A comprehensive review of authentication schemes in vehicular ad-hoc network

Azam, Farooque; Yadav, Sunil Kumar; Priyadarshi, Neeraj; Padmanaban, Sanjeevikumar; Bansal, R. C.

Published in:
IEEE Access

DOI (link to publication from Publisher):
10.1109/ACCESS.2021.3060046

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 2, 2021, accepted February 8, 2021, date of publication February 18, 2021, date of current version March 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3060046

A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network

FAROOQUE AZAM[1,2], (Student Member, IEEE), SUNIL KUMAR YADAV[1], NEERAJ PRIYADARSHI[3], (Member, IEEE), SANJEEVIKUMAR PADMANABAN[3], (Senior Member, IEEE), AND R. C. BANSAL[4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Sangam University, Bhilwara 31100, India
[2]School of Computer Science and Engineering, REVA University, Bengaluru 560065, India
[3]Center for Bioenergy and Green Engineering, Department of Energy Technology, Aalborg University, 6700 Esbjerg, Denmark
[4]Department of Electrical Engineering, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Farooque Azam (farooque53786@gmail.com)

ABSTRACT Vehicular ad-hoc network (VANET) has been gaining importance due to the fast growing technology as well as its requirements in intelligent transportation systems (ITS) and vehicular social network (VSN). VANET facilitates vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication and improves the ride quality with value added services. The number of connected vehicles is expected to grow to a huge number with enormous exchange of safety and non-safety messages which are susceptible to security and privacy threat. To ensure secured communication, VANET must implement an authentication protocol to resist the attack and preserve the privacy. In this paper, a detailed discussion on the taxonomy for authentication schemes in VANET has been presented. The authentication schemes have been compared with security, privacy and scalability requirement. The use of recent technologies such as 5G, 5G-SDN, and Blockchain to design authentication schemes with low cost, and low communication, computational overhead has been discussed. Finally, the paper concludes with open challenges in VANET authentication. This paper is expected to open new avenues for researchers working in the domain of VANETs.

INDEX TERMS Blockchain, 5G, ITS, VANET, VSN.

I. INTRODUCTION

The emergence of huge number of connected vehicles and vehicular social network draws attention from both academia and industry. The connectivity of vehicles offers facilities on wheels such as comfort, convenience, entertainment, and infotainment [1]. As predicted, most of the useful time will be wasted in traffic, and road accidents will be fifth among the leading reason of deaths by 2030 [2]. Also, globally, value for connected vehicles as forecasted will reach to $225,160 million in 2027 as compared to $63,026 million in 2017 with growth of 17.1% annually between 2020-2027 as shown in Figure 1. Thus, a robust and powerful network is required which facilitates online communication in a secured way. Intelligent transportation systems play a pivotal role in managing road traffic; provide innovative and comprehensive services to control these undesirable events for connected vehicle in (VANET). Dedicated short range communication (DSRC) and wireless access in vehicular environment (WAVE) facilitate communication in VANET. Onboard unit (OBU), road side unit (RSU) and trusted authority (TA) are the main components of a VANET system [1]–[4].

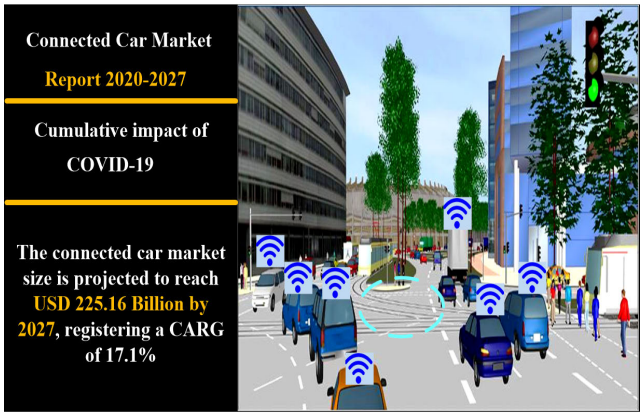

FIGURE 1. Growth of connected vehicle forecast 2020-2027 [3].

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

TABLE 1. Summary of some recent surveys on VANET.

Paper	Domain (s) Surveyed	Year
[5]	Authentication schemes for VANETs	2017
[6]	VANet security challenges and solutions	2017
[7]	Attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV	2017
[8]	Security attacks in VANETs: Communication, applications and challenges	2019
[9]	Recent Advances in Vehicular Network Security, Trust, and Privacy	2019
[10]	Authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)	2020
[11]	Certificate Revocation Schemes in Vehicular Networks	2020
[12]	Authentication and Privacy Schemes in VANET	2021
[13]	Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET	2020
[14]	Authentication Techniques in VANETs	2020

Though, VANET is gaining popularity, it suffers from several design and deployment challenges because of its dynamic nature (vehicle can join and leave at will).

When a vehicle say 'X' wants to communicate to a vehicle say 'Y' by sending a beacon, there must be a way to assure the legitimacy of X and Y as well the message through which they communicate. The former is known as entity authentication and the latter is known as message authentication. VANET must be secure enough to resist attacks and ensure goal of security services such as authentication, availability, confidentiality, integrity and non-repudiation. Privacy is also a major concern where vehicle's (driver) identity and location should only be known to authentic entity. Apart from security services, privacy preservation, conditional privacy, and scalability must be considered for the successful design and deployment of the VANET.

A. RELATED WORK

Several security and privacy solutions have been discussed in the various literature and researchers have made careful survey for the same. TABLE 1, consists of some recent surveys done in VANET which are briefly discussed as follows.

Manvi and Tangade [5] have discussed a survey on authentication scheme and made a comparative analysis based on the security attack, security requirement and computational and communication overhead. They have not compared the schemes based on conditional privacy, un- observability, location tracking and scalability. They have also not discussed recent technologies such as Blockchain, SDN, 5G, etc.

In [6], VANET characteristics, and challenges in VANET for efficient implementation have been discussed. Apart from this, the author discussed the well-known security architectures and standards, classification of attacks and its solution. However, the authors didn't discuss simulators and also didn't give a very clear picture of authentication schemes as given in [5].

In [7], overviews of threats and prevention mechanisms from existing literatures have been discussed. An OBU based solutions have been presented in which author claim that Sybil attack has been addressed by most of the researchers as compared to other types of attacks. They also discussed internet of vehicle (IOV) and claimed that most of the IoT devices will be in the vehicle and measures to improve various security challenges to be addressed. However, authors have not discussed the solution to IOV in comprehension.

In [8], authors have presented about the Intelligent Transportation Systems to VANET and discussed the security and privacy issues. They addressed the VANET and cloud computing effectiveness and solution to security and privacy concern. Finally, they discussed the applications and open issues in VANET.

In [9], authors have discussed VANET architecture, security classification and solutions. The author also discussed the trust in VANET, its challenges and mitigations. Also, various simulators were discussed.

Manivannan *et al.* [10] have presented the security, privacy and message dissemination in VANET. They reviewed ten years of work done (2009-2010) and presented open challenges in VANET.

In [11], Wang *et al.* have discussed existing certificate revocation scheme and classified these schemes based on its place of storage. They gave challenging issues and key techniques at each stage.

Al-Shareeda *et al.* [12] discussed the security and privacy issues and solutions based on the security and privacy requirement and also done comparison based on computational overhead and security threat. Finally, authors have provided open challenges in VANET.

In [13], an overview of VANET and SDN controller has been presented. They have explained the SDN layers and infrastructure. The author also discussed open issues and the requirement of robust routing protocol, latency, connectivity, and security challenges for future SDN-VANET architectures.

Farooq *et al.* [14] have discussed the VANET authentication schemes and its mitigation in several attacks. It discussed the advantages and disadvantages of various schemes and also provided research direction in the area of VANET authentication.

None of the above survey gave clear and comprehensive overview of VANET authentication and solutions to key distribution. Also, none have discussed about 5G technology and Blockchain application in VANET. This survey in complementary to above will provide lucid, easy to understand authentication, key distributions, etc. in VANET.

