IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 26, 2021, accepted October 27, 2021, date of publication November 4, 2021,
date of current version November 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3125521

A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues

SAGHEER AHMED JAN[1], NOOR UL AMIN[1], MOHAMED OTHMAN[2,3], (Senior Member, IEEE), MAZHAR ALI[4], ARIF IQBAL UMAR[1], AND ABDUL BASIR[1]

[1]Department of Information Technology, Hazara University Mansehra, Dhodial 21300, Pakistan
[2]Department of Communication Technology and Network, Universiti Putra Malaysia (UPM), Serdang, Seri Kembangan, Selangor 43400, Malaysia
[3]Laboratory of Computational Science and Mathematical Physics, Institute of Mathematical Research (INSPEM), Universiti Putra Malaysia(UPM), Serdang, Seri Kembangan, Selangor 43400, Malaysia
[4]Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abbottabad 22060, Pakistan

Corresponding authors: Noor Ul Amin (namin@hu.edu.pk), Mohamed Othman (mothman@upm.edu.my), and Mazhar Ali (mazhar@cuiatd.edu.pk)

This work was supported by Malaysian Ministry of Education through the Research Management Center, Universiti Putra Malaysia under UPM Journal Publication Fund.

ABSTRACT Vehicular ad hoc Networks (VANETs) are an emerging technology with robust applications in Intelligent Transport System. It consists of smart vehicles and roadside infrastructure which communicate through open access wireless networks. The rapid growth in vehicles results in VANETs becoming large-scale, dynamic, heterogeneous and it is possible for the attacker to harm vehicular communication which leads to life-endangering situations. VANETs must ensure secured vehicular communication using strong privacy-preserving and authentication mechanisms. In addition, efficiency is also a major concern in VANETs. Numerous studies have been discussed in literature for VANETs privacy and security. Nevertheless, no one covered the privacy and security issues as a holistic view. In this paper, we have given a detailed background overview of VANETs. Details of different possible attacks in VANET are also given in this paper. We have classified privacy and authentication schemes into four major groups with their security mechanisms, security requirements, strength, limitations, attacks countermeasures and performance measures. Finally, we have discussed some open issues in the field of VANETs security.

INDEX TERMS Authentication, privacy, vehicles, safety, security, vehicular and wireless technologies.

I. INTRODUCTION

In the modern era each and every thing is going toward automation to facilitate and save the human being from unexpected incidents. The population is increasing day by day and requires an automatic autonomous system which controls each and every aspect related to human life. The Internet of Things (IoTs) makes the basis of a smart and autonomous society in which billions of intelligent sensors and devices constantly interact with each other, networks, services, and humans to achieve goals [2], [3]. Such intelligent and connected devices show a wonderful novation for changing physical environments to digital environments. There are numerous autonomous intelligent systems which are based on IoTs, for example e-Health care, e-commerce, defense, agriculture etc. Vehicular Ad Hoc Networks (VANETs) are one of the prominent factors of smart and autonomous Intelligent Transport System [1] in which vehicles can communicate with each other and roadside infrastructure [4]. The rapid growth in vehicles makes the vehicular ad hoc network dynamic, heterogeneous and large-scale, making it hard to fulfill basic requirements such as enormous connection of 5G network, high mobility, extremely latency and top security [5], [6]. All of the involved entities in VANETs need efficient and safe transportation communication mechanisms. Basically, the Intelligent Transport System requires two types of wireless communication: Short range wireless communication and long range Communication [7]. Short

The associate editor coordinating the review of this manuscript and approving it for publication was Chunsheng Zhu.

range communication includes emerging technologies such as Dedicated Short Range (DSR) communication and IEEE 802.11b for establishing an Ad hoc network. In contrast, for establishing long range communication it depends on existing infrastructure such as cellular networks [7]. Using these wireless technologies vehicles communicate with each other and Road Side Units. Figure. 1 shows the basic VANETs scenario. There are three entities involved: Onboard Unit (OBU), Road Side Unit (RSU) and Trusted authority (TA), according to the given scenario. OBU is mounted within the vehicle through which the vehicle sends or receives the transmitted message. In case of exception, the vehicle's drivers take an early decision on the basis of transmitted information he/she received. For example, Table 1 shows the exchanged messages between vehicles and RSUs about road safety [8]. Beside roadside, RSUs are fixed over the recommended distance and work like a base station (i.e WiMAX, WiFi etc) [9]. OBU and Trusted authority communicate with each other using RSU as an intermediate node. The main task of the TA is to register OBUs and RSUs. The other responsibilities of the TA are revocation management, certificate distribution, identity authentication and storage of information for future use.

Security is the biggest challenge for VANETs due to open wireless communication [10]–[13]. Vehicles communicate with each other through open wireless channels and attackers can easily alter, intercept and delete transmitted messages in VANETs [14]. An attacker can capture the traffic related message and it could be dangerous for the driver's life. If an attacker alters the message and broadcasts a false message then it can cause serious traffic problems like road accidents, turn drivers to dense traffic routes, an attacker's choice route etc. Therefore, the security of VANETs has become a hot research topic and drawn increasing attention [15]. The solution to security issues in VANETs required end-to-end authentication to avoid intrusion in the VANETs [16]. It also required robust and lightweight authentication solutions for resource constraint nodes [17]. Another promising component is privacy of the individual rights to act independent of any record conducted without their consent [18], [19]. The service provider cannot mishandle the personal data without the consent of the owner and necessary measures should be taken to hide the real identity of the user. Beside this latency impact of work flow will be considered to ensure the service quality. There should be efficient security solutions for protecting the availability of resources and services [20]. The delay of vehicle emergencies has led to many serious consequences [21]. The efficiency depends upon computational cost and communication overhead. Less computational overhead guaranteed fast vehicular communication [22]. Due to aforesaid uncertainties the drivers feel reluctant to adopt the VANETs.

All of the involved entities in VANETs communicate with each other over the insecure network. Therefore security is another main issue regarding VANETs. Since different nodes (i.e OBUs, RSUs) are exchanging sensitive information with each other and there is a chance of leakage of such sensitive information. An intruder is an active node which performs malicious activities like information modification, information leakage and packet dropping etc. So there should be certain security mechanisms that detect and prevent the normal network behavior from intruder attacks automatically [23].

TABLE 1. Road related information [8].

Information about Traffic	
Information	**Range**
Traffic signal	205 m
School Zone	52 m
Petrol station	144 m
Speed Breaker	40 m
Accident Zone	385 m
Curve speed warning	70 m
Road interactions	300 m

A. MOTIVATIONS

In recent era road accidents or injuries are the ninth biggest cause of death. According to a World Health Organization WHO report published in 2018 [24], about 1.35 million people died each year. A survey conducted by WHO predicted that the road accident will be the fifth biggest cause of death by 2030 [25]. In 2007, CARE: European Road Accident Database issued a report that 1.8 million people injured and 43000 people die each year in European Union member states which cost 160 billion Euros [26]. The total cost related to road accidents accounts for about three percent of world's GDP [27]. About 78% of road accidents are caused due to driver's irresponsibility. If the driver of the vehicle is warned at least one-half second prior to vehicle collision then about 60% of the road accident can be avoided [28]. Another main issue is the traffic jams which cause fuel wastage. Hence in this work we focus on different lightweight security techniques that help the driver from future harm.

B. OUR CONTRIBUTIONS

The major contributions of this study are as follows.

- We have conducted a comprehensive survey to investigate existing security techniques and categorize various security attacks in VANETs.
- The classification of aforementioned security schemes are made on the basis of various characteristics (Pseudonym based, identity based Signature, hashed function based, Group Signature Based).
- The security requirements covered by each classification, attacks controlled by each classification and performance analysis of each classification are discussed in detail.
- On the basis of common properties, these schemes are compared with themselves and with other schemes.

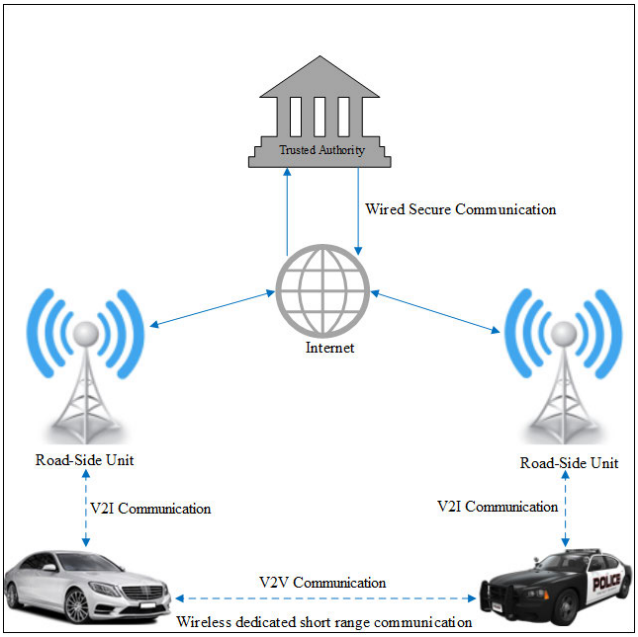

FIGURE 1. A typical VANET scenario.

- We also present some open issues that are encountered while implementing security in VANETs.

We organized the remaining part of the paper as follows. The detailed background study is given in Section 2. Section 3 provided an overview of different authentication and privacy schemes in VANET. Section 4 presented a brief overview of existing surveys. The classification of authentication and privacy schemes are presented in section 5. In section 6, discussion and open issues are discussed. Section 7 concluded this paper.

II. BACKGROUND AND OVERVIEW

In this section, we introduced the historical background of the Vehicular Ad hoc Networks (VANETs). Here, we need to elaborate VANET architecture. VANET characteristics are presented here. We also discussed basic Security requirements for VANETs and security challenges of VANET. In addition, we identify different security threats and attacks in the field of VANET.

A. VANET

The concepts of all the ad hoc networks come from Wireless ad hoc network (WANET) [29]. Vehicular ad hoc network is the variant of Mobile Ad hoc Network (MANET) [30]. In MANET mobile nodes communicate with each other without a central network and where each node is equipped with self-healing network. The topology in MANET changes frequently with passage of time as nodes are allowed to move randomly. Each node works as a router and shows its autonomous behavior. On other hand, VANET has emerged as a more reliable and challenging variation of MANET. In VANET, the nodes are free to enter or leave the network and calls for routing protocols than MANET [31].

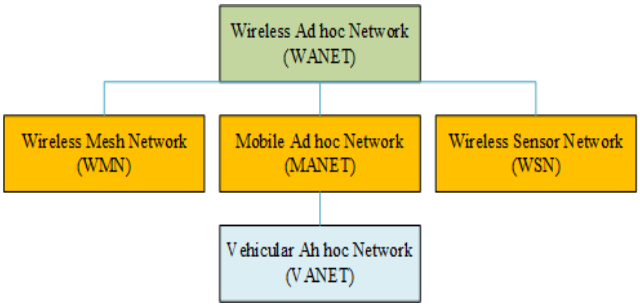

FIGURE 2. Ad hoc networks classification [32].

VANET consists of mobile nodes and roadside units (RSU). Each vehicle is embedded with sensing device call onboard units (OBU) for incoming and outgoing data processing. RSUs are installed at roadside to work like a gateway between mobile nodes and the trusted authority. The main service of VANET is to provide a safe and conformable driving environment by data sharing through the internet. Figure 2 has shown the historical background of VANET.

B. VANET ARCHITECTURE

The main purpose of VANET is to provide the environment where vehicles can communicate with their neighboring vehicles. According to ISO/IEC 42010 [33] and IEEE 1471-2000 [34], the entities involved in VANET can be divided into three sub domains.

1) GENERAL DOMAIN

It consists of two infrastructures: private and internet. The computing resources like nodes and servers which are involved in any kind of activity for VANET come under this domain.

2) INFRASTRUCTURE DOMAIN

There are two parts of this domain: roadside infrastructure and central infrastructure. The roadside infrastructure consists of fixed roadside units such as poles, traffic lights etc. whereas, central infrastructure comprises central controlling authority such as traffic management center, trusted authority etc.

3) MOBILE DOAMIN

This domain also consists of two domains: vehicle domain and mobile devices domain. First domain comprises constantly moving vehicles such as cars, trucks, buses etc. second domain comprises portable devices such as laptop, PDAs etc.

There is another form of architecture called communication architecture. In vehicle communication architecture, basically there are three types of communication which are described as follow:

4) INTER-VEHICULAR COMMUNICATION

In this, the inner performance of the system of vehicle is detected and different factors are determined such as driver

drowsiness or exhaustion etc. For public and driver safety the determinations of these factors are very important [35].

5) VEHICLE-TO-VEHCLE COMMUNICATION

The vehicle exchanges data with each to assist the drivers from any uncertain situation like road accident, road blockage, weather condition etc. It does not depend on fixed infrastructure for exchanging data [36].

6) VEHICLE-TO- ROADSIDE INFRASTRUCTURE

In this type of communication, the vehicles and roadside infrastructure communicate with each other in order to collect data. RSU works as an intermediate node between vehicles and TA [37]. It updates the vehicle about environmental situations like weather conditions, road congestion etc.

C. VANET CHARACTERISTICS

Following are the characteristics which are required to understand and important for designing the privacy and authentication in VANET [38].

1) REAL-TIME CONSTRAINTS

The vehicles communicate in a limited timely manner, therefore vehicles have to respond or take decisions within a limited time.

