IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE (AI)-EMPOWERED INTELLIGENT TRANSPORTATION SYSTEMS

Received March 2, 2020, accepted March 13, 2020, date of publication March 17, 2020, date of current version March 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2981397

Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges

PALAK BAGGA[1], ASHOK KUMAR DAS[1], (Senior Member, IEEE), MOHAMMAD WAZID[2], (Senior Member, IEEE), JOEL J. P. C. RODRIGUES[3,4], (Fellow, IEEE), AND YOUNGHO PARK[5], (Member, IEEE)

[1]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500 032, India
[2]Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun 248 002, India
[3]PPGEE, Federal University of Piauí (UFPI), Teresina 64049-550, Brazil
[4]Instituto de Telecomunicações, 1049-001 Lisboa, Portugal
[5]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Science, ICT and Future Planning under Grant 2017R1A2B1002147, in part by the BK21 Plus project funded by the Ministry of Education, South Korea, under Grant 21A20131600011, in part by the FCT/MCTES through national funds and when applicable co-funded EU funds under Project UIDB/EEA/50008/2020, in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 309335/2017-5, and in part by the Ripple Centre of Excellence Scheme, CoE in Blockchain, IIIT Hyderabad, India, under Grant IIIT/Research and Development Office/Internal Projects/001/2019.

ABSTRACT Internet of Vehicles (IoV) is treated as an extension of Vehicle-to-Vehicle (V2V) communication network. IoV helps in enhancing driving aids with the help of vehicle Artificial Intelligence (AI) awareness of other vehicles and their actions. IoV is connected in an adhoc networking environment which utilizes each vehicle in the network as a node, called Vehicular Ad Hoc Network (VANET), where the vehicles may be also connected to the public Internet. It is specifically important for the autonomous vehicles because they can instantaneously communicate with other vehicles surrounding them. In addition, safely avoiding accident prone zones is crucial in order to continue secure and smart transportation. Since the communication among various entities involved in the IoV environment is via open channel, it gives an opportunity to a passive/active adversary to intercept, modify, delete or even insert fake information during communication. It is then a serious concern for the vehicles users to determine whether the received information is genuine. In this survey paper, various security aspects, threats and attacks, network and threat models related to the IoV environment are discussed. Next, a taxonomy of security protocols is given that is essential to provide IoV data security. In particular, focus on various authentication protocols is given that is needed for mutual authentication among the involved entities in the IoV environment for secure communication. A detailed comparative analysis among various state-of-art authentication protocols proposed in the related IoV environment is provided to show their effectiveness as well as security and functionality features. Moreover, some testbeds are described that were designed and implemented for the IoV environment. In addition, some future challenges for IoV security protocols are also highlighted that are necessary to address in the future.

INDEX TERMS Internet of Vehicles (IoV), vehicular adhoc networks (VANETs), authentication, batch verification, security.

I. INTRODUCTION

Technology in today's scenario should be updated and scalable according to its needs and benefits. This devastating growth in the transport system leds to the researchers to combine various technologies like VANETs, IoV, cloud computing forming VANET-based clouds in order to decrease the mishappenings that can occur on road due to high traffic and other drawbacks of consequential changes in transportation. Keeping in mind of increase population, number of vehicles and their users, IoV has become one of the most stretched incentives in todays world. The backbone of the concept

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

lies in the fact of the consumers ease in using mobile and Internet [1].

The IoV technology forced hardware of the vehicle to advance by installing various intelligent devices, processors, sensors inside the vehicle that involve accessorized parts of the car and external sensors like cameras, location tracking, some sensors for drivers sensors to analyze the physical mental and emotional condition of the driver, actuators providing a multisensory platform and many more through interconnection and interoperability [1]. It uses the intelligence and the network capacity of the vehicles in conjunction with outside entities (human, environment and riders) supported by protocols and standards like IEEE.802.11p, thereby providing amazing services throughout. It has three basic building blocks: a) vehicle to vehicle communication within a network, b) communication between one vehicular network and other, and c) connectivity between vehicle and mobile [2]. IoV is an intelligent system that learns the behavior of the role players in the real time environment, and then uses this data to learn and implement in the future for instant decision making. An example includes the use of data like the behavior of the driver, movement of hands, eyes, legs, external environmental conditions, rate of steering movement, delay of the driver in applying brakes, location, position in creating an automatic car without a human driving it. But the truth lies behind this experiment which was processed under a closed environment without real data. To apply it in the current situation, the collection of information becomes a privacy issue. Although it is clear that the automated vehicles will flow smoothly than a human driven vehicle on road unless a disaster occurs in which artificial intelligence or human brain is required keeping the delay tolerance and privacy under control.

IoV got its luck through some limitations in VANETs. VANETs only consider the conditioned networking of the vehicles in and out of coverage range. Certain shortcomings like the restrained capacity of the processor to convert the global received data which is collected among the devices into meaningful information halts the vehicles to become smart devices, less priority to vehicular informative interaction. Another important obstruction in successful VANETs was its inability to manage the identities of the participating vehicles. VANETs do not analyze the drops of packets in the network even when the network is a wireless network. Using this weakness, various eavesdropping or Denial-of-Service (DoS) attacks are possible [3]. These stumbling blocks in VANETs evolved IoV paradigm to a large extent [4].

IoV overcomes the limitations of VANETs through the essence of vehicular cloud that provides an open interface. The vehicles over an area are classified into different clusters based on similarities and differences. All the cluster members interact with their cluster heads which in turn save the data in the cloud. This reduces the band of spectrum required if all the data communication was between all the members instead of just the cluster heads. Not only this, but also it provides a distributed spying over the network for tracking in and out of data. It supports high level of mobility, instant management of the risk situations like maintaining lower delay, delivering high reliability and robustness, increase in peer to peer communications (including vehicles and outside world entities), fulfilling challenges that resist continuous interaction among the vehicles, maintenance of the collected data, processing and analyzing data into information to provide the benefits to consumers and business. IoV enables the automated vehicles to run on road without human intervention which can be advantageous and disastrous at the other moment if malicious activities are not taken care of. Vehicles on given highly efficient processors and sensors have the ability to sense the roads. All the vehicles calculate the intensity of traffic from their timestamp exchange the data amongst the fellow vehicles and then calculate the route with least traffic and risks. But this interaction leads to immense amount of information being shared daily. So the researchers tried to convert the data into graphical representation that represents some disturbance in the traffic through patches or non-uniform distribution of the graph, called as vehicular shock waves. This helps the drivers to adapt themselves to the upcoming situation avoiding risks. The major issue that is resolved in IoV through protocols is security. The vehicles undergo high mobility in out of their registered coverage area. Hence, new connections are formed and broken at every instant. The authentication of the liable vehicles, data integrity, privacy and safety of the vehicles become important issues [2], [5].

IoV would mark a new revolution and a boon in the transport system providing enumerable benefits as provided below [6]:

- *Cost effective:* Better control on the traffic will lead to reducing insurance rates, operational money, warranty cost, public health rate, etc.
- *Time efficient:* Excellent examined traffic will scrutinize time of drivers, riders and all the consumers.
- *Reducing life threatening risks:* By inspecting the traffic, road conditions accident prone situations could be avoided by guiding the traffic through navigation, emergency services or instantaneous services.
- *Evolution of smart cities:* IoV let the cities to become organized by providing services like prior informative parking and better navigation, providing real time view of the traffic, accident proclamation, route optimization.
- Lowering the greenhouse gases effect to avoid the hazard to the nature.
- Alarming and automated warning system.
- Smart automated driving including services like meals on wheels, music on road.
- Luxurious pick and drop of the passengers and the customers using it.
- Video of the fatal occurrences (catastrophes, hazardous calamity) on road also known as pics on wheel [7] helps the vehicles running on the roads to become a witness of any mishap occurring with the fellow vehicles or any tragedy on road. This service will be an asset in maintaining decorum, avoiding forensic proofs for investigations, etc. Hussain *et al.* [7] framed an architecture

in which a vehicle captures a picture through on-board cameras and becomes a witness of tragic incidence on road and uploads it to their respective or generic clouds. The architecture supports identity hiding by adding the pseudonyms to a technique in which the identities are swapped among the intended vehicle and the neighbor vehicle. By providing credits to the participating vehicle through receipt system, the vehicles collect the receipts and the total receipt calculations the work described increase the service contributions.

A. RESEARCH CONTRIBUTIONS

The research contributions made in this survey work are listed below:

- First, various security requirements, security threats and attacks are discussed that are needed in the IoV environment.
- Next, the network and threat models related to the IoV environment are discussed.
- A taxonomy of various security protocols is discussed to provide IoV data security including key management, authentication, intrusion detection, access control, privacy preservation and secure routing protocols. In particular, we focus on various authentication protocols that are essential for providing mutual authentication process among various involved entities in the IoV environment for secure communication.
- A detailed comparative analysis among various state-of-art authentication protocols proposed in the related IoV environment by the researchers is also provided. The effectiveness as well as security and functionality features of the compared authentication protocols is then shown.
- Furthermore, several testbeds that are developed and implemented by the researchers for the IoV environment are described.
- Finally, some open challenges that are necessary to be addressed in the future to provide better security in the IoV deployment are also discussed.