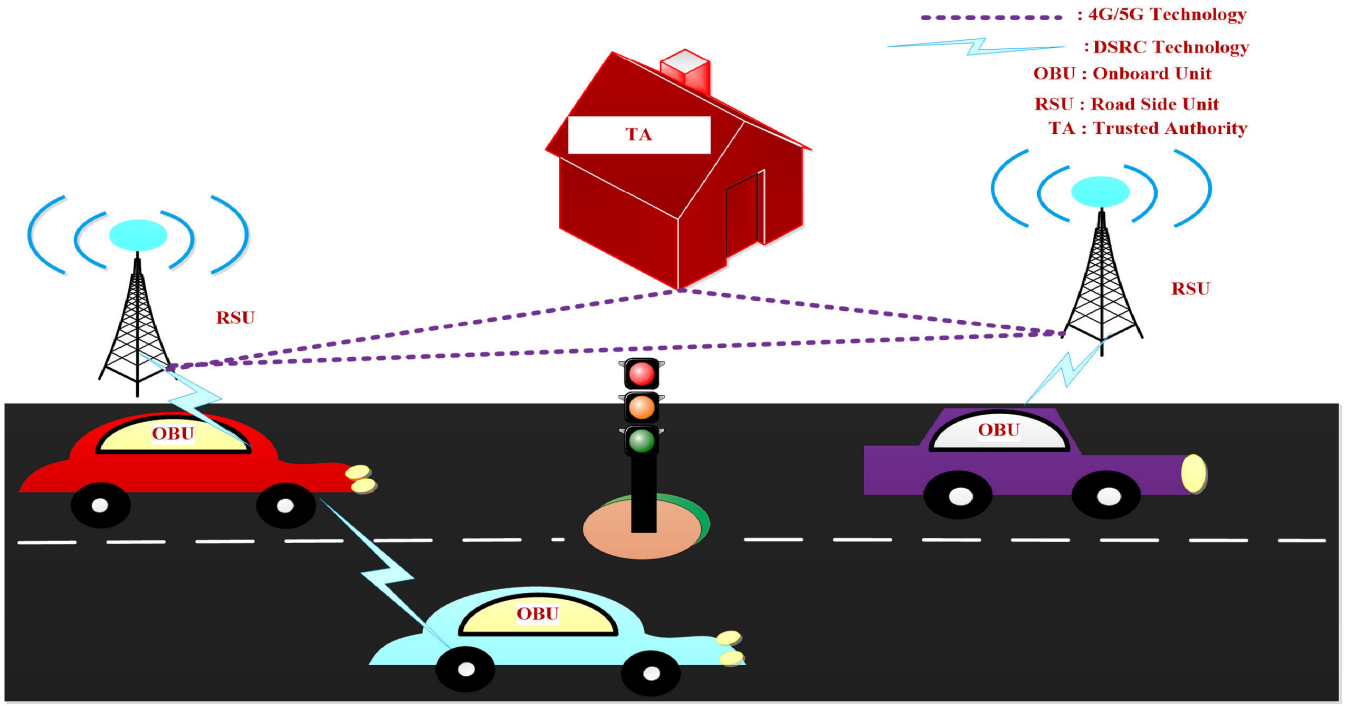

FIGURE 2. VANET System architecture.

B. OUR CONTRIBUTIONS

Our contributions to this survey are highlighted as:

1. A clear understanding of VANET, its requirements and challenges have been presented.
2. The basics of authentication in VANET and how a RSU provides the service has been presented.
3. Various authentication schemes have been discussed and compared in terms of its security, privacy, and scalability requirement.
4. Recent technologies such as Blockchain, 5G, SDN, etc. applications in VANET for authentication have been discussed.

This holistic survey is organized as follows: Section II elaborates an understanding of architecture, communication, characteristics, attack classification, attack and security requirements. Section III discusses the basics of authentication in VANET, meaning of certificate, and services provided by RSU. Section IV presents the taxonomy of authentication schemes in VANET. Security schemes in each category have been analyzed based on the security, privacy and scalability requirements. Section V discusses the recent advancements in the technology to address the key distribution, timely distribution of keys, certificate revocation list (CRL) and communication and computational overhead. Finally, conclusion and future directions have been presented in Section VI.

II. UNDERSTANDING THE VANET

A. VANET ARCHITECTURE

Figure 2 shows a typical VANET system consisting of vehicle, RSU, TA, etc.

Communication range in DSRC varies from 100 to 1000 meter while the data rate between 6 to 27Mbps. A safety related message is usually sent in every 100-300s. Vehicle communicates either to the other vehicle or RSU. RSU usually sends beacon messages at regular intervals.

The federal communications commission (FCC) has provided 75MHz band wide spectrum between 5.85-5.925GHz for DSRC. The different components of VANET are described as follows:

- *Onboard unit (OBU)*: Each vehicle is equipped with OBU which acts a transceiver to other vehicle's OBU or RSU.
- *Road side unit (RSU)*: RSU is deployed along the road/intersection/dedicated points. It has network device for DSRC as well as communication with the infrastructure/TA/CA. RSU does tasks such as a) It relays the messages to other OBUs and RSUs. b) It periodically runs the safety applications. c) It facilitates the internet connectivity to OBUs.
- *Trusted authority (TA)*: TA sometimes also called as certificate authority (CA) holds huge responsibility such as trust and security of entire VANET. It verifies the authenticity of a vehicle as well as the RSU to establish secure communication. It holds power to revoke the legitimacy of a vehicle or RSU if it misbehaves and become malicious. Thus it is desirable that the TA must have high computational capability and storage.

The WAVE model shown in Figure 3 is a layered architecture consisting of standards such as IEEE 802.11p, 1609.4, 1609.3, 1609.2, 1609.1.

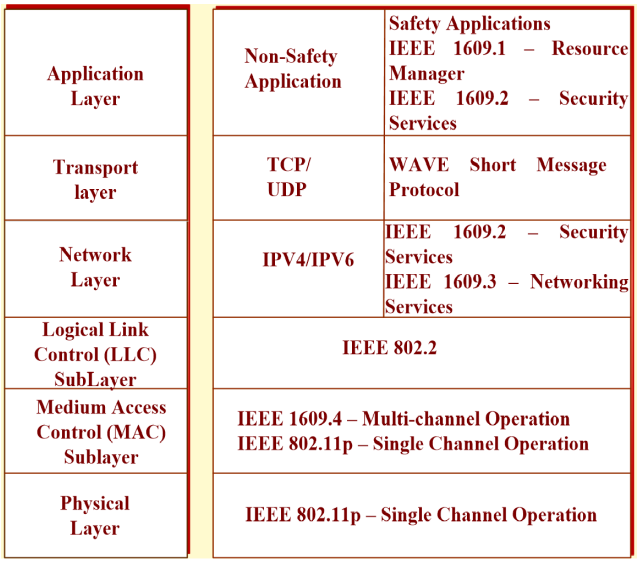

FIGURE 3. WAVE model with IEEE standards.

B. VANET CHARACTERISTICS

Following characteristics of the VANET are noteworthy in the understanding and designing the authentication schemes.

- *Mobility:* Since nodes (vehicles) are moving at high speed, so a small delay in V2V communications leads to a catastrophe.
- *Dynamic network topology*: It is difficult to find the malicious vehicle moving with high speed due to dynamic network topology.
- *Real-time constraints*: Transmission in VANET follows time constraints and the vehicles need to respond or take decision with the given time limit.
- *Computation and storage*: It is usual to process large volume of data of vehicle and infrastructure. Hence, storage and computation are challenging issues in VANET.
- *Volatility*: Vehicle can join or leave VANET at will. So, a vehicle which has joined the VANET may not join later. Hence, it poses security challenges in VANET.