2) DYNAMIC NETWORK TOPOLOGY

Due to dynamic network topology, it is very difficult to detect malicious vehicles which are moving with high speed.

3) HIGH MOBILITY

In VANET, vehicles move at high speed and cannot tolerate delay during V2V communication [39], [40].

4) VOLATILITY

At any time, vehicles can participate in VANETs. So, the vehicle which has early joined the VANET may not be joining later. Therefore, it is a big security challenge in VANETs. In VANETs, vehicles can join or leave the networks at will. So, a vehicle which has joined the VANET may not join later. Hence, it possesses security challenges in VANET.

5) COMPUTATION AND STORAGE

The vehicles have small storage capacity and some time it requires to process large amounts of data. Therefore, small storage capacity and large volume data processing is the challenging issue in VANET.

D. NECESSARY SECURITY REQUIREMENTS

Vehicles communicate with each other and roadside infrastructure through public networks. The transmitted information among VANETs components is insecure. Therefore, protection of transmitted information should be necessary. According to literature [41], [42] the principle security requirements for vehicular communication are shown in Figure 3 and discussed below.

1) AUTHENTICATION

Authentication is the most important component of secure communication. Authentication is necessary in VANETs for secure vehicular communication. If there is no proper authentication mechanism between VANETs components then transmitted information can be received by unauthorized persons, which can be harmful [43].

2) INTEGRITY

The second most important factor of secure communication in VANETs is integrity. The integrity shows that the transmitted information has not altered during the communication between vehicles and roadside infrastructure. In other words the received message is the same as sent by the sender. If there is no proper integrity ensuring mechanism then it can cause serious consequences. Therefore ensuring integrity is the top priority [44].

3) CONFIDENTIALITY

The third most important factor of security is confidentiality. In some situations it is necessary to encrypt sensitive information for protection from intruders. In VANETs sometimes vehicles transmit sensitive information with each other like in army convoys. So this sensitive information needs to be transmitted in encrypted form so that no one can understand the contents of the messages. And there is no need for data encryption for non-sensitive messages because of resource wastage [45].

4) NON-REPUDIATION

Non repudiation is an important component of secure communication which provides the evidence of communication between two parties. Two vehicles communicate with each other and later cannot deny the message exchanged between them [46], [47].

5) PRIVACY

Privacy is an important factor for deploying VANETs. The driver's personal information should be kept secret from the outside world except law enforcement authorities. The location of the vehicle must be prevented from other participants [48]. The location privacy of the vehicles can be protected by applying the anonymity property. The misleading vehicle should be traced by the trusted authority.

6) ALIABILITY

For receiving critical messages of vehicles, the availability of the wireless channel is the most concern of VANETs. If the intruder applies the Denial of Service Attack (DoS) for jamming the traffic then necessary information cannot be broadcast among the vehicle and the vehicle becomes useless. Hence the high availability of the wireless channel is needed [49].

7) ACCESS CONTROL

Within the wireless channel the most important task is to specify the access level of different entities [50]. There should be such a mechanism that the law enforcement authorities can revoke malicious vehicles from communication networks.

8) PHYSICAL SECURITY

The protection of cryptographic credentials from unauthorized access is the most important task. It can be achieved by adopting tamper proof hardware within the Vehicle's OBU.

9) FARWARD SECRECY

The vehicles joining the new group cannot use their key to read messages sent by new group member

10) BACKWARD SECRECY

The vehicles leaving the group cannot use their key to read messages sent by new group member.

11) PERFECT FORWARD SECRECY

If the system has perfect forward secrecy, then no one can compromise the session key which is derived from a set of long-term keys, even if one of the long-term key compromise in future.

12) KEY INDEPENDANCE

The key independence is achieved through backward and forward secrecy.

13) UNFORGEABILITY

The signature on the transmitted message from a valid member cannot forged by the attacker. An attacker can reuse the original message and forge the signature.

14) UNLINKABILITY

The attacker cannot link the signature on the message to know the real identity of the respective vehicle. Through unlinkability property, the secret information of vehicles in VANET is hidden from others.

15) TRACEABILITY AND REVOCATION

If any of the vehicles is found involved in malicious activity, trusted authority can trace the real identity of the malicious vehicle and can revoke malicious vehicle from VANET.

16) TRANSPARENCY

According to this, all the operations performed by trusted authority should be reliable and trustworthy. Transparency property ensures the trust of members upon trusted authority and corresponding members in VANET.

E. SECURITY CHALLENGES FOR VANETs

In VANETs, messages transmitted between Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside Unit (V2R) may face many security challenges. The VANET is considered as a highly dynamic ad hoc network and can suffer from various security challenges which need high attention in the area. In literature [51] highlight various security challenges as shown in Figure 4.

1) SCALABILITY

VANETs is a dynamic wireless ad hoc network in which it is difficult to predict the actual size of the network at initial deployment stage [52]. So, it is a big challenge to define security schemes from the whole network at the initial stage because of the high scalability nature of the network. As long as the number of the vehicle increases the security requirement also increases and more resources are also needed.

2) HIGH MOBILITY

The traditional security scheme cannot directly apply to VANETs because of high mobility of vehicles [53]. There should be such cryptographic techniques that require minimum computational cost and communication overhead but provide the same security services as provided by traditional schemes. An efficient realistic VANETs communication modeling is shown in [54].

3) RSU COMMUNICATION RANGE

The RSUs communication range has a high impact on VANETs. The RSUs communication range is about 500m in radius. The distances between RSUs should be 1km which is infeasible for congested traffic for developed countries. In [55] different VANETs communication patterns have shown.

4) HURDLES IN TRUST MANAGEMENT

The VANET is a highly scalable network so there are fewer chances in which two vehicles have trust with each. As vehicles communicate with thousands of vehicles daily, data in OBU is difficult to manage. So it is uneasy to manage a huge amount of information. In [56] trust modeling and trust references have shown.

5) DEPEND ON INFRASTRUCTURE

Before becoming the part of vehicular communication it is necessary for each vehicle to authenticate itself to trusted authority. Authentication is necessary for non-repudiation and revocation. The signal became weak during the vehicular communication and needed to be amplified by infrastructure [57]. So for secure vehicular communication, vehicles depend on road infrastructure.

6) HUGE DATA

The increasing numbers of vehicles in the country produced a huge amount of data daily. Therefore, variation in data size creates difficulties for central authority in management. Decentralization approach is the best substitute but this approach may hinder non-repudiation and revocation.

7) HIGH COST

Due to limited communication range, numbers of the RSUs are fixed at recommended range for flexible vehicular communication. All of the vehicles are equipped with wireless communication facilities, computational power and storage capacity which cause high manufacturer cost [58]. These extra facilities increase the cost of the vehicle.

8) BLOCK CHAIN

The blockchain technology is a new paradigm in which peers communicate with each other without involvement of trusted central authority [59]. Due to this technology, it is heavily performing vehicle to vehicle communication. However, blockchain communication ensures anonymous communication without compromising the ability to trace a vehicle. So, if we totally trust in V2V communication, we may lose the authenticity as well as non-repudiation properties of VANETs.

III. SECURITY THREATS AND ATTACKS IN VANETs

In VANETs, vehicles move with high speeds and frequently disconnect due to high speed, therefore more sensitive to attacks. Due to high speed mobility of vehicles, network topology changes suddenly every moment. Therefore, the link disconnection occurred between vehicles frequently. Moreover, the vehicles moving in opposite directions have limited connection with each other, and communicate for a limited period of time. And perhaps did not meet again. Therefore, the VANETs are vulnerable to attacks and malicious vehicles are difficult to recognize.

Secure vehicular communication is possible due to significant knowledge of attacks and threats. Various attacks in VANETs have been identified by researchers in [1], [12], [45], [60]–[63]. Below we have discussed different attacks and security threats on each security service in VANETs.

A. ATTACKS ON AVALIABILIT

Availability of the information plays an important role in VANETs. The absence of availability of information at the right time has a bad effect on VANETs efficiency [47]. Availability in VANETs faces the following attacks.

1) *Denial of Service (DoS) Attacks:* In DoS an attacker makes the network not accessible to the user. This attack can be internal or external in nature. An attacker blocks the communication in three ways in DoS attack: loading the network, blocking the communication channel and closing the packets [64].
2) *Jamming Attack:* VANET is dynamic in nature and vehicles share communication channels due to which traffic jams occur [65]. By using heavy signals with equivalent frequency an attacker can disturb the communication channel. This attack is most dangerous for vehicles safety because of not following the safety alert. An attacker using a jammer can block the useful signals during an effective communication.
3) *Malware Attack:* This attack is used to control the OBUs and RSUs through software components [66]. Due to this attack components of VANETs start malfunctioning.
4) *Broadcast Tampering Attack:* In such a type of attack an attacker in inter-vehicle communication behaves as a transmitted node and copies the same message by inserting a new message in VANETs [44]. So the correct safety alert message becomes hidden due to which it causes dangerous road accidents.
5) *Black Hole Attack:* In VANETs each node is considered as a router. In VANETs this attack targets availability in ad hoc networks. The black hole is the area in the VANETs, which redirects the vehicles and malicious nodes to drop or refuse the packets or forward to the wrong destination or nodes refuse to participate in the communication network [67].
6) *Gray Hole Attack:* Another attack which works like black hole attack is a gray hole attack. In a gray hole attack an untrusted vehicle forward some of the packet and other packets are dropped without tracking [44].
7) *Greedy Behavior Attack:* In such attacks malicious vehicles misuse MAC for increasing bandwidth which affects other users. This causes traffic overloads and causes collisions on communication channels and causes delay [68].
8) *Spamming Attack:* In this attack an attacker injects large amounts of spam messages in VANETs which cause collision and utilize more bandwidth [10].

B. ATTACKS ON CONFIDENTIALITY

The certificate and public key is used to make the exchanged message confidential and only designated vehicles can get access to these messages. Therefore, malicious vehicles cannot get confidential and private information that is exchanged among vehicles. Confidentiality can be possible through different cryptographic techniques. Following are some common attacks to confidentiality.

1) *Eavesdropping Attack:* An eavesdropping attack is one which gets confidential data. Non-registered users get the secret information like data location and user identity, then using these data attackers track the vehicle [69]. The possible solution to prevent these attacks is encryption of sensitive and confidential data.
2) *Traffic Analysis Attack:* Traffic analysis attack is the most dangerous attack that affects the VANET confidentiality. By this attack an attacker listens to the message transmission then analyzes the transmitted messages frequency and tries to extract and gather useful data [70]. These attacks are prevented by vehicle-to infrastructure communication privacy enforcement protocol [166]. It is robust against traffic

analysis attacks. The vehicle directly sends their messages to RSU.

3) *Man-in-the-Middle Attack:* The attacker gets control over inter-vehicles communication and alters the exchanged message by this attack. The communicating entities think that their communication is secure [71]. These attacks can be prevented using robust authentication mechanisms such as digital certificates and key based or strong cryptography based confidential communication [45].
4) *Timing Attacks:* In these attacks, the time slot of the message is altered by adding some delay. These attacks are avoided by using timestamp mechanisms with robust cryptographic operations for packets of delay-sensitive applications in reliable platforms [45].
5) *Social Attack:* This attack is used to disturb the attention of the driver. The attackers send unethical messages to the driver to get the reaction of the driver. This attack affects the performance of the vehicles in VANETs [72]. These attacks can be prevented using

C. ATTACKS ON AUTHENTICATION

The most important part of vehicular communication is authentication, in which nodes authenticate each other and protect themself from unauthorized access. Authentication protects nodes from internal as well as external attacks [73]. Below are some possible attacks on authentication VANETs.

1) *Sybil Attack:* In this attack an attacker, by using multiple fake IDs, broadcasts multiple fake messages to disturbed the normal operations of the VANETs system. These attacks showed the behavior of the vehicles by showing the road is congested and compelled the driver to change the route [74].
2) *Tunneling Attack:* In this attack an attacker initiates private communication using the same network. By utilizing an extra communication channel called tunnel, an attacker joins two far away parts by utilizing extra communication. The faraway node communicates as a neighbor.
3) *GPS Spoofing:* By this attack, the attacker shows false GPS location information for dodging vehicles about his correct location [75].
4) *Node Impersonation Attack:* The attacker pretends to be the original user by guessing the valid identity of the registered user [76].
5) *Replay Attack:* In this attack the valid data is fraud fully transmitted to unauthorized nodes. The VANET system requires much time source with large cache memory to handle this attack for comparing the received messages.
6) *Message Tampering:* In this attack, an attacker alters the messages which are exchanged between V2V or V2I [77].
7) *Masquerading Attack:* In this attack, an attacker uses false IDs to show him as a legal user and obtains unauthorized access. The attacker did not show his real identity in this attack [78].
8) *Known Session-Specific Temporary Information Attack:* In this attack, on the disclosure of a temporary secret value e.g. random number, an attacker attempts to obtain the current secret key.
9) *Key Compromise Impersonation Attacks:* In this attack, if an attacker compromises the private key then he/she can eavesdrop and decrypt past or future conversation, by pretending to be a trusted entity to the victim.

D. ATTACKS ON DATA INTEGRITY

The integrity of the exchanged data ensures the originality of the data. The threats possible to integrity of data are as follows.