B. PAPER OUTLINE

The security requirements in the IoV environment is discussed in Section II. We then discuss several potential attacks and threats that are possible in the IoV environment in Section III. The state-of-art reviews and survey works with our survey are also discussed in Section IV. While Section V discusses about network and threat models relevant to the IoV environment, Section VI includes a taxonomy of security protocols needed for securing IoV environment. Section VII particularly focuses on analyzing various existing authentication schemes proposed in the IoV environment. A detailed comparative analysis of discussed authentication protocols is provided in Section VIII. Various tesbeds developed or implemented in the IoV experiments are discussed in Section IX. Various open security issues and challenges needed for IoV data security are discussed in Section X. Final section (Section XI) concludes the survey paper.

II. SECURITY REQUIREMENTS IN IoV ENVIRONMENT

Gafencu and Scripcariu [8] stated that the vehicular communication is governed by two security standards: one is defined by IEEE Wireless Access in Vehicular Environments (WAVE) and the other by European Telecommunications Standards Institute (ETSI) Intelligent Transport Systems (ITS) G5. Both of the suites follow the basic scenario with a difference that IEEE 1609.2 defines message formats, certificate handling, authenticating, signing and revoking format and works in hierarchy that is with one certificate authority, while ITS G5 defines specification for architecture, management, trust models, threats and overcoming vulnerabilities etc with each network having a different central certificate authority. However, every evolving technology has some associated risks and threats along with it. When the entities be in its infrastructure, things or vehicles on a network, the major issues that can lead to disaster are misleading data or apocryphal attacks on the data or the devices on the network. Features of IoV are advantageous to the environment, but it also welcomes certain threats. The features like portability of the nodes in the area, involvement of the third party in the paradigm to certify the nodes forms an open source for the attacks. Moreover, presence of limited amount of bandwidth makes certain attacks on the real time data even easier. In IoV, this can lead to loss of generosity even lives. There can be several attacks on IoV which will not only cause harm to the drivers or consumers, but also to the whole industrial business. This susceptibility of the paradigm extorts the researchers to ponder more on the security aspects like integrity, confidentiality and authentication. Attacks could be categorized on the basis of the cluster location that is within the cluster or outside the cluster as inter-cluster attacks and intra-cluster attacks. On the same notion one such inter-cluster attack can allow excessive delude vehicles to appear on the desired area to depict congestion, or the automated system of the vehicles can take wrong decisions on receiving prank or trickery data like theft kidnapping on the road [3]. Identifying such flagitious vehicles locally becomes far easier and more necessary that letting it affects the global data. Hence, the cluster members are responsible for catching the vicious vehicles by conspiring and comparing the received message from the attacker with the local records, and identifying the real time environment situations simultaneously being on network to calculate the soundness of the received signal. Using the concept of vehicular cloud and edge clouding even the large amount of data can be managed in a delay tolerant fashion [2]. On the other hand, one attack could directly harm the authentication mechanism in which an attacker could use the private credentials of the legitimate nodes and use them further to flow injurious information within the cluster to mislead the entities in the network.

IoV can be subjected to intra-cluster attack as follows. Being the subset of Internet of Things (IoT), IoV blends many technologies together forming a heterogeneous network. The technologies involved have their own standards and policies; hence, they become more vulnerable to attacks. The sensors in consolidation with the vehicles form a complete IoV setup which is then responsible for any deleterious effect on the network. Any external data to the sensors from the adversary related to environment, brake system, smoke detection, alarming system, and road condition could mislead the full network creating a baleful situation. Another category of open attack found its way through cloud computing. Cloud attackers can launch a continuous DoS attack harming the true users by violating their access to the technology.

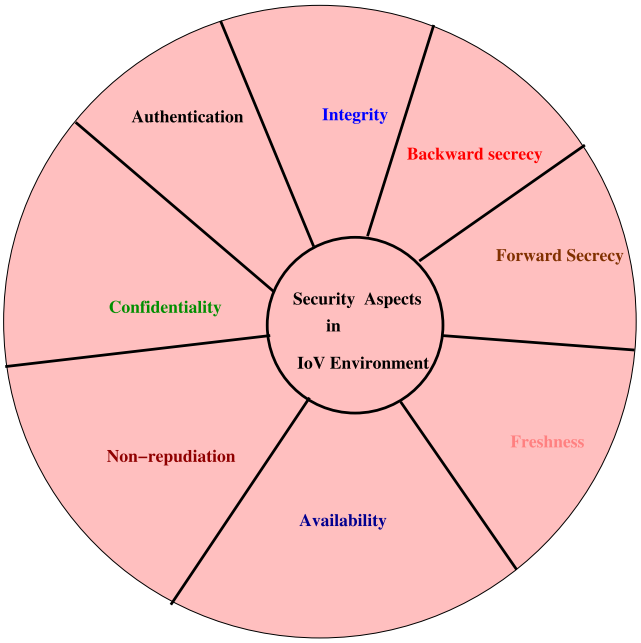

FIGURE 1. Various security aspects in IoV environment.

Keeping in mind of the above attacks which are big threats to IoV, the researchers have studied and presented several works in order to safeguard the security and privacy of IoV categorizing the security aspects into following main points. The security aspects are as follows [9]–[12] (which are also briefed in Fig. 1):

- *Integrity:* The data sent and the data received should be identical, that is, no distorting of the data in the way on the network. Attacks like message tampering, masquerading, black hole, gray hole, fabrication, and malware (use of hashing technologies) are possible.
- *Authentication:* No imitation of the vehicles sending the data should be allowed. The vehicle, actuator or sensor who has sent the data should be the true sender or the vehicle it is claiming to be. The receiving sensor should not be spoofed by the false sender of the data claiming the innocent sender without right identity (ID). The system should be able to differentiate between the fair canonical vehicles and crooked vehicles (private signatures). Sybil attack allows multiple nodes to participate in the network and hamper the resultant behavior of the network according to their attack. Global Positioning System (GPS) spoofing will update the corresponding nodes with its wrong location information affecting various application that use GPS. Black hole attack will redirect all the packets towards the attacker and the adversary will drop all the packets leading the instant decision making of the vehicles affected by not letting the real time packets to reach to the vehicle to protect the safety of the drivers and customers at risk. Worm hole attack will redirect the packets to some other network with malicious users. Fabrication attack allows the attacker to send the false messages to the members of customers to create utter confusion among the cluster members. There are also other attacks, such as replay attack, gray hole attack, message tampering, masquerading attack and malware. All these mentioned attacks are the possible attacks on authentication.
- *Confidentiality:* Although certain information in IoV needs to be public, still the privacy and the security of the customers or the business involved in IoV is the utmost important part of the paradigm. Hence, the private or delicate data should not be known by the adversary (encryption being the solution). Eavesdropping will allow the adversary to analyze the traffic or the data without interfering in the network, ID disclosure, traffic analysis, and malware.
- *Non repudiation:* Any emergency accidental cases on road requires to identify the correct culprit. In order to fulfill this requirement, it is necessary for all the involved users within the accidental communication range to not be able to deny any sent message.
- *Availability:* With the increase in the number of vehicles on road, the participants of IoV are also continuously increasing. So break down of the network is possible with more number of requests messages or during congestion [10]. Hence, one of the basic responsibilities of the system is to be available to all the legitimate users. Few possible attacks on availability are DoS, black hole, gray hole, spamming throws spam messages throughout the network which consumes lot amount of bandwidth affecting the latency of the normal packets in the network, jamming and malware attacks [3].
- *Scalability:* The essence of a good connected vehicular network lies in the fact of ease in increasing the network load and nodes. Hence, an increase in the network size arises security issues on scaling a network. Hence, scalability becomes an important issue in the requirements [9].
- *Time constraint or Freshness:* IoV is all about real time situations where any delay could be hazardous. Hence, the emergency warnings and signals should be delivered on time without any tampering in order to implement

the correct results. This requirement would stop various replay and time based attacks. Moreover, the foremost requirement of authentication should also be done without delay to flow the authenticated messages in the network.

- *Forward secrecy:* IoV is a type of network where the nodes are in continuous mobility. Hence, the membership of a node towards a place changes continuously. Thus, it becomes an utmost importance that the network needs to be refreshed every time any node makes an entry or exit in the network to maintain privacy. If any vehicle node leaves an IoV network, the vehicle should not be exposed to the messages after its exit from the network.
- *Backward secrecy:* If any new vehicle node joins an existing network, the user of the joined vehicle should not know about the messages flown before its entry in the network.

III. SECURITY THREATS AND ATTACKS IN IoV ENVIRONMENT

There could be different types of attackers like active, passive, malicious, rational, local or outsider. Ultimately, each attacker who get a chance to involve in the network affects the legibility of the network [10], [13], [14]. In the following some of the potential attacks and threats are discussed that are possible in the IoV environment.