C. ATTACKERS CLASSIFICATION, SECURITY ATTACKS AND REQUIREMENTS

VANET is susceptible to security attacks and hence it is important to identify the attack and mitigate so that attacker cannot alter the safety message. An attacker can be classified based on their behavior and scope of damage they can do in VANET [15]. The description of attacker classification is as follows:

- *Active attacker*: These attackers generate bogus message as well as stop forwarding the received message.
- *Passive attacker*: These attackers only eavesdrop on the wireless channel collecting traffic information and forward it to other attackers.
- *Inside attacker*: These attackers possess complete knowledge of the network configuration and hence are very dangerous compared to other attackers.
- *Outsider Attacker*: These attackers being not authenticated are less dangerous than the insider attackers.
- *Malicious Attacker*: These attackers have the main goal of harming other nodes without any personal benefit. They can severely damage the network.
- *Rational Attacker*: These attackers harm the network for their personal benefit and can be easily tracked.
- *Local Attackers*: These attackers can perpetrate only to limited area.
- *Extended Attackers*: These attackers have higher range and can attack across the network.

Researchers have identified various attacks in VANET which are explained as follows:

- *Impersonation attack:* In this the vehicle uses the identity (ID) of other vehicle and shows to be trustworthy.
- *Modification attack:* Here the attacker modifies the message to put false information
- *Replay attack:* In this, the attacker creates a dilemma to vehicles in VANET in case of emergency situation by continuously injecting old beacons and messages.
- *Bogus information attack:* Here, the attacker puts false and incorrect information in the broadcasted message.
- *Sybil attack:* A Sybil is any vehicle which forges the identity of other vehicle to abrupt the normal functioning of the VANET.
- *ID disclosure attack:* When a vehicle is able to steal or get the ID details of another vehicle.
- *Location tracking:* In location tracking, an attacker tries to locate the vehicle, i.e. they track the location.
- *Denial of service (DoS):* This attack happens when an insider or outsider jams the communication channel or overrides the VANET resources.

For secured communication, the requirements such as node authentication, message authentication, privacy preservation, non-repudiation, low communication and computational overhead, traceability and un-linkability must be satisfied by the authentication schemes in VANET.

III. BASICS OF AUTHENTICATION IN VANET

Authentication in VANET is done at node level as well as message level. At node level, vehicles and RSUs are usually authenticated which verify its legitimacy in the network. At message level, message is authenticated to guarantee the integrity of the message.

Vehicle owner physically provides the details such as electronic license plate (ELP) provides unique ID and processes cryptography operation which is installed on every new vehicle consisting of driver identity, and home address etc. to the CA/TA as a part of the registration. The registration with the CA/TA is mandatory initial step to provide services to the legitimate users.

FIGURE 4. V2V message format.

Each vehicle gets the private, public key pairs and certificate with unique identity from the CA/TA. The process involves key generation that utilizes digital signature algorithms normally.

The certificate issued to a vehicle is a public key certificate which is used in combination of the private key for V2V and V2I communication. To send a safety message, each vehicle uses its private key and attaches its certificate issued by the Certificate Authority as shown below by eq. (1) [15]:

$$S_V \rightarrow \#: S_m, Sig_{\Pr KV}[S_m \mid T_S], CertS_V \quad (1)$$

where,

S_V = Sending vehicle

$\#$ = Number of message receivers

S_m = sending message

$Sig_{\Pr KV}$ = signature of sending vehicle using private key$^{\Pr KV}$

$\mid$ = used for concatenation operation

T_S = Timestamp

$CertS_V$ = Public key Certificate of sending vehicle issued by CA

While at the receiver side, the certificate $CertS_V$ of the sending vehicle S_V must include the values as shown in eq. (2):

$$CertS_V = PubKS_V \mid Sig_{\Pr KCA}[PubKS_V \mid ID_{CA}] \quad (2)$$

where,

$PubKS_V$ = Public key of sending vehicle $^{\Pr KCA}$

$Sig_{\Pr KCA}$ = CA's signature with its private key

ID_{CA} = CA's ID

In V2V communication:

- A vehicle initiates the entity (other vehicle) and messages authentication on the reception of a safety message.
- The recipient vehicle performs the authentication of received message.
- It checks the certificate revocation list (CRL) for the revocation status.
- If the sending vehicle is there in the revocation list, then the message is dropped else recipient vehicle verifies the certificate and digital signature of sender's vehicle on the received message.

CRL is maintained by the Certificate Authority/Trusted Authority for recording the certificates of malicious vehicle. Researchers specify different message format for communication. Figure 4 shows a typical message format in V2V scenario.

- *Group ID*: Identify a vehicle associated with a particular group.

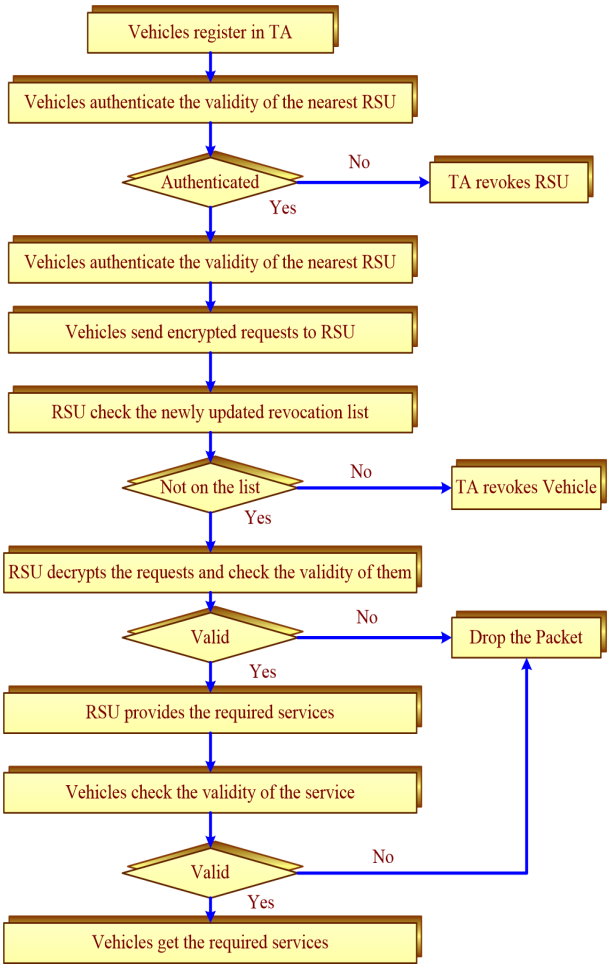

FIGURE 5. Process for acquiring the services through the RSU.

- Payload: Consists of traffic-related messages to help the driver to respond in case of emergency.
- Timestamp: Replay attack can be prevented by using timestamp.
- Signature: To validate the integrity of the message.
- Valid time: The time the message would last, i.e. lifetime in VANET.

In V2I communication, a vehicle requests to the nearest RSU when they require services such as nearest restaurant information, internet services, etc. In several research works, RSU authenticates the vehicle. Authors [16], [17] have mentioned the vehicle authentication by the RSU before the vehicle broadcasts the message. Also the vehicle checks the authenticity of the RSU in case it is fake or compromised. Figure 5 presents the process of services being provided by the RSU to a requesting vehicle. TA/CA revokes the malicious vehicle/RSU.

IV. TAXONOMY OF AUTHENTICATION SCHEMES

Among all security requirements, authentication is of prime importance. It is the first line of defense which guarantees that the message has been received from an authentic sender

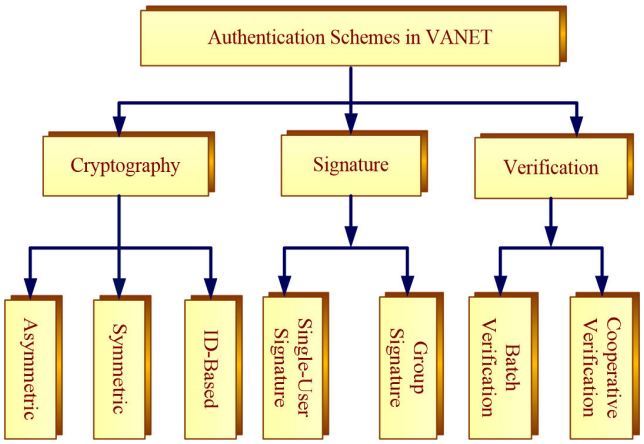

FIGURE 6. Authentication schemes in VANET.