1) *Masquerading Attack:* In this attack the attacker, by using registered user password and ID, broadcasts false messages and shows that the message comes from the registered node [79].
2) *Message Tampering Attack:* In this attack the attacker alters the transmitted message for instance when the road is congested then the attacker shows that the road is clear and diverts the vehicle direction.
3) *Illusion Attack:* In this attack by using the existing road condition an attacker generates the traffic warning message which creates the illusion for the vehicle. The illusion attack is caused by the traffic congestion and road accident and degrades the VANETs performance [80].

E. ATTACKS ON NON-REPUDIATION

The non-repudiation property ensures that the receiver and sender cannot deny later from an exchanged message in case of any dispute.

1) *Repudiation Attack:* In this attack an attacker denies the message which he/she has sent in case of any dispute [81].

IV. AUTHENTICATION AND PRIVACY SCHEMES: AN OVERVIEW

In VANETs, authentication and privacy are the basic security requirements. Different entities in VANETs authenticate each other to accept the valid traffic related messages. There are two phases in the authentication process namely: signing phase and verification phase. In the first phase, the sender vehicle signs the messages and sends them to the other vehicle. Upon the receiving of the signed message, the receiver vehicle verifies the signed message [82]. The whole communication between vehicles is very sensitive in VANETs; therefore threats can exist in vehicular communication. For instance, an attacker can generate a fake message, alter a traffic related message, deny the service, forge the message and disseminate wrong vehicle position etc. The first and the most important step that guards the traffic related information from an attacker is the authentication process [83]. The basic purpose of authentication in VANETs is to ensure that the

received message is generated by an authentic source and then the verification process guarantees that the message has not been altered during the source to destination delivery. Therefore, it ensures the integrity of the message, authentication is considered as vigorous security requirements in VANETs [84]. Another most prominent issue that affects VANETs is privacy [85], [86]. Westin and Review [87] has defined privacy as a right of an individual through which he/she can manage, edit, delete and control information about himself and decide how, what and when an information is disseminated to others. An individual can keep a vehicle for a long period of time, therefore an attacker can easily link vehicle's generated messages to the most sensitive information like traveling routes, location and vehicle identity [88]–[90]. Wei *et al.* [91] proposed an authenticated key agreement mechanism for secure vehicle to infrastructure and vehicle to vehicle communication in VANETs. They divide the whole process into three phases. In the first phase, vehicles, RSU and TA authenticate each other. The second phase is about the key agreement process and the last phase is about a tree-based key agreement algorithm. To prevent the side-channel attack and to improve the efficiency, an efficient conditional privacy-preserving authentication scheme is proposed in [92]. For secure communication in VANETs, Alshudukhi *et al.* [93] proposed a lightweight authentication scheme which satisfied conditional privacy-preserving property. According to authors, their scheme is most suitable for privacy and security issues in the field of vehicular communication because it combined TPD based scheme and RSU based scheme. Beside this, their scheme is also robust against common security attacks. A lightweight authentication and privacy preserving scheme based on elliptic curves is proposed in [94]. The privacy preservation has been achieved using Pseudo-id-based authentication. For secure and confidential vehicular communication, symmetric key cryptography is used. The issues which hinder VANET security are integrity, confidentiality, identity privacy, and authentication. To overcome these issues, a protocol for VANET called privacy-preserving anonymous authentication is proposed in [95]. For anonymous authentication, they design identity based signature algorithms. Their designed algorithm enables the vehicle to communicate anonymously and disseminate messages confidentially. Alshudukhi *et al.* [22] showed that the scheme called lightweight conditional privacy-preserving authentication protocol by Wei *et al.* [96] is insured and forgeable. According to the authors, in that scheme any one can forge the valid signature on a message and it did not satisfy the conditional privacy. Beside cryptanalysis, they suggested a solution for handling attacks. An efficient and secure self-checking Authentication Scheme for VANET has been proposed in [151]. In this scheme, pseudonyms are used as a substitute of traditional authentication and involve TA in the process of authentication to reduce computational cost. Besides, the appropriate used group signature to reduce authentication frequency. In [152], an anonymous authentication scheme based on blockchain has been proposed. The RSU authenticates each vehicle anonymously and they use session keys for future secure communication. The blockchain is used to preserve the integrity of the transmitted message. The confidentiality of the transmitted message is also provided in VANET by this scheme. Zhang *et al.* [153] proposed a bilinear pairings based authentication protocol for VANET. The vehicle's identity authentication and message verification is realized by this protocol. This protocol also prevents legitimate vehicles from being tracked by malicious vehicles. The batch authentication method is used to improve the efficiency of message verification. An improved password-authenticated key exchange protocol for VANET has been proposed in [154]. This protocol generates a physical randomness based high-entropy secret shared information and the pre-shared short password, and then establishes session keys based on high-entropy secret shared information. To improve the protocol efficiency, this scheme uses XOR operation instead of exponential operations. In [155], an unlinkable authenticated key agreement with collusion resistant for VANETs has been proposed. The TA generates multiple tickets to hide the real identity of the vehicle to meet unlinkability of V2I. Using homomorphic encryption, the vehicle generates pseudonyms and the RSU uses a ticket for the authentication process. A lightweight privacy preserving authentication protocol has been proposed in [156]. Initially, Moore curve technique is used to convert all the RSUs to vectors, then each vehicle uses BGN homomorphic encryption to get the information of RSU from its planning route before beginning its trip. The authentication process between vehicle and RSU is fast due to deduced information of RSU.

The protection of an individual's privacy can be gained through anonymity methods. In vehicular communication, the privacy of vehicles can be ensured through pseudonyms. Therefore, it is necessary to keep the real identity of the vehicles secret from the receiver except for Trusted Authority. When any dispute occurs the real identity of the vehicle can be traced by TA and can detect the malicious vehicles. Therefore privacy and authentication are the most prominent components for secure and safe vehicular communication.

V. EXISTING SURVEYS

A large number of authentication and privacy techniques have been discussed in literature. However, there are no comprehensive surveys that cover security requirements, performance efficiency, counter measures, open issues, attacks and security challenges as a holistic view. Many surveys exist in literature that have discussed different aspects of vehicular communication.

Various privacy and security aspects have been discussed in [41], [51], [97]–[103]. This survey focuses on different cryptographic techniques namely: Pseudonym based Identity Based, hash function based, and group signature based Cryptography. The reviews of latest cryptographic security and trust oriented models are given in this survey. In addition, a comprehensive analysis of the different techniques is presented in detail. Arif *et al.* [104] presented a survey on

TABLE 2. Comparison of existing surveys in VANETs.

Ref.	VANETs Overview	Domain	Security Requirements	Security Challenges	Attacks	Performance Measures	Counter Measures	Open Issues
[41]	×	✓	✓	×	×	✓	×	✓
[104]	×	✓	✓	×	×	×	×	✓
[105]	✓	×	✓	✓	×	×	✓	×
[42]	✓	×	✓	×	×	×	✓	×
[106]	×	✓	✓	×	×	✓	×	✓
[51]	✓	✓	✓	×	×	✓	✓	✓
[79]	✓	✓	✓	×	×	×	✓	✓
[107]	×	×	×	✓	×	×	×	×
Proposed Survey	✓	✓	✓	✓	✓	✓	✓	✓

different possible security attacks in the field of VANETs. They also discussed necessary communication protocols for each network layer with possible attacks that occurred at each layer. Moreover, they also highlight application send challenges along with open research issues in VANET. Ali *et al.* [105] proposed authentication and privacy schemes for vehicular ad hoc networks. In this survey authors categorized privacy and authentication schemes on the basis of security requirements, performance parameters, possible attacks and mechanism. In [42], Chen described various authentication schemes and applications used in VANETs. The security requirements of various authentication schemes were analyzed. They ensure authentication identity which is necessary for any application. Sakiz and Sen [106] discussed different attacks and their corresponding detection mechanism. The authors classified different attacks according to their goals and methods and present their solution with advantages and disadvantages. An extensive overview of various security challenges, their causes and solutions have been presented in [51]. The detailed security architecture and well known security protocols are given. They classified the various attacks in literature and their solutions. Furthermore, they discussed certain research challenges and open research issues. In [79], sheikh *et al.* have given a detailed survey of security services, attacks, and applications for VANETs. First, they discussed the functions and basic model of the VANRTs. Second, they present different authentication schemes that protect VANETs from various attacks. Third, they analyzed the performance of different authentication schemes in VANETs. Kuutti *et al.* [107] presented contemporary localization techniques for vehicles and investigated that how these techniques are applicable for autonomous vehicles. They focus on those techniques which only use the information obtained from the vehicle's onboard unit. Secondly, in addition to sensory information obtained from the vehicle's onboard unit, they analyzed those techniques which take the advantages from off-board information obtained from the vehicle to everything communication channels. A brief study on different security challenging issues in VANET along with their existing possibilities are presented in [108]. The authors have given the current solution and defined future goals. Mahmood *et al.* [109] discussed various security challenges and countermeasures in VANET. They focused on security issues such as attacks and threats which affect different protocol layers of VANETs architecture.

The aforesaid surveys are comprehensive and cover most of the security requirements in the field of VANETs but still need some improvement. First we differentiate our work from aforementioned surveys in terms of different authentication and privacy schemes and with other strengths and weaknesses. For example, Malhi *et al.* [41] categorized the cryptographic techniques into four groups: Symmetric Key Cryptography, Public Key Cryptography, Certificateless Cryptography and Identity Based Cryptography. Ali *et al.* [105] classified privacy and authentication techniques into HAPS, GAPS, PAPS, and IAPS. They have

reviewed and compared those techniques along with their security attacks, limitations and strength, security requirements, and performance parameters. Sheikh *et al.* [79] classified authentication schemes on the basis of cryptography and signature. They further divide the cryptograph-based authentication schemes into two categories: identity-based cryptography, symmetric cryptography (Hash Function and timed efficient stream loss-tolerant authentication (TESLA)) and asymmetric cryptography (PKI certificate and ECDSA), and Kuutti *et al.* [107] classified sensor based localization techniques into five categories: Global Positioning System (GPS) based techniques; cameras based techniques, radar based techniques, Light Detection and Ranging (LiDAR) based techniques, and ultrasonic sensors based techniques. Second, we present the VANETs security in terms of security requirements, security challenges, counter measures and classified different attacks while the above surveys did not cover all these security factors as whole, especially Arif *et al.* [104] addressed VANET's privacy and security attacks along with their applications and challenges. They also presented the effectiveness of cloud computing and VANETs with security and privacy issues and architecture. Sakiz and Sen [106] classified different attacks and the corresponding detection mechanisms along with their effects and solutions. They also described their advantages and disadvantages. A comprehensive overview of security challenges and their causes along with existing solutions are addressed extensively in [51]. They have given the details of the recent security architectures and the well-known security standards and protocols. Their study concentrated on the classification of the different attacks known in the literature and their solutions. Third, we measure the efficiency of each scheme in terms of computational cost and communication overhead while performance measures have not been presented in literature in detail.

In short, we present classification of authentication and privacy schemes, security requirements, security challenges, countermeasures, performance measures and discuss open issues in VANETs as a holistic view while all of the above surveys did not cover these factors holistically. We have compared aforementioned schemes in tabulated form. In Table 2, our contributions with respect to the aforesaid surveys are presented. The ✓" and ✗" denote whether the domain specified in the column has been discussed in the survey or not.

VI. CLASSIFICATION OF AUTHENTICATION AND PRIVACY SCHEMES IN VANET

The authentication and privacy play an important role in vehicular communication to provide trust between entities. In this domain, several authentication and privacy schemes have been discussed in literature to protect the message from unauthorized entities and resist against different possible attacks. To implement these schemes, modern cryptographic mechanisms such as symmetric key cryptography, asymmetric key cryptography and certificateless public key cryptography are used. In addition, these schemes are constructed on the basis of bilinear pairings, pseudonyms or elliptic curve cryptosystems (ECC) for generating signature and verification of the signature. However, these schemes still suffer from either different security issues or performance efficiency. These schemes highlight various authentication and privacy schemes to some extent but did not fully cover the efficiency. To address these issues we classify authentication and privacy schemes into five groups: Pseudonym Based Privacy Preserving Authentication Schemes (PNBPAS), Identity Based Privacy Preserving Authentication Schemes (IDBPAS), Hash Functions Based Privacy Preserving Authentication Schemes (HFBPAS), Group Signature Based Privacy Preserving, Authentication Schemes (GSBPAS) and Blockchain-Based Privacy Preserving Authentication Schemes (BBPAS). Most of these schemes used batch verification of the signature in the verification process. The hardness of one way hash function, elliptic curve cryptography, Bloom Filter and bilinear pairing is discussed as follows.

