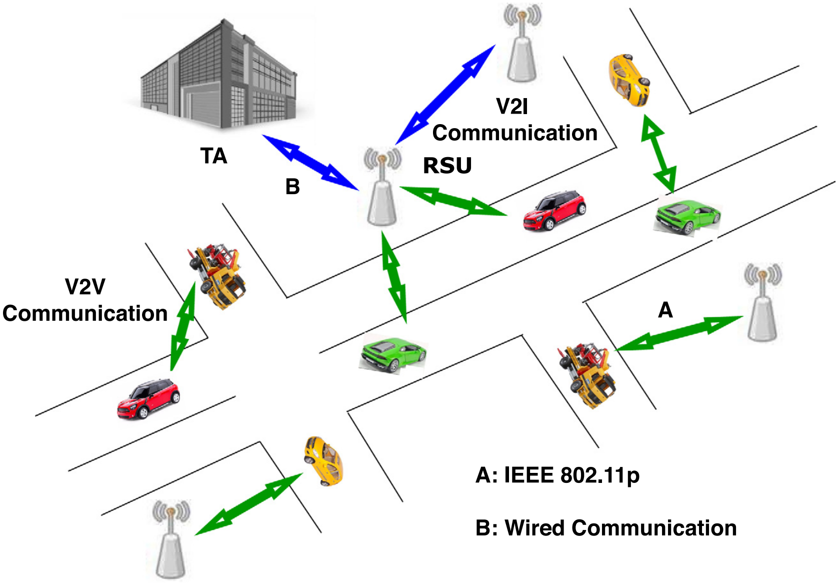

Fig. 1. Basic architecture of VANET.

3. 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.
4. We have classified the existing schemes into seven 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.
5. 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.
6. In the end, we have provided a summary of cryptographic methods used in VANETs along with their key features and drawbacks.

Manuscript organization: The rest of the manuscript is organized in the following sections as: Section 2 presents the basic system model, properties, types of standards, and messages in VANETs. In Section 3, fundamental security requirements in VANETs are explained. Section 4 provides the classification of existing schemes based on cryptographic methods used during their implementation. In Section 5, a brief discussion about the security mechanisms used to ensure security in VANETs is presented. Finally, Section 6 concludes the proposed survey by highlighting its strengths and observations.

2. Background of VANET

In this section, we explain the system model and security properties, types of messages and standards, and some preliminaries in VANETS briefly.

2.1. System model

Fig. 1 shows the basic system model of a VANET that generally contains the following components [22].

- **OBU:** Each vehicle in the network is fitted with an onboard unit that communicates with RSUs and other vehicle's OBU. It contains sensors, processing units, systems, and storage devices. The processing unit processes the gathered information from sensors and forms messages. Later, these messages are transmitted to adjacent members using wireless channels.
- **RSU:** The roadside units are usually stationary devices, and they are located along the roadside, crossings, or parking spaces. RSUs have a transmission device that supports DSRC as well as infrastructural communication. The primary objectives of RSUs are: (1) To make internet services available to OBUs. (2) To increase the transmission range of VANETs by repeating messages to other RSUs and OBUs. (3) To report traffic conditions or accidental situations.
- **TA:** The trusted authority is connected with RSUs using a wired channel. It acts as an administrator and manages the entire network. Also, TA is responsible for generating, broadcasting, and periodically updating the system parameters in the network. Moreover, it authenticates vehicles and removes them if they are involved in malicious activity or transmitting fraud messages. Hence, TA is having huge storage capacity and high computation power as compared to OBU and RSUs.

2.2. Properties of VANETs

Following are the basic unique properties of VANETs:

1. *Computation and storage capacity:* The processing of received information, computation of desired results, and storing and forwarding them to other members is crucial. Hence, the calculation and storage of data is a challenging issue in VANETs [23].
2. *Mobility:* Vehicles in VANETs generally travel at high speeds. Hence, a small delay that occurred during transmission in V2V communication may lead to severe problems [23].
3. *Network topology:* Due to the high speeds of vehicles, the topology of VANETs changes rapidly. Hence, network vulnerability increases, and it becomes difficult to recognize a malicious vehicle [23].
4. *Unpredictability:* Because of vehicles' high mobility, the connection between two members is established only once while traveling. Hence, it is not easy to preserve real identity or personal information in VANETs [24].

2.3. Types of standards in VANETs

The communication in VANETs takes place using the following standards:

- *IEEE 802.11p:* This standard is specially added to IEEE 802.11 protocols to assist the VANET. It gives the physical and medium access layers specifications for VANETs [25].
- *DSRC:* A bandwidth range from 5850 to 5925 GHz and a 75 MHz spectrum has been allotted for DSRC by the federal communications commission (FCC). DSRC band is divided into channels numbered 172, 174, 176, 178, 180, 182, and 184. All channels are service channels except for 178, which is the control channel. The channel 172 is used for important life-safety applications that need low latency and high availability, while channel 184 is used for public safety [26].
- *WAVE:* The WAVE (*i.e.*, IEEE 1609 family) specifies architecture, protocols, and interfaces to set up V2I and V2V communications. It also defines a wide range of applications for transportation as well as security services [27].

2.4. Messages in VANETs

V2V communication is used to transmit crucial information (*e.g.*, accidents, road conditions) among vehicles [28]. Similarly, the safety messages are exchanged between infrastructure and vehicles using V2I communication. The messages in VANETs can be classified into different categories, as follows:

1. *Beacon messages:* These are transmitted periodically to adjacent RSUs and vehicles containing values of speed, location, direction, *etc* [29].
2. *Warning messages between vehicles:* These need to be transmitted to a specific or set of vehicles to warn about fatal accidents. Hence, to send messages securely, a reliable and efficient routing protocol is needed [29].
3. *Warning messages between vehicles and RSUs:* RSUs broadcast warning messages to vehicles within their range when major threats are detected to ensure driver's safety. Transmission of such messages is high where there are big crossings or high traffic density [30].
4. *Batch communication:* These messages are transmitted to accelerate traffic movements, increase the safety of vehicles, and communicate the current status of road conditions [30].

3. Security requirements in VANETs

A VANET has two differentiating characteristics that guarantee the authentication of vehicles [31]. One, vehicles continually change their neighborhood so that the interaction between vehicles is temporary, and two, V2V communication facilitates information exchange between vehicles without intervention or infrastructure participation. However, V2V communication also necessitates vehicles to trust the information transmitted by other vehicles. Authentication of vehicles is necessary to mitigate this tendency. However, the process of authentication of vehicles may reveal the identity of vehicles. The privacy breach may be a serious threat to the drivers whose identity is revealed through their vehicle. This threat may outweigh the advantages of benefits of VANET and desist a vehicle owner to join the VANET.

Moreover, the lack of vehicle authentication to preserve privacy may lead to a broadcast of forged malicious messages. Unconditional privacy may also lead to malicious messaging by a vehicle. The privacy should be conditional to allow non-repudiation so that a vehicle's identity can be revealed if needed by law. Thus, privacy-preserving authentication is necessary for the viability and acceptance of VANET. A VANET cannot be used without fulfilling these essential security requirements.

3.1. Authentication in VANETs

The primary issue that occurs while deploying VANETs is when securing V2I and V2V communications. If a vehicle successfully executes any attack, then it can seriously affect the network operations and services. The attacker may remove, modify, track, or repeat messages to unsettle the network. It may alter the crucial information transmitted by the authority or vehicles using messages [32]. Similarly, it may also duplicate the messages or their contents and try to stop transmitting messages. Besides, the attacker may interrupt the connection or listen attentively to the communication and use the fetched secret information to perform malicious operations or attacks. It may also configure traffic signals deliberately to make road jams or street blockage. A vehicle must be prevented from broadcasting fraudulent messages into the network. Hence, detecting and removing a malicious vehicle from VANET is a highly important job of the authority. Besides, authentication of the vehicle's real identity is also required. Therefore, vehicle authentication is a critical security requirement in VANETs that helps to determine whether the valid member has transmitted the message or not [33].

Similar to identity authentication, message authentication is also necessary for VANETs. It is required to stop fraud messages from getting forwarded into the network and remove them instantly. It ensures that the message is not duplicated or modified during transmission. TA may convey the wrong decision or instruction, resulting in a disordered traffic situation if the attacker modifies the contents of the received message [34,35]. Hence, the receiver must check the correctness of the message and finish message authentication within a suitable time. The vehicle may need to authenticate a massive number of messages. Also, the number of received messages increases with time, as the vehicle may receive plenty of messages within a short duration. Sometimes, the receiver may not complete the authentication process because of its small storage and less computation power. The malicious content of the message can seriously harm the receiver or its operations (*e.g.*, an accident of the vehicle, causing injury to the driver) [36,37]. The administrator needs to go through many difficulties when it tries to identify and differentiate between operations of authorized and unauthorized members. A vehicle may broadcast malicious information in the network to fulfill personal interest [38,39]. Therefore, message authentication is essential in VANETs, and a vehicle must verify the authenticity of the message.

3.2. Privacy in VANETs

The authority or receiver must preserve the sender's privacy when performing the authentication procedure. An attacker may use the authorized vehicle's real identity to transmit malicious information while keeping its identity secret into the network. It may also leak the authorized vehicle's private information. Alternatively, the attacker may try to get the location of the vehicle using its route or navigation information and harass its owner [40]. Therefore, the VANET must ensure identity privacy and location privacy to its users. Sometimes, the authorized vehicle may be involved in fraud actions and try to interrupt the regular traffic. Hence, the authority must have the requisite information about the vehicle to reveal it when required. To protect the real identity of a legitimate vehicle and to discover and remove a malicious vehicle from the network simultaneously is an essential, complicated operation in VANETs. Hence, the authority must ensure conditional privacy-preserving authentication to all the vehicles in the network.

Moreover, complete privacy is also needed in certain conditions so that the sender's real identity needs to be protected at any cost (*e.g.*, the information of the accident's witness) [41]. In such conditions, the witness does not want its real identity to be exposed to avoid future problems. Therefore, the authority must ensure complete privacy to vehicle owners in such cases.