- *Flow of bogus information:* An attacker may fool the authenticated user by flowing fake or rotten information making them believe the false environment.
- *Message injection attack:* In message injection attack, the attacker sends an authorized message in the network to get access and control over the entities which can be further used to send malicious hazardous messages.
- *Replay attack:* The adversary in this attack iterates the already flown messages within the network in order to illegally access the services and resources of a network.
- *Cookie theft attack:* Similar to the replay attack, in cookie theft attack an attacker saves the cookies and then uses them ahead in the network whenever required to access the network resources [15].
- *Sybill attack:* The attacker creates some fictitious vehicles around a targeted vehicle for generating a jam signal while the path is clear enough which compels the user to take a different route. This fake jamming is done by using enumerable false ids for a single node giving an essence of more than one node.
- *Man-in-middle attack:* An attacker impersonates between the sender and receiver there by receiving all the messages from the sender and sending forth to the receiver. It could be active or passive attack.
- *Denial-of-Service (DoS) attack:* In order to reduce the efficiency of the network, an attacker throws heavy legal message load on a particular communication channel more than its handling capacity to congest it in order to use the limited resources of the network illegally. This attack would let a worst consequence to occur during the real time urgency even if the attacker has least knowledge about the network. The vital nodes such as Road-Side Units (RSUs) in the IoV environment are targeted which are meant to provide services by sending update, messages and resources to handle requests flooded to it at once [12]. The advanced version of DoS attack, known as Distributes DoS (DDoS) attack in which the attacker may attack system from outside to a single targeted system to agitate its functionality and network.
- *Dissimulation of GPS attack:* It refers to an act of intercepting and modulating GPS signals sent by any vehicle or RSU within a network before it gets received by an intended receiver. This directly effects the security of the driver and the passenger by letting them take wrong directional decisions [12].
- *Impersonation attack:* Under this kind of attack, the adversary would use the identity of some authenticated user evacuating it out of the network to mock the present innocent vehicles and spoof them using fake and dangerous messages.
- *Masquerading attack:* Similar to impersonation attack with a difference of having just one entity copying a real id of any node within the network, the adversary can spoof the receiver by creating two different senders with same identity.
- *Warm hole attack:* Also known as tunneling attack, an attacker node fakes a wrong information regarding its distance from the targeted node to make all the messages coming from the sender flow through it. This creates a deadlock and exposes all the messages to the attacker node before flowing in a network.
- *Eavesdropping attack:* In this attack, the attacker does not participate actively in the communication within the network, but becomes a part of a network from outside in order to attain some private confidential data of the drivers or the customers illegally to use it against their privacy without even letting them know.
- *Message holding attack:* This attack involves an active attacker in which an attacker drops some of the messages with demanding information that could affect the whereabouts of the road condition or the drivers state of requirement and eventually affect the drivers decision. It also lets the drivers save the message and the information with them which can be utilized in future within the network [10].
- *Message manipulation attack:* An attacker modifies the content of the messages to harm the decisions of the receiving entity paralyzing the overall system.
- *Message deletion attack:* An outsider envy, being an attacker, can delete the message which was supposed to be send before it got sent to halt the flow of intended information in the network.
- *Hardware intrusion attack:* An attacker can successfully intrude the hardware of the network like location of

RSUs or hacking the information table out of it and spoofing the entities in the network.

- *Channel hindrance attack:* This attack is the process of interrupting the channel to slow down or weaken the communication process which affects the real time decision in an IoV network.
- *Data falsification attack:* It is a type of an integrity attack which can create congestion and jam within the network by a little change in the data. Rawat *et al.* suggested an algorithm that uses contention window technique that increases the throughput and also hash functional verification that puts a check on the falsified data. It is a cluster based algorithm that makes cluster heads to communicate with each other for reducing the congestion in the network [16].
- *Malware attack:* This attack corresponds to infusing malicious worms or viruses through files in the system to infect the network in future [17].
- *Fuzzy attack:* The attacker in this type of attack sends messages by befooling the identifiers in any order using a constant data hampering the functioning of the system. The attacker needs to study a vehicle for a long time to observe the identifiers behavior in order to change its pattern [18].
- *Guessing attacks:* In this attack, an attacker can guess identity, password (in case of password-based authentication mechanism) and/or biometrics of a registered user (in case of biometric-based authentication mechanism) from the intercepted messages and extracted information from a lost/stolen OBU of a vehicle or smart card of a registered user.
- *Session linking attack:* An attacker can attack by linking any of the two random sessions of any vehicle with other entities in the network which can reveal all credentials after little calculation.

Table 1 summarizes all the possible attacks classified on the basis of various aspects of security which form threats to IoV paradigm.

The ultimate goal of IoV is to gift the world an efficient and reliable transportation that includes to check the rise and fall of pollution, the condition of the roads, reducing time of the users by constantly checking the traffic congestion, safety of the passengers and the vehicles. Hence, the researchers in both academia and industries have found out the elucidation for almost all the known attacks. Understanding the problem is the first step towards solving it. Thus, representation of the attacks graphically can represent the prototype of the attacks in the real environment. Intrusion Detection System (IDS) marked a benchmark for the researchers as it helps in monitoring the network as a whole; the interaction among the actors the flow of data and the real time attacks. This system provides relief from both inter cluster and intra cluster attacks.

Honeypots proved out to be another security asset for IoV. This system is different from other schemes involved for preserving security. The main goal of this scheme is to create signatures of the attackers by keenly studying their behaviors

TABLE 1. Attacks and threats in IoV environment, and their remedies.

Attacks on	Types of attacks	Recommended remedies
Authentication	* Sybil attack * Masquerading attack * Replay attack * Message injection attack * Impersonation attacks * Warm hole attack * GPS deception	* Group signatures * Identity based cryptography * Tampered proof devices * One time identity based aggregate signature * Multiplicative secret sharing technique * Individual message digital signature
Availability	* Channel interference attack * DoS attack * DDoS attack	* Hardware related side channels, visual lights, ultrasonic audio * Authentication method using Public Key Infrastructure (PKI) * Symmetric key cryptographic techniques.
Confidentiality	* Eavesdropping attack * Man-in-the-middle attack * Message holding attack * Message deletion attack	* Encryption
Integrity	* Data manipulation attack * Data falsification attack * Malware attack	* Intrusion detection system * Packet message entropy

throughout the network. This signature could then be used in IDS. Although routing requires exchange of packets, still the confidential data should not be leaked and this issue is taken care by routing privacy protection mechanism which uses only the appropriate data to be revealed. The salient feature of the whole process lies in the management of the key. The whole process starting from the generation, distribution and using key should be highly monitored in order to maintain authentication. One such quick fix is the use of signatures, which is formed by using any personal information of the user detected for its correctness on its other end after being received. The vehicles should sign the data being sent before flowing it on the network along with the trusted Certificate Authority (CA). The other attacks like spoofing could be avoided if the vehicles within the clusters can detect the physical presence of the other vehicles around the network through physical equipment. Use of RSUs and IDS can do wonders for the notion. Daily increase in the number of authenticated users makes handling, managing and preserving big data or intensively large data an important and hard issue. They are certain methodologies that can analyze the behavior and various heuristic measures. A cloud server can act as a third trusted party characterizing malwares, and illegitimate and innocent entities. Adding nonce to the protocols proved to be a big help to all the concerned researchers. Adding time to live value also helped reducing the traffic on the network. Applying one-way cryptographic hash function or cryptographic Message Authentication Code (MAC) can provide confidentiality of the data within the network.

TABLE 2. Comparative study on existing surveys in IoV and VANETs environments.

Reference	Year	Benefits of IoV	Security requirements	Testbeds designed	Key areas covered
Mokhtar *et al.* [20]	2015	×	✓	×	* Security requirements and challenges * Classification of attacks and threats associated to different layers of OSI model * Discussion on open areas in research
Sun *et al.* [9]	2015	×	✓	×	* Security requirements along with threats and their counter measures * Future trends of research directions
Joy *et al.* [21]	2017	×	✓	×	* Evolution of IoV from vehicles to vehicular cloud * Emerging applications of IoV * Haystack privacy to maintain data privacy and accuracy
Joy *et al.* [2]	2017	×	×	×	* IoV architecture that enables both V2V and V2I communication * Security and privacy issues of crowdsourced data
Talib *et al.* [3]	2018	×	✓	×	* Comprehensive approach towards threats, attacks, and their solutions in all network layers * Solutions to various problems illustrated
Abassi [22]	2018	×	✓	×	* VANET projects * Security issues and challenges * Attacks and threats * VANET opportunities and challenges
Castillo [1]	2018	✓	✓	×	* VANET technologies and architecture * Security requirements
Priyan and Usha Devi [23]	2019	×	✓	×	* Survey on IoT, IoV and Internet of Everything (IoE) * Discussed challenges and issues in IoT, IoV, and IoE systems * Identified some research problems
Our survey	2020	✓	✓	✓	* System models (network and threat models) * Security aspects and challenges * Attacks and threats * Taxonomy of various security protocols in IoV paradigm * Analysis of authentication protocols * Detailed comparative analysis of authentication protocols * Discussion of various designed/implemented testbeds suggested in IoV security * Discussion of various open challenges and issues

Note: ✓: survey supports the specified features; ×: survey does not support the specified features

Security and privacy are two parallel concepts which cannot be achieved together and deciding between the two becomes even more difficult. Anyhow the privacy can be differentiated and scaled keeping the accuracy constant. A little benefit by applying different types of privacy according to the system can be attained. The differential privacy concept lets the driver to share the data with surety of not losing their privacy. To summarize it states that information can be accessed when the vehicles data in the database, and can also be accessed when the vehicles data is absent in the database. Second is the distributional privacy which manages to reveal only the distributed information even if the whole sole information is released. This makes it stronger than differential privacy. The others are zero knowledge sampling which is used when accuracy is not a primary goal. It works by sampling the data set concept [20]. IoV has several users already with large number of users joining daily. Hence, the coordination between the users becomes an issue. The same was studied by Joy and Gerla [20] in the haystack privacy management under vehicular clouds suggests that all the owners need to reserve their data exclusively prior to adding them in the cloud in an autonomous manner. The queries are dimensionally represented and are answered twice by each data owner in a yes/no fashion.