1) **One way hash function:** On the basis of following properties, one way hash function is said to be secure [110]:
   - Hash function can take a variable size message as input and produce a fixed size message digest r as output. For given r, it is easy to compute $y = h(r)$. However for given y, it is infeasible to compute $r = h^{-1}(s)$
   - For given r, it is infeasible compute $r' \neq r$ and $h(r') \neq h(r)$
2) **Elliptic Curve Cryptography (ECC):** An elliptic curve is a plane curve over a finite field F_p which is made up of the points satisfying the equation: $y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$ and $a,b \in Fp$ [111], [112]. Let R be the point at infinity then R and other points on curve make an additive elliptic curve group G having order q and generator P_1. The elliptic curve group G has the following properties:
   - Point addition: Let P_1 and P_2 are two random points lying on elliptic curve such that $(P_1, P_2) \in G$, where G *is a group generated by* P_1. If $P_1 \neq P_2$ then $R = P_1 + P_2$ can be computed, here R is the intersection point of curve and the line which connects P_1 and P_2. If $P_1 = P_2$ then $R = P_1 + P_2$, and if $P_1 = -P_2$ then $P_1 + P_2 = R$. Figure 6 represents point addition in the elliptic curve.
   - Scalar multiplication: The scalar multiplication on the elliptic curve EC is defined as $nP_1 = P_1 + P_2 + P_3 \ldots P_n$ for n times, where $n \in Z_q^*$ and $n > 0$
   - Elliptic Curve Discrete Logarithm (ECDL) problem: It is a hard problem and infeasible to compute. Given points P_1 and P_2 are two random points lying on elliptic curve such that $(P_1, P_2) \in G$, where G *is a group generated by* P_1. ECDLP is used to compute *an integer* x *such that* $P_2 = xP_1 \in G$, *where* $x \in Zq^*$ is an unknown integer.
3) **Bloom filter:** Bloom filter [113] is a data structure that is designed to represent a set $S = X_1 + X_2 + X_3 \ldots X_n$ of

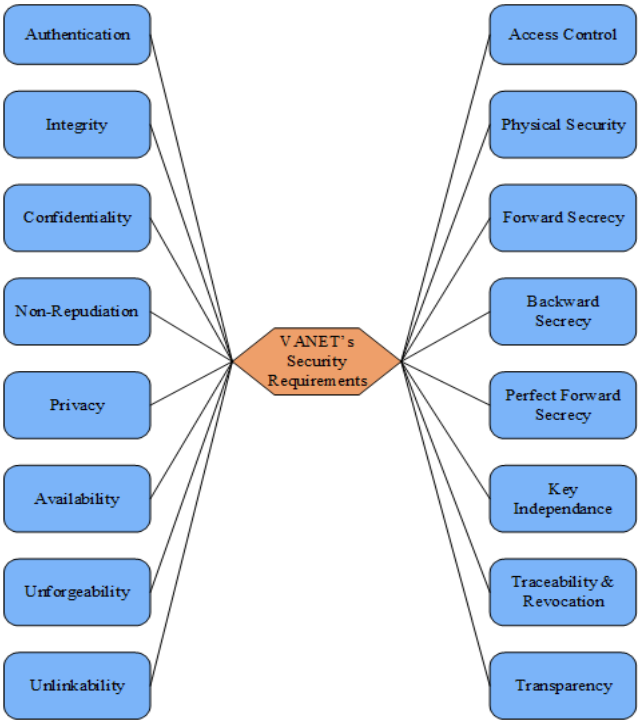

FIGURE 3. Necessary security requirements for VANETs.

n elements to support membership queries. The vector V_i with m bits and k hash, initially all bits set to 0, for adding an element to Bloom filter, take the hash of that element for a short time and set the bits in the bit vector at the index of those hashes to 1. To check whether the given value c is in S, we can check the position of bit at $h(c)$. If the position is set to be 1, then element c may be in set S.

1) **Bilinear pairing:** Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group with the same prime order q respectively. The point $P_1 \in G_1$ generates the group G_1. Let e: $G_1 \times G_2 \rightarrow G_2$ be a bilinear pairing which satisfies the following properties [114], [115]:
   - Bilinearity: For all $P_1, P_2, R \in G_1$, $e(P_1 + P_2, R) = e(P_1, P_2)e(P_2, R)$ and $e(P_1, P_2 + R) = e(P_1, P_2)e(P_1, R)$. Similarly, for all $a,b \in Z_q^*$, $e\ (aP_1, bP_1) = e(P_1, P_1)\ ab = e(P_1, abP_1) = e\ (abP_1, P_1)$.
   - Non-degeneracy: There exists two points $P_1, P_2 \in G_1$, such that $e(P_1, P_2) \neq 1$ or $e(P_2, R) \neq e(P_1, P_1)$, where 1 is the identity element in G_2.
   - Computability: There must be an efficient algorithm to compute e (P_1, P_2) for all $P_1, P_2 \in G_1$.

A. PERFORMANCE PARAMETERS

In proposed classification of privacy-preserving authentication schemes every scheme has been surveyed along with strength and limitations. Each classification is presented with security requirements, attacks and performance parameters in distinct tables. The attacks and security requirements are shown on the basis of aforementioned cryptographic operations. The efficiency of each classification is measured on the basis of performance parameters. The implementation of different cryptographic operations have been done using PBC, MIRACL, JPBC, and CHARM crypto libraries [105]. The computational cost of these schemes can be measured on the basis of different cryptographic operations like bilinear pairing, hash function, bloom filter or elliptic curve cryptography. The symbols used to represent bilinear pairing, hash function and ECC cryptographic operations are shown in Table 4.

The aforementioned cryptographic operations have computational cost and communication overhead. We consider message signature generation and verification of concerned schemes as computational cost. Moreover,

TABLE 3. Execution time needed to perform various cryptographic operations.

Cryptographic operations			
Cryptographic operations	T_{PAO}	T_h	T_{SMg}
Execution time (ms)	*0.0018*	*0.0001*	*0.4420*

TABLE 4. Execution time needed to perform various cryptographic operations.

Symbol	Description
h(.)	Secure One way hash function
r	Message digest
P_1, P_2	Two points on Elliptic Curve
T_h	Execution time required to perform a one-way general hash function operation
T_{PA}	Execution time required to perform point addition operation in G_1, i.e. in $P_1 + P_2$, P_1, $P_2 \in G_1$.
T_{PO}	Time require to perform a pairing operation i.e. $e(P_1, P_2)$, where $P_1, P_2 \in G_1$.
T_{SMO}	Execution time require to performs scalar multiplication operation in G_1, i.e. in aP_1, $a \in Z_q^*$ and $P_1 \in G_1$
T_{PAO}	Execution time require to performs point addition operation in G, i.e. in $P_1 + P_2$, P_1, $P_2 \in G$.
T_{MPH}	Execution time require to performs map-to-point hash operation.
T_{SMg}	Execution time required to perform scalar multiplication operation in G, i.e. in aP_1, $a \in Z_q^*$ and $P_1 \in G$.
G_1	A cyclic additive group
G_2	A cyclic multiplicative group

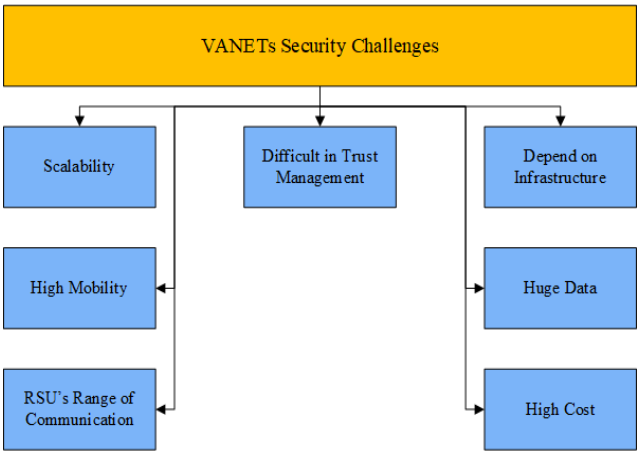

FIGURE 4. VANETs security challenges.

TABLE 5. Measurement for performance parameters.

Range of Values			
Performance parameters	***Low***	***Medium***	***High***
Computational Cost (ms)	*0-3*	*3-6*	*6-10*
Communication Overhead (in byte)	*1-50*	*51-100*	*101-150*

we measure communication overhead of each scheme in terms of size of message signature and the extra bits transmitted with plaintext. The total size of traffic related message-signature includes pseudo-ID, time-stamp, type-id, certificate, message-ID, payload/message, etc. are measured in the form of bits or bytes.

Table 3 presents execution time required to perform aforementioned cryptographic operations and Table 5 to decide which of the schemes has either low or medium or high overhead [105].

We have classified privacy-preserving authentication schemes into five groups, i.e. Pseudonym Based Authentication and Privacy Preserving Schemes (PNBAPS), Identity Based Authentication and Privacy Preserving Schemes (IDBAPS), Hash Functions Based Authentication and Privacy Preserving Schemes (HFBAPS), Group Signature Based Authentication and Privacy Preserving Schemes (GSBAPS) and Blockchain-Based Authentication and Privacy Preserving Schemes (BBAPS). These schemes are discussed as followed:

B. PSEUDONYM BASED AUTHENTICATION AND PRIVACY SCHEMES

The name used as an alternative to real name is called pseudonym. The concept of pseudonym is first given by Chaum [116] which allows the entities to communicate with each other anonymously using a false name. Each entity in an organization is known through pseudonyms instead of real names to preserve the identity-anonymity and privacy. These pseudonyms are generated in such a way that it cannot link to get the real information about the entity and later by using his/her credential, prove a relation to concern and thereby provide unlinkability. Beside this, a pseudonym mechanism is used to achieve the conditional privacy preservation in IoV [117].

Singh *et al.* [118], addressed a privacy preservation in VANETs called Cooperative Pseudonym Exchange and Scheme Permutation. This scheme allowed the vehicles to exchange their pseudonyms cooperatively. The scheme permutation is used to enhance location privacy preservation. The pseudonyms are exchanged between vehicles, therefore it eliminates the location tracking by service provider. This scheme has no extra communication overhead because trusted authority is not involved in the process. Li *et al.* [119] Proposed pseudonym swap mechanism and design appropriate utility metric. It selects a pseudonym for a vehicle by adapting a differential privacy preserving mechanism to satisfy pseudonym in-distinguishability. This scheme guarantees that if two vehicles have high similarity of driving states, it is impossible for attackers to link the vehicles and their pseudonyms after swap. The theoretical analyses proved that this mechanism satisfies the proposed privacy definition, thus ensuring the unlinkability between the new pseudonym and the old pseudonym. To enhance the privacy of the user of the vehicle, Jiayu *et al.* proposed "a secure and efficient identity-based anonymous authentication scheme and uses pseudonyms" [120]. They improved existing public key infrastructure of vehicles and introduced a Bloom filter to compress the Certificate Revocation List (CRL). They ensured the user's privacy through an efficient pseudonym revocation scheme. A batch pseudonym revocation is done in this scheme and makes the pseudonym unlinkable. According to the authors, their scheme is secure and meets the privacy requirement in VANETs and CRL distribution. For the solution of security conflicts and privacy preservation, the RSU-aided trust framework is proposed in [121]. According to this framework, the reliability of the message is evaluated by assigning the reputation label certificate by roadside unit for every vehicle in its communication range. To evaluate the behavior of vehicles, the authors used localized reputation label certificates and the central reputation value. To ensure privacy, reputation label certificate shows two statuses to substitute specific reputation value. Then these reputation values are stored in a central database. They designed a reputation update algorithm with different weights to encourage vehicles to follow the rules. Moreover on the revocation of reputation label certificate, privacy and security is not protected. A Strong Pseudonym-based Authentication (SPATA) framework has been presented for preserving the real identity of vehicles [122]. Vehicles are allowed to generate pseudonyms in private and secure ways according to SPATA. Without SPATA, the privacy of the vehicle cannot be preserved by

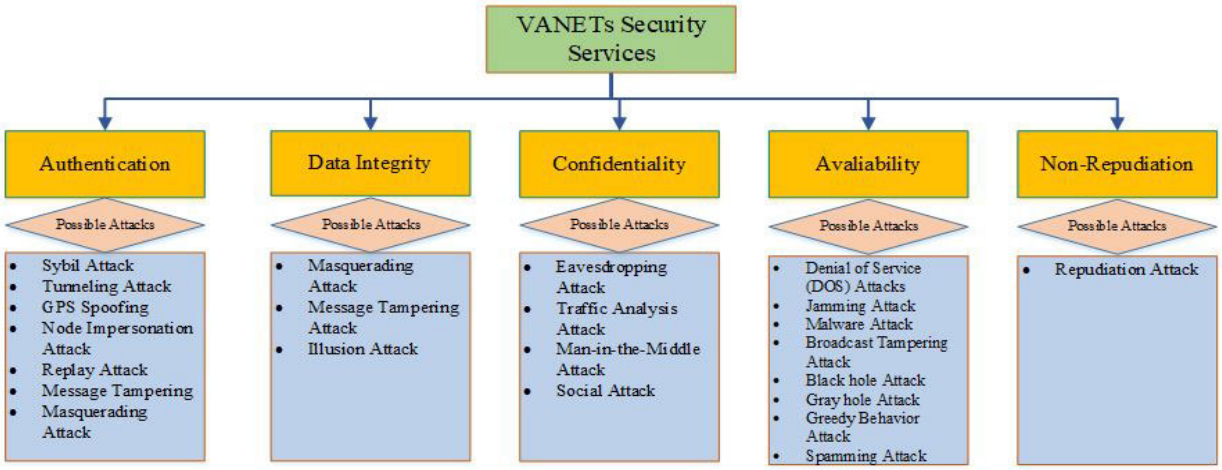

FIGURE 5. VANET security services with possible attacks.