Apart from authentication and privacy, the following are some of the basic requirements in VANETs [42]:

- *Availability:* This property ensures that the network's hardware or software would operate normally even if the attacker executes an attack in the network. The components of the network must be available under any threat and maintain its performance.
- *Confidentiality:* This property ensures that the safety message or information transmitted is delivered to its corresponding recipient or members in the original format. Only the designated members have the right to view or read the contents of the message. The violation of this property can leak secret information about the sender or receiver.
- *Integrity:* This property ensures that the information or messages are transmitted in the network without any modification or update. The attacker may update or add its content in the message to create disturbance in the network. The receiver must verify the message to ensure it is not corrupted or modified during transmission.
- *Non-repudiation:* This property ensures that the sender would not deny the message ownership. This property is required when a mishap or accident happens because of transmitting fraud messages in the network. Hence, the sender must take responsibility for the messages that it has transmitted while traveling.
- *Scalability:* This property ensures that network efficiency and productivity would not reduce even if the number of registered members continually varies. The vehicles in VANETs regularly travels due to which the vehicle density can increase or decrease suddenly. The scalability ensures that this sudden variation would not affect the performance of the vehicles, RSUs, or authorities.
- *Unforgeability:* This property ensures that an attacker would not forge the signature of the correct message transmitted by the valid member of the network. An attacker may replay or reuse the correct message and create a duplicate signature.
- *Unlinkability:* This property ensures that an attacker would not link the given signature or message to the respective vehicle's driver or its real identity. This property helps the VANET to maintain the vehicle's secret information hidden even though the message, its contents, or signature are analyzed.
- *Traceability and member revocation:* This property ensures that the tracing manager or trusted authority can find out or disclose the real identity of the malicious vehicle if desired. Even though the vehicle's real identity must be protected, but sometimes finding the same is required to maintain the order in the network. Moreover, the authority must be able to remove the malicious vehicle from VANET before it does some damage to the network. The member revocation is essential so that the malicious vehicle does not affect the normal functioning of the network and the remaining vehicles.
- *Transparency:* This property ensures that the operations of the trusted authority or administrator are trustworthy and reliable. The VANET must fulfill this property so that each member of the network believes the operations performed by the authority or other members.

4. Classification of authentication and privacy-preserving schemes

In this section, we provide the classification of existing authentication and privacy-preserving schemes. This classification is based on mechanisms applied using symmetric key cryptography, public key cryptography, identity-based cryptography, pseudonyms, group and ring signature, and blockchain.

4.1. Symmetric key cryptography-based schemes

This category depends on the symmetric key cryptography schemes in which a symmetric key is mainly used to deliver security in VANETs. Both the sender and receiver can efficiently compute the symmetric key and use it to achieve privacy during communication. Moreover, message authentication code (MAC) is also used to authenticate messages in these schemes. For each message, the sender produces a MAC using the shared secret key. A member of the network having the same key can verify the MAC received along with the message. These schemes are used in VANETs as they have less computation and communication costs, and the verification can be performed rapidly.

In [43], two techniques, *i.e.*, dual authentication and key management have been proposed to achieve secure data transmission in VANETs. In case of the first technique, the members provide their essential details such as identity, email-id, address to the TA during *offline registration*. Then, the vehicle is authenticated using the fingerprint stored in the smart card. Later, TA's authentication is performed and the *authentication code* is also generated. In the second technique, the TA produces two different dual keys for two separate groups operating in the network. In the *initial setup* stage, TA chooses group key and secret key values from a multiplicative group. Next, the group members register to TA and receive the group keys. Then, the vehicles can securely communicate with other vehicles and TA. Similarly, when a primary user joins or leaves the network, the corresponding group key is updated and communicated to all the group members. However, this scheme does not provide information about packet loss ratio and end-to-end delay in VANETs.

In [44], privacy-preserving authentication and key distribution techniques have been proposed. In the first approach, an anonymous authentication protocol has been proposed to preserve privacy and achieve the message integrity of the broadcast messages. The sender produces a temporary anonymous certificate and transmits a signature along with the message. Later, the receiver can authenticate the source and message by verifying the certificate and signature. In the second approach, a secure key distribution process is conducted in which each member of the network gets an anonymous group key. Even if an RSU is involved in any malicious activity, the TA can determine its real identity. This scheme provides conditional tracking, non-repudiation, and resistance against man-in-the-middle (MITM) attack. However, this scheme does not offer resilience against the replay attack and impersonation attack.

A two-factor lightweight privacy-preserving authentication scheme (2FLIP) using bilinear pairing has been proposed in [45]. It depends on the decentralization of certificate authority (CA) and two-factor authentication using a biological password. This scheme requires producing a MAC for signing messages. In this, each vehicle is fitted with a telematics device (TD) for using biometric technology (*e.g.*, eye detection, face recognition, fingerprint) and TD jointly works with the vehicle's TPD. Digital signature verification is used when a vehicle wants to change the system keys. The decentralization technique reduces the certificate management and distribution load of CA. This scheme can ensure conditional privacy and non-repudiation using biological password-based 2FA. It need not maintain information about revoked vehicles and also provides resilience against denial of service (DoS) attack. Moreover, 2FLIP increases network efficiency by reducing the communication, computation, and key updation overhead. However, this scheme does not provide batch message verification.

In [46], a bilinear pairing-based efficient anonymous batch authentication (EABA) scheme has been proposed. It uses a hash-based message authentication code (HMAC) and a group-based scheme to eliminate the memory requirement of certificate revocation lists (CRLs) and huge communication overhead. It ensures that only authorized vehicles enter the group and do not need to spend time on the CRLs checking process. Also, it uses pseudonyms and identity-based signatures to ensure conditional privacy and batch message verification, respectively. The major advantage of HMAC is that it increases network performance by removing the need for CRLs. However, the transmission delay of EABA is high, and packet loss also increases as the speed increases. Table 3 gives a summary of symmetric key cryptography-based schemes.

4.2. Public key cryptography-based (PKC) Schemes

This category depends on the public key cryptography-based schemes in which TA controls public–private key pairs' composition and distribution to valid members for communication purposes. This infrastructure contains the vehicle's public key and CA's digital signature for authentication. These schemes are used to deploy a robust and secure method for the privacy-preserving authentication of vehicles. The traceability is achieved using certificates issued by CA.

A bilinear pairing-based authentication scheme using proxy vehicles has been proposed in [47] to reduce the load on RSUs. This scheme uses the concept of distributed computing as the RSU cannot authenticate each message-signature pair. The previously decided proxy vehicles authenticate multiple signatures at a time, and the output results are passed on to the related RSU. If any incorrect result is found after verifying all the results received from each proxy vehicle, then such results are withdrawn. This scheme can perform well, even if a few proxy vehicles are compromised. Also, the TA can remove the proxy vehicle from the network if it performs any malicious activity. However, the policies for choosing proxy vehicles within an RSU range and for removing malicious vehicles from the network are doubtful.

In [48], a privacy-preserving authentication scheme for vehicular communication with hierarchical aggregation and fast response has been proposed. A vehicle registers itself to the key generation center (KGC), which keeps the details of registered vehicles in the members list (ML). Next, the vehicle requests short-term pseudonyms (STP) and short-term private key (STK) associated with STP to KGC. Then, the sender signs the message using the common string and signature generation protocol to ensure secure vehicular communications. However, it does not provide a comparative analysis to prove its effectiveness over other schemes.

A computationally efficient privacy-preserving anonymous authentication scheme has been proposed in [49]. In this, the TA provides a password, re-encryption key, public–private key pair, and license to each vehicle after its offline registration completion. Then, TA stores the vehicle's real identity in its tracking list to achieve traceability. Later, a vehicle authenticates itself to the RSU (within its range) by using the short-lived public key, private key, and anonymous certificate. However, the maintenance and revocation of pseudonym certificates are time-consuming and inefficient operations.

In [50], an efficient anonymous conditional privacy-preserving authentication scheme using bilinear pairing has been proposed.

Table 3
Symmetric key cryptography-based schemes.

Scheme	Properties and advantages	Limitations
[43]	This scheme provides authentication of each member and ensures efficient key distribution for secure data transmission in the network	It does not provide information about packet loss ratio and end-to-end delay in VANETs.
[44]	This scheme proposes an anonymous authentication and key distribution protocol that preserves privacy as well as achieves message integrity.	It does not provide resilience against the replay attack and impersonation attack.
[45]	This scheme is based on the decentralization of CA and two-factor authentication method that uses a biological password. It reduces the computation and key updation overhead.	It does not provide batch message verification.
[46]	This scheme proposes an anonymous batch authentication method using bilinear pairing. It eliminates the requirement of CRLs by employing an HMAC and group-based scheme.	It has increased transmission delay, and packet loss increases with speed.

In this, vehicles and RSUs authenticate each other anonymously without any involvement of TA. The increase in vehicle numbers within an RSU region slightly affects the message loss ratio while achieving scalability. However, the management and revocation of anonymous certificates increase the communication and computation cost notably. Each vehicle must store a large number of anonymous certificates in advance to ensure privacy. Besides, the TA gets affected by the heavy burden of storing and managing each vehicle's anonymous certificate.

In [51], an anonymous message authentication protocol using local identity (LIAP) has been proposed. A vehicle requests a local master key to registered RSU within its range during the *master key retrieval* stage. After getting the key, a vehicle generates its anonymous identity to produce a signature over the message. Later, the malicious vehicle's real identity can be tracked, and the corresponding vehicle can be revoked from the network. This scheme provides message authentication and integrity, non-repudiation, and conditional privacy. Also, it provides resistance to collusion attack and replay attack. However, the certificate distribution, CRL management, and member revocation increase the computation and communication overhead.

Similarly, an efficient fog computing-based revocation scheme has been proposed in [52] that uses the Merkle hash tree instead of CRL. The Merkle hash tree removes the time needed for CRL checking. The roads are divided into different regions, in which fog nodes supervise all the vehicles locally and act as a trusted gateway. The fog node is responsible for issuing certificates to all the vehicles within its range and passes the vehicle's request of certificate issuance to CA. The fog node updates the vehicle when it receives the certificate. CA builds the Merkle hash tree to maintain the record of certificate revocation, and revoked certificates are kept at leaf nodes. Later, the fog node broadcasts the tree to vehicles during operation. However, maintaining a fresh copy of the tree at each node is difficult.

A privacy-preserving certificate linkage or revocation scheme has been proposed in [53]. In this, a vehicular public key infrastructure (VPKI) without linkage authority (LA) is used. Also, the contributions to improve and solve the issues found in the security credential management system (SCMS) are provided. Firstly, to improve the system's long-term privacy, two birthday attacks against the certificate revocation process of SCMS are described and solved. Secondly, a process to simplify SCMS's architecture is proposed that eliminates the requirement of LA. This process removes the deployment costs that lower the chances of systems attack especially replay attacks. Table 4 gives a summary of the public key cryptography-based schemes.

4.3. Identity-based cryptography (IBC) schemes

This category depends on the identity-based cryptography schemes. In this, the vehicle's necessary information (*e.g.*, telephone number, email id) is used to generate its public key. Hence, the requirement of certificate management and distribution is eliminated. These schemes do not use certificates for message authentication. The KGC issues private key to each member and acts as a trusted third-party member.

An identity-based privacy-preserving authentication scheme in VANETs has been proposed in [54]. A regional transportation authority (RTA) loads a pool of short-lived pseudonyms into the vehicle's TPD. When a vehicle wants to transmit the message, a local shared secret key will be derived from each member which is involved in communication. Later, the trusted dealer (TD) uses the corruption-resistant threshold signature scheme to compute and distribute secret shares among the authorities. Similarly, the RTA uses a threshold authentication-based defense scheme to authenticate group members and to track a malicious vehicle. This scheme can ensure traceability, confidentiality, non-repudiation, and integrity. However, it does not provide any mathematical proof or graph to demonstrate the network performance. Besides, no comparison is given to show the scheme's efficiency and effectiveness over other schemes.