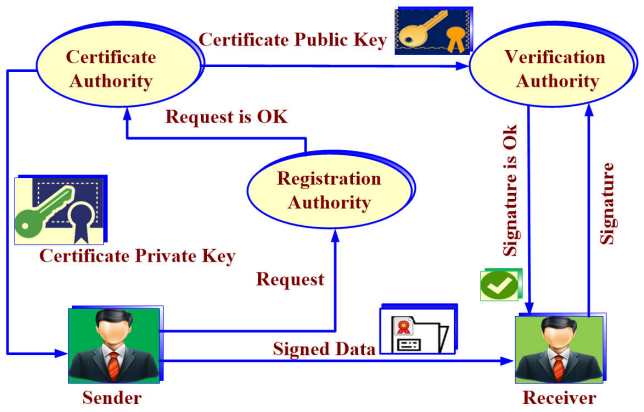

FIGURE 7. Working of PKI based system.

and hence checks masquerading attack. Figure 6 shows the taxonomy of authentication schemes.

A. AUTHENTICATION SCHEMES BASED ON CRYPTOGRAPHY

Authentication involving asymmetric (first key is used for encryption and the second key is used for decryption), symmetric (single key is used both for encryption and decryption) and ID-based (similar to asymmetric schemes except the user identity information is used to generate the public key) are broadly comes under the authentication schemes based on cryptography.

Public key infrastructure (PKI) is a framework which binds public keys with respect to identities of the User. The binding is done through registration and issuance of certificate by the certificate authority (CA). The registration is done by registration authority (RA) which ensures the authentication of requesting entity. The private key also called as secret key is used for signing and public key is used for verification. Figure 7 shows the working of PKI based system.

ECDSA uses elliptical curve cryptography along with the variant of a digital signature algorithm. It is used to encrypt the message and only the authentic user can access the information and hence provide more security. Different digital signature algorithms are available.

PKI and ECDSA are examples of asymmetric cryptography schemes. Though authentication is one of indispensible requirement for secured communication in VANET, privacy preservation is another important requirement which cannot be neglected. Privacy is the ability of a person to selectively reveal to special people/organization. During authentication, the identity, address of the owner, vehicle location, etc. used to generate the certificate, should not be revealed to any other person/vehicle except the competent authority such as CA/TA which is private to a user. Hence, authentication scheme must ensure privacy preservation. Thus, the requirement for privacy-preservation such as location tracking, un-linkability, un-observability must be safeguarded.

Anonymity is a situation where real identity is not known or spoken by anyone. Authentication schemes involving PKI preloads large anonymous certificates roughly forty-three thousand eight hundred (43,800) and respective private keys. Raya *et al.* [15] proposed anonymous authentication where in spite of using a single public key, anonymous public keys were used to preserve the privacy. With this, the recipient does not identify the owner of the keys. Due to the high revocation of malicious node, the list grows.

In [18], [19], authors have pointed out the requirements of large storage space as well as delay in checking the revocation list and timely distribution of CRL as a challenging issue in VANET.

Calandriello *et al.* [20] have proposed pseudonymous on the fly pseudonym generation using baseline pseudonym and self-certification in combination of group signature to overcome the storage and delay criteria as mentioned in [15].

Conditional privacy is a situation in which the identity is anonymous as long as it is not a malicious node. Rajput *et al.* [21] proposed a mechanism to achieve conditional privacy. In this, a vehicle was provided with two levels of pseudonyms such as (i) base pseudonym and (ii) short time pseudonyms.

Digital signature is a way to enhance the security in VANET, thereby ensuring the authenticity, integrity, non-repudiation of the message. ECDSA schemes are recommended by IEEE 1609.2 to verify the messages [22]. Authentication schemes based on ECDSA yield less computation overhead in contrast to Rivest–Shamir–Adleman (RSA) employed authentication schemes. Researchers [23]–[25] have discussed ECDSA.

Symmetric key cryptography also known as private key cryptography, where single key called as secret key is used for both encryption and decryption. Since same secret key is exchanged between the sender and the receiver, it is faster in execution and simpler in design than asymmetric cryptography schemes.

Xi *et al.* [26] have used the concept of symmetric random key set approach to provide the less overhead of the onboard unit (OBU) and ensure privacy. However, symmetric cryptography schemes do not guarantee non-repudiation since

same secret key is used by the sender as well as receiver for authentication process.

Authentication scheme such as (i) Message Authentication Code (MAC), (ii) Timed Efficient Stream Loss-tolerant Authentication (TESLA) and (iii) Hash function fall under symmetric key cryptography.

The MAC algorithm takes secret key and message as input and generates a tag and appends it before sending. At the receivers' end, same secret key is used to calculate the tag. A message is authenticated only when the two tags are same. MAC algorithm guarantees message integrity and authenticity.

Lin *et al.* [27] proposed timed efficient and secure vehicular communications (TSVC) scheme where they used short MAC tag appended to each packet for the packet authentication. Simulation results demonstrated that TSVC performs well in terms of packet loss ratio compared to existing PKI based schemes when there is a heavy traffic.

In [28], author proposed a conditional privacy preservation schemes based on message authentication code. In this, a vehicle can get its group key using verifiable secret sharing for message generation and authentication. It satisfies the basic security and privacy requirements as well as incur less computational and communication overhead.

The hash function is employed to test the message integrity. The hash function generates the hash value or the messages digest for a given message as an input which is appended to the message before sending to ensure message integrity. If the attacker modifies the message in transition, then it will generate a different hash value for the altered message and hence the message will be dropped by the receiver.

In [29], authors have proposed authentication scheme based on the Chinese remainder theorem (CRT) to ensure conditional privacy preserving. They have eliminated the storage of master key into the tamper proof device (TPD) to reduce the computational overhead. The scheme does not use bilinear pairing and operation such as map to point during authentication process and hence achieves faster signature verification even the number of signature grows high. The scheme is able to resist common attack and achieve better performance with less communication and computational overhead.

In [30], authors have employed a decentralized lightweight authentication scheme named as Trust Extended Authentication Mechanism (TEAM) for V2V communication. They have used hash chain for calculating the secure secret key set. It satisfies anonymity and other security requirements.

The TESLA uses precise MAC and also employs hash chain. TESLA allows the recipients to check the integrity and authenticity of source for each packet in multicast or broadcast data streams [31].

Bao *et al.* [32] proposed lightweight authentication based on TESLA and Bloom Filters to prevent active attacks and ensure a privacy-preserving.

Identity based cryptography (IBC) uses its identity information such as email to generate the public key. It does not use certificate to authenticate the message, hence the message overhead is reduced and low. Also, it improves the VANET communication due to non-maintenance and management of CRL.

In [33], authors have proposed a decentralized privacy preservation scheme using asymmetric identity and hash based message authentication code (HMAC). Simulation result shows that the given scheme is lightweight, robust and is able to resist common attack. However, the scheme does not ensure conditional privacy, location tracking and unobservability.

In [34], authors have discussed a privacy preservation authentication scheme. The scheme includes four phases and uses a single hash function, secret key and pseudo-identity. Proverif tool has been used to verify that the scheme satisfies the security and privacy requirements. The scheme is lightweight, robust and incurs less computational and communication overhead as it uses only hash and exclusive-OR operation and authors discussed the improvement of work in scenario of 5G and edge computing applications in VANET.

Azees *et al.* [35] used anonymous authentication to avoid entry of malicious vehicle into the VANET and employ conditional privacy tracking mechanism to revoke the vehicle in case of any misbehavior. They used bilinear pairing technique. Anonymous authentication is achieved through five dedicated phases, i.e. (i) registration and key generation, (ii) anonymous certificate generation, (iii) signature generation, (iv) verification, and (v) conditional tracking. The performance analysis has been carried out in terms of computational cost of the certificate, RSU serving capability, and signature verification process. It provides minimum certificate and signature verification cost with location tracking. The scheme is able to resist the common attack and ensure privacy preservation.

B. AUTHENTICATION SCHEMES BASED ON SIGNATURE

Cryptography schemes such asymmetric, symmetric and ID based use single user signature for authentication which pose the issues such as key management, frequent change of public/private key pair and computation/communication overhead. Researchers have proposed authentications schemes using Group signature. Authentication based on Group signature resembles the similarity of public and private key pair with one change. Anonymous authentication is provided to preserve the privacy [36] which is a property of Group signature. Here, any member in the group can use its private key to sign the safety message. The recipient at the receiving end confirms the sender by verifying the signature using group public key and it only reveals the identity of the group manager.

Vijayakumar *et al.* [37] have used a dual authentication scheme based on group communication in VANET. The scheme depends on the vehicle secret key and finger print of individual user.

Here, CRT based key management is used to minimize the computation. Also, the information to update the group key

TABLE 2. Comparison of schemes based on the security requirement.

Requirement	Paper																		
	[15]	[20]	[21]	[24]	[26]	[27]	[28]	[29]	[30]	[32]	[33]	[34]	[35]	[37]	[38]	[40]	[41]	[42]	[43]
Entity authentication	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
Message authentication	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
Traceability	×	×	×	×	×	×	×	√	√	×	√	√	√	√	√	×	√	√	√
Non-repudiation	×	×	×	√	×	×	×	√	×	×	√	√	√	√	√	√	√	√	√
Sybil attack	×	×	×	×	×	×	×	√	×	×	√	√	√	√	√	×	×	√	√
Modification attack	×	×	×	×	×	×	×	√	√	×	√	√	√	√	√	√	√	√	√
DoS	×	×	×	×	×	×	×	×	√	√	√	√	√	√	√	√	√	√	√
Impersonation attack	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	×	√	√	√
ID-disclosure	√	√	√	×	×	×	×	√	√	×	√	√	√	√	√	√	√	√	√
Replay attack	×	√	√	×	×	×	×	√	√	×	√	√	√	√	√	√	√	√	√
Location Tracking	×	×	×	×	×	×	×	√	√	×	×	√	√	×	√	×	√	×	√

TABLE 3. Comparison of schemes based on the privacy, conditional privacy and overhead.

Requirement	Paper																		
	[15]	[20]	[21]	[24]	[26]	[27]	[28]	[29]	[30]	[32]	[33]	[34]	[35]	[37]	[38]	[40]	[41]	[42]	[43]
Privacy	√	√	√	×	×	√	√	√	√	×	√	√	√	√	√	√	√	√	√
Low Communication	×	×	×	×	×	×	√	√	×	×	√	√	√	√	×	×	×	×	×
Low Computational	×	√	×	√	√	√	√	√	×	×	√	√	√	√	×	×	×	√	√
Un-linkability	×	×	×	×	×	×	×	√	√	×	√	√	√	√	√	×	√	√	×
Un-observability	×	×	×	×	×	×	×	√	×	×	×	×	√	×	√	×	√	√	×
Conditional Privacy	×	×	√	×	×	×	√	√	×	×	×	×	×	×	√	×	√	×	×
Scalability	×	×	×	×	×	×	×	√	×	×	√	√	×	√	√	√	√	√	√

in case of group membership is also minimized. The scheme incurs less computational and communication overhead and is able to resist common attack but fails to resist location tracking, conditional privacy.

In [38], authors have employed regional trust authority in its anonymous authentication scheme (AAAS) in VANETs. They have used Group signature to satisfy the anonymity and conditional privacy.

Islam *et al.* [39] have employed Password based and Group key generation protocol to achieve conditional privacy. The protocol does not employ bilinear pairing and elliptical curve, hence incur less computational overhead.

C. AUTHENTICATION SCHEMES BASED ON VERIFICATION

In VANET communication, a vehicle can transmit safety messages and it must be verified within 300ms by the RSU/other vehicles in the range. At areas with dense traffic, the number of messages grows and starts accumulating for verification. If the messages do not get verified within the time limit, it will be either invalidated or discarded. Also, it may lead to accident or any grievous situation. In order to tackle the timely verification of messages with less delay and less communication and computational overhead, verification of messages can be done either batch wise or cooperative way. The class of authentication algorithm designed can be (i) Authentication scheme based on batch verification and (ii) Authentication scheme based on cooperative verification.

Wu *et al.* [40] have proposed a batch assisted verification scheme to verify the message faster with reduced delay. In this scheme, they have taken some terminals and RSU to jointly carry the task of message verification. Also, the scheme scales ten times more as compared to the schemes where RSU is the only verifier for message verification.

In [41], authors have proposed an identity based batch verification scheme to ensure security and conditional privacy. The scheme performs well as compared to schemes using bilinear pairing technique.

In VANET, each vehicle verifies the safety messages as soon as it receives it and in traditional system it is a redundant process which incurs delays in verification process when number of messages grows to a huge number. One solution is to use, cooperative message authentication.

Lin and Li [42] have proposed an efficient cooperative message authentication (ECMA) scheme to reduce the redundant authentication process on the same message by each vehicle in the range. Free riding attacks are used by selfish vehicle. To avoid free riding attack, the scheme introduces an evidence token to find out the contribution of the vehicle

authentication process without the involvement of the TA. A vehicle obtains an evidence token as soon as it passes by the RSU which reflects its contribution in the past.

In [43], authors have employed a reliable cooperative authentication scheme. In this, they have used success report to avoid synchronization problem between cooperative and non-cooperative vehicles. The simulation results show that there is no message loss even when there are 200 vehicles per km.

The comparison of schemes discussed in Section IV (A, B, and C) based on the (i) security requirement, (ii) privacy requirement and scalability are listed in TABLES II and III.

V. RECENT ADVANCEMENTS IN VANET AUTHENTICATION

A. 5G NETWORK AND 5G-SDN FOR VANET

5G technology with its improved data rate, latency, and coverage in contrast to 4G is going to boost the VANET experience [44]. Karagiannis *et al.* [45] have found poor scalability and low capacities in their studies to IEEE 802.11p which have been extensively used for VANET communication. Taking note of its deficiencies, Araniti *et al.* [46] have discussed the strength and weakness of Long-Term Evolution (LTE) as a promising technology for VANET communication. However, the LTE standard fails to meet the delay requirements of vehicular communication and network performance is down because of high interference as pointed by Ge *et al.* [47].

Inclusion of technologies such as millimeter waves, visible light communication, and massive multiple-input-multiple-output (MIMO), 5G can scale to 10 to 100 times connected vehicles and user data rate [48].

Lai *et al.* [49] have reviewed security and privacy in 5G enabled VANET. They have discussed the architecture of a 5G enabled VANET comprising of three layers viz. (i) vehicle stratum, (ii) network stratum and (iii) application stratum as shown in Figure. 8. DSRC, millimeter-wave (mmWave), LTE-V-Direct may be used by vehicles in vehicle stratum for communication. Vehicle can access the 3GPP core network through base station or RSU. 3GPP core network, trusted third party (TTP), service provider and cloud are the main components of network stratum. Vehicles can use the cloud via the 3GPP core network. Network function virtualization (NFV) consists of (i) data function (DF), (ii) control and management function (CMF), (iii) security and privacy function (SPF). Access, mobility management, police control, session management, authentication, channel establishment, etc. are some of the functions of CMF. DF just contributes to packet forwarding while security and privacy services are taken care by SPF.

TTP consists of CA and trusted identity manager (TIM). (i) vehicle to infrastructure (V2I), (ii) vehicle to network (V2N), (iii) vehicle to vehicle (V2V) and (iv) vehicle to pedestrian (V2P) are four v2X communication supported by 3GPP. They have discussed essential security requirements such as confidentiality, integrity, authenticity and replay attack with available solution and privacy issues. Security and privacy in autonomous platoon has been discussed as a case study. Open research challenges such as inclusion of Internet Protocol Version 6 (IPv6) in 5G technology, resource utilization, etc. have been discussed.

Ouaissa *et al.* [50] have proposed an authentication and key agreement protocol over 5G network. They have used Elliptic Curve Diffie-Hellman (ECDH) and MAC. They have analyzed their protocol on automated validation of internet security protocols and applications (AVISPA) and found to have less computational overhead as well able to resist the attack such as message modification, Man in middle attack, replay attack, DoS attack and also fulfill the security requirement. However, the scheme does not guarantee privacy requirement.

Zhang *et al.* [51] have proposed an authentication scheme by employing 5G technology and edge computing. At first an edge computing vehicle is authenticated and selected using fuzzy logic rule. Secondly, the edge computing vehicle and ordinary vehicle undergoes mutual authentication. The scheme is fast, incurs low computational overhead and is able to resist common attack and ensure privacy preservation.

Quan *et al.* [52] have proposed software defined vehicular networks with collaborative crowd sensing using smart identifier networking (SINET-V). Experimental response shows that SINET-V satisfies the quality of service requirements in realistic urban vehicular scenario.

Huang *et al.* [53] have proposed crowd sensing via Deep Reinforcement Learning to enhance the privacy preservation. With rise of internet of things (IoT), crowd sensing is of huge importance. In this, incentive is provided for the participants ensuring resistance to privacy leakage. Extensive simulation has been carried out to prove its effectiveness in ensuring privacy preservation.

Zhang *et al.* [54] have proposed 5G-SDN based privacy-preservation authentication scheme. Software defined network (SDN) when used with 5G enhances the performance. In this scheme, they have used elliptical curve cryptography and registration list (RL) for securing the VANET. In this scheme, they have obtained conditional privacy and thousand messages can be authenticated within short time period. The scheme is able to resist the attack, ensure conditional privacy and scalability requirement.

Nakamoto [55] have proposed drone assisted anonymous authentication for rural and mountainous areas where signal is poor with lot of interference using 5G technology. In this, DSRC interact and communicate with drone for vehicle in areas having bad signal strength. The drone communicates to the control center through 5G technology. This way, the scheme is able to a cover a wide area and uses hybrid cryptography schemes to resist various attacks and ensure privacy. Also, the scheme incurs less computational and communication overhead as per the simulation results.

B. BLOCKCHAIN FOR VANET

PKI based system rely on TA/CA and certificate which leads to cumbersome certificate management while ID-based scheme relies on key generation which suffers from key

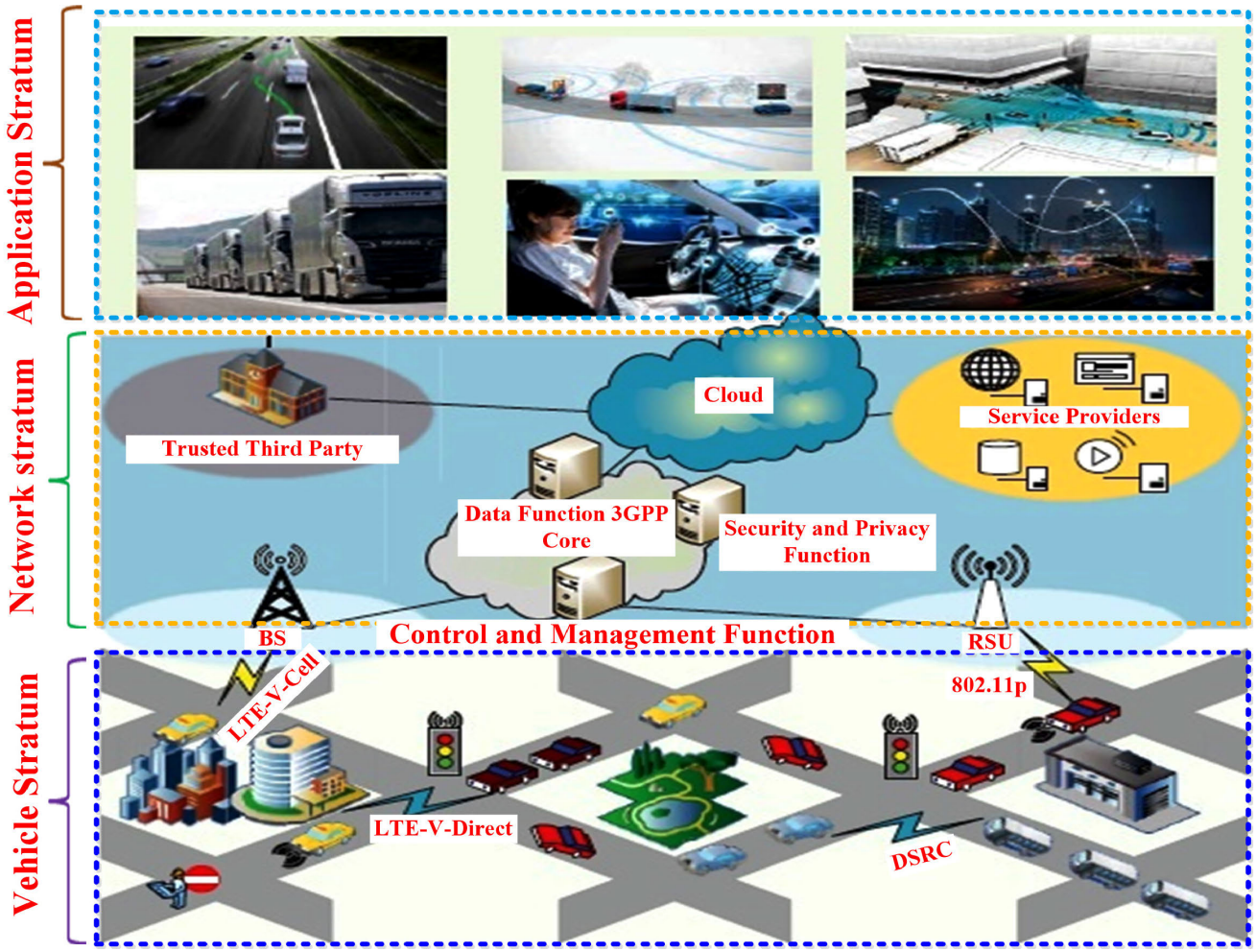

FIGURE 8. Architecture of 5G enabled VANET [49].

escrow problem. Though, a hybrid scheme can overcome the issue but it may not be scalable enough. Also, key management and certificate storage becomes a major issue when CRL grows. In case of electric vehicle (EV) charging, vehicles have to rush to charging station at regular interval because of limitation of km per charge which raises privacy issues for the user. Currently, vehicular social networks (VSN) take lead in the establishment of vehicular based services. Thus user data and privacy taking care as VSN is going to generate voluminous data. To mitigate all the above mentioned issues, Blockchain first proposed by Nakamoto [55] can be exploited because of its attractive features such as (i) Decentralization (ii) Tamper-proof (iii) Trustworthiness, and (iv) Anonymity. Figure 9 shows the basic architecture of a Blockchain. In this, each block consists of two hash values such as current and previous to build the chain. Block 2 consists of hash value of Block 1 (a previous block) and Block 3 consists of hash value of Block 2 a previous block) and so on.

- *Decentralization:* A Blockchain is not governed by a single authority rather a group of peer maintains the network, making it decentralized in nature.

FIGURE 9. Blockchain architecture.

- *Tamper-proof:* Every created block has hash value of previous block and if anyone wants to tamper the data of a particular block then the hash value will change which makes Blockchain as tamper-proof.
- *Trustworthiness:* Each transaction in a block consists of many transactions and is recorded as hash value. As it is tamper-proof, no intruder can add or change the block which attracts the trustworthiness of the user.
- *Anonymity:* Since the content is in hash value and not the exact content, hence displays anonymity.