storing information regarding vehicles in a single location. Therefore, through mapping the real identity to pseudonyms, it eliminates the concept of linkability of certificates based on single authority. The CRL kept only the most recently revoked communication pseudonyms due to which the size of CRL became small. Through a distributed mechanism, the privacy of the vehicle is preserved during the resolution phase and revocation. An efficient pseudonym changing and management framework (PRIVANET) is proposed in [123]. This framework showed vehicular geographic area as a grid and has hierarchical structure. Each grid cell is divided into one or many logical zones, called vehicular location privacy zones (VLPZs). It is easy to deploy these zones over the extensive roadside infrastructures [124], such as gas stations, to provide a secure management of pseudonyms. The main building block of the said frameworks are: an adapted user-centric privacy model, a method to generate the IP and MAC addresses from the pseudonym, a reputation-based mechanism to motivate selfish vehicles to enter VLPZs, effective VLPZ-based pseudonym changing strategy, a secure hybrid mechanism for the distribution of pseudonyms sets and CRLs, a stochastic model to estimate the number of VLPZs required at a given cell, and a mathematical model for an optimal placement of the VLPZs over RIs to reduce the transportation cost of vehicles in terms of time. To handle the security and privacy of vehicles in the Intelligent Transport System, Ali *et al.* [125] proposed Advanced Strong Pseudonym based Authentication (ASPA). Only vehicles with valid pseudonyms are allowed to communicate in ITS. All the vehicles are assigned pseudonyms in a secure way. To avoid the chance of likability of vehicle pseudonyms certificates, the pseudonym mappings of vehicles are stored at different locations. In addition, the size of CRL becomes small due storage of most recent communication pseudonyms and malicious vehicles are revoked. Therefore, the size of CRL does not increase exponentially. The distributed framework of ASPA guarantees the vehicles privacy preservation in the real identities mapping and revocation phase. Arain *et al.* [126] proposed an efficient dynamic pseudonymous based multiple mix-zones authentication protocol for privacy preservation to enhance security of vehicular networks. According to authors, most of the existing schemes either used group signature based approaches or pseudonym based approaches with certificate revocation lists that cause significant communicational and storage overhead, which increase computational cost. To overcome these problems the authors present a dynamic pseudonymous based multiple mix-zones authentication protocol that only requires mobile vehicles to communicate with the reported server for registration and dynamic pseudonym change. Furthermore, to achieve the user privacy they define a mechanism to provide users with dynamic pseudonyms named. Finally, they analyzed the robustness of their scheme. Liu *et al.* [127] present intelligent traffic light control schemes which are based on fog computing. In this scheme traffic light is considered as a fog device that generates and verifies one puzzle for each vehicle in a fixed time interval. Agustina and Hakim [128] have designed a secure protocol to ensure authentication and privacy using hierarchical pseudonyms with blind signature. Using blind signature, the signer signs the message without knowing the contents of the message. This scheme works in three phases: design of the detailed protocol, requirement analysis, and provable security. This scheme improves the security and privacy to some extent but cannot reduce computation cost and verification delay. It did not consider the verification of vehicle signature on the message by RSU.

No mathematical proof is given to ensure security requirements. No graph is given to illustrate exactly the performance of the proposed protocol. The security requirements, security attacks controlled by PNBAPS and PNBAPS performance analysis are shown in (Tables 6, 7, and 8)

TABLE 6. Security requirements fulfill by PNBAPS.

Ref.	Message Authentication	Privacy	Non-repudiation	Source authentication	Collision resistance	Identity Anonymity	Traceability	Unlinkability	Unforgability
[118]	✓	✓	✓	×	×	✓	×	✓	✓
[119]	×	✓	×	✓	✓	×	×	✓	×
[120]	✓	✓	×	✓	×	✓	✓	✓	✓
[121]	✓	✓	×	✓	✓	✓	×	✓	×
[122]	✓	✓	✓	✓	×	✓	×	✓	×
[123]	✓	✓	×	✓	×	✓	×	×	×
[125]	✓	✓	✓	✓	×	✓	×	×	✓
[126]	✓	✓	×	✓	×	×	×	×	×
[127]	✓	✓	✓	✓	×	✓	×	×	×
[128]	✓	✓	×	✓	×	✓	✓	×	×

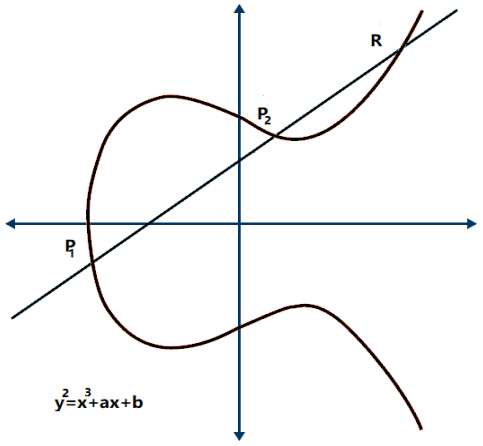

FIGURE 6. Elliptic curve cryptography points addition.

C. IDENTITY BASED SIGNATURE AUTHENTICATION AND PRIVACY SCHEMES

Shamir proposed identity based cryptographic systems to reduce the load of digital certificate management which was suffering from traditional public key infrastructure [129]. In identity based cryptographic systems, the public key of an entity is derived from his/her well-known public identity information, for instance contact number, email, and identity number etc. Identity based public key cryptographic systems are replacing traditional public key cryptographic systems to eliminate a certificate management effort. There is no need for a certificate for authentication of messages in identity based public key cryptography. Therefore, it reduces the overhead produced due to certificates in the message. Hence it improves the efficiency of VANETs.

An identity based conditional privacy preserving and authentication scheme based on bilinear map has been proposed for vehicles to infrastructure communication [130]. The authors used one way hash functions in this scheme instead of map to point hash functions. The efficiency of signing and verification of the message is increased at the RSU side. In addition, their scheme used batch signature verification and allowed them to authenticate multiple traffic related messages due to which computational cost has significantly decreased. According to authors, their scheme is efficient with respect to computational cost as compared to similar schemes. A local identity based anonymous message authentication protocol for VANETs is presented to handle inherent issues [131]. The certification authority issued a unique long term certificate to each vehicle and roadside unit. Each roadside unit is responsible for assigning the local master keys to every vehicle that comes in its communication range. When the vehicles go to the communication range of another roadside unit, they authenticate each other by their long term certificate. To generate the localized anonymous identity, the valid vehicle can obtain the local master keys from the current RSU. The privacy of vehicles can be protected by choosing randomly anonymous identity to sign the safety related message which can be verified using either a single or both authentication method. Wei *et al.* [132] proposed an identity-based signature scheme to achieve unforgeability against chosen-message attack without random oracle. They design two secure and efficient outsourcing algorithms for exponential operations in order to reduce the computational cost. The authors also presented a privacy-preserving protocol for VANETs by using outsourcing computing and identity based signature. They also used a proxy re-signature scheme for authentication. To hide the real identity of the vehicle, trusted authority authorized the roadside units to act as agents and roadside units convert the onboard unit's signature into trusted authority's signature. Later the TA can access the real identity of the vehicle using its secret key when the dispute occurs. According to the author their scheme is efficient in terms of computational cost. For vehicle-to-vehicle communication, Ali *et al.* [133] proposed an efficient identity based signature with conditional privacy-preserving authentication scheme based on the Elliptic Curve Cryptography (ECC) and general one-way hash functions. Their

TABLE 7. Security attacks controlled by PNBAPS.

Ref.	Replay	DoS	Sybil	Modification	Location tracking	Impersonation	ID disclosure	Bogus information
[118]	✓	✓	×	✓	✓	×	✓	✓
[119]	✓	✓	✓	✓	✓	✓	✓	×
[120]	✓	✓	✓	✓	×	✓	✓	✓
[121]	×	✓	×	✓	×	×	✓	✓
[122]	✓	×	✓	✓	×	✓	✓	×
[123]	✓	✓	×	✓	×	×	✓	✓
[125]	✓	×	✓	✓	×	✓	✓	×
[126]	✓	×	×	✓	×	✓	✓	×
[127]	✓	×	×	✓		✓	✓	✓
[128]	✓	✓	×	✓	✓	✓	✓	×

TABLE 8. PNBAPS performance analysis.

Performance parameters		
Schemes	**Computation Cost**	**Communication overhead**
[118]	Medium	low
[119]	Low	Low
[120]	High	Medium
[121]	High	High
[122]	Medium	High
[123]	High	Medium
[125]	Medium	Medium
[126]	High	High
[127]	Low	Low
[128]	×	×

TABLE 9. Security requirements fulfill by IDBAPS.

Proposed schemes	Message authentication	Privacy	Non-repudiation	Source authentication	Collision resistance	Identity Anonymity	Traceability	Unlinkability	Unforgability
[130]	✓	✓	×	✓	✓	✓	✓	✓	×
[131]	✓	✓	✓	✓	✓	✓	✓	×	×
[132]	✓	✓	×	✓	✓	✓	✓	×	✓
[133]	✓	✓	✓	✓	×	✓	✓	✓	×
[134]	✓	✓	✓	✓	✓	×	✓	×	✓

scheme used the batch signature verification method to enable each vehicle to authenticate a large number of messages simultaneously. The authors used a random oracle model for security proof of their proposed scheme. They proved the security robustness of their scheme in the random oracle model. To secure vehicular communication, an efficient distributed aggregate privacy-preserving authentication protocol based on bilinear pairing is presented by Zhang *et al.* [134]. Due to the powerful system architecture of their scheme it depends only on the practical tamper proof device (TPD) instead of ideal TPD. In their scheme, trusted authority and roadside units cannot learn the secret keys of vehicles and do

TABLE 10. Security attacks controlled by IDBAPS.

Ref.	Replay	DoS	Sybil	Modification	Location tracking	Impersonation	ID disclosure	Bogus information
[130]	✓	×	×	✓	✓	✓	✓	×
[131]	✓	✓	×	✓	✓	✓	×	✓
[132]	✓	✓	✓	✓	×	✓	✓	✓
[133]	×	✓	×	✓	×	×	✓	✓
[134]	✓	×	✓	✓	×	✓	✓	×

TABLE 11. IDBAPS performance analysis.

Performance parameters		
Schemes	**Computation Cost**	**Communication overhead**
[130]	High	High
[131]	Low	Medium
[132]	High	High
[133]	Low	High
[134]	Low	Low

not allow any entity to pretend to be valid vehicles. According to the authors, if any vehicle is compromised then only a limited number of the vehicle can be affected by the attacker. The security requirements, security attacks controlled by IDBAPS and IDBAPS performance analysis are shown in (Tables 9, 10, and 11).

D. HASH FUNCTION BASED AUTHENTICATION AND PRIVACY SCHEMES

Hash function is responsible for providing the integrity of the message without encryption of the message. When a hash function is applied to a message, it generates a fixed value referred to as message digest. To achieve message integrity, a hash value must be attached to the sending message. A novel lightweight authentication protocol is presented for secure communication in VANETs, which only uses one way hash function and exclusive-OR operations [135]. This protocol consists of four phases: Initialization, vehicle registration, RSU registration, and message authentication. For achieving the security goals they analyzed the protocol using BAN logic. According to the authors, their scheme is robust against some attacks and the data kept secret during the communication. The performance analysis showed that their scheme is efficient in terms of communication cost and computational cost. Alfadhli *et al.* [136], proposed a lightweight privacy preserving authentication scheme for VANETs, which only used general one way hash functions. The driving problem occurring in dangerous areas is overcome in this scheme. The VANETs system administrator authenticates the vehicle once during the movement of the vehicle, in this way the system reduces the authentication redundancy and the efficiency of the system is improved. The one way hash functions have negligible computational cost, so computational cost and communication overhead is significantly decreased and efficiently fulfills security needs. A secure and privacy preserving hashed based authentication and revelation protocol using internet of vehicle has been discussed in [137]. In this scheme the vehicles exchange the message about local and global warming. This scheme is secure against some well-known attacks and provides a better security service in a cost effective manner. Cui *et al.* [138] propose a conditional privacy-preserving authentication scheme based on the hash function, which does not use complex bilinear mapping and elliptic curve encryption for identity authentication to prevent illegal vehicle interference and ensure the legitimacy of the source. They used a group key agreement mechanism based on the Chinese remainder theorem (CRT) to distribute the group key for authenticated vehicles. The group key can be updated when the vehicle joins and leaves the group. In the process of anonymous message generation and verification, analysis of the results shows that their proposed scheme satisfied the basic security requirements and has significant advantages in terms of computation cost and communication overhead as compared to existing schemes. Zhu *et al.* [139], presented a lightweight and scalable secure communication framework for VANET. It consists of five protocols namely: (a) V2I, (b) group key agreement protocol without RSU (c) RSU-aided two-party communication protocol, (d) two-party communication protocol without RSU, and (e) RSU-aided group key distribution protocol. Roadside units used hashed MAC functions to authenticate the messages and AES to encrypt the messages. Due to hashed MAC function the

efficiency of the protocols is increased. The security analysis shows that this scheme is secure against various attacks. The hash function and group secret key based efficient privacy preserving authentication scheme for VANETs is discussed in [140]. Vighnesh *et al.* [141] proposed a vehicular authentication scheme using authentication code and hash chaining. In this way vehicles and roadside units can communicate in a secure way. The encryption takes place using the master key. RSU attach its identity with the message before sending it to the authentication center. Various authentication schemes have been discussed in literature but they suffer from high computational cost, especially in the certificate revocation list verification process. On the other hand various pseudonym-ID schemes use system key signature but suffer from communication overhead. This scheme used a temporary group secret key and permanent vehicle pseudonym-ID due to which the process of verification and authentication significantly improved. This scheme is also robust against various security attacks. The security requirements, security attacks controlled by HFBAPS and HFBAPS performance analysis are shown in (Tables 12, 13, and 14).