In [55], an id-based online/offline signature (IBOOS) scheme has been proposed to achieve privacy preservation. Similarly, an id-based online/offline signature scheme is used for V2I authentication. This scheme also includes cross-RSU V2V authentication (CRVVA) and cross-region authentication (CRA). In CRVVA, an authentication of the vehicle whose pseudonym is not present in the verifier's storage is performed. In CRA, authentication of the vehicle which has traveled from another region is performed. However, the IBOOS scheme is inappropriate for VANETs as large storage space is required during the offline process. Moreover, these schemes need to deal with the key escrow problem as the private key generator (PKG) know each vehicle's private key. Also, the complexity of this scheme is high as it involves separate authentication for vehicles and RSUs.

The elliptic curve cryptography (ECC)-based authentication scheme without bilinear pairing has been proposed in [56] that uses a one-way hash function to provide the source and message authentication. In this, a pseudo-identity is used to generate the private key. The TA can reveal the vehicle's real identity involved in a dispute using message-signature pair. This scheme is resistant to an adaptive chosen message attack under the random oracle model (ROM). However, the message loss ratio is not considered when the density increases.

A one-time identity-based authenticated asymmetric group key agreement (OTIBAAGKA) protocol alongside a cryptographic mix-zone (CMIX) protocol has been proposed in [57] in which a private group key is used to encrypt safety messages. The CMIX can prevent attackers from joining the network. Moreover, any vehicle in CMIX can work as a private key distributor. When the group's private key needs to be updated, a vehicle needs to distribute a small ciphertext, and then each vehicle can upgrade to the new private key. This protocol does not depend upon trusted dealers entirely and operates with efficient key updation. However, vehicles need to use the same group private key to

Table 4
Public key cryptography-based (PKC) schemes.

Scheme	Properties and advantages	Limitations
[47]	This scheme lowers the burden on RSUs and TA by using the distributed computing. The TA can remove malicious vehicles from the network to ensure conditional privacy.	The policies for choosing proxy vehicles and removing malicious vehicles from the network are doubtful.
[48]	This scheme uses short-term pseudonyms to provide hierarchical aggregation and fast response. Also, it employs signature generation and aggregation protocol to ensure secure vehicular communications.	It does not provide comparative analysis to prove its effectiveness over other schemes.
[49]	This scheme is computationally efficient and provides privacy-preserving anonymous authentication to the network members. It also prevents the adversary from making the sender's real identity public.	The operations involving the maintenance and revocation of pseudonym certificates are time-consuming and inefficient.
[50]	This scheme provides anonymous conditional privacy-preserving authentication using bilinear pairing. Vehicles and RSUs authenticate each other without TA.	The management and revocation of anonymous certificates increase communication and computation cost notably.
[51]	This scheme proposes message authentication using the local identity. It ensures message authentication and integrity, non-repudiation, and traceability.	The certificate distribution, CRL management, and member revocation increase the computation and communication costs.
[52]	This scheme uses the fog computing and Merkle hash tree that eliminates the time requirement of CRL checking.	Updating and maintaining the fresh copy of the Merkle tree at each member is difficult.
[53]	This scheme provides the privacy-preserving certificate linkage or revocation. It employs the vehicular public key infrastructure without linkage authority.	It does not provide comparison with existing schemes to prove its efficiency and cost-effectiveness.

encrypt and decrypt the messages. If the attacker gets this key, it can easily access the private information sent through messages.

In [58], a provably secure identity-based signcryption (IBSC) scheme using bilinear pairing, decisional modified bilinear strong Diffie–Hellman (MBSDH), and modified bilinear Diffie–Hellman inversion (MBDHI) assumptions have been proposed. The sender generates a private key using the *Extract* algorithm. Then, it produces ciphertext CT over message M using its real identity, private key, and receiver's identity. At the receiving side, the algorithm verifies CT using the receiver's private key. The algorithm returns M upon successful verification. This scheme achieves security and unforgeability but the complexity and computation cost increases due to bilinear pairing.

A privacy-preserving authentication scheme has been proposed in [59] using the ECC, binary search, and cuckoo filter. The cuckoo filter helps to attach or revoke entities, *e.g.*, timely removal of signature which is not within the specified range. The RSU can simultaneously verify the signatures received from multiple vehicles. However, the key escrow problem can devastate the proposed scheme as the TA can easily compute all the vehicle's private keys.

In [60], the improved identity-based batch verification (IBV) scheme has been proposed to solve the security and privacy issues in VANETs. It uses batch message verification that requires point multiplication as well as pairing operations and provides security under the ROM. The TA pre-loads the real identity, password, and private keys into each vehicle's TPD. Then, the vehicle produces an anonymous identity and uses it to sign the message. The receivers can also verify the message-signature pair within the time. However, this scheme involves a complex process of anonymous identity generation as well as message signing and verification.

The efficient, lightweight authentication and key agreement scheme has been proposed in [61] that uses only bitwise XOR operations and a one-way hash function. It uses a cluster-based VANET and carries out three different types of authentication methods. First is authentication among OBUs, second is authentication between OBUs and their corresponding cluster heads (CHs), and third is authentication between CHs and related RSUs. The secret keys are also used to secure the communication between adjacent RSUs. A vehicle's driver can locally update the password, thus minimizing the burden on TA. Besides, it is resistant to impersonation attack, man-in-the-middle attack, and replay attack. However, it cannot provide conditional privacy and batch message verification. Also, the communication delay may affect network performance.

In [62], an identity-based privacy-preserving authentication scheme (SIPAR) has been proposed to support the efficient revocation of vehicles. In this, the system's master key is not kept at TPD to enhance security. Besides, the bilinear pairing operation is also eliminated to ensure fast verification. The message is signed using a private key and pseudonym during the *message signing* stage. The receiver verifies messages and signatures using batch verification. This scheme ensures anonymity, non-repudiation, traceability, authentication, and provides resistance against modification attack, replay attack, impersonation attack. However, it does not give any information about the message or packet loss ratio.

The identity-based signature scheme without bilinear pairing has been proposed in [63] to achieve conditional privacy-preserving authentication (IBS-CPPA) in VANETs. It uses the batch signature verification based on a one-way hash function and ECC. The TA generates a secret key for the vehicle using its real identity and a random number. Later, the vehicle generates a signature over message m using its secret key and anonymous identity. The receiver verifies the message-signature pairs using the batch signature verification. This scheme is resilient against impersonation attack, DoS attack, stolen verifier table attack, and replay attack.

In [64], the identity and HMAC-based trust management hybrid cryptography (TMHSC) scheme has been proposed. The agent trusted authority (ATA) calculates the vehicle's trust value using rewards points. In *pre-authentication and trust-value updation*, all vehicles which are registered offline with the regional transport office (RTO) need to register with adjacent ATA online. It is achieved by doing pre-authentication using RSU to update the vehicle's trust value which is needed during V2V communication. Using *V2V authentication, trust evaluation, and new trust-value computation*, the message is authenticated, trust value is verified, and also, a new trust value for the sender is computed. Besides, this scheme provides vehicle authentication, message authentication and integrity, traceability, non-repudiation, and unlinkability. However, it does not consider the batch verification of messages and signatures.

A secure and privacy-preserving communication scheme for the establishment and data dissemination of vehicular cloud (VC) has been proposed in [65]. This scheme permits a group of adjacent vehicles to form a secure, anonymous, and dynamic VC.

Table 5
Identity-based cryptography schemes.

Scheme	Properties and advantages	Limitations
[54]	This scheme provides privacy-preserving authentication using anonymous identity. It ensures traceability, confidentiality, non-repudiation, and integrity.	It does not provide any mathematical proof or graph to demonstrate the performance and effectiveness over other schemes.
[55]	This scheme provides id-based online/offline signature to achieve privacy preservation. It includes cross-RSU V2V authentication and cross-region authentication.	The complexity is high because of separate mutual authentication mechanism for vehicles and RSUs.
[56]	This scheme uses a one-way hash function to ensure the source and message authentication. It is resistant to an adaptive chosen message attack.	The message loss ratio is not given when the density increases.
[57]	This scheme has proposed the identity-based authenticated asymmetric group key agreement protocol and cryptographic mix-zone protocol. It entirely does not depend upon trusted dealers and operates with efficient key updation.	Vehicles need to use the same group private key to encrypt and decrypt the messages. If the attacker gets this key, it can easily access the secret information sent through messages.
[58]	This scheme employs the anonymous identity, bilinear pairing, and various Diffie–Hellman assumptions. It provides message authentication and unforgeability.	The bilinear pairing operation increases the complexity and computation overhead.
[59]	This scheme uses the ECC, binary search, and cuckoo filter to achieve privacy-preserving authentication. An RSU can verify the group of signatures received from many vehicles at the same time.	The key escrow problem can dismantle the entire network as the TA can compute all the vehicle's private keys.
[60]	This scheme solves the security and privacy issues using the identity-based batch verification. The TA pre-loads the real identity, password, and private keys into each vehicle's TPD.	The computation overhead is high as it involves a complex process of anonymous identity generation as well as message signing and verification.
[61]	This scheme employs bitwise XOR operations and one-way hash function to ensure lightweight authentication and key agreement.	It cannot provide conditional privacy and batch message verification.
[62]	This scheme performs an efficient revocation of vehicles using the identity-based privacy-preserving authentication. To increase the security, system's master key is not kept at the TPD.	It does not provide the details of message and packet loss ratio.
[63]	This scheme uses identity-based signature to achieve conditional privacy-preserving authentication. It provides message authentication, traceability, unlinkability, and non-repudiation.	It does not give end-to-end delay in VANETs.
[64]	This scheme uses identity and HMAC-based hybrid cryptography to secure vehicular communications. The TA calculates the vehicle's trust value using rewards points.	It does not consider the batch verification of messages and signatures.
[65]	This scheme allows a cloud user to restrict where the data can be processed using a new location based encryption scheme.	It is difficult to broadcast messages if vehicles are sparsely located.

After the formation of VC, a sender can transmit and deliver the message securely inside the network. It allows the resources to be integrated and then shared anonymously and securely, using pseudonyms and dynamic identity. A vehicle's public key is its pseudonym which is used only once during the message transmission. Table 5 gives a summary of the identity-based cryptography schemes.

4.4. Certificateless signature-based schemes

This category depends on the certificateless signature-based schemes in which the need for certificates is removed. These schemes eliminate the CRL management issue in traditional PKC-based schemes and key-escrow problem in IBC schemes. Moreover, these schemes do not require the certificate distribution to vehicles and their revocation from the network.

An elliptic curve-based signature scheme without bilinear pairing has been proposed in [66]. In this, a KGC provides a partial private key to a vehicle generated using its real identity. Next, the vehicle randomly chooses a secret value and produces its complete private key using public parameters, partial private key, and the secret value. Similarly, the vehicle generates its public key using the public parameters and the secret value. A vehicle signs the message using the private key, and the receiver verifies the message-signature pair using the public key. However, the comparative analysis and communication and computation overhead of the proposed scheme are not provided.