Ma *et al.* [56], have proposed a decentralized key management protocol for VANET using Blockchain technology to automatically register, update and revoke the user's public

key. They have proposed mutual authentication and key agreement by employing bivariate polynomial. The scheme is able to mitigate the DoS, internal attack, public key tampering attack and collusion attack. At the same time the protocol performs well with less storage, computational and communicational overhead. The scheme removes the dependencies on TA as in case of PKI system and at the same time ensures the anonymity which is required for privacy preservation.

Lu *et al.* [57] have proposed an authentication schemes for privacy preservation in VANET. Merkel Patricia tree (MPT) has been used to provide distributed authentication schemes free from revocation list. Vehicles were allowed to use multiple certificates to achieve conditional. The performance of each entity has been tested on Hyperledger Fabric (HLF) platform. The simulation results demonstrate that the scheme meet the real time constraint as each vehicle is able to authenticate below 1ms. Also, storage and processing time has been considerably reduced as compared to the previously implemented schemes.

Lin *et al.* [58] have proposed an effective certificate management scheme. In this scheme, PKI based Elliptical Curve Digital Signature Algorithm (ECDSA) based on a public Blockchain (Ethereum) have been used for secured communication. This way, participating vehicle need not to store private keys which further reduces verification time and cost. The scheme has been tested on Rinkeby (Etherum test Network) and simulation has been carried out on NS-2 and VanetMobiSim for its effectiveness. The scheme is able to meet security and conditional privacy requirement for the deployment of the VANET.

In [59], authors have proposed Blockchain based secure payment scheme in VANET taking two scenarios (i) park toll management system and (ii) electronic toll collection. The payment scheme viz. (i) V-R transaction and (ii) V-Rs transaction are effective and robust. In this only RSU takes part in the consensus and all transaction run in the smart contract automatically. Also, it is able to mitigate security and privacy requirement.

Liu *et al.* [60] have used Consortium Blockchain based unlinkability authentication scheme. In this scheme, the service manager (SM) is dispersed to constitute a distributed database for data sharing. Each vehicle generates different pseudonyms and initiate authentication. SM uses local data to verify the authenticity of the vehicle. This scheme is able to ensure stronger anonymity and unlinkability but fails to resist collusion attack between SMs and linkability by cooperating SMs.

Liu *et al.* [61] have presented a software defined vehicular networks with collaborative crowd sensing using smart identifier networking (SINET-V). Experimental response shows that SINET-V is able to provide the quality of service in realistic urban vehicular scenario.

VI. CONCLUSION

In this comprehensive review, a clear understanding of VANET architecture and challenges in the deployment has been presented. Then, a basic idea of authentication is elaborated in terms of message exchanged between V2V and service provided by RSU. Further, a detailed discussion and comparison on the taxonomy of authentication schemes from recent work based on security, privacy, scalability, low communication and computational overhead has been presented. The authors have found the gap, such as reliance on TA/CA, maintaining a CRL, privacy of a EV in case of visiting charging station frequently because of per charge limitation, wide coverage where signals are weak, emergence of VCN and huge data generation etc. To mitigate the above issues, an overview of 5G, 5G-SDN and Blockcahin application for VANET authentication and privacy mitigation have been presented. Furthermore, researchers are motivated to use hybrid schemes such as SDN-Blockchain along with traditional cryptography schemes to build a robust and scalable scheme for the successful deployment of the VANET. Trust is another important research domain in VANET which needs critical attention.

REFERENCES

[1] S. Olariu, "A survey of vehicular cloud research: Trends, applications and challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2648–2663, Jun. 2020, doi: 10.1109/TITS.2019.2959743.

[2] *Global Status Report on Road Safety 2015*, World Health Organization, Geneva, Switzerland, 2015.

[3] A. Singh and L. Katare, *Connected Car Market by Technology (3G, 4G/LTE, and 5G), Connectivity Solution (Integrated, Embedded, and Tethered), Service (Driver Assistance, Safety, Entertainment, Well-Being, Vehicle Management, and Mobility Management), and End Use (Original Equipment Manufacturer (OEMs) and Aftermarket): Global Opportunity Analysis and Industry Forecast, 2020-2027*, 2020. [Online]. Available: https://www.alliedmarketresearch.com/connected-car-market

[4] F. Azam, N. Priyadarshi, H. Nagar, S. Kumar, and A. K. Bhoi, "An overview of solar-powered electric vehicle charging in vehicular ad hoc network," in *Electric Vehicles. Green Energy and Tech*. Singapore: Springer, 2020, doi: 10.1007/978-981-15-9251-5_5.

[5] 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, doi: 10.1016/j.vehcom.2017.02.001.

[6] 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, doi: 10.1016/j.vehcom.2017.01.002.

[7] 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, doi: 10.1016/j.adhoc.2017.03.006.

[8] M. Arif, G. Wang, M. Z. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANets: Communications, applications and challenges," *Veh. Commun.*, vol. 19, pp. 1–36, Sep. 2019, doi: 10.1016/j.vehcom.2019.100179.

[9] 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. 2019, doi: 10.1109/TITS.2018.2818888.

[10] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs)," *Veh. Commun.*, vol. 25, pp. 1–18, Oct. 2020, doi: 10.1016/j.vehcom.2020.100247.

[11] Q. Wang, D. Gao, and D. Chen, "Certificate revocation schemes in vehicular networks: A survey," *IEEE Access*, vol. 8, pp. 26223–26234, 2020, doi: 10.1109/ACCESS.2020.2970460.

[12] 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. 2021, doi: 10.1109/JSEN.2020.3021731.

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

[14] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Survey of authentication techniques in vehicular ad-hoc networks (VANETs)," *IEEE Intell. Transp. Syst. Mag.*, early access, May 12, 2020, doi: 10.1109/MITS.2020.2985024.
[15] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw. SASN*, 2005, pp. 11–21.
[16] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.
[17] K.-A. Shim, "$\mathcal{CPAS}$: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.
[18] M. Nowatkowski and H. Owen, "Certificate revocation list distribution in VANETs using most pieces broadcast," in *Proc. IEEE SoutheastCon*, Concord, NC, USA, Mar. 2010, pp. 238–241.
[19] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 595–604, Mar. 2011.
[20] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw. - VANET*, 2007, pp. 19–28.
[21] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for VANET," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 643–650.
[22] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages*, Standard 1609.2-2006, Jun. 2006.
[23] F. Qu, Z. Wu, F. 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, doi: 10.1109/TITS.2015.2439292.
[24] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message authentication in vehicular ad hoc networks: ECDSA based approach," in *Proc. Int. Conf. Future Comput. Commun.*, Apr. 2009, pp. 16–20, doi: 10.1109/ICFCC.2009.120.
[25] K. Ravi and S. A. Kulkarni, "A secure message authentication scheme for VANET using ECDSA," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–6, doi: 10.1109/ICCCNT.2013.6726769.
[26] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. 8th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2007, pp. 344–351.
[27] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008, doi: 10.1109/T-WC.2008.070773.
[28] X. Li, Y. Liu, and X. Yin, "An anonymous conditional privacy-preserving authentication scheme for VANETs," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun.; IEEE 17th Int. Conf. Smart City; IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Aug. 2019, pp. 1763–1770, doi: 10.1109/HPCC/SmartCity/DSS.2019.00242.
[29] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Depend. Sec. Comput.*, early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.
[30] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014, doi: 10.1109/JSYST.2012.2231792.
[31] *Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*. Accessed: Nov. 17, 2020. [Online]. Available: https://tools.ietf.org/html/rfc4082
[32] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom filters," *ICT Exp.*, vol. 4, no. 4, pp. 221–227, Dec. 2018, doi: 10.1016/j.icte.2017.12.001
[33] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8647–8655, Sep. 2018, doi: 10.1109/TVT.2018.2839979.
[34] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020, doi: 10.1109/JSYST.2020.2991168.
[35] 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, doi: 10.1109/TITS.2016.2634623.
[36] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108, doi: 10.1109/MOVE.2007.4300813.
[37] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016, doi: 10.1109/TITS.2015.2492981.
[38] 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, doi: 10.1109/ACCESS.2020.2997840.
[39] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018, doi: 10.1016/j.future.2017.07.002.
[40] F. Wu, X. Zhang, C. Zhang, X. Chen, W. Fan, and Y. Liu, "Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8144–8156, Sep. 2020, doi: 10.1109/JIOT.2020.3004811.
[41] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015, doi: 10.1109/TIFS.2015.2473820.
[42] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, Sep. 2013, doi: 10.1109/TVT.2013.2257188.
[43] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 4, pp. 1065–1079, Apr. 2018, doi: 10.1109/TITS.2017.2712772.
[44] M. Shahzad and J. Antoniou, "Quality of user experience in 5G-VANET," in *Proc. IEEE 24th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Sep. 2019, pp. 1–6, doi: 10.1109/CAMAD.2019.8858442.
[45] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011, doi: 10.1109/SURV.2011.061411.00019.
[46] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: A survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013, doi: 10.1109/MCOM.2013.6515060.
[47] X. Ge, Z. Li, and S. Li, "5G software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 87–93, Jul. 2017, doi: 10.1109/MCOM.2017.1601144.
[48] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016, doi: 10.1109/TVT.2016.2541862.
[49] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020, doi: 10.1109/MNET.001.1900220.
[50] M. Ouaissa, M. Houmer, and M. Ouaissa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in *Proc. 3rd Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Sep. 2020, pp. 1–8, doi: 10.1109/CommNet49926.2020.9199641.
[51] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020, doi: 10.1109/TVT.2020.2994144.
[52] W. Quan, Y. Liu, H. Zhang, and S. Yu, "Enhancing crowd collaborations for software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 80–86, Aug. 2017, doi: 10.1109/MCOM.2017.1601162.
[53] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8542–8554, Aug. 2020, doi: 10.1109/TVT.2020.2996574.

[54] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Oct. 9, 2020, doi: 10.1109/TNSE.2020.3029784.
[55] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[56] 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, doi: 10.1109/TVT.2020.2972923.
[57] 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, doi: 10.1109/TVLSI.2019.2929420.
[58] C. Lin, D. He, X. Huang, N. Kumar, and K.-K.-R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 30, 2020, doi: 10.1109/TITS.2020.3002096.
[59] X. Deng and T. Gao, "Electronic payment schemes based on blockchain in VANETs," *IEEE Access*, vol. 8, pp. 38296–38303, 2020, doi: 10.1109/ACCESS.2020.2974964.
[60] J. Liu, X. Li, Q. Jiang, M. S. Obaidat, and P. Vijayakumar, "BUA: A blockchain-based unlinkable authentication in VANETs," in *Proc. ICC - IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148863.
[61] Y. Liu, H. Wang, M. Peng, J. Guan, and Y. Wang, "An incentive mechanism for privacy-preserving crowdsensing via deep reinforcement learning," *IEEE Internet Things J.*, early access, Dec. 24, 2020, doi: 10.1109/JIOT.2020.3047105.

FAROOQUE AZAM (Student Member, IEEE) received the bachelor's degree in computer science and engineering from Visvesvaraya Technological University, India, in 2011, and the master's degree in computer science and engineering from Jawaharlal Nehru Technological University, India, in 2013. He is currently pursuing the Ph.D. degree with Sangam University.

He is also associated with the School of Computer Science and Engineering, REVA University, Bengaluru, India. He has authored scientific articles in international journals. His research interests include renewable energy and vehicular communication. He has received the Best Paper Award in First IEEE International Conference on Advances in Information Technology, organized by Adichunchunagiri Institute of Technology (AIT), Karnataka, India, in July 2019. He is a Reviewer of IEEE Access and *SN Journal of Applied Sc*.

SUNIL KUMAR YADAV is currently the Deputy Dean and an Associate Professor with the Department of Computer Science, Sangam University, Bhilwara, India. He is also the Head of the Department of Computer Science and Engineering. He has published more than 30 research articles in various international journals. His research interests include computer security, cloud computing, the Internet of Things, and complier design.

NEERAJ PRIYADARSHI (Member, IEEE) received the M.Tech. degree in power electronics and drives from the Vellore Institute of Technology, Vellore, India, in 2010, and the Ph.D. degree from the Government College of Technology and Engineering, Udaipur, India.

He held a postdoctoral position with Aalborg University, Denmark, in 2020. He was with the University of Jammu, Geetanjali Institute, Global Institute, and SS Group, India. He has published over 40 papers in journals and conferences. His current research interests include power electronics, control systems, power quality, and solar power generation. He is a Reviewer of the IEEE Systems Journal, the *International Journal of Modeling and Simulation*, and the *International Journal of Renewable Energy Research*.

SANJEEVIKUMAR PADMANABAN (Senior Member, IEEE) received the bachelor's degree from the University of Madras, India, in 2002, the master's degree (Hons.) from Pondicherry University, India, in 2006, and the Ph.D. degree from the University of Bologna, Italy, in 2012.

From 2012 to 2013, he was an Associate Professor with the Vellore Institute of Technology (VIT). He joined the National Institute of Technology, Puducherry, India, as a Faculty Member, in 2013. He was invited as a Visiting Researcher with Qatar University, Qatar, supported by the Qatar National Research Foundation (Government of Qatar), in 2014. He was also a Lead Researcher with the Dublin Institute of Technology, Ireland. From 2016 to 2018, he was an Associate Professor with the Department of Electrical and Electronics Engineering, University of Johannesburg, South Africa. Since 2018, he has been a Faculty Member of the Department of Energy Technology, Aalborg University, Esbjerg, Denmark. He has authored over 350 scientific articles. He has authored or coauthored *Lecture Notes in Electrical Engineering* (Springer). He is a Fellow of the Institute of Electronics and Telecommunication Engineers (FIETE 2018), India, and the Institute of Engineers (FIE 2018), India. He was invited as a member of various committees for several international conferences, including the IEEE and the IET. He has received the Best Paper cum Most Excellence Research Paper Award from IET-SEISCON 2013 and IET-CEAT 2016 and five best paper awards from ETAEERE 2016. He serves as an Editor/Associate Editor/Editorial Board member for many-refereed journals, in particular, the IEEE Systems Journal, IEEE Access, *IET Power Electronics*, and the *Journal of Power Electronics*, South Korea. He serves as a Subject Editor for *IET Renewable Power Generation*, *IET Generation, Transmission, and Distribution*, and *FACTS* Journal (Canada).

R. C. BANSAL (Senior Member, IEEE) was employed by the University of Queensland, Australia, the University of the South Pacific, Fiji, BITS Pilani, India, and the Civil Construction Wing, All India Radio. He was a Professor and the Group Head (Power) with the ECE Department, University of Pretoria (UP), South Africa. He is currently a Professor with the Department of Electrical Engineering, University of Sharjah. He has more than 25 years of diversified experience of research, scholarship of teaching and learning, accreditation, industrial, and academic leadership in several countries. He has significant experience of collaborating with industry and Government organizations. He has made significant contribution to the development and delivery of B.S. and M.E. programmes for Utilities. He has extensive experience in the design and delivery of CPD programmes for professional engineers. He has carried out research and consultancy and attracted significant funding from Industry and Government Organizations. He has published over 325 journal articles, presented papers at conferences, books, and chapters in books. He has Google citations of over 11000 and h-index of 47. He has supervised 25 Ph.D. and four Postdoctorals. His research interests include renewable energy, power systems, and smart grid. He is a Fellow and Chartered Engineer IET-UK, Fellow Institution of Engineers (India). He is an Editor of several highly regarded journals, including the IEEE Systems Journal, *IET Renewable Power Generation*, and *Technology and Economics of Smart Grids and Sustainable Energy*.