E. GROUP SIGNATURE BASED AUTHENTICATION AND PRIVACY SCHEMES

In group signature, all the group members are allowed to sign the message on the behalf of the group leader. A single group public key is used to verify the signature but the identity of the signer is kept secret. Moreover, it is impossible to judge whether a group member has been issued two signatures. However, in case of any dispute a designated group manager can disclose the real identity of signer [142].

A group signature based anonymous authentication scheme is proposed [143]. To provide the anonymous authentication of vehicles a regional trusted authority is added as group manager. Conditional privacy and anonymity are achieved by adopting group signature methods. According to the authors this scheme is efficient and robust in terms of performance and security. An efficient and secure group signature based authentication and key distribution scheme is proposed [144]. In this scheme the computational load is distributed from trusted authority to roadside units. The RSUs in a specific domain form a group. Each group of RSUs has group leader and member RSUs. The member RSU and vehicle established a shared symmetric key with each other. Then a group key is provided to the vehicle from leader RSU on behalf of TA. Vehicle uses this group key to communicate with RSUs within the desired group. Moreover, this scheme ensures security in an efficient manner. Zhang *et al.* [145] proposed authentication protocol for VANETs which is based on combination of group session key and group signature. The aforesaid signature verification method achieves robust security against impersonation attack and reduces computational cost by reducing bilinear pairing operations. Zheng *et al.* [146] proposed an anonymous authentication scheme based on group signature for VANETs. On the basis of certificateless group signature, it used elliptic curves to perform calculations and used synchronization factor to improve the computational efficiency of group members while joining, revoking and signing. This scheme ensures anonymity, forward security, traceability and unforgeability. A group signature framework based on an efficient and anonymous authentication protocol is proposed [147]. To ensure forward security, this protocol uses a complete sub-tree method which achieves membership revocation. This protocol used decentralized group model to reduce the heavy workload on TA by generating group certificates for OBUs. The OBUs retrieved revocation list from TA. For the management of routing messages in VANETs, a Trustworthy VANET routing with group authentication keys is proposed [148]. The TROPHY messages are received recursively by authorized nodes. It allowed those nodes to refresh their cryptographic credentials and update the authentication keys across the network. Then distribute those messages epidemically across the network and construct in such a manner that any node found as lost or physically compromised will not be able to perform the refreshment using them. A central authority where all the credentials are stored, they use a mechanism to recover from any unauthorized physical access and disclose such material at one time without human intervention on reset of devices due to the use of a Key Distribution Centre (KDC). An ID based group signature scheme for VANETs has been discussed in [149]. This scheme used an ID based group signature scheme to avoid complex certificate management for protection of user privacy. They also used pseudonym methods to protect the real identity of vehicles and malicious nodes can be traced easily. Zhu *et al.* [150] proposed a privacy preserving authentication scheme based on group signature in VANETs. Their scheme is divided into different domains. In their scheme group private keys are distributed by RSUs. The RSUs are also responsible for managing vehicles in a local manner. Before group authentication, the authors used hash message authentication code to ensure integrity. At last, the entities authenticate each other in cooperative message authentication fashion. In this way each vehicle will have to authenticate a small number of messages, hence reducing the authentication burden. The security requirements, security attacks controlled by GSBAPS and GSBAPS performance analysis are shown in (Tables 15, 16, and 17).

F. BLOCKCHAIN BASED AUTHENTICATION AND PRIVACY SCHEMES

In this section, a blockchain based authentication and privacy preserving schemes are presented. All the vehicles stored in the blockchain are assigned a certificate or pseudo identity by Certification Authority (CA). Each receiver is provided information regarding the entry pointer for verification. The most prominent benefit of blockchain is transparency and decentralization [157]. The blockchain technology has irreversible property, i.e, the information once which is saved in blockchain cannot be modified later. Ali *et al.* [158] proposed a public key signature scheme based on blockchain for V2I Communication in VANET. Their scheme is certificateless

TABLE 12. Security requirements fulfill by HFBAPS.

Ref.	Message Authentication	Privacy	Non-repudiation	Source authentication	Collision resistance	Identity Anonymity	Traceability	Unlinkability	Unforgability
[135]	✓	✓	×	✓	✓	✓	✓	✓	×
[136]	✓	✓	✓	×	✓	✓	✓	✓	×
[137]	✓	✓	×	✓	✓	✓	✓	✓	✓
[138]	✓	✓	✓	✓	✓	×	✓	✓	×
[139]	✓	✓	✓	✓	✓	✓	×	✓	×
[140]	✓	✓	×	✓	✓	×	×	✓	✓
[141]	✓	✓	✓	×	✓	×	×	×	✓

TABLE 13. Attacks controlled by HFBAPS.

Ref.	Replay	DoS	Sybil	Modification	Location tracking	Impersonation	ID disclosure	Bogus information
[135]	✓	✓	×	✓	×	✓	×	✓
[136]	✓	✓	×	✓	✓	✓	×	×
[137]	✓	✓	✓	✓	×	✓	✓	✓
[138]	✓	✓	×	✓	✓	✓	✓	×
[139]	✓	×	✓	✓	✓	✓	×	✓
[140]	✓	✓	×	✓	×	✓	✓	✓
[141]	✓	✓	✓	✓	×	×	×	✓

TABLE 14. HFBAPS performance analysis.

Performance parameters		
Schemes	**Computation Cost**	**Communication overhead**
[135]	Medium	High
[136]	Low	Low
[137]	Low	Low
[138]	Low	High
[139]	Medium	High
[140]	Low	Medium
[141]	Low	Low

and conditional privacy is achieved using bilinear pairing. To make the verification process fast, they used batch signature and aggregate signature verification. The pseudo-identity revocation transparency is achieved by using blockchain. Their scheme satisfied efficient revocation and traceability property along with authentication and identity. However, the batch signature and aggregate verification process increases its complexity. A secure data sharing and storage based on blockchain in VANET has been proposed in [159]. The data coins are allocated using smart contracts for the vehicles which are participating in the communication network. The signature on the message is generated using ECC to fulfill non-repudiation and authentication properties. The pre-selected node can establish a distributed agreement

TABLE 15. Security requirements fulfill by GSBAPS.

Ref.	Message Authentication	Privacy	Non-repudiation	Source authentication	Collision resistance	Identity Anonymity	Traceability	Unlinkability	Unforgability
[143]	✓	✓	✓	✓	×	✓	×	✓	×
[144]	✓	✓	✓	✓	✓	✓	✓	×	✓
[145]	✓	✓	✓	×	✓	✓	✓	×	✓
[146]	✓	✓	✓	×	✓	✓	✓	×	✓
[147]	✓	✓	✓	✓	✓	✓	✓	×	✓
[148]	✓	✓	✓	×	✓	✓	×	×	✓
[149]	✓	✓		✓	×	✓	×	✓	✓
[150]	✓	✓	×	✓	✓	×	✓	×	×

TABLE 16. Attacks controlled by GSBAPS.

Ref.	Replay	DoS	Sybil	Modification	Location tracking	Impersonation	ID disclosure	Bogus information
[143]	✓	✓	×	✓	✓	✓	✓	×
[144]	✓	✓	×	✓	✓	✓	✓	×
[145]	✓	✓	✓	✓	✓	✓	×	✓
[146]	✓	✓	✓	✓	✓	×	✓	×
[147]	✓	✓	✓	✓	✓	✓	×	✓
[148]	✓	✓	×	✓	×	✓	✓	×
[149]	✓	✓	×	✓	✓	✓	✓	✓
[150]	✓	✓	×	✓	×	✓	✓	✓

TABLE 17. GSBAPS performance analysis.

Performance parameters		
Schemes	**Computation Cost**	**Communication overhead**
[143]	**High**	**Medium**
[144]	**High**	×
[145]	**Medium**	**Medium**
[146]	**Low**	**Medium**
[147]	**High**	**High**
[148]	**Medium**	**Medium**
[149]	**Medium**	**Medium**
[150]	**Low**	**Low**

before adding a block to the ledger. Using signal verification method or batch verification method, the receiver can verify the exchanged message. However, time complexity is significantly increased due to the combination of blockchain and bilinear pairing. Lu *et al.* [160] proposed a privacy-preserving authentication scheme for VANET based on blockchain technology. They used Merkle Patricia tree (MPT) and chronological Merkle tree (CMT) to extend the conventional blockchain. A node containing public key, certificate and encrypted link is added to MPT by Law Enforcement Authority (LEA). The information about the entry pointer to the leaf node is provided to the corresponding vehicle. The identity of the sender is authenticated by the receiver using a distributed authentication process. The certificate

TABLE 18. Security requirements fulfill by BBAPS.

Ref.	Message Authentication	Privacy	Non-repudiation	Source authentication	Collision resistance	Identity Anonymity	Traceability	Unlinkability	Unforgability
[158]	✓	✓	✓	✓	✓	✓	✓	✓	×
[159]	✓	✓	✓	✓	×	✓	✓	×	✓
[160]	✓	✓	×	×	✓	✓	✓	✓	✓
[161]	✓	✓	✓	✓	×	✓	✓	✓	✓
[162]	✓	✓	×	✓	✓	✓	✓	✓	×
[163]	✓	✓	×	✓	×	✓	✓	✓	✓
[164]	✓	✓	×	✓	✓	✓	✓	✓	✓
[165]	✓	✓	✓	✓	×	✓	✓	✓	×

TABLE 19. Attacks controlled by BBAPS.

Ref.	Replay	DoS	Sybil	Modification	Location tracking	Impersonation	ID disclosure	Bogus information
[158]	✓	✓	×	✓	✓	✓	✓	×
[159]	✓	✓	×	✓	✓	×	✓	×
[160]	✓	✓	✓	✓	✓	✓	×	✓
[161]	✓	✓	×	✓	✓	✓	✓	✓
[162]	✓	✓	✓	✓	✓	×	✓	×
[163]	✓	✓	✓	✓	✓	✓	×	✓
[164]	✓	✓	×	✓	✓	✓	✓	✓
[165]	✓	✓	×	✓	✓	✓	✓	×

TABLE 20. BBAPS performance analysis.

Performance parameters		
Schemes	**Computation Cost**	**Communication overhead**
[158]	**High**	**Low**
[159]	**High**	**Low**
[160]	**High**	**High**
[161]	**Medium**	**Low**
[162]	**Low**	**Low**
[163]	**High**	**Medium**
[164]	**High**	**High**
[165]	**Low**	**Low**

of a particular vehicle is revoked by LEA on expiry of its certificate or on its malicious activity. The LEA broadcasts CRL to corresponding vehicles to indicate that a particular certificate has been revoked and no further communication should be made to that particular vehicle. The malicious vehicle's real identity is disclosed on decryption of the link from the corresponding leaf node. However, computation cost and communication overhead is significantly increased due to integration of CA and LEA. A traffic event validation and trust verification scheme based on blockchain is proposed in [161]. This framework includes three main features: 1) Proof-of-event (PoE), 2) RSUs's Trust verification, 3) two-phase transaction for fast event notification. The PoE is used for two pass validation when unproven

incidents occur. The traffic related information is gathered by RSU and the vehicle adjacent to it can verify that information. The PoE mechanism did not allow RSU to transmit false notification. All the verified events are added into the blockchain to ensure the trust verification. However, computation cost is increased due to verification of transactions for PoE. Wang *et al.* [162] proposed a blockchain based trustworthiness scalable computation for V2I authentication. The main focus of this scheme is to compute trustworthiness of vehicles and handing over of vehicles from one RSU to another in a secure way. This scheme is vulnerable against replay attacks. However, it did not provide a comprehensive review of existing schemes. In [163], a blockchain based decentralized key management mechanism for VANET is presented]. In this scheme, each vehicle and their corresponding RSU share a session key between them. The vehicle service provider (VSP) updates the expired private and public keys of vehicles using smart contracts. The main responsibility of VSP is to detect malicious key pairs and revoke them from the smart contract. It is secure against public key tampering attacks, internal attacks, DoS attacks and collusion attacks. Zhang *et al.* [164] proposed a secure data sharing system for IoV based on blockchain. The authors divided the entire system into multiple regions and each region used two types of blockchain for storage of messages: primary blockchain and secondary blockchain. The announcement message is signed anonymously using blind signature and threshold secret sharing. In [164], a secure authentication and key management scheme based on blockchain in VANET is proposed. They used the Chinese Remainder Theorem (CRT) in the V2V group formation phase. All the vehicles come in the communication range of specific RSU form a group. The consortium blockchain is used to update the group key during the dynamic key updating phase. Furthermore, this scheme is robust against various attacks like reply attack, impersonation attack etc. A new technique called Proof of Driving (PoD) has been proposed in [165]. The PoD is used to select random honest miners for generation of blocks for blockchain-based VANET applications. Besides, a Service Standard Score (SSS) based filtering technique is used to detect and remove the malicious nodes of the vehicular miner nodes. This scheme also addresses fairness and efficiency issues caused by PoD and PoW. The security requirements, security attacks controlled by BBAPS and GSBPAS performance analysis are shown in (Tables 18, 19, and 20).