In [67], a certificateless and bilinear pairing-based short signature scheme has been proposed. It supports low bandwidth and less storage capacity devices. Also, it has less signature generation and verification costs. Besides, this scheme does not use the MapToPoint hash operation and the signature length is just one group element. Moreover, it is secure against super type I and II adversaries under the ROM if collusion attack algorithm with k traitors (k-CAA) and computational Diffie–Hellman problem (Inv-CDHP) cannot be broken, respectively.

Similarly, an efficient certificateless aggregate signature scheme for V2I communication has been proposed in [68]. It provides conditional privacy-preserving authentication by which the vehicle's real identity is protected. This scheme is existentially unforgeable against adaptive chosen message attack if the computational Diffie–Hellman (CDH) problem is hard. Besides, the message verification needs a few numbers of pairing operations that do not depend upon the number of aggregated signatures. However, this scheme suffers from the scalability issue as the complexity and computation of certificateless aggregate signature increases with the increase in vehicle numbers. Similar to [68], a certificateless aggregate signature scheme has been proposed in [69] in which all the signatures are aggregated and the verification process is conducted using the aggregated signature.

In [70], the improved certificateless aggregate signature (CLAS) scheme without bilinear pairing has been proposed. In this, the brief review and security analysis of the existing Cui et al.'s certificateless scheme [71] are given, which shows that their scheme is erroneous and defective. Besides, the claim of the existing scheme that it is existentially secure against forgery under the elliptic curve discrete logarithm problem (ECDLP) has been shown as incorrect. Also, two sound attacks have been executed against the existing scheme to prove their faults. Besides, it describes the

RSU run batch message verification to speed up the verification process and increase efficiency. However, the complexity of this scheme is high compared to other CLAS schemes.

In [72], a privacy-preserving authentication scheme has been proposed using signature aggregation which not only performs message authentication but also reduces the load on computation and transmission devices. Also, the signature length is static which helps to lower the storage and transmission cost. Certain attributes are computed in advance to reduce the signature generation cost when a vehicle enters the new RSU's communication range. This scheme is secure and existentially unforgeable against the adaptive public-key-replacement attack, chosen identity attack, and chosen message attack. However, the complex signature aggregation and pseudonym generation and its verification significantly increase computation and communication costs.

A certificateless aggregate signature scheme has been proposed in [73] to perform secure routing in VANETs. It provides solutions to the routing problems present in less storage and resource-limited devices. It also reduces communication and computation costs that increase systems performance. However, this scheme involves complex and time-consuming bilinear pairing operations not only increase computation delay but also reduces the network's performance. Table 6 gives a summary of certificateless signature-based schemes.

4.5. Pseudonym-based schemes

This category depends on pseudonyms-based schemes. First, the vehicle sends its real identity and related information to TA through RSU using the secure channel. After verifying the details, TA transmits the pseudo-identity and its validity to the corresponding vehicle. The pseudo-identity is used to achieve authentication and complete anonymity during vehicular communication. Two pseudonyms of the same vehicle cannot be linked with each other to get the real identity or to find out the exact vehicle, which helps to ensure unlinkability. Also, the TA can reveal the vehicle's real identity using the pseudonym if it is involved in any malicious activity.

In [74], a pseudonym-based authentication scheme (PASS) has been proposed to achieve privacy preservation in VANETs. It provides strong privacy as attackers cannot determine the vehicle's real identity. After verifying the real identity, TA provides the sets of secret keys, pseudonymous certificates, and the signing certificates to the vehicle. Then, TA saves the link between a vehicle and its pseudo-identities. The TA keeps the information about revoked vehicles in CRLs. Moreover, when the TA removes an RSU R_j, it adds R_j's certificate to the CRL. At the same time, certificates issued by R_j are automatically revoked from the network. This scheme provides authentication, identity revocation, conditional privacy, and non-repudiation. However, it suffers from a heavy load of CRL management.

An identity-based conditional privacy-preserving authentication scheme for VANETs (CPAV) has been proposed in [75]. It solved the problems of bilinear pairing operation (present in [76]) which is a time-consuming cryptographic operation. It uses a collision-resistant hash function and ECC to increase the network's performance and efficiency. Moreover, this scheme provides security against the adaptive chosen signature and chosen message attacks under the ROM. The advantage of this scheme is that the batch message verification takes less time, even though the number of messages increases. The message and signature size do not affect the transmission overhead. However, it does not explain the message verification rate.

In [77], the bilinear pairing-based access control of message distribution and authentication scheme has been proposed. It uses a pseudo-identity and identity-based signature to ensure message authentication. When a vehicle receives many messages at a time, it uses batch message verification that completes authentication in just 300 ms to enhance efficiency. This scheme employs ciphertext policy attribute-based encryption (CPABE) method that gives confidentiality and access control for the communication. Also, the experimental results show that it is better in case of certain fixed attributes. However, this scheme does not provide conditional privacy, communication delay, and verification costs.

In [78], a hierarchical pseudonyms-based secure protocol using a blind signature has been proposed. In case of a blind signature, the signer and message owner are different, and the signer can sign the message without knowing the message contents. It is described using three stages, *i.e.*, requirement description, complete protocol design, and security analysis. However, this protocol does not discuss how an RSU verifies message signatures received from vehicles. Moreover, it does not provide any graph or figure to describe the protocol's performance or any security proof to ensure the requirements of the VANET.

A distributed aggregate privacy-preserving authentication protocol has been proposed in [79]. It uses multiple trusted authority one-time identity-based aggregate signature method (MTA-OTIBAS). An RSU gets the certificate and public key from TA. Similarly, a vehicle gets the internal pseudo-identity *IPID* and authentication key K_i from TA. The TA also maintains a members list (*ML*) in its database where vehicles *IPID, ID*, and K_i are stored. Later, the vehicle receives the member secrets and authorized period and stores them into the TPD. Then, the vehicle broadcasts the message and its signature in the network. The receiver verifies message signature pairs using bilinear pairing to ensure non-repudiation and correctness. The TA can achieve traceability by using the information about the vehicle stored in the ML. This scheme is secure against DoS attack, Sybil attack, side-channel attack. However, a vehicle needs to go through the fresh authentication each time it switches the network.

In [80], a privacy-preserving anonymous mutual and batch authentication scheme has been proposed. Firstly, anonymous mutual authentication is performed to ensure the security and privacy of V2V transmission. Additionally, an anonymous batch authentication is carried out, which not only confirms the vehicle's authenticity but also helps to verify messages transmitted by an RSU. The major benefit of this scheme is that a load of authentication is equally transferred to vehicles which reduce the burden on RSUs and TA. Each vehicle needs to generate a short-lived anonymous certificate and signature once registered to TA. It is used to perform authentication among RSUs and vehicles which helps to increase the network performance. However, this scheme did not explain the message loss ratio and transmission overhead.

A fog computing-based two secure and intelligent traffic light control schemes have been proposed in [81]. Both the schemes assume a traffic light as the fog device that produces and verifies one puzzle in the given time for all vehicles. The security of these schemes depends upon the hash collision puzzle and the hardness of the CDH problem. The first scheme does not give efficiency in case the vehicle density is large but provides security against DoS attack. The second scheme authenticates vehicles efficiently even when the vehicle density is large and works effectively with a fog device. The benefit of this scheme is that the puzzle generation and its verification by traffic lights can lower the communication and computation overhead. However, the batch generation of puzzles and their verification at the same time for multiple vehicle owners by traffic lights have not been performed.

A conditional privacy-preserving authentication scheme has been proposed using ECC in [82]. It does not use both the bilinear

Table 6
Certificateless signature-based schemes.

Scheme	Properties and advantages	Limitations
[66]	This is an elliptic curve-based signature scheme without using bilinear pairing. A vehicle signs the message using the private key, and the receiver verifies the signature using the public key.	It does not give the communication and computation overhead in the network.
[67]	This is a bilinear pairing-based certificateless short signature scheme that does not use MapToPoint hash operation, and the signature length is just one group element.	The communication efficiency decreases when the vehicle density increases.
[68]	This is a certificateless signature aggregation scheme that provides conditional privacy so that the legal authority can determine the real identity of a malicious vehicle.	It suffers from the scalability issue as the complexity and computation of certificateless aggregate signature increases with the increase in the number of vehicles.
[70]	This is an improved certificateless aggregate signature scheme. RSUs run the batch message verification to speed up the verification process and to increase efficiency.	The complexity is high compared to the existing certificateless aggregate signature schemes.
[72]	This scheme uses a pseudo-identity mechanism to achieve conditional privacy. The signature aggregation method performs message authentication and reduces the load on computation and transmission devices.	The complex signature aggregation and pseudonym generation and its verification, significantly increase computation and communication costs.
[73]	This scheme provides solutions to the routing issues in less storage and resource-limited members of VANET. It reduces communication and computation costs.	It involves complex and time-consuming bilinear pairing operation that increase computation delay and reduces network performance.

pairing and map-to-point hash operations to increase efficiency. In this, an RSU can verify plenty of messages simultaneously to reduce the signature verification time. A sender generates a complete private key using a partial private key provided by KGC. Then, it produces a signature over a message using the pseudo-identity and complete private key before transmission. This scheme can perform single message as well as batch message verification. Also, it is existentially unforgeable in the ROM under the elliptic curve discrete logarithm (ECDL) problem. However, it does not provide information about packet loss ratio and communication overhead.

In [83], a conditional privacy-preserving authentication scheme using bilinear mapping has been proposed. An RSU verifies the message-signature pairs received from vehicles. This scheme is unforgeable against the adaptive chosen identity attack and chosen message attack under the ROM. It provides traceability and unlinkability as well as resistance against various attacks. However, the bilinear mapping operation increases complexity and computation overhead.

A conditional privacy-preserving authentication (RCPPA) scheme using pseudonyms and ring signature has been proposed in [84]. Though the ring signature ensures unconditional privacy, the pseudonym obtained from TA is used to reveal the malicious vehicle's real identity. The main advantage of RCPPA is that only authenticated vehicles can generate a ring signature. A vehicle sends its real identity to TA and requests public pseudo-identity *PPID* and authentication key K_i. Next, the vehicle authenticates itself to TA and accesses the network services. Later, the sender takes a message, *PPID*, private key, public keys of ring members as input and produces ring signature as output. A receiver can verify the signature to authenticate the message without disclosing any information about the sender. Furthermore, the process of reauthentication can reduce the time required by the vehicle for fresh authentication to TA when it leaves the current network and travels into another network. The RCPPA ensures unlinkability and unforgeability. Also, it provides resistance to modification attack, replay attack, MITM attack, and impersonation attack.

In [85], a secure privacy-preserving authentication scheme has been proposed. TA issues internal pseudo-identity (IPID) to the vehicle using its real identity. Then, the vehicle selects an encryption key and puts it into TPD along with IPID. After authentication to TA, the vehicle generates public pseudo-identity (PPID) and subsequently, produce a signature over the given message. The receiver verifies the message by validating the signature. In the end, the vehicle updates the values of IPID and encryption key periodically for preventing leakage of information. Moreover, this scheme provides confidentiality, unlinkability, non-forgery, and is resistant against the side-channel attack. However, it does not provide details of the end-to-end delay of messages.