IV. EXISTING SURVEYS IN IoV ENVIRONMENT

In this section, the state-of-art reviews and survey works are discussed that are already presented by several researchers, such as Mokhtar and Azab [19], Sun *et al.* [9], Joy and Gerla [20], Talib *et al.* [3], Abassi [21], Castillo-Castillo *et al.* [1], and Priyan and Devi [22]. Table 2 shows the comparison among the existing surveys, and also our survey in IoV environment from the year 2015 to 2019. In this comparison, the benefits, security requirements, developed/designed tesbeds and also the key areas covered by the considered surveys are considered. In reference to the comparison, our survey work gives an advanced analysis to study IoV deployment by discussing system models, threats, security aspects and their counter measures, taxonomy of various security protocols, detailed analysis of existing authentication protocols and their performance study analysis, and even various testbeds that are designed by the researchers.

V. SYSTEM MODELS

This section gives a specific network model of IoV and also a threat model that describes the possible capabilities of an adversary to breach the data security in the IoV environment.

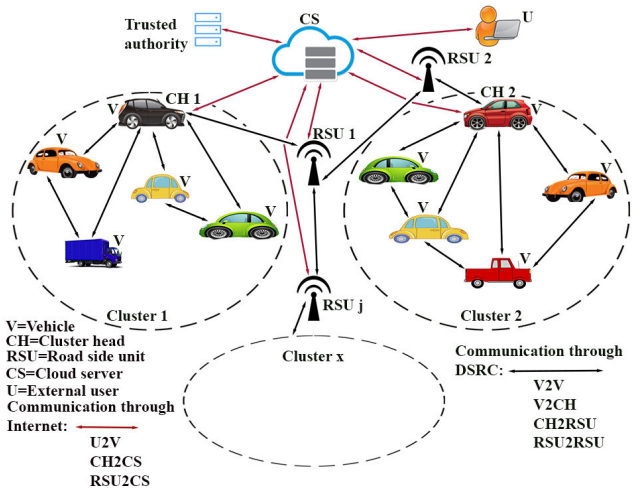

FIGURE 2. A network model of IoV environment.

A. NETWORK MODEL

The network model for IoV communication environment given in Fig. 2 contains different types of communicating parties, such as vehicles (V), cluster heads (CH), roadside units (RSU), cloud servers (CS), external network data users (U) and a trusted authority (TA). In such communication environment, communication happens through the Dedicated Short-Range Communications (DSRC) protocol and the Internet. The entire network is divided into certain number of clusters in which there is cluster head node that is basically a vehicle elected periodically as a leader. Each cluster head collects data from its cluster member vehicles, processes and sends that data to the RSU (via DSRC) as well as to the cloud server (via the Internet). As each vehicle has an On-Board Unit (OBU) that can be assigned an IP address communicates to the cloud server via the Internet. Cluster based approach helps to reduce the communication as well as computation overheads in the network. The parties which can communicate through *DSRC* are vehicle-to-vehicle (V2V), vehicle-to-cluster head (V2CH), cluster head-to-roadside unit (CH2RSU) and roadside unit-to-roadside unit (RSU2RSU). Various types of communication exist in an IoV environment: a) RSU-to-cloud server (RSU2CS), b) CH-to-cloud server (CH2CS), and c) user-to-vehicle (U2V). The TA is responsible for the registration of various network communicating parties (Vs, CHs, RSUs, CSs and Us). For this purpose, the TA usually generates the credentials, such as identities, secret keys etc., for Vs, CHs, RSUs, CSs and Us. After storing the generated information into the memory of these entities, they are deployed in the network. The TA is also responsible for the registration of external network data users and provide them the information either in a smart card or a smart phone in case of an authentication protocol. The user can also access the data of the deployed vehicles. The registration information stored by the TA in the memory of these different devices is used to perform the authentication procedure. The CHs and RSUs participate in local decision making (i.e., chances of occurrence of accidents in a particular region). On the basis of local decision making, the alarm system gives a warning message to the driver of that particular vehicle. In addition, CHs, RSUs and CSs also participate in global decision making (i.e., traffic condition in a particular street of a city). Such types of information can be provided to the driver of the vehicles moving in other sides of a city. The external network data users, who are interested to get the information about a particular vehicle, can communicate to that vehicle through cloud server. To start any kind of communication, all these parties need to mutually authenticate among each other. After completing mutual authentication successfully, the communicating parties can communicate among each other securely using the established secret session keys [5]. Furthermore, the key management and access control among the communicating vehicles in a cluster, and intrusion detection for detecting malicious vehicles in the IoV environment are essential. The intrusion detection can be applied either in distributed way (i.e., by the individual vehicles and cluster heads) or in a centralized manner (i.e., by the RSUs) depending upon the applications.

B. THREAT MODEL

To figure out the associated threats related to the IoV communication environment (discussed in Section I-B), the widely-used Dolev-Yao (DY) threat model [23] can be used. The DY model insists that any two communicating parties communicate over an open (insecure) channel, and the end-point communicating parties are not also trusted. An adversary $\mathcal{A}$ can then eavesdrop (read) the communicated messages and can also delete or modify the communicated messages as the channel is in secured. Moreover, the Canetti and Krawczyk's adversary model, also called as the CK-adversary model [24] is applied which is a current *de facto* standard model in the modeling of an authentication & key establishment security protocol. Under the CK-adversary model, $\mathcal{A}$ has all capabilities as in the DY model along with the ability to compromise the secret credentials as well as the session states & session keys in the sessions. Furthermore, $\mathcal{A}$ can physical capture the onboard units (OBU) of the vehicles and obtain the stored credentials from these devices using the sophisticated power analysis attacks [25]. It is also assumed that the smart phone (smart card) of a user can be lost or stolen. Hence, the secret credentials stored in his/her smart phone or smart card can be extricated using the power analysis attacks [25]. The extricated data can be then utilized in some unauthorized malicious tasks, such as computation of session key, vehicle impersonation attack, replay attack, man-in-the-middle attack and privileged-insider attack. Finally, the trusted authority (TA) is assumed to be full trusted entity in the IoV communication environment and it will not be compromised, whereas the cloud servers are treated as the semi-trusted entities.

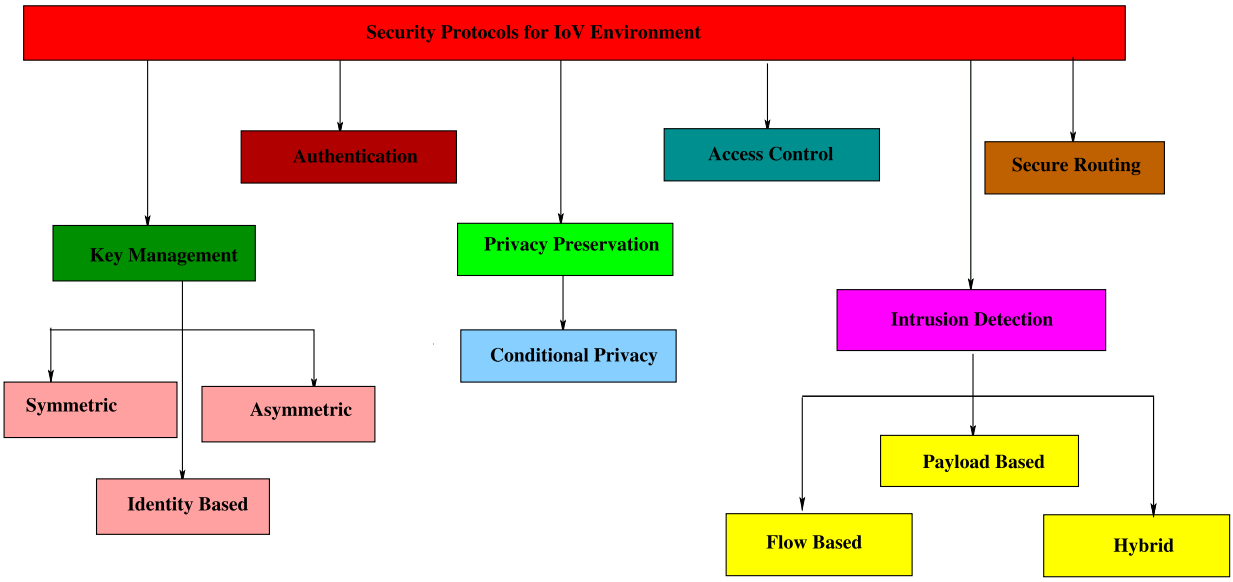

FIGURE 3. A taxonomy of security protocols in IoV environment.