VII. DISCUSSIONS AND OPEN ISSUES

In VANETs the most crucial part is to manage the vehicular communication in terms of low communication overhead and inexpensive delay of messages transmitted between vehicles and infrastructure. The vehicular communication must ensure that it fulfills the entire basic security requirement and provide reliable vehicular communication. Security is the major concern for successful deployment of VANETs. There exist some open issues which may be considered while dealing with these security concerns. These issues need special consideration of researchers and become an open research area in future. Below, we highlight some of the open issues which may become a hot research topic in future.

1) FIGURE AXIS LABELS REVOCATION, CRL MANAGEMENT AND DISTRIBUTION PROCESS

In the revocation process, the misbehaving vehicles are detected and revoked and the list of revoked vehicles is distributed. On the detection of misbehavior of vehicles, how should the process of revocation be carried out? What will be the mechanism of CRLs distribution? These issues are still not fully covered and need researcher consideration. CRLs still has no infrastructure that manages CRLs with short lifetime certificates. The modern cryptographic solution did not present authorization and certificate revocation so what are the alternates of these?

2) CRYPTOGRAPHIC METHODS FOR PRIVACY, SECURITY AND TRACEABILITY

Key management is a basic concept of cryptographic techniques. Are key management and distribution exclusive to the vehicle manufacturer or government? For lightweight secure communication, what should be the key size? How to handle time delay for management and distribution of keys? How to deal with keys within a short duration of time? What will be the method of dealing with a key without a certificate? How to achieve privacy and traceability? How to secure pseudonyms for non-traceability?

3) EVALUATION OF TRUSTWORTHINESS AND VEHICLES MISBEHAVIOR DETECTION MECHANISM

An evaluation of a vehicle's trust and detecting misbehavior of them in VANETs is the hard problem. How to check the trustworthiness of nodes? Is the calculated trust ids reliable or not for disseminating critical messages? On the successful calculation of trust, what actions should be taken? Are the punishment factors clearly defined or not? In case of a wrong trust calculation, how to revoke a malicious vehicle?

4) DATA CONTEXT TRUST AND VERIFICATION

The basic goal of VANETs is to ensure cooperative and safe driving. This can be possible by providing the right information at the right time. Therefore, it is necessary to verify the exchanged message in VANETs.

This should have a strong intrusion detection system. How do VANETs handle the uncertain situation of detection of a malicious vehicle suddenly? How to check the robustness of tamper proof hardware?

5) SELF-ORGANIZING CAPABILITIES OF NETWORKS VIA A HIGH MOBILE NETWORK ENVIRONMENT

It is feasible that vehicles can form a cluster communication. How to deliver across cluster partitions in VANET still not well-defined? How do groups communicate across the jammed signals? How to select the cluster head? is there infrastructure to handle cluster communication?

VIII. CONCLUSION

VANETs play a key role in intelligent transport systems to prevent vehicles from unexpected situations. Traffic safety related messages are exchanged between the vehicles to meet safe and secure journeys. However, the communication in VANETs takes place via open wireless channels and faces some security challenges. The intruder can easily compromise the privacy and security of the message. This paper has presented a detailed study on various authentication and privacy schemes used in the field of VANET. We have categorized different authentication and privacy schemes into five groups: PNBAPS, IDBAPS, HFBAPS, GSBAPS and BBAPS. We have compared and reviewed these schemes with their security requirements, security attacks and performance parameters. Moreover, we have discussed security challenges which help the researcher to deploy the VANETs technology, infrastructure and service efficiently and securely. Finally, we have discussed some open issues in the field of VANETs.

ACKNOWLEDGMENT

The authors would like to thank the financial support and facilities provided by Universiti Putra Malaysia and the Ministry of Education Malaysia for the execution, completion and publication of this paper.

REFERENCES

[1] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study," *Int. J. Secur. Appl.*, vol. 10, no. 5, pp. 261–274, May 2016.

[2] J. King and A. I. Awad, "A distributed security mechanism for resource-constrained IoT devices," *Informatica.*, vol. 40, no. 1, pp. 1–12, 2016.

[3] M. G. Samaila, M. Neto, D. A. Fernandes, M. M. Freire, and P. R. Inácio, "Security challenges of the Internet of Things," in *Beyond Internet Things*. Cham, Switzerland: Springer, 2017, pp. 53–82.

[4] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for vehicular ad hoc NETworks (VANETs): A survey," *Veh. Commun.*, vol. 11, pp. 20–31, Jan. 2018.

[5] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[6] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and solutions for cellular based V2X communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 222–255, 1st Quart., 2021.

[7] A. Awang, K. Husain, N. Kamel, and S. Aissa, "Routing in vehicular ad-hoc networks: A survey on single- and cross-layer design techniques, and perspectives," *IEEE Access*, vol. 5, pp. 9497–9517, 2017.

[8] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[9] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[10] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

[11] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[12] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 1050–1055.

[13] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1621–1632, May 2018.

[14] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2020.

[15] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[16] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and end-to-end authentication," *IEEE Access*, vol. 6, pp. 46558–46567, 2018.

[17] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs," *IEEE Access*, vol. 8, pp. 142858–142874, 2020.

[18] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1779–1790, Jul. 2018.

[19] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[20] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021.

[21] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14248–14257, Sep. 2021.

[22] J. Zhang and Q. Zhang, "On the security of a lightweight conditional privacy-preserving authentication in VANETs," *IEEE Trans. Inf. Forensics Security*, early access, Mar. 17, 2021, doi: 10.1109/TIFS.2021.3066277.

[23] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 1981–1996, 2014.

[24] WHO, "Road traffic injuries," *Key Facts*, Feb. 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[25] WHO. (2020). *Global Status Report on Road Safety 2015*. [Online]. Available: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en

[26] CARE. (2020). *European Road Accident Database*. [Online]. Available: https://ec.europa.eu/transport/road_safety/specialist/statistics/map-viewer/

[27] UNECE. *United Nations Economic Commission for Europe*. Accessed: Jun. 19, 2020. [Online]. Available: https://unece.org/publications/oes/welcome

[28] C. D. Wang and J. P. Thompson, "Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network," Google Patents 5 613 039, Mar. 18, 1997.

[29] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: Challenges and directions," *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 20–22, May 2002.

[30] R. Tomar, M. Prateek, and G. H. Sastry, "Vehicular adhoc network (VANET)—An introduction," *Int. J. Control Appl.*, vol. 9, no. 18, pp. 8883–8888, 2016.

[31] R. Prabhakar and K. Ahirwar, "Comparative study of VANET and MANET routing protocols," in *Proc. Int. Conf. Advance Comput. Commun. Technol. (ACCT)*, 2011, pp. 1–7.

[32] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, "Vehicular ad-hoc network (VANET)," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, May 2018, pp. 1–6.

[33] D. Emery and R. Hilliard, "Every architecture description needs a framework: Expressing architecture frameworks using ISO/IEC 42010," in *Proc. Conf. Softw. Archit. Eur. Conf. Softw. Archit. (IEEE/IFIP)*, Sep. 2009, pp. 31–40.

[34] M. W. Maier, D. Emery, and R. Hilliard, "ANSI/IEEE 1471 and systems engineering," *Syst. Eng.*, vol. 7, no. 3, pp. 257–270, 2004.

[35] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, Aug. 2015, Art. no. 745303.

[36] W. Schinkel, T. van der Sande, and H. Nijmeijer, "State estimation for cooperative lateral vehicle following using vehicle-to-vehicle communication," *Electronics*, vol. 10, no. 6, p. 651, Mar. 2021.

[37] B. M. Masini, G. Ferrari, C. Silva, and I. Thibault, "Connected vehicles: Applications and communication challenges," *Mobile Inf. Syst.*, vol. 2017, Aug. 2017, Art. no. 1082183.

[38] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021.

[39] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–25, Jan. 2020.

[40] L. Feng, Y. Xiu-Ping, and W. Jie, "Security transmission routing protocol for MIMO-VANET," in *Proc. Int. Conf. Cloud Comput. Internet Things*, Dec. 2014, pp. 152–156.

[41] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101664.

[42] C.-L. Chen, "A survey of authentication protocols in VANET," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Cham, Switzerland: Springer, 2018, pp. 572–577.

[43] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[44] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[45] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. Ad Hoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[46] F. Al-Hawi, C. Y. Yeun, and M. Al-Qutayti, "Security challenges for emerging VANETs," in *Proc. 4th Int. Conf. Inf. Technol.*, Jordan, Amman, 2009, pp. 3–5.

[47] M. Kassim, R. A. Rahman, and R. Mustapha, "Mobile ad hoc network (MANET) routing protocols comparison for wireless sensor network," in *Proc. IEEE Int. Conf. Syst. Eng. Technol.*, Jun. 2011, pp. 148–152.

[48] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey," *Future Internet*, vol. 13, no. 4, p. 96, Apr. 2021.

[49] Y. Qian and N. Moayeri, "Design of secure and application-oriented VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2008, pp. 2794–2799.

[50] T. Wang, L. Kang, and J. Duan, "Dynamic fine-grained access control scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 188, Apr. 2021, Art. no. 107872.

[51] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[52] S. S. Moni and D. Manivannan, "A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs," *Internet Things*, vol. 13, Mar. 2021, Art. no. 100350.

[53] S. Harrabi, I. B. Jaafar, and K. Ghedira, "Performance analysis of vanets routing protocols," Res. Square, Univ. Mannouba, Manouba, Tunisia, Tech. Rep., 2021, doi: 10.21203/rs.3.rs-487685/v1.

[54] N. Akhtar, S. C. Ergen, and O. Ozkasap, "Vehicle mobility and communication channel models for realistic and efficient highway VANET simulation," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 248–262, Jan. 2014.

[55] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 119–125, Nov. 2008.

[56] Y. Ruan and A. Durresi, "A survey of trust management systems for online social communities–trust modeling, trust inference and attacks," *Knowl.-Based Syst.*, vol. 106, pp. 150–163, Aug. 2016.

[57] M. Jerbi, S.-M. Senouci, T. Rasheed, and Y. Ghamri-Doudane, "An infrastructure-free traffic information system for vehicular networks," in *Proc. IEEE 66th Veh. Technol. Conf.*, Sep. 2007, pp. 2086–2090.

[58] S. A. Rashid, L. Audah, M. M. Hamdi, and S. Alani, "An overview on quality of service and data dissemination in VANETs," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2020, pp. 1–5.

[59] M. Abdelhafidh, N. Charef, A. B. Mnaouer, and L. Chaari, "A survey of blockchain-based solutions for IoTs, VANETs, and FANETs," in *Enabling Blockchain Technology for Secure Networking and Communications*. Hershey, PA, USA: IGI Global, 2021, pp. 110–148.

[60] M. Houmer, M. L. Hasnaoui, and A. Elfergougui, "Security analysis of vehicular ad-hoc networks based on attack tree," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Jun. 2018, pp. 21–26.

[61] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Veh. Commun.*, vol. 4, pp. 30–37, Apr. 2016.

[62] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," *Int. J. Comput. Theory Eng.*, vol. 4, no. 6, p. 1007, 2012.

[63] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. 3rd Int. Workshop Veh. Ad Hoc Netw. (VANET)*, 2006, pp. 67–75.

[64] H. Singh and V. Dhir, "Distributed agent based technique for detecting distributed denial-of-service (DDoS) attacks in WLAN," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 1, pp. 248–262, 2018.

[65] A. T. Nguyen, L. Mokdad, and J. Ben Othman, "Solution of detecting jamming attacks in vehicle ad hoc networks," in *Proc. 16th ACM Int. Conf. Modeling, Anal. Simulation Wireless Mobile Syst.*, Nov. 2013, pp. 405–410.

[66] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," *Int. J. Comput. Sci.*, vol. 2, no. 1, pp. 88–96, 2013.

[67] W. Ahmed and M. Elhadef, "Securing intelligent vehicular ad hoc networks: A survey," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2017, pp. 6–14.

[68] I. A. Sumra, H. B. Hasbullah, and J.-L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Vehicular Ad-Hoc Networks for Smart Cities*. Singapore: Springer, 2015, pp. 51–61.

[69] A. K. Mishra, A. K. Tripathy, and M. Sinha, "Customized score-based security threat analysis in VANET," in *Advances in Distributed Computing and Machine Learning*. Singapore: Springer, 2021, pp. 3–13.

[70] P. Kohli, S. Painuly, P. Matta, and S. Sharma, "Future trends of security and privacy in next generation VANET," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2020, pp. 1372–1375.

[71] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," *Comput. Secur.*, vol. 25, no. 3, pp. 184–189, 2006.

[72] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *Proc. 5th Swiss Transp. Res. Conf. (STRC)*, 2005.

[73] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 325–338, Sep. 2013.

[74] P. Druschel, M. F. Kaashoek, and A. I. Rowstron, *Revised Papers From the First International Workshop on Peer-to-Peer Systems*. Berlin, Germany: Springer-Verlag, 2002.

[75] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2005, pp. 1285–1290.

[76] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst.*, Dec. 2012, pp. 1–9.

[77] Z. Xu, D. He, N. Kumar, and K.-K.-R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in VANETs," *Secur. Commun. Netw.*, vol. 2020, pp. 1–12, Feb. 2020.

[78] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Jul. 2020, pp. 821–825.

[79] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[80] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8.

[81] B. T. Rao, R. L. Patibandla, and V. L. J. C. Narayana, "Comparative study on security and privacy issues in VANETs," *Cloud IoT-Based Veh. Ad Hoc Netw.*, vol. 12, pp. 145–162, Apr. 2021.