A secure, robust, and flexible cooperative downloading scheme based on the reputation using selection mechanism and ordered signatures has been proposed in [86]. In this, only those vehicles having highest expected downloading capacities will be selected as proxy vehicles. This scheme ensures the strong security by providing authentication, message confidentiality, privacy preservation, and process authentication. Table 7 gives a summary of pseudonym-based schemes.

4.6. Group signature and Ring signature-based schemes

This category depends on the group signature and ring signature-based schemes. Normally, the group consists of a manager and members. Each group member is having a public key and an individual private key. The group signature algorithms consist of four major algorithms, *i.e., KeyGen, Sign, Verify, Find*. The *KeyGen* algorithm generates public–private key pair, *Sign* algorithm produces signature over the message, *Verify* algorithm verifies the message-signature pair, and *Find* algorithm reveals the malicious vehicle. An adversary cannot link two signatures produced by the same vehicle using its real identity, thus providing unlinkability. During the verification, only the public key is used, which helps to ensure scalability. No member can produce a signature on behalf of another group member.

An optimized signature verification system has been proposed in [87] using identity-based group signature (IBGS). It uses a batch-scheduling algorithm for efficient signature verification. The trusted escrow authority (TEA) produces private keys for vehicles, group managers (GM), RSUs. Then, the vehicle needs to execute a *group join* protocol to obtain a membership certificate from GM. When the vehicle wants to send a message, it produces a group signature using the secret key and certificate. The receiver can validate the message by verifying the signature using the batch message verification. This scheme provides source and message authentication, traceability, and member revocation. However, it does not provide the computation and communication overhead and the end-to-end delay.

In [88], a privacy-preserving authentication scheme has been proposed to achieve location-based service (LBS) in VANETs. A sender transmits a ciphertext C_1 obtained using the group signature generation algorithm to RSU. Upon successful validation,

Table 7
Pseudonym-based schemes.

Scheme	Properties and advantages	Limitations
[74]	This scheme provides the pseudonym-based authentication to achieve conditional privacy. Attackers cannot determine the vehicle's real identity.	It suffers from a heavy load of CRL management.
[75]	This scheme uses a collision-resistant hash function and ECC to increase efficiency and to achieve privacy-preserving authentication.	It does not give the statistical analysis about the number of messages verified in a second.
[77]	This scheme ensures message authentication and its efficient distribution across the network. It uses a pseudo-identity and identity-based signature to provide secure communication.	It does not provide conditional privacy if a vehicle involves in any dispute.
[78]	This scheme is based on hierarchical pseudonyms and blind signature to ensure authentication and privacy to the network members.	It does not discuss how an RSU verifies message signatures received from vehicles.
[79]	This is a privacy-preserving authentication protocol using the distributed approach that includes bilinear pairing-based message aggregation and authentication.	A vehicle needs to go through the fresh authentication each time it switches the network.
[80]	This is an anonymous mutual and batch authentication scheme based on bilinear pairing. It uses digital signatures and anonymous certificates to achieve secure vehicular communications.	It did not explain the message loss ratio and transmission overhead.
[81]	This contains two secure, intelligent traffic light control schemes based on the fog computing. The puzzle generation and its verification by traffic lights can lower the communication and computation overhead.	The batch generation of puzzles and its verification at the same time for multiple vehicle owners by traffic lights have not been performed.
[82]	This scheme does not use both the bilinear pairing and map-to-point hash operations to increase the efficiency. RSUs can verify multiple messages simultaneously to reduce the signature verification time.	It does not provide information about packet loss ratio and communication costs.
[83]	This conditional privacy-preserving authentication scheme secures V2I communication using bilinear mapping. This scheme is unforgeable against the adaptive chosen-identity attack.	The bilinear mapping operation increases complexity as well as computation overhead.
[84]	This scheme ensures the conditional privacy using the pseudo-identity. It provides resistance to modification attack, replay attack, and MITM attack.	It does not provide batch message verification to the network members.
[85]	This mutual authentication scheme uses pseudo-identity to protect the real identity of the vehicle from attackers.	This scheme does not provide details of the end-to-end delay.
[86]	This scheme introduces the notion of process authentication which authenticates the order of file blocks and the order of the assisting vehicles.	The average download delay using multi-path forwarding method increases with the increase in network congestion.

RSU forwards the C_1 to an LBS provider L_1. When L_1 receives the C_1, it extracts the group signature from the C_1 and verifies it using the verification algorithm. Besides, KGC can revoke malicious vehicles using members list *ML* and revocation list *RL*. Besides, this scheme can ensure message confidentiality and integrity, conditional privacy, and non-repudiation. However, it does not provide any comparison results to prove its effectiveness.

An accumulative pseudonym exchanging scheme to enhance location privacy in vehicular social networks has been proposed in [89]. In this, pseudonyms are used along with group signature, and pseudonym-changing regions are formed to exchange pseudonyms alternatively. Hence, the doubt about a particular pseudonym is increased for the tracing attacker, which in turn improves location privacy. RSUs selects a group leader (GL) to distribute and manage group identity (GID), associated keys and certificates to vehicles within the region. When a vehicle becomes a group member, it exchanges pseudonyms with other group members. The vehicle needs to activate pseudonyms before the exchange from the registration authority (RA). The GL removes the entry from the member's list when a vehicle leaves the group. The RA adds a malicious vehicle's identity into the blacklist and broadcasts the modified list into the network. However, the computation and communication overheads of this scheme are high because of the complex operations involved.

In [90], a group signature-based threshold anonymous authentication protocol has been proposed. It lowers the heavy burden of group certificate generation from TA. The protocol uses the new group signature scheme (GSS) that can authenticate the signer as well as the received message. An OBU generates the signature over a message and transmits both the message-signature pair within its range. Then, a receiver can verify many received signatures using the *Verify* stage. Moreover, the tracing manager (TM) can reveal the vehicle's original identity related to a correct signature produced using the wrong message. This protocol provides anonymity, unforgeability, and efficient revocation. However, creating and maintaining the group is a difficult operation as vehicles are constantly moving in the network.

Similarly, a group signature-based authentication and secure key distribution scheme has been proposed in [91]. It is based on the short group signature protocol [92]. The network's area is divided into different domains, and each domain contains leader RSUs (L-RSU) and member RSUs (M-RSU). The leader RSU works as a key generator and provides group private keys within the domain. In each domain, there is one group public key and multiple related group private keys so that a member can generate a signature over the given informative message using any group private key. Later, the signature can be successfully verified by remaining members using the group public key. The M-RSU performs the job of key distribution, but only L-RSU has the right to produce or issue group keys. Besides, it is possible to find out group private key using signatures and tracing. This scheme provides a secure key management and distribution mechanism. However, how the L-RSU and M-RSU are decided is not provided.

In [93], the efficient hiding technique for GL's location has been proposed. This group leader proxy (GLP) technique is based on the shadow concept and hides the GL's location from the attackers. To ensure location privacy, GLP focuses on the communication of GL with the nearby infrastructure, and the ways by which the location trackers can access GL's location. Similarly, the GL needs to hide the group members' location from the potential attackers. However, this technique cannot achieve scalability, *i.e.*, GLP's performance weakens with the increase in vehicle numbers.

A composite privacy-preserving authentication scheme has been proposed in [94]. This scheme does not need certificate management and revocation. The trapdoor mechanism helps to track, identify, and remove malicious vehicles from the network. In this, the region-based grouping is used instead of vehicle-based grouping. At first, the vehicle gets the certificate from the *identity* *verification and enrollment (IdVE)* module. The sender chooses one of the pseudonyms matching the beacon's broadcast time in the *message broadcast* stage. The message is signed with the region's private key, and then the beacon is broadcasted. Besides, the *law enforcement authority (LEA)* can identify the vehicle's identity which has transmitted the malicious beacon. This scheme is resilient against replay attack, sybil attack, and modification attack. However, the process of finding and revoking malicious vehicles from the network is time-consuming and complex.

In [95], a privacy-preserving authentication algorithm using the group signature has been proposed. First, the TA chooses hash and bilinear mapping function and produces a private key. When RSUs and vehicles receive the message, its signature is verified. If the signature is found invalid, an error report is sent to TA. Once the signature is verified, the malicious vehicle's certificate is immediately revoked. The batch message verification reduces the verification time by verifying several messages simultaneously. However, this scheme did not explain its performance in terms of the packet loss ratio, packet delivery ratio, and end-to-end delay.

An authentication scheme for cluster-based VANET using a trust mechanism has been proposed in [96]. In this, vehicles are grouped in the form of clusters, and the degree of trust of each vehicle is calculated [97]. The final trust degree is the summation of direct and indirect trust degree. The direct trust degree is calculated using previous communication with neighbors. Similarly, the indirect trust degree is calculated using the most adjacent neighbors. Then, the cluster heads (CHs) are chosen according to the calculated final trust degree. Before transmission, the sender signs the message and encrypts it using the private key. Later, the receiver decrypts the message and verifies the signature. However, the procedure to select cluster heads is not provided in this scheme.

Similarly, the ring signature is also used to achieve unconditional privacy in VANETs. Sometimes, keeping the vehicle's identity secret (*e.g.*, information about the accident witness) is required. The vehicle's owner does not want its identity to be disclosed in public anyhow to avoid future threats. The accused may create problems for such vehicle owners so that they will not give testimony in court if needed.

In [98], a ring signature-based conditional privacy-preserving authentication scheme has been proposed. It allows the vehicle to transmit crucial information into the network and to remain hidden from others. The mechanism does not reveal member's secret information to other members or adversaries. However, a vehicle can use complete anonymity in the wrong way. Therefore, along with anonymity, conditional privacy is also achieved in this scheme. A sender uses public keys of adjacent vehicles to produce a ring signature over the given message. A vehicle can achieve identity privacy as well as location privacy and hide from the public. However, this scheme does not explain the computation and communication overhead.

A dual-protected ring signature scheme has been proposed in [99]. It gives security to both the message transmission and the message receiving. The vehicle first encrypts the message before transmission. Next, it produces a signature upon the encrypted message using its private key and ring members' public keys. The receiver accepts the encrypted message only after the successful signature verification. This scheme can ensure correctness, unforgeability, and complete anonymity. However, the complexity gets increased due to the message encryption and decryption.

In [100], a double authentication preventing ring signature (DAPRS) scheme using lattice has been proposed. The major advantage of this scheme is that all the members are relatively equal as the group administrator is not required. When a vehicle receives the message-signature pair, it verifies the signature using a collision-resistant hash function. After the signature's successful verification, the receiver assumes that one of the ring members has transmitted the message. This scheme ensures message authentication, integrity, unforgeability, and anonymity. It is secure against quantum computer attacks and adaptive chosen message attacks. However, it requires the CRL management and needs to check whether the public keys used during the signature generation are in the CRL or not.

An efficient lattice-based ring signature scheme to achieve message authentication (LRMA) has been proposed in [101]. The vehicles in closed proximity form a ring for a short period. A vehicle produces a ring signature using its private key, public keys of all ring members, and the message. Then, the receiver verifies the signature using all ring members' public keys. This scheme provides the security of anonymity if solving *search-LWE (Learning with errors)* and *decisional-LWE* are hard problems. Besides, it provides the security of unforgeability if finding a collision in collision-resistant hash function is difficult. Along with unconditional privacy, this scheme also ensures location privacy. Additionally, it is resilient against forgery attack, replay attack, impersonation attack, and identity-revealing attack. It has quasi-linear time complexity, *i.e.*, $\mathcal{O}(n \log_2 n)$. Table 8 gives a summary of group signature and ring signature-based schemes.

4.7. Blockchain-based Schemes

This category depends on blockchain-based identity authentication and revocation frameworks. CA authority assigns pseudo-identity or certificate to vehicles that are stored in the blockchain. Also, the information about the entry pointer is provided to the receiver for verification. The most significant advantages of using blockchain are decentralization and transparency [102]. The information added to the blockchain is immutable, *i.e.*, once it is saved into the blockchain, no one can modify it. Besides, CA does not suffer from a load of CRL management and distribution.

In [103], a blockchain-based privacy-preserving authentication scheme (BPPA) has been proposed. In this, conventional blockchain is extended using chronological Merkle tree (CMT) and Merkle Patricia tree (MPT). The LEA adds a corresponding node into MPT containing the certificate, public key, and the encrypted link between the certificate and real identity. Also, it provides information about the entry pointer to the leaf node to the respective vehicle. The receiver uses a *distributed authentication process* to authenticate the sender's identity. The LEA can revoke the certificate when a vehicle is caught performing any malicious activity, or its certificate has expired. It broadcasts *certificate revocation* transactions indicating that the particular certificate is revoked, and the corresponding vehicle is prevented from further communication in the network. Later, the LEA decrypts the link from the corresponding leaf node from MPT to reveal the malicious vehicle's original identity. However, the computation and communication cost increases due to the inclusion of CA in addition to LEA.

A blockchain-based public key signature scheme (CL-PKS) has been proposed in [104]. It is certificateless and uses bilinear pairing to achieve conditional privacy. It uses batch signature and aggregate signature verification for the fast verification process. Besides, it uses blockchain to achieve pseudo-identity revocation transparency. Along with identity and message authentication, this scheme ensures traceability and efficient revocation. Moreover, it is resilient against replay attack, impersonation attack, modification attack. However, the complexity of this scheme is high due to the involvement of batch signature aggregation and verification.

A traffic event validation and trust verification scheme using blockchain (BTEV) has been proposed in [105]. It uses the proof-of-event (PoE) consensus instead of a proof-of-work. The RSUs

Table 8
Group signature and Ring signature-based schemes.

Scheme	Properties and advantages	Limitations
[87]	This is an optimized signature verification scheme proposed using the identity based group signature. It employs the batch-scheduling algorithm for the efficient verification.	It does not provide the computation and communication overhead of the network.
[88]	This is a secure privacy-preserving authentication scheme to achieve value-added applications and primarily focuses on location-based services.	It does not provide any comparison results to prove its effectiveness over existing schemes.
[89]	This is an accumulative pseudonym exchanging scheme to improve location privacy in VANETs. The pseudonyms are used with the group signature.	The computation and communication overheads are relatively high because of the complex operations involved.
[90]	This is a group signature-based threshold anonymous authentication protocol that lowers the heavy burden of group certificate generation for OBUs from TA.	The formation and maintenance of the group is a difficult operation as vehicles are constantly moving in the network.
[91]	This is a group signature-based authentication and secure key distribution scheme in which the burden of computation is transferred from TA to RSUs.	The way in which the L-RSU and M-RSU are decided is not explained.
[93]	This efficient hiding technique is based on the shadow concept and gives protection to the group leader's location information against the attackers.	It cannot achieve the scalability, as the scheme's performance weakens with the increase in vehicle numbers.
[94]	This scheme uses the group signature and pseudonym mechanism to ensure message authentication and conditional privacy, respectively.	The process of finding and revoking malicious vehicles from the network is time-consuming and complicated.
[95]	This is a privacy-preserving authentication scheme based on the group signature. The batch message verification reduces the verification time.	It does not describe its performance in terms of the packet loss ratio, packet delivery ratio, and end-to-end delay.
[96]	This is a cluster-based authentication scheme using the trust mechanism. In this, vehicles are grouped in the form of clusters, and the degree of trust for each vehicle is calculated.	The procedure to select cluster heads is not provided.
[98]	This is a ring signature-based authentication mechanism that does not reveal member's real identity to the attacker. It does not require advance installation or setup.	It does not explain the computation and communication overhead and the packet loss ratio.
[99]	This scheme provides security to both the transmission as well as the receiving of the message. It ensures the correctness, unforgeability, and complete anonymity.	The complexity gets increased due to the encryption and decryption of the message.
[100]	This is a double authentication preventing ring signature scheme based on lattice. All the members are relatively equal as there is no group administrator requirement.	It requires the CRL management and needs to check whether the public keys used during the signature generation are in the CRL or not.
[101]	This is a lattice-based ring signature scheme to ensure message authentication. It is resilient against forgery attack, replay attack, impersonation attack, and identity-revealing attack.	It cannot revoke malicious vehicles from the network.

gather the traffic information and adjacent vehicles can verify that information. The *PoE mechanism* blocks RSUs from transmitting fraud notifications. The synchronization process helps ensure the maintenance of blockchain and efficient distribution of warning messages. The *trust verification* ensures that all the verified events are permanently saved into the blockchain. However, each member must verify the transactions for PoE and PoW that takes more time.

In [106], a consortium blockchain-based data security sharing and storage scheme (DSSCB) has been proposed. It uses smart contracts to allocate data coins for the vehicles that are participating in data contribution. It uses the elliptic curve to generate signatures over the data-sharing messages to achieve message authentication and non-repudiation. The pre-selected node (PSN) having the right for recording can establish a distributed consensus before a block is added to the ledger. Next, the sender produces a final message signature using a partial signature received from signer RSU. Later, the receiver can verify the messages using single and batch message verification. However, the complexity of DSSCB increases due to the bilinear pairing in addition to blockchain.

The secure authentication and key management scheme using blockchain has been proposed in [107]. In the V2V group construction stage, the Chinese remainder theorem (CRT) has been used. Vehicles within the range of a particular RSU join together to form a group. During the dynamic key updating stage, an efficient strategy to update the group key using consortium blockchain has been proposed. This strategy can update the V2V group key that includes current as well as revoked vehicles. Furthermore, this scheme is resilient against the replay attack and provides conditional privacy, unforgeability against the chosen message attack.

A decentralized key management mechanism using blockchain (DBKMM) has been proposed in [108]. Besides, the mutual authentication and key agreement protocol using the bivariate polynomial has also been proposed. In this, a session key is shared between each vehicle and corresponding RSU. Once the public–private key pair of a vehicle is expired, the vehicle service provider (VSP) updates the same using a smart contract. VSP can detect malicious key pairs using the voting process and removes them from the smart contract. Moreover, this scheme provides security against collusion attack, DoS attack, and public key tampering attack. However, the complexity of this scheme is high for lightweight and resource-limited devices in VANETs.

In [109], a trustworthiness scalable computation scheme (B-TSCA) using blockchain has been proposed. It mainly focuses on the computation of a vehicle's trustworthiness and secure handover of a vehicle from the current RSU to the next RSU. At first, a vehicle produces a secret key using RSU's public key and vice-versa. Then, the vehicle computes a session key using RSU's message, the vehicle's unique identity number (ID), and trustworthiness level (TL) at a given time. Later, the RSU computes the session key using its secret message, ID, and TL. Next, the system transfers the communication between the vehicle and RSU when the vehicle travels from the transmission range of one RSU to the next RSU. This scheme is secure against the replay attack and MITM attack. However, it does not give any comparative analysis with existing schemes to prove its efficiency over other schemes.

A blockchain-based secure data sharing system has been proposed for the internet of vehicles (IoV) in [110]. In this paper, priority is given to the security of announcement messages in IoV.

The entire system is divided into multiple regions. Each region is having a parent blockchain and an auxiliary blockchain for storing the messages. This system uses a method based on fair blind signatures and threshold secret sharing which is used to sign announcement messages anonymously. Table 9 gives a summary of blockchain-based authentication schemes.

5. Discussion

An authentication mechanism tries to ensure the correctness of a message by authenticating its source and also preserve the identity privacy of a vehicle. Each cryptographic mechanism used has certain merits and demerits. The deployment of a particular mechanism depends on the specific requirements by the authorities and members of the network.

The symmetric key cryptography-based schemes [43–46] have fewer communication costs and computation overhead. However, the use of MAC or identical key during the signature generation and verification can easily help the attacker breach security and privacy. In [43], an authentication code for TA is produced. All the members need to register to TA to receive group key. The TA can authenticate the vehicle using its fingerprint. In [44], anonymous authentication and key distribution approach not only preserve identity privacy but also achieve message integrity. In [45,46], HMAC is used for message signing and authentication. It also removes the CRL requirement for source authentication which increases network performance.

In public key cryptography-based schemes [47–53], each member possesses a public–private key pair and a certificate. The CA receives the certificate issuance request from RSUs and vehicles, and it issues the certificate only after verifying the corresponding details. In contrast to symmetric key cryptography-based schemes, two different keys are used at the sender and receiver side, *i.e.*, a private key is used during signature generation, and a public key is used during verification. Moreover, the security in the network can be increased simultaneously with the performance. However, the certificate distribution and revocation issue affect the property of scalability. Also, the CRL verification and management increase the communication cost of the network.

The identity-based cryptography (IBC) schemes [54–65], each member's personal information is used during public key generation. The major advantage of these schemes is that a load of certificate management and distribution is eliminated. The KGC or TA manages the key generation and distribution process and monitors the entire network. In these schemes, TA helps the network members to achieve source anonymity, non-repudiation, and message authentication. Also, it can reveal the identity of the malicious vehicle using the public key and information. In these schemes, attacker can obtain the sender's real identity by analyzing the public key and message-signature pairs.

In certificateless signature-based schemes [66–68,70,72,73], the sender does not transmit any type of certificate along with the message. Other cryptographic mechanisms are employed during signature generation or verification instead of certificates. However, the computation cost significantly increases due to signature aggregation and storage. Similarly, pseudo-identity is used in pseudonym-based schemes for source authentication. The attacker cannot get the sender's private information by the analysis of pseudo-identity. However, the vehicle needs to store multiple pseudo identities into TPD in advance. Also, the TA should maintain the database of the link between pseudo-identity and the real identity of each member to identify malicious vehicles if needed.

In pseudonym-based schemes [74,75,77–86], a pseudo-identity for each network member is used instead of real identity. The PID is obtained from TA by providing original identity and public key. It is also used during signature generation over the message. A vehicle transmits the PID along with the message signature during the communication with the adjacent vehicles. A receiver can verify the PID to achieve source authentication with the help of TA. The major advantage of these schemes is that the adversary cannot extract the sender's real identity from the analysis of its PID or message-signature pair. A vehicle can ensure complete anonymity, source authentication, unlinkability, and non-repudiation in the network. However, handling and finding the solution to sybil attack is complex.

In group and ring signature-based schemes [87–91,93–96,98–101], vehicles form a group and produce their public–private key pair for communication. A sender signs the message using private and public keys, and the receiver verifies the signature using everyone's public keys. The primary issue with these schemes is that the verification of group signature is usually a time-consuming operation, which makes it unfit for time-bound devices of VANETs. Ring signatures provide unconditional privacy. This may increase the tendency of an authenticated malicious user to send false messages. The ring signature mechanism must be modified or used in conjunction with other methods to allow non-repudiation.

In blockchain-based authentication schemes [103–110], each member of the network is guaranteed transparency and immutability. Any member of the network can verify the operations performed by the trusted authority. The main advantage of deploying blockchain is that no member can modify or delete the information saved in the blockchain. The current blockchain-based methods are limited, as some entities need to be trusted for updating the blockchain, which may lead to cartel formation by such entities. Moreover, given the vast nature of VANET and the local nature of messages sent by vehicles, blockchain-based methods need to evolve a mechanism to keep the size of blockchain small while catering to all vehicles that enter and leave a neighborhood within a short period.

6. Conclusion

The primary objective of VANETs is to ensure secure traffic conditions and provide safety to the drivers by broadcasting informative messages in the network. However, the attackers can breach the security and privacy given to the vehicle owners due to the use of an open wireless medium. In this paper, we surveyed different authentication and privacy-preserving schemes, along with the state-of-the-art techniques used in VANETs. We find that a single cryptographic mechanism is unable to meet all the security needs of the VANET, and a basket of techniques needs to be evolved. Each scheme lacks in providing certain security requirements in VANET. Also, major schemes cannot offer unconditional privacy required in some cases.

The main limitations of current cryptographic mechanisms and the focus of current studies are computation and communication efficiency, dispensing centralized entities, large memory requirements for certificates and corresponding revocation lists, and allow non-repudiation by making privacy provisioning conditional. Moreover, robustness against various attacks and meeting of all the security requirements is also being studied. It is observed that just the cryptographic techniques are not sufficient, and need complementarity by techniques from other domains like machine learning, *etc.* to fulfill the security requirements of VANETs and their members. Moreover, with new features and emerging technologies, such as the Internet of vehicles and 5G, different security and privacy challenges will arise. In the future, the existing mechanisms will need to evolve and modify themselves to meet these unforeseen security requirements and challenges in the new environment.

Table 9
Blockchain-based schemes.

Scheme	Properties and advantages	Limitations
[103]	This is a blockchain-based privacy-preserving authentication scheme in which a conventional blockchain is extended using chronological Merkle tree and Merkle Patricia tree.	The computation and communication costs increases due to the inclusion of CA in addition to LEA.
[104]	This is a blockchain-based certificateless, public key signature scheme proposed using bilinear pairing. It employs blockchain to achieve pseudo-identity revocation transparency.	The complexity is high due to the batch signature aggregation and verification.
[105]	This is a traffic event validation and trust verification scheme using blockchain. It proposes a concept of proof-of-event consensus instead of a proof-of-work approach.	Each member must verify the transactions for PoE and PoW that takes more time.
[106]	This scheme employs smart contracts to allocate data coins for the vehicles that are participating in data contribution. It uses the elliptic curve to generate signatures over the data sharing messages.	The complexity increases due to the bilinear pairing in addition to blockchain.
[107]	This is a blockchain-based secure authentication and key management scheme in which edge computing technique is employed to ensure sufficient storage and computing power to the network members.	The cost of signature generation and verification is high.
[108]	This is a decentralized key management mechanism using blockchain. Also, the mutual authentication and key agreement protocol using the bivariate polynomial has been proposed.	The complexity is high for lightweight, resource, and storage limited devices of VANETs.
[109]	This scheme mainly focuses on the computation of vehicle's trustworthiness and the handover of a vehicle from the current RSU to next RSU securely.	It does not provide any comparative analysis with existing schemes to prove its efficiency over other schemes.
[110]	This scheme prevents the acceptance of fake messages as well as mitigates the throughput limitation of blockchain.	The system may suffer from rogue key attack if a traditional signature scheme is used.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Zhang, Trust management for VANETs: challenges, desired properties and future directions, Int. J. Distrib. Syst. Technol. (IJDST) 3 (1) (2012) 48–62.

[2] I. Ali, M. Faisal, S. Abbas, A survey on lightweight authentication schemes in vertical handoff, Int. J. Coop. Inf. Syst. 26 (01) (2017) 1630001.

[3] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, A. Ksentini, Named data networking in vehicular ad hoc networks: State-of-the-art and challenges, IEEE Commun. Surv. Tutor. 22 (1) (2020) 320–351.

[4] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, Ad Hoc Netw. 61 (2017) 33–50.

[5] Q. Xu, T. Mak, J. Ko, R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, ACM, 2004, pp. 19–28.

[6] L.N. Balico, A.A.F. Loureiro, E.F. Nakamura, R.S. Barreto, R.W. Pazzi, H.A.B.F. Oliveira, Localization prediction in vehicular ad hoc networks, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2784–2803.

[7] M. Azees, P. Vijayakumar, L.J. Deborah, Comprehensive survey on security services in vehicular ad-hoc networks, IET Intell. Transp. Syst. 10 (6) (2016) 379–388.

[8] R. Jain, I. Kashyap, An qos aware link defined OLSR (LD-OLSR) routing protocol for MANETS, Wirel. Pers. Commun. (2019) 1–14.

[9] M. Aloqaily, B. Kantarci, H.T. Mouftah, Multiagent/multiobjective interaction game system for service provisioning in vehicular cloud, IEEE Access 4 (2016) 3153–3168.

[10] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Veh. Commun. 9 (2017) 19–30.

[11] R. Mishra, A. Singh, R. Kumar, VANET security: Issues, challenges and solutions, in: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), IEEE, 2016, pp. 1050–1055.

[12] J. Cui, L. Wei, J. Zhang, Y. Xu, H. Zhong, An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 20 (5) (2018) 1621–1632.

[13] M. Aloqaily, S. Otoum, I. Al Ridhawi, Y. Jararweh, An intrusion detection system for connected vehicles in smart cities, Ad Hoc Netw. (2019).

[14] S. Otoum, B. Kantarci, H.T. Mouftah, Detection of known and unknown intrusive sensor behavior in critical applications, IEEE Sensors Lett. 1 (5) (2017) 1–4.

[15] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: A survey, IEEE Commun. Surv. Tutor. 17 (1) (2014) 228–255.

[16] F. Qu, Z. Wu, F.-Y. Wang, W. Cho, A security and privacy review of VANETs, IEEE Trans. Intell. Transp. Syst. 16 (6) (2015) 2985–2996.

[17] A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks, IEEE Commun. Surv. Tutor. 20 (1) (2017) 770–790.

[18] Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Trans. Intell. Transp. Syst. 20 (2) (2018) 760–776.

[19] I. Ali, A. Hassan, F. Li, Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey, Veh. Commun. 16 (2019) 45–61.

[20] D. Manivannan, S.S. Moni, S. Zeadally, Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs), Veh. Commun. 25 (2020).

[21] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66.

[22] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, J. Netw. Comput. Appl. 37 (2014) 380–392.

[23] A. Dhamgaye, N. Chavhan, Survey on Security Challenges in VANET 1, Citeseer, 2013.

[24] R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13.

[25] D. Jiang, L. Delgrossi, IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments, in: VTC Spring 2008-IEEE Vehicular Technology Conference, IEEE, 2008, pp. 2036–2040.

[26] F.C. Commission, et al., Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Service in the 5.850-5.925 GHz Band, Tech. Rep. FCC, FCC, Washington, DC, USA, 2002, pp. 02–302.

[27] S.A. Ahmed, S.H. Ariffin, N. Fisal, Overview of wireless access in vehicular environment (WAVE) protocols and standards, Environment 7 (2013) 8.

[28] S.S. Kaushik, Review of different approaches for privacy scheme in VANETs, Int. J. Adv. Eng. Technol. 5 (2) (2013) 356.

[29] J.M. De Fuentes, A.I. González-Tablas, A. Ribagorda, Overview of security issues in vehicular ad-hoc networks, in: Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI global, 2011, pp. 894–911.

[30] B. Premasudha, V. Ravi Ram, J. Miller, R. Suma, A review of security threats, solutions and trust management in VANETs, Int. J. Next-Gener. Comput. 7 (1) (2016).

[31] H. Talat, T. Nomani, M. Mohsin, S. Sattar, A survey on location privacy techniques deployed in vehicular networks, in: 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), IEEE, 2019, pp. 604–613.

[32] M.A. Hossain, R.M. Noor, K.A. Yau, S.R. Azzuhri, M.R. Z'aba, I. Ahmedy, Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks, IEEE Access 8 (2020) 78054–78108.

[33] A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks, IEEE Commun. Surv. Tutor. 20 (1) (2017) 770–790.

[34] M. Bayat, M. Barmshoory, M. Rahimi, M.R. Aref, A secure authentication scheme for VANETs with batch verification, Wirel. Netw. 21 (5) (2015) 1733–1743.

[35] A. Luckshetty, S. Dontal, S. Tangade, S.S. Manvi, A survey: comparative study of applications, attacks, security and privacy in VANETs, in: 2016 International Conference on Communication and Signal Processing (ICCSP), IEEE, 2016, pp. 1594–1598.

[36] Y. Lai, Y. Xu, F. Yang, W. Lu, Q. Yu, Privacy-aware query processing in vehicular ad-hoc networks, Ad Hoc Netw. (2019) 101876.

[37] F. Goudarzi, H. Asgari, H.S. Al-Raweshidy, Traffic-aware VANET routing for city environments—A protocol based on ant colony optimization, IEEE Syst. J. 13 (1) (2018) 571–581.

[38] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Jararweh, T. Baker, A profitable and energy-efficient cooperative fog solution for IoT services, IEEE Trans. Ind. Inf. (2019).

[39] S. Otoum, B. Kantarci, H.T. Mouftah, On the feasibility of deep learning in sensor network intrusion detection, IEEE Netw. Lett. 1 (2) (2019) 68–71.

[40] A. Ullah, X. Yao, S. Shaheen, H. Ning, Advances in position based routing towards ITS enabled FoG-oriented VANET–A survey, IEEE Trans. Intell. Transp. Syst. 21 (2) (2019) 828–840.

[41] Y. Cui, L. Cao, X. Zhang, G. Zeng, Ring signature based on lattice and VANET privacy preservation, Chin. J. Comput. 40 (169) (2017) 1–14.

[42] O.S. Al-Heety, Z. Zakaria, M. Ismail, M.M. Shakir, S. Alani, H. Al-sariera, A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET, IEEE Access 8 (2020) 91028–91047.

[43] P. Vijayakumar, M. Azees, A. Kannan, L.J. Deborah, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (2015) 1015–1028.

[44] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, B. Balamurugan, Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks, Cluster Comput. 20 (2017).

[45] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET, IEEE Trans. Veh. Technol. 65 (2) (2015) 896–911.

[46] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on HMAC for VANETs, IEEE Trans. Intell. Transp. Syst. 17 (8) (2016) 2193–2204.

[47] Y. Liu, L. Wang, H.-H. Chen, Message authentication using proxy vehicles in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 64 (8) (2014) 3697–3710.

[48] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput. 65 (8) (2015) 2562–2574.

[49] P. Vijayakumar, M. Azees, L.J. Deborah, CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks, in: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, IEEE, 2015, pp. 62–67.

[50] M. Azees, P. Vijayakumar, L.J. Deboarh, EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 18 (9) (2017) 2467–2476.

[51] S. Wang, N. Yao, LIAP: A local identity-based anonymous message authentication protocol in VANETs, Comput. Commun. 112 (2017) 154–164.

[52] A. Alrawais, A. Alhothaily, B. Mei, T. Song, X. Cheng, An efficient revocation scheme for vehicular ad-hoc networks, Procedia Comput. Sci. 129 (2018) 312–318.

[53] M.A. Simplicio, E.L. Cominetti, H.K. Patil, J.E. Ricardini, L.T.D. Ferraz, M.V.M. Silva, Privacy-preserving certificate linkage/revocation in VANETs without linkage authorities, IEEE Trans. Intell. Transp. Syst. (2020) 1–11.

[54] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Trans. Parallel Distrib. Syst. 21 (9) (2010) 1227–1239.

[55] H. Lu, J. Li, M. Guizani, A novel ID-based authentication framework with adaptive privacy preservation for VANETs, in: 2012 Computing, Communications and Applications Conference, IEEE, 2012, pp. 345–350.

[56] N.-W. Lo, J.-L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, IEEE Trans. Intell. Transp. Syst. 17 (5) (2016) 1319–1328.

[57] L. Zhang, OTIBAAGKA: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 12 (12) (2017) 2998–3010.

[58] A. Karati, S.H. Islam, G. Biswas, M.Z.A. Bhuiyan, P. Vijayakumar, M. Karuppiah, Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments, IEEE Internet Things J. 5 (4) (2017) 2904–2914.

[59] J. Cui, J. Zhang, H. Zhong, Y. Xu, SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter, IEEE Trans. Veh. Technol. 66 (11) (2017) 10283–10295.

[60] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, M.K. Khan, Enhancing security and privacy for identity-based batch verification scheme in VANETs, IEEE Trans. Veh. Technol. 66 (4) (2017) 3235–3248.

[61] M. Wazid, A.K. Das, N. Kumar, V. Odelu, A.G. Reddy, K. Park, Y. Park, Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks, IEEE Access 5 (2017) 14966–14980.

[62] Y. Wang, H. Zhong, Y. Xu, J. Cui, G. Wu, Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs, IEEE Syst. J. (2020).

[63] I. Ali, T. Lawrence, F. Li, An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs, J. Syst. Archit. 103 (2020) 101692.

[64] S. Tangade, S.S. Manvi, P. Lorenz, Trust management scheme based on hybrid cryptography for secure communications in VANETs, IEEE Trans. Veh. Technol. (2020).

[65] L. Zhang, X. Meng, K.-K.R. Choo, Y. Zhang, F. Dai, Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud, IEEE Trans. Dependable Secure Comput. 17 (3) (2018) 634–647.

[66] K.-H. Yeh, K.-Y. Tsai, C.-Y. Fan, An efficient certificateless signature scheme without bilinear pairings, Multimedia Tools Appl. 74 (16) (2015) 6519–6530.

[67] J.-L. Tsai, A new efficient certificateless short signature scheme using bilinear pairings, IEEE Syst. J. 11 (4) (2015) 2395–2402.

[68] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, M.K. Khan, An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Inform. Sci. 317 (2015) 48–66.

[69] A.K. Malhi, S. Batra, An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks, 17 (1) (2015) 317.

[70] X. Yang, C. Chen, T. Ma, Y. Li, C. Wang, An improved certificateless aggregate signature scheme for vehicular ad-hoc networks, in: 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), IEEE, 2018, pp. 2334–2338.

[71] J. Cui, J. Zhang, H. Zhong, R. Shi, Y. Xu, An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks, Inform. Sci. 451 (2018) 1–15.

[72] H. Zhong, S. Han, J. Cui, J. Zhang, Y. Xu, Privacy-preserving authentication scheme with full aggregation in VANET, Inform. Sci. 476 (2019) 211–221.

[73] Z. Xu, D. He, N. Kumar, K.-K.R. Choo, Efficient certificateless aggregate signature scheme for performing secure routing in VANETs, Secur. Commun. Netw. 2020 (2020).

[74] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Trans. Veh. Technol. 59 (7) (2010) 3589–3603.

[75] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2681–2691.

[76] K.-A. Shim, CPAV: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (4) (2012) 1874–1883.

[77] Q. Kang, X. Liu, Y. Yao, Z. Wang, Y. Li, Efficient authentication and access control of message dissemination over vehicular ad hoc network, Neurocomputing 181 (2016) 132–138.

[78] E.R. Agustina, A.R. Hakim, Secure VANET protocol using hierarchical pseudonyms with blind signature, in: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), IEEE, 2017, pp. 1–4.

[79] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, IEEE Trans. Intell. Transp. Syst. 18 (3) (2017) 516–526.

[80] P. Vijayakumar, V. Chang, L.J. Deborah, B. Balusamy, P. Shynu, Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks, Future Gener. Comput. Syst. 78 (2018) 943–955.

[81] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, J. Shen, Secure intelligent traffic light control using fog computing, Future Gener. Comput. Syst. 78 (2018) 817–824.

[82] Y. Ming, H. Cheng, Efficient certificateless conditional privacy-preserving authentication scheme in VANETs, Mob. Inf. Syst. 2019 (2019) http://dx.doi.org/10.1155/2019/7593138.

[83] I. Ali, F. Li, An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs, Veh. Commun. 22 (2020).

[84] P. Mundhe, V.K. Yadav, A. Singh, S. Verma, S. Venkatesan, Ring signature-based conditional privacy-preserving authentication in VANETs, Wirel. Pers. Commun. (2020) http://dx.doi.org/10.1007/s11277-020-07396-x.

[85] J. Cui, W. Xu, Y. Han, J. Zhang, H. Zhong, Secure mutual authentication with privacy preservation in vehicular ad hoc networks, Veh. Commun. 21 (2020) 100200.

[86] Y. Zhang, L. Zhang, D. Ni, K.-K.R. Choo, B. Kang, Secure, robust and flexible cooperative downloading scheme for highway VANETs, IEEE Access 9 (2021) 5199–5211.

[87] M.S.I. Mamun, A. Miyaji, An optimized signature verification system for vehicle ad hoc network, in: 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE, 2012, pp. 1–8.

[88] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, B. Liu, Practical secure and privacy-preserving scheme for value-added applications in VANETs, Comput. Commun. 71 (2015) 50–60.

[89] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, S. Gjessing, MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks, IEEE Trans. Dependable Secure Comput. 13 (1) (2015) 93–105.

[90] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs, IEEE Trans. Veh. Technol. 65 (3) (2015) 1711–1720.

[91] K. Lim, K.M. Tuladhar, X. Wang, W. Liu, A scalable and secure key distribution scheme for group signature based authentication in VANET, in: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, 2017, pp. 478–483.

[92] Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs, IEEE J. Sel. Areas Commun. 29 (3) (2011) 616–629.

[93] S. Aljallad, R.S. Al-Qassas, M. Qasaimeh, A group leader location hiding technique for VANETs, Int. J. Distrib. Syst. Technol. (IJDST) 8 (3) (2017) 67–80.

[94] U. Rajput, F. Abbas, H. Eun, H. Oh, A hybrid approach for efficient privacy-preserving authentication in VANET, IEEE Access 5 (2017) 12014–12030.

[95] L. Zhang, C. Li, Y. Li, Q. Luo, R. Zhu, Group signature based privacy protection algorithm for mobile ad hoc network, in: 2017 IEEE International Conference on Information and Automation (ICIA), IEEE, 2017, pp. 947–952.

[96] R. Sugumar, A. Rengarajan, C. Jayakumar, Trust based authentication technique for cluster based vehicular ad hoc networks (VANET), Wirel. Netw. 24 (2) (2018) 373–382.

[97] A. Daeinabi, A.G. Rahbar, An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks, Comput. Electr. Eng. 40 (2) (2014) 517–529.

[98] B.K. Chaurasia, S. Verma, Conditional privacy through ring signature in vehicular ad-hoc networks, in: Transactions on Computational Science XIII, Springer, 2011, pp. 147–156.

[99] Y. Han, N.-N. Xue, B.-Y. Wang, Q. Zhang, C.-L. Liu, W.-S. Zhang, Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks, IEEE Access 6 (2018) 20209–20220.

[100] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, H. Zhang, Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks, Tsinghua Sci. Technol. 24 (5) (2019) 575–584.

[101] P. Mundhe, V.K. Yadav, S. Verma, S. Venkatesan, Efficient lattice-based ring signature for message authentication in VANETs, IEEE Syst. J. (2020) 1–12.

[102] S. Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system, 2008, (2008).

[103] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for vanets, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 27 (12) (2019) 2792–2801.

[104] I. Ali, M. Gervais, E. Ahene, F. Li, A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs, J. Syst. Archit. 99 (2019) 101636.

[105] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based traffic event validation and trust verification for VANETs, IEEE Access 7 (2019) 30868–30877.

[106] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[107] H. Tan, I. Chung, Secure authentication and key management with blockchain in VANETs, IEEE Access (2019).

[108] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, W. He, An efficient decentralized key management mechanism for VANET with blockchain, IEEE Trans. Veh. Technol. (2020).

[109] C. Wang, J. Shen, J.-F. Lai, J. Liu, B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs, IEEE Trans. Emerg. Top. Comput. (2020).

[110] L. Zhang, M. Luo, J. Li, M.H. Au, K.-K.R. Choo, T. Chen, S. Tian, Blockchain based secure data sharing system for internet of vehicles: A position paper, Veh. Commun. 16 (2019) 85–93.

Pravin Mundhe has completed Ph.D. in 2021 from Indian Institute of Information Technology, Allahabad (Prayagraj), India. He completed his MTech. in Cyber Law and Information Security in 2016 from IIIT-Allahabad and B.E. in Information Technology in 2012 from University of Pune, India. His research interest areas are Computer networks, Wireless sensor networks, Information and Network security, Operating system, Blockchain technology, and VANETs security.

Shekhar Verma received the Ph.D. degree in computer networks from the Indian Institute of Technology, Varanasi, India, in 1993. He is currently working as a Professor (IT) with the Indian Institute of Information Technology, Allahabad, India. His research interests include machine learning, computer networks, wireless sensor networks, wireless networks, information and network security, vehicular technology, and cryptography.

S. Venkatesan received the Ph.D. degree in computer science and engineering from Anna University, Chennai, India, in 2010. He is currently working as an Assistant Professor (IT) with the Indian Institute of Information Technology, Allahabad, India. His research interests include machine learning, computer networks, information and networks security, cryptograph, cloud computing, and blockchain.