VI. TAXONOMY OF SECURITY PROTOCOLS FOR IoV

In this section, a taxonomy of various security protocols in the IoV environment is discussed that are crucial to provide data security. The security protocols involved in an IoV environment can be divided into various categories, such as *key management*, *authentication*, *intrusion detection*, *access control*, *privacy preservation* and *secure routing* as represented in Fig. 3.

A. KEY MANAGEMENT

Key management is one of the security protocols that provides establishment of secret keys among various communicating entities (between vehicles, between vehicles and RSUs, and between RSUs) so that secure communication among these entities take place. Key management can be categorized into two ways: symmetric and asymmetric key distribution approaches.

In symmetric key management, the trusted *TA* is responsible for registering all the deployed vehicles and RSUs by pre-loading the secret credentials in their memory before their placement in the IoV environment. Next, after deployment the communicating entities will establish pairwise secret keys among them using the pre-loaded information available in their memory. The verification of established secret key can be done by the communicating entities with the help of challenge-response protocol as it is done in other networks, including wireless sensor networks and Internet of Things (IoT) environment (for example, the key pre-distribution schemes suggested in [26]–[39]).

In asymmetric (public key) management, the initial stage also involves the registration process of the vehicles to the *TA* in order to validate themselves and to legally participate in the communication process. During the registration process, the *TA* allots them a pair of private and public keys. Sender vehicles can use their private keys to sign the messages before sending to be away from being exposed to the attackers. On the other hand, receiving vehicles would execute the verification process to find the legitimacy of the messages received. For the key pairs, some researchers have used public key infrastructure (PKI) which do not fulfill the conditional privacy and has huge latency. For encrypting the messages, the sender vehicle can encrypt the messages using the public key of the receiver vehicle, and the receiver vehicle will be able to decrypt this as it has only the matching private key corresponding to the encryption public key.

Symmetric cryptography was used to provide the same key for both signing and verification, which suffers through non repudiation. Identity-based cryptography was also highlighted which uses public information of the entity to derive the key. The public-key based cryptographic techniques, such as RSA [40], Elliptic Curve Cryptography (ECC) based encryption and signature, known as Elliptic Curve Digital Signature Algorithm (ECDSA) [41] and Diffie-Hellman key exchange [42] can be used to generate key pair further. The only drawback that asymmetric cryptography has latency and overheads issues. It is mentioned that the 80-bit key size of a ''symmetric key cryptographic algorithm (e.g., Double Encryption Standard (DES) with two keys)'' provides the equivalent security for the ''1024-bit RSA'' and ''160-bit ECC'' [43]. This implies that ECC supports the same security as that for RSA with much smaller key size. To reduce burden of public key-based key management, the Timed Efficient Stream Loss-tolerant Authentication (TESLA) was implemented in VANETs which uses symmetric cryptography paralleling it with time [44]–[46].

The authors in [47] presented a new key management scheme using fog computing which also provides authentication. Key management process was followed by two phases of initialization and registration. The key management phase involved parallelly a mutual authentication among various entities of the network. The vehicle and the fog server decide a session key and also authenticate themselves in the first step. This is then followed by a session key between RSU and fog server applying hash functions and ECC. Mutual key agreement between the fog server and the cloud server marks the end of key agreement scheme of their protocol.

Guo *et al.* [48] also defined a scheme in which key management server was responsible for validating the identity and providing a key to all the entities by applying homomorphic key agreement scenario by comparing the MAC. Their scheme was found to be more secure than password-based key settlement.

B. AUTHENTICATION

One of the primary features of a security protocol is to enable the entities (for example, user of a vehicle) to authenticate themselves to the RSU and also to check the authenticity of the RSU. RSU on receiving the vehicles message request checks the revocation list and states the validation of the vehicle.

The authors in [49] explain the basic authentication procedure in which a vehicle before joining a network sends the request to the trusted authorities via the nearest RSU. The *TA* would let a vehicle to join the network and accept the request only after validating the legitimacy of both vehicle and RSU. Earlier the researchers were depended on location or PKI security for authentication, but that was not helping to maintain in nominate identity. Now, when the networks are scaled to a large extent, conditional privacy becomes important cloud computing and working with pseudo identity is implemented.

The authors in [49] also proposed a protocol that registration phase uses unique identities for every vehicle with an assumption that the registration channel is secure. A smart card (mobile device) is issued to the user by the *TA* with credentials. The credentials of the smart card are validated against the saved parameters, and thus breached smart card by the attacker cannot initiate the communication. The services are provided only to the vehicles that fulfill the validating criteria.

Typically, a user authentication mechanism in the IoV environment involves the following phases as stated in [50]:

- *System setup:* Under this phase, the *TA* is responsible for generating the system parameters.
- *Registration:* Before installing or deploying the vehicles and RSUs, they require to be registered with the *TA*. The essential credentials are then pre-loaded in the On-board Unit (OBU) of the registered vehicles and RSUs prior to deployment.
- *User registration:* To access service from RSUs, a user requires to register with the *TA*. The user needs to provide his/her credentials (for example, identity, password and also biometrics in case of biometric-based user authentication scheme) securely to the *TA*, and after analyzing the registration information a smart card or mobile device is issued by the *TA* securely to the registered user.
- *Login:* Using this phase, a user provides his/her credentials, and after validation of the credentials by his/her smart card/mobile device, a ''login request message'' is generated and then sent to the RSU via public channel.
- *Authentication and key agreement:* Upon reception of the login request message, the RSU validates the message and send the ''authentication request message'' to the user. The user also checks the validity of the received message, and then sends the ''authentication reply message'' to the RSU. After validating the received message from the user, the RSU and user agree on a common session key for secret communication among them.
- *Password & biometric update:* This phase is essential when a registered user wishes to update his/her password and/or biometrics for providing maximum security. This phase should be executed at any time locally without contact of the *TA* anymore.
- *Smart card/mobile device revocation:* This phase is essential when a smart card/mobile device of a legal registered user is lost/stolen by an adversary. The revocation phase should permit to issue a new smart card/mobile device with fresh credentials stored into it.
- *Dynamic node addition:* This phase permits a new vehicle or an RSU to be joined after initial deployment.

C. INTRUSION DETECTION

Cyber threats have always been challenging tasks for an IoV network since the day it evolved. The older vehicles were not able to implement dedicated countermeasures because of hardware insufficiency. Now a days, proactive remedies are not much helpful for the large network of vehicle and other components. Hence, intrusion detection came out as flying color in implementation of an IoV network. There are certain factors that need to be taken care of before implementing Intrusion Detection System (IDS) like all the entities should have IDS installed. Moreover, the capability of the network should complement the speed, latency, storage, and accuracy of an IDS. It is an elucidation for both inter and intra vehicular networks. An IDS basically works against internal attacks. Conventional knowledge based and anomaly based IDS work in the same orthodox manner by learning attack patterns and having a match while the later works on mismatch of the system from its usual pattern [51].

Al-Jarrah *et al.* [17] categorized the inter vehicular IDS into three types. Flow based IDS observes the frequency and interval of the messages and plays an alarm during a unusual frequency pattern without accessing the content of the message. Payload based IDS looks on the payload of the messages. Hybrid IDS uses the features of both payload and

flow based IDS. They further classified the system based on rules, frequency, and learning. Furthermore, once the attack is detected it becomes an important aspect to announce and reveal to the concerned entities which can be done through multimedia audio video hardware installed in the vehicles. They also proposed various metrics to measure against the systems.

Fu *et al.* [52] proposed an ''Field Programmable Gate Array (FPGA) based IDS'' which utilizes less power and it works in real time with negligible latency. They claimed about its easy installation and less space requirement. Their IDS depends on multi stride ''Non-Deterministic Finite Automata (NFA)'' which works on the basis of matching regular expressions. They also explained bit optimization and link-NFA. Alshammari *et al.* [18] explained an IDS based on controller area network protocol which provides a bus for the messages to flow without revealing the sender and receiver information. Various factors like rate of flow of messages over the bus can detect an attack.

An IDS based on machine learning allows to identify an attack is based on the change in the packet form of the malicious packet. Another approach is based on making the IDS to learn the behavior pattern of both historical clean data and historical dirty data to analyze the changes. Watchdog module also became a part of IDS. Furthermore, Honeypots are like supporters to intrusion detection system going hand in hand with them which are placed as an attractive spot in the network for the attackers. Information and patterns using machine learning are also applied for tracking the attackers [8].

D. ACCESS CONTROL

Access control is another important security service for providing security in the IoV environment. New nodes (vehicles and RSUs) deployment in the IoV environment is essential for providing services. However, a deployed node may not be an authenticate node as an adversary may deploy some malicious nodes in the network. Therefore, it is a tough task to differentiate the malicious new nodes joining in the network from the existing genuine nodes. This demands an access control mechanism so that the deployed malicious nodes can be prevented from entering the network. An access control mechanism has basically the following two tasks [50]:

- *Node authentication:* This requires that the newly joined nodes (vehicles and RSUs) must authenticate themselves to their neighbor nodes in order to prove that they are authorized registered nodes to access the services from other deployed nodes.
- *Key establishment:* Under this task, a newly deployed node needs to generate the shared secret key with its neighbor nodes once mutual authentication between them happens successfully. The established secret keys are then utilized for secure communication.

User access control mechanism is also another essential security service for providing access right only to authorized registered users for various services, information and resources available in the IoV environment.

Dua *et al.* [15] designed a two-level access control mechanism for secure communications among vehicles in an IoV-based smart city environment. In their first level authentication, the cluster head (*CH*) among a group of vehicles in a cluster is verified by an exchange of messages between *CH* and the trusted certification authority (*CA*). The authenticated *CH* is then responsible for authentication of other vehicles in its cluster in the second level authentication, which is performed by exchange of messages among *CH* and its associated vehicles.

E. SECURE ROUTING

IoV does not require simple handshake protocols for authentication and defining the routes. Instead, they need security aspects like hash functions and message authentication code (MAC) added to the protocols to protect them against various attacks and threats like Denial-of-Service (DoS) or route modification attack, and also privacy management that does not reveal the information about the nodes during a route discovery [8].

Yadav *et al.* [53] and Devangavi and Gupta [54] summarised the routing procols along with stating their merits and demerits. Those works presented comparative study on all the active routing protocols.

Secured routing protocol is divided by the researchers in three main categories [55]. The first one is the cryptographic based solution which implements crytographic technique to safeguard confidentiality and authentication issues along with giving an optimal route. The number of verifications required made in this approach is a little lazy. The second one is the trust based approach which requires the vehicles to communicate only with other vehicles on which they build a trust on the fellow vehicles depending on their reputation and behavior requiring less overheads and avoiding mitigating attacks. The trust based solution also identifies insider attacks which were ignored by cryptographic solutions. The researchers then combined both the approaches to give out a hybrid approach, which is the third category.

Bhoi and Khilar [56] in the paper proposed a secure station to station key management routing protocol, called the ''Position Based Secure Routing Protocol (PBSRP)'', which finds an efficient route using the Euclidean distance along with maintaining security by using session key for encrypting the messages. This protocol works the best in the presence of a malicious attacker showing minimum latency and good packet delivery ratio. Their scheme executes with some assumptions like each node will be a responsible node with the ''Global Positioning System (GPS)'' installed for route discovery in three phases: initialisation phase followed by best route discovery phase and then secure delivery of the packet phase. A malicious driver if there in the network can be detected in the verification phase using hello packets. No third party is involved and the security is taken care by

certificates and mutual verification by the vehicles on the level of trust.

Slama *et al.* [55] described a ''Trust Cryptographic Secure Routing protocol (TCSR)'' protocol for a secure routing. The authors focused on reducing communication involved in multiple authentication by considering only the highly trusted neighboring nodes for broadcasting the routing messages. Their scheme executes in two phases. First phase generates the trust amongst the neighboring nodes and in the second phase the privacy of the shared message is secured. The trust value of the vehicles depends on the successful or unsuccessful transmission of the vehicle based on additive increase and multiplicative decrease. Every time the communication between two nodes is preceded by trust value calculation. The security is led by asymmetric cryptography underlying the ''Public Key Infrastructure (PKI)'' model. Each message is attached with a digital signature which can only be decrypted by the intended receiver.

Logeshwari and Logeshwari [57] explained the limitation of GPS on some crucial places and situation, and hence, other localization system becomes important. To implement other localization positioning methods like time of arrival and received signal strength, the nodes need to increase their distance ranging capabilities. Their scheme attempts to validate different localization techniques by implementing an algorithm as a pre requisite. The algorithm works in three phases. Node localizability is done by choosing unique nodes and finding their global locations. Rest all other nodes find their locations with respect to the Euclidean distance from the unique nodes. Second phase is to analyse the structure by having a response from all the nodes regarding their interactions with other nodes. Last phase is the network adjustment phase where some nodes are placed in the network according to their global positions, while others are added according to the Euclidean distance from the known nodes. The ''greedy parameter stateless routing'' is used that uses the position of the routers and the packets ultimate destination to find the routes while the network is being scaled.

Kou *et al.* [58] overcame the problem that occurs due to selfish nodes in an IoV network. They applied a detect and punish selfishness algorithm that compels the nodes to function according to the network. It not only increases the performance of the nodes, but also the nodes' network performance overall. Their scheme implements watchdogs and ''Ad Hoc On-Demand Distance Vector (AODV)'' protocol [59] on the basis of the reputation calculation. Signal to noise ratio of all the nodes helps the detecting node to find selfish nodes. Creditworthiness or reputation value of each node is also calculated based on the nodes helping hand in transmitting data using probability. The last step of the algorithm is to give the node a punishment that forces it to actively participate in transmitting data in the network. This punishment is only given to the nodes with less desired reputation value.

Sandou *et al.* [60] used an opportunistic adaptive neighbour selection (OANS) along with vehicular localization protocol to choose the best route for transmitting messages. Each vehicle checks the density of the in-range vehicle by broadcasting a message. For all slow moving vehicles moving towards the destination are selected and the message is sent using a nearby road-side unit (RSU). RSU also updates the neighboring node in its table according to the distance, the mobility of the considered node, and the neighbouring node from the source node. Finally, after the selection of the node a link state is formed and updated along with its acknowledgement being sent.

F. PRIVACY PRESERVATION

If an attacker gets some private information, the conditional privacy forms the actual basis of the security requirement in IoV network. In order to maintain the privacy, an unacknowledged digital signature scheme is implemented to find a temporary identity of a user which has no straight relationship with the actual identity. An unauthorized person can never know the sender's identifier even when he/she is exposed to its digital signature. A group based digital signature is used in which the members of a group can sign a message using a group public key, and hence, making it difficult to find the genuine sender of the message amongst the group. Another privacy preserving method depicted is based on anonymous identity being provided to the users for a prepaid time validity, thereby maintain conditional privacy. The false identities can be loaded in the tampered device of the vehicles in a fixed timed round robin fashion and renewed every time with a new identity before the initiation of a communication process. Another method could be installing all the identity certificates at once initially. The later method has a high storage latency. To avoid overheads the vehicles can request the nearest RSU for a pseudo identity. RSU maintaining the grace of conditional privacy sends the same pseudo identity to more than one device by utilizing bandwidth of the network with different symmetric keys. Lately, the vehicles use short signature scheme to generate their own signature pseudonyms using the tokens received after authenticating themselves to RSU [10]. All the methods have the same backbone of changing the pseudonyms randomly within short interval of times. Every vehicle when in idle state or in optimum condition with respect to traffic, congestion or neighbor state performs the replacement of pseudonyms for the next round of communication.

Hwang *et al.* [61] proposed an identity based privacy preserving authentication scheme that not only provides confidentiality, but also authentication, non-repudiation and traceability. Rajput *et al.* [62] used a hierarchy of pseudonyms based on their time period. Their protocol decides the use of the pseudonym based on the lifetime. Each vehicle uses longer lifetime pseudonyms to communicate with the trusted authorities and the shorter lifetime pseudonyms are used to communicate with the fellow vehicles.

Cui *et al.* [63] gave a solution to preserve privacy using k-anonymity, virtual location and path confusion. Any user cannot differentiate the information from the other users in the same message request. In-spite of using a real time

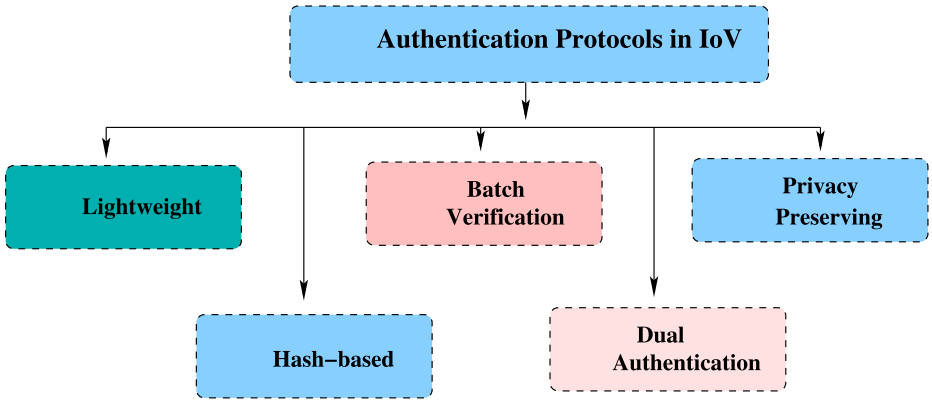

FIGURE 4. A taxonomy of authentication mechanisms in IoV environment.

location based service, their scheme controls the access of the location information; thus, it maintains the privacy. Each vehicle sends two requests to location based server (LBS) using its own location through GPS and using a location of a near by virtual vehicle obtained through the ''Dedicated Short Range Communication (DSRC)'' protocol [64]. A vehicle chooses the virtual vehicle that has the most common route. They termed it as shadow. The difference in the location and the routes of the vehicle, and the shadow vehicle is minimum. Both the request messages have same pseudonym identities and timestamps, but different yet similar locations. The server responses for both the request messages. So, one waste reply message is discarded by the vehicle and other involving its own location is used.

Zhu *et al.* [65] cleverly used the bond between humans and the mobiles along with OBU of vehicles to form a ''Social Internet of Vehicles (SIoV)'', where vehicles are also socially interacting with the entities. Their scheme is based on communities which are formed by a group of people having same interest. Their scheme forwards messages, but keeps the interest of the people private. Cars, buses and people walking around are considered as nodes which have only one interest and are registered from the trusted authorities. The delivery of the messages depends on the community energy of the nodes which is determined by the same shared interests of the nodes within the community or inter community. Each node selects the best forwarder of the message by looking at the community energy per node. Every time the community energy changes the decisional forwarder also changes. Buffer management is also considered by them as the nodes are limited by the resources.

Vijayalakshmi and Sasikumar [66] presented an identity-based privacy preserving method which uses asymmetric cryptography for communication. Their scheme is accomplished through two suggested algorithms: ''Identity-Based Signature (IBS)'' that is applied between vehicles to RSU or RSU to vehicles authentication, and ''ID-Based Online/Offline Signature (IBOOS)'' which is applied for vehicle to vehicle communication and authentication. Digital signature also marks the mode of authentication.

VII. EXISTING AUTHENTICATIONS PROTOCOLS IN IoV ENVIRONMENTS

The primary focus of this survey paper as stated before is on authentication in IoV environment. We consider the recent authentication techniques and categorized them on the basis of their mechanisms and algorithms into five types as illustrated in Fig. 4: a) light-weight authentication, b) hash-based authentication, c) batch verification-based authentication, d) dual authentication, and e) privacy-preserving authentication.

A. LIGHT-WEIGHT AUTHENTICATION

Vasudev and Das [67] described a model that is a two-tier structure and it has a trusted vehicle server with exceptional storage and computational capabilities in the upper layer and vehicles as the part of bottom layer. Their protocol proceeds with a setup phase followed by registration and authentication phases that go hand in hand, and finally it enabling Vehicle-to-Vehicle (V2V) communication. The setup phase lets the vehicle server to generate a key and every vehicle will register themselves on coming on the road and receive some values from the server. The received values are then reviewed for authenticity during the second phase, wherein the vehicles individually prove their identities. The vehicles entering into the third phase are the ones which have gone through the second phase positively. Request, reply and time stamp values help in the communication phase between the vehicles performed through insecure channel. Their protocol is also proved to be secure against impersonation attack by the fact that the malicious vehicles are unable to generate request messages as it involves passing through the second mandatory phase, and also against data modification, replay attacks and password guessing attack. Moreover, this light-weight protocol provides benefits in battery usage, communication overhead, implementation cost and computation time.

Bao *et al.* [69] proposed an authentication scheme which mainly focused quick messages authentication, integrity, and non-repudiation along with denial of service attack using bloom filters which are one of the best data structures when it comes to fast storage and retrieval management. Timed Efficient Stream Loss-tolerant Authentication (TESLA) [71] formed the back bone of their scheme that initiates with a symmetric cryptography which in time becomes asymmetric cryptography by sharing keys using one-way function through CAs in order to avoid retransmission and DoS attacks. The other modules being RSUs that are placed globally and OBUs placed inside the vehicles. RSUs are responsible for the rapid change of the vehicles pseudonyms in fixed time slots ensuring privacy. The vehicles are grouped according to their similar characteristics like speed and location (surrounding) and given a same timestamp value to exchange pseudonyms in order to confuse the attacker. The authentication of the vehicles is verified against the ''Bloom Filter (BF)'' value which is calculated by RSU on receiving keys from all the vehicles on road and the private key of the fellow vehicles. The new vehicle initiating a communication would request a BF value from the corresponding RSU and key from existing companion vehicle. The encrypted packets consisting of key and BF is received which are signed by the private key of the vehicle and the RSU, respectively. The same BF value and key in both the packets sustain authenticity of the keys. The revocation step is performed by the CA on request generated by a vehicle on suspecting a malicious node. Their scheme is able to manage malicious nodes and it is also insecure against inside attacks, but it helps in reducing delay and latency.

Zhou *et al.* [70] presented another light weight authentication scheme which bans the compromise of the key. It has a ''Public Key Generation (PKG)'' algorithm which generates the set of keys for both vehicles and RSUs. On addition to this, it also provides vehicles with OBUs and ''Tampered Proof Devices (TPD)'', trusted parties and RSUs. Their scheme is based on elliptic curve cryptography (ECC) and hardness of the ''Elliptic Curve Discrete Logarithmic Problem (ECDLP)''. Their scheme authenticates in four phases as follows. The initialization phase allows the PKG to generate parameters of ECC, and computes the public keys of TPD and RSUs corresponding to their chosen secret keys. The second phase will let the vehicles to create their own secret keys using the public keys of OBU and TPD, identities of the agents involved and some randomized parameters. In the third phase, OBU sends the signature to the RSU for verification which is done in the last phase. RSU first discards the unauthenticated message based on the difference between the timestamp of the message and its current timestamp, and the verifies the received message against the new parameters by using hash functions. Their scheme is secure against various chosen plaintext attacks and forgery attack as its private key is of two parts: one part is with TPD and other is with the vehicle itself.

Wazid *et al.* [68] described an aggrandized version of light weight decentralized authentication and key agreement scheme. The vehicles that possess the same velocity form a cluster and the cluster head (CH) is chosen amongst the members of the cluster. The CH has the highest trust value as compared to the fellow members. The authentication is performed between vehicle to vehicle within the cluster (V2V); vehicle to CH (V2CH) and cluster head to the nearest RSU (CH2RSU). The agreement of the keys is only amongst the RSU involved. Similar to various light weight authentication schemes, this scheme is also divided into phases. The registration of RSU and the vehicles is performed in the first phase. The RSU is given an identity pseudo-identity (RID) by which it calculates time dependent identity (TID) and secret key is configured before its installation. The vehicle registration is done by the help of the TA after when the user of the vehicle chooses its ID, password and some random numbers. Finally, the processed information is stored in the OBU of every vehicle. The registration is followed by authentication phase which is again divided into sub-phases involving authentication between vehicles, vehicle to cluster head, and cluster head to RSU. The secret behind the scheme lies in the last simultaneous phase which allows vehicles to change their password periodically ensuring authentication. Their scheme allows any new road side unit to be deployed whenever it comes in the frame. It is also secure against replay attack, man in middle attack, password guessing attack and impersonation attack.

Sandou *et al.* [60] proposed a light weight authentication mechanism along with key agreement that uses opportunistic adaptive neighbor selection along with vehicle localization routing protocol. Their light-weight authentication guarantees lesser number of bits in keys by using one way hash function. It also implements public key cryptography to attain the security. The hashing function applied to the input generates the same length output which is impossible to invert. Any of the two keys could be used for encryption of the data while the corresponding is used for decryption. The system model for the scheme has trusted authorities, RSU, and vehicles. Their scheme starts with a setup phase which makes the TA responsible for generating credentials to be loaded in the cluster heads or RSUs or vehicles. The authors have used ''n^{th} degree truncated polynomial ring (NTRU)'' as a public key cryptosystem which although uses high key size and cipher text size, but it still provides better speed, and security while utilizing less memory as compared to other systems. NTRU has also got similar phases, like set up, key generation, encryption and decryption. Their scheme proves itself outstanding in terms of packet delivery ratio, overall latency, throughput and packet loss. It is also secure against attacks, like replay attack, man in the middle attack, stolen OBU attack and impersonation attack.

The summarized tabular description is presented in Table 3 to give a clear comparative view of the light weight authentication mechanisms in the IoV environment.

TABLE 3. Summary of characteristics of light weight authentication protocols.

Scheme	Year	Concept applied	Network model entities	Phases or steps	Benefits and limitations
Wazid *et al.* [69]	2017	* One way hash function and bit wise XOR operations	* Vehicles (V) * Cluster heads (CH) * RSUs application server and * Trusted authority	* Registration phase (road side unit registration, vehicle registration) * Authentication and key agreement phase, CH2RSU authentication and key agreement phase * RSU2RSU key establishment phase * Password updation phase	* Secure against replay attack, man in middle attack, password guessing attack, impersonation attack * Untraceable * Anonymous
Vasudev and Das [68]	2018	*Communication range *DSRC *Timestamp	*Two layers-vehicle server *Vehicles with OBUs installed	*Three phases *Initial set up *Registration *Authentication	*Secure against impersonation attack, data modification attack, replay attack and password guessing attack *Limited battery usage *Communication overhead *Implementation cost and time
Bao *et al.* [70]	2018	*TESLA and bloom filters	*Certificate authorities (CA) *Road side units (RSU) *OBUs vehicles	*Pseudonym initialization *Verifying authenticity *Revocation	*Provides authentication *integrity *non-repudiation *inside attacks with delay, latency and compromised key during quick messages
Jhou *et al.* [71]	2018	*Public key algorithm *Elliptic curve cryptography *Hardness of discrete logarithmic problem	*Public key generator (PKG) *RSU *Vehicles	*Initialisation *Key generation *Signing phase *Verification	*Secure against chosen plain text attack *Forgery with no key being compromised
Sandou *et al.* [61]	2018	*NTRU public cryptosystem *SHA *Secured routing	*TA *Cluster heads *RSU *OBU	*Set up phase *Key generation *Encryption, decryption	*Great packet delivery ratio *Decreased overall latency *Throughput and packet loss *Secure against replay attack, man in the middle attack, stolen OBU attack, impersonation attack and lack of anonymity

B. BATCH VERIFICATION-BASED AUTHENTICATION

A batch verification method optimizes an authentication protocol by performing the verification of the received signatures together in batches on verifying side. Table 4 presents the characteristics of the discussed batch verification protocols related to the IoV environment in this section.

Gayathri *et al.* [74] presented an authentication scheme which requires less computational overheads by avoiding the use of certificates and pairing techniques, and it is based on batch verification. The model of this scheme consists of four participating candidates. TA and KGC are the most trusted parties of the model which can never be attacked. All the RSUs and vehicles register themselves to the TA initially. Hence, the TAs only have the real identities. KGC is used to generate secret keys for the vehicles. RSUs fill the gap between the network model by a wired network with the TA and the KGC, and a wireless connection with the vehicles. RSU provides a pseudo identity to the vehicles every time when a vehicle come across. To reduce computation, a group of RSUs form an autonomous system by reducing multiple times allocation and updation of the pseudo identities to the moving vehicles. Lastly, each vehicle is given an OBU which communicates with RSU and other vehicles using temporal synchronization. Their scheme works in seven different steps. The first phase (initialization) issues key pair, public parameters, hash functions and a token to the vehicles. The second phase lets KGC outputs a partial private key on token as an input after checking the non-existence of the vehicle in the revocation list. In the third phase, the TA computes public/private key pair after receiving token and partial key generated in the second phase as an input. Then, the RSU generates a pseudo random identity by using token from the TA as an input in the fourth phase. The fifth stage is the phase where a vehicle signs a message by taking a message, private/public key pair, partial private key and the random identity to produce a signature. Before the communication starts, each vehicle verifies a signature using the same parameters and a timestamp value. Finally, the RSU verifies all the signatures in a single instance abiding by the batch verification policy. This scheme made the authentication secure against forgeability, traceability, anonymity and revocation.

Bayat *et al.* [72] considered a model with trust authorities, OBUs and RSUs. The TA being a fully trusted agent cannot be forged and compromised, and it is responsible for

TABLE 4. Summary of characteristics of batch verification authentication protocols.

Scheme	Year	Concept applied	Network model entities	Phases or steps	Benefits and limitations
Bayat *et al.* [73]	2014	*ECC *Bilinear pairing *Computational Diffie-Hellman problems	*TA *OBUs *RSUs	*Key generation and pre-distribution *Pseudo identity generation *Message signing *Message verification	*Authentication *Identity privacy preserving *Traceability *Impact of velocity changes *Position based verification
Jiang *et al.* [74]	2016	*Hash chains *Bilinear pairing *Elliptic curve discrete logarithmic problem (ECDLP) *Computational Diffie-Hellman problem	*TA *RSUs *OBUs	*System initialization *RSUs certificate issuing *Vehicles pseudonyms *Private keys generation *Mutual authentication *Secure group key distribution *Group key periodic update	*Authentication *Non-repudiation *Identity revocation *Backward privacy *Integrity *Conditional anonymity *Resistance to colluding attacks * Less overhead
Gayathri *et al.* [75]	2018	*Digital signature *Elliptic curve discrete logarithm problem (ECDLP)	*TA *KGC (Key Generation Center) *RSU *OBU	*System initialization *Partial key generation *Vehicle key generation *Pseudo identity generation *Signature generation *Signature verification *Batch verification	*Authentication *Integrity *Revocation *Anonymity *Traceability *Non-repudiation with reduced transmission overheads *Less computational cost
Celes *et al.* [76]	2018	*Position verification	*GPS *Sensors	*A seven-step algorithm	*Falsified information *Identification of bogus nodes *No false threat

registering RSUs and OBUs of the corresponding vehicle with the information, such as keys, computing parameters and identity related parameters. All the information necessary to be communicated like distance of the vehicle, position, speed and location is performed by OBUs, which is used by other participating vehicles or RSUs. Their scheme has assigned the work of verification to the on place trusted RSUs. This scheme involves the concept of elliptic curves, bilinear pairing and computational Diffie Helman problem. Their scheme is accomplished in three phases, which are distribution of the key and other parameters in the first phase, signing the message for authenticity in the second phase, and verification of the message in the last phase. The generation of the keys are done out of a cyclic group and some random numbers denoted as master keys used in calculating two public keys and public parameters which along with real identities and passwords are installed in the vehicles and RSU before the communication starts. The second phase uses the identity and password to execute the process of computing pseudo identity. The tampered proof device calculates pseudo identity by verifying the submitted ID and password, and applying map to point hash function outputs two pseudo identities and secret keys that a vehicle uses the ID and key to sign the message, and then sends the message, signature, timestamp and pseudo identity along with the current timestamp to the nearest RSU or the vehicle. The receiver side of the message first validates the message based on the current timestamp and the received timestamp. RSU then performs batch verification on the received messages. The batch verification is then performed. Message integrity is maintained by using secret values which are unknown to an adversary. The real identity is also safe guarded because every time the vehicle uses its pseudo identity ID to initiate the communication and tracing the original sender of the message, and for the existence of the malicious vehicle by the TA knowledge of RID is also the part of this scheme.

Jiang *et al.* [73] introduced an anonymous batch authentication scheme (ABAH) which uses the ''Certificate Revocation List (CRL)'' to verify the signatures and revoke, which was more of an overhead burden and latency, and transmission delay on the network. Hence, this scheme is efficient because it uses batch method and ''Hashed Message Authentication Code (HMAC)'' on the messages to avoid heavy packets. The TA being the first uncompromised unit is the centralized unit which divides the network into different zones. The TA passes each zone's information to the inter-zonal RSU unit through a tunnelling wired channel and to OBUs of the vehicles through unreliable wireless connection. RSU bridges the gap between TA and vehicles by providing all relevant services. OBU along with tamper-proof

TABLE 5. Summary of characteristics of privacy preserving authentication protocols.

Scheme	Year	Concept applied	Network model entities	Phases or steps	Benefits and limitations
He *et al.* [77]	2015	*Elliptic curve cryptography *Diffie-Hellman computational problem *Schnorr signature *Timestamps	*TA *RSU * AS	*System initialization phase *Anonymous identity generation *Message signing phase *Message verification phase	*Authentication *Identity privacy preserving *Traceability and unlinkability *Secure against impersonation, modification, stolen verifier and man in middle attack *Low computational cost
Islam *et al.* [78]	2017	*Hash function *Group key agreement *Passwords	*TA *RSU *OBU *Vehicles	*System initialization phase *RSU registration phase *Vehicle registration phase *Authentication message generation phase *Authentication message verification phase *Group-key generation phase *Vehicle leaving phase *Vehicle joining phase *Vehicle password change phase	*Identity maintenance *Authentication *Forward and backward secrecy *Secure against replay attack, impersonation attack, modification attack and offline password guessing attack
Vijaykumar *et al.* [79]	2017	*Bilinear pairing *Hash function	*TA *RSU *OBU in vehicles	*Setup phase *Registration phase *Anonymous mutual authentication phase	*Secure from impersonation attack and man in the middle attack *User authentication, non-repudiation and conditional privacy

device (TPD) pass relevant traffic, road, environment or passenger information to let the vehicles and customers enjoy services from the TA. Batch authentication in their scheme is implemented when the concurrent requests are sent to RSUs from multiple vehicles and when many vehicles send messages updates or status to the same vehicle. Their scheme uses hash chaining, bilinear pairing annd ECC techniques.

Celes and Elizabeth [75] opposed a new attack known as *bogus* attack by using position verification method. Their scheme commences by detecting the false position information being spread by false nodes, and thus, it reduces the bogus attack. The position based process has either a greedy approach or it applies GPS to mutate the position with the fellow vehicles. The heart of their scheme lies on an algorithm which starts by each node by sending a packet to RSU. The verifier after verifying the packet instructs the vehicle by letting it to accept or reject the message based on the truth value residing in the message.

C. PRIVACY PRESERVING-BASED AUTHENTICATION

The privacy of the users have always been the foremost priority of the researchers. Hence, the authentication schemes need to be designed in the IoV environment that should preserve the privacy of the users along with providing authentication. Table 5 shows some of the state-of-art authentication schemes based on privacy preserving mechanism.

Keeping the complexity of bilinear pairing into consideration, He *et al.* [76] designed a scheme which uses only ECC with an additive group avoiding scalar multiplications using the Diffie -Hellman computational problems hardness. To make the scheme a bit more efficient, they used batch verification at the end. The system model for their scheme is a two-tier model, which has the TA and the Application Server (AS) in the first layer. The second layer comprises of RSUs and vehicles. The TA as always the trusted party meant for pre loading and verifying the other agents. The AS communicates basically with RSUs to help with application. RSU present in the second layer monitors the locally indulged vehicles