[82] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[83] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247.

[84] M. Bellare and P. J. U. C. Rogaway, "Introduction to modern cryptography," *Ucsd Cse.*, vol. 207, p. 207, 2005.

[85] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2562–2574, Aug. 2015.
[86] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.
[87] A. F. J. W. Westin and L. L. Review, "Privacy and freedom," *Washington Lee Law Rev.*, vol. 25, no. 1, p. 166, 1968.
[88] J. Cui, J. Wen, S. Han, and H. Zhong, "Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3491–3498, Oct. 2018.
[89] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.
[90] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA: CRC Press, 2016.
[91] L. Wei, J. Cui, H. Zhong, Y. Xu, and L. Liu, "Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs," *IEEE Trans. Mobile Comput.*, early access, Feb. 4, 2021, doi: 10.1109/TMC.2021.3056712.
[92] J. S. Alshudukhi, B. A. Mohammed, and Z. G. Al-Mekhlafi, "An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 226624–226636, 2020.
[93] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633–15642, 2021.
[94] T. Nandy, M. Y. I. Idris, R. M. Noor, A. W. A. Wahab, S. Bhattacharyya, R. Kolandaisamy, and M. Yahuza, "A secure, privacy-preserving, and lightweight authentication scheme for VANETs," *IEEE Sensors J.*, vol. 21, no. 18, pp. 20998–21011, Sep. 2021.
[95] X. Zhang, W. Wang, L. Mu, C. Huang, H. Fu, and C. J. W. P. C. Xu, "Efficient privacy-preserving anonymous authentication protocol for vehicular ad-hoc networks," *Wireless Pers. Commun.*, vol. 120, pp. 1–17, Jun. 2021.
[96] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2020.
[97] M. A. Elsadig and Y. A. Fadlalla, "VANETs security issues and challenges: A survey," *Indian J. Sci. Technol.*, vol. 9, no. 28, pp. 1–8, Jul. 2016.
[98] M. A. Razzaque, A. Salehi, and S. M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: Survey and the road ahead," in *Wireless Networks and Security*. Berlin, Germany: Springer, 2013, pp. 107–132.
[99] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.
[100] A. Luckshetty, S. Dontal, S. Tangade, and S. S. Manvi, "A survey: Comparative study of applications, attacks, security and privacy in VANETs," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2016, pp. 1594–1598.
[101] E. B. Ajulo, R. O. Akinyede, and O. S. Adewale, "Security threats and privacy issues in vehicular ad-hoc network (VANET): Survey and perspective," *J. Inf.*, vol. 4, no. 1, pp. 1–9, 2018.
[102] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.
[103] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, Jul. 2020.
[104] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, Oct. 2019, Art. no. 100179.
[105] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.
[106] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.
[107] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 829–846, Apr. 2018.
[108] R. Hemalatha, "A survey: Security challenges of VANET and their current solution," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 1239–1244, Apr. 2021.
[109] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: Challenges and countermeasures," *Secur. Commun. Netw.*, vol. 2021, pp. 1–20, Jun. 2021.
[110] W. Mao, *Modern Cryptography: Theory and Practice*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2003.
[111] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1985, pp. 417–426.
[112] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 2, Mar. 2005, pp. 1187–1192.
[113] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.
[114] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.
[115] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.
[116] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, Oct. 1985.
[117] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Syst. J.*, vol. 15, no. 1, pp. 245–256, Mar. 2020.
[118] P. K. Singh, S. N. Gowtham, S. Tamilselvan, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100183.
[119] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, and X. Huang, "PAPU: Pseudonym swap with provable unlinkability based on differential privacy in VANETs," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11789–11802, Dec. 2020.
[120] J. Qi and T. Gao, "A privacy-preserving authentication and pseudonym revocation scheme for VANETs," *IEEE Access*, vol. 8, pp. 177693–177707, 2020.
[121] S. Wang and N. Yao, "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," *Wireless Netw.*, vol. 25, no. 3, pp. 1099–1115, 2019.
[122] Q. E. Ali, N. Ahmad, A. H. Malik, G. Ali, M. Asif, M. Khalid, and Y. Cao, "SPATA: Strong pseudonym-based AuthenTicAtion in intelligent transport system," *IEEE Access*, vol. 6, pp. 79114–79128, 2018.
[123] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 8, pp. 3209–3218, Aug. 2020.
[124] T. Neudecker, N. An, O. K. Tonguz, T. Gaugel, and J. Mittag, "Feasibility of virtual traffic lights in non-line-of-sight environments," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. (VANET)*, 2012, pp. 103–106.
[125] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din, and G. Ali, "ASPA: Advanced strong pseudonym based authentication in intelligent transport system," *PLoS ONE*, vol. 14, no. 8, Aug. 2019, Art. no. e0221213.
[126] Q. A. Arain, D. Zhongliang, I. Memon, S. Arain, F. K. Shaikh, A. Zubedi, M. A. Unar, A. Ashraf, and R. Shaikh, "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Pers. Commun., Int. J.*, vol. 95, no. 2, pp. 505–521, Jul. 2017.
[127] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 817–824, Jan. 2018.
[128] E. R. Agustina and A. R. Hakim, "Secure VANET protocol using hierarchical pseudonyms with blind signature," in *Proc. 11st Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2017, pp. 1–4.

[129] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Appl. Cryptograph. Techn.*, vol. 1984. Springer, 1985, pp. 47–53.
[130] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228.
[131] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.
[132] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, "A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62785–62793, 2019.
[133] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.
[134] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2016.
[135] X. Li, T. Liu, M. S. Obaidat, F. Wu, and P. Vijayakumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3547–3557, May 2020.
[136] S. A. Alfadhli, S. Lu, A. Fatani, H. Al-Fedhly, and M. Ince, "SD2PA: A fully safe driving and privacy-preserving authentication scheme for VANETs," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–25, Dec. 2020.
[137] H. Vasudev and D. Das, "P^2-SHARP: Privacy preserving secure hash based authentication and revelation protocol in IoVs," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107989.
[138] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Veh. Commun.*, vol. 14, pp. 15–25, Oct. 2018.
[139] X. Zhu, Y. Lu, X. Zhu, and S. Qiu, "Lightweight and scalable secure communication in VANET," *Int. J. Electron.*, vol. 102, no. 5, pp. 765–780, May 2015.
[140] S. A. Alfadhli, S. Alresheedi, S. Lu, A. Fatani, and M. Ince, "ELCPH: An efficient lightweight conditional privacy-preserving authentication scheme based on hash function and local group secrete key for VANET," in *Proc. World Symp. Softw. Eng. (WSSE)*, 2019, pp. 32–36.
[141] N. V. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in *Proc. IEEE Symp. Wireless Technol. Appl. (ISWTA)*, Sep. 2011, pp. 96–101.
[142] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proc. Annu. Int. Cryptol. Conf.* Springer, 1997, pp. 410–424.
[143] Y. Jiang, S. Ge, and X. Shen, "AAAS: An anonymous authentication scheme based on group signature in VANETs," *IEEE Access*, vol. 8, pp. 98986–98998, 2020.
[144] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2017, pp. 478–483.
[145] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. Ma, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019.
[146] Y. Zheng, G. Chen, and L. Guo, "An anonymous authentication scheme in VANETs of smart city based on certificateless group signature," *Complexity*, vol. 2020, pp. 1–7, Jun. 2020.
[147] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao, and Y. He, "An efficient and secure anonymous authentication scheme for VANETs based on the framework of group signatures," *IEEE Access*, vol. 6, pp. 62584–62600, 2018.
[148] P. Cirne, A. Zúquete, and S. Sargento, "TROPHY: Trustworthy VANET routing with group authentication keys," *Ad Hoc Netw.*, vol. 71, pp. 45–67, Mar. 2018.
[149] T. Gao and J. Qi, "An anonymous access authentication scheme for VANETs based on ID-based group signature," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Springer, 2018, pp. 490–497.
[150] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for VANETs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 4609–4614.
[151] H. Jiang, L. Hua, and L. Wahab, "SAES: A self-checking authentication scheme with higher efficiency and security for VANET," *Peer Peer Netw. Appl.*, vol. 14, no. 2, pp. 528–540, Mar. 2021.
[152] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Feb. 2021.
[153] J. Zhang, Q. Zhang, X. Lu, and Y. Gan, "A novel privacy-preserving authentication protocol using bilinear pairings for the VANET environment," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Jun. 2021.
[154] Y. Chen, J. Yuan, and Y. Zhang, "An improved password-authenticated key exchange protocol for VANET," *Veh. Commun.*, vol. 27, Jan. 2021, Art. no. 100286.
[155] X. Li, J. Liu, M. S. Obaidat, P. Vijayakumar, Q. Jiang, and R. Amin, "An unlinkable authenticated key agreement with collusion resistant for VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7992–8006, Aug. 2021.
[156] S. Lv and Y. Liu, "PLVA: Privacy-preserving and lightweight V2I authentication protocol," *IEEE Trans. Intell. Transp. Syst.*, early access, Feb. 24, 2021, doi: 10.1109/TITS.2021.3059638.
[157] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[158] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, Oct. 2019, Art. no. 101636.
[159] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.
[160] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.
[161] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.
[162] C. Wang, J. Shen, J. F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Sep. 2020.
[163] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.
[164] L. Zhang, M. Luo, J. Li, M. H. Au, K.-K.-R. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for internet of vehicles: A position paper," *Veh. Commun.*, vol. 16, pp. 85–93, Apr. 2019.
[165] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.
[166] P. Cencioni and R. Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication," *Comput. Commun.*, vol. 31, no. 12, pp. 2790–2802, Jul. 2008.

SAGHEER AHMED JAN received the bachelor's degree (Hons.) in computer science from Hazara University Mansehra, Pakistan, in 2012, and the master's degree in computer science from Hazara University Mansehra, in 2015, with a specialization in information security, where he is currently pursuing the Ph.D. degree in computer science. He has served as a SST IT at the Elementary and Secondary Education KPK, Pakistan. Later, he joined as a Lecturer at Hazara University Mansehra. Currently, he is serving as a Lecturer for the Higher Education Department KPK. His research interests include wireless networks, the IoT, applied cryptography, and information security.

NOOR UL AMIN received the master's degree in computer science from the University of Peshawar, Pakistan, in 1996, and the Ph.D. degree in computer science from the Department of Information Technology, Hazara University Mansehra, Pakistan. He was the Head of the Department of Information Technology and the Director of IT, Hazara University Mansehra, for 11 years, where he is currently the Chair of the Department of Telecommunication. He has recently completed a Research and Development Project sponsored by the Ministry of Science and Technology, Pakistan. He has established seven hi-tech research and development labs.

MOHAMED OTHMAN (Senior Member, IEEE) received the Ph.D. degree (Hons.) from the National University of Malaysia. He was the Deputy Director of the Information Development and Communication Center, where he was in charge of the UMPNet Network Campus, uSport Wireless Communication Project, and the UPM Datacenter. He is also an Associate Researcher and a Coordinator of the high-speed machine with the Laboratory of Computational Science and Mathematical Physics, Institute of Mathematical Research, Universiti Putra Malaysia (UPM). He is currently a Professor in computer science with the Department of Communication Technology and Network, UPM. He has published over 300 international journals and 330 proceeding papers. He has also filed six Malaysian, one Japanese, one South Korean, and three U.S. patents. His main research interests include computer networks, parallel and distributed computing, high-speed interconnection networks, network design and management (network security, wireless, and traffic monitoring), consensus in IoT, and mathematical model in scientific computing. He is a Life Member of the Malaysian National Computer Confederation and the Malaysian Mathematical Society. In 2017, he received an Honorable Professor from South Kazakhstan Pedagogical University, Shymkent, Kazakhstan, and also a Visiting Professor with South Kazakhstan State University, Shymkent, and L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. He was a recipient of the Best Ph.D. Thesis by Sime Darby Malaysia and the Malaysian Mathematical Science Society.

MAZHAR ALI received the M.S. degree from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 2009, and the Ph.D. degree from the Department of Electrical and Computer Engineering, North Dakota State University (NDSU), Fargo, ND, USA, in 2015. He is currently an Assistant Professor with the COMSATS University Islamabad, Abbottabad, Pakistan. His current research interests include cloud computing, information security, smart health, and data and social network analysis.

ARIF IQBAL UMAR received the M.Sc. degree in computer science from the University of Peshawar, Pakistan, and the Ph.D. degree in computer science from Beihang University (BUAA), Beijing, China. He has been working as an Associate Professor of computer science with the Department of Information Technology, Hazara University Mansehra. He has been leading the Department as the Chairperson. He has supervised seven Ph.D. candidates and 34 M.S. candidates. He is the author of more than 70 research publications in the leading research journals and conferences. He has at his credit 27 years' experience of teaching, research, planning, and academic management. His research interests include data mining, machine learning, information retrieval, digital image processing, computer networks security, and sensor networks.

ABDUL BASIR received the bachelor's degree (Hons.) in computer science from Hazara University Mansehra, Pakistan, in 2008, and the master's degree in computer science from Hazara University Mansehra, in 2015, with a specialization in information security, where he is currently pursuing the Ph.D. degree in computer science. He has served as a Visiting Lecturer for Hazara University Mansehra. Currently, he is serving as a SST for the Elementary and Secondary Education KPK, Pakistan. His research interests include wireless networks, the IoT, applied cryptography, and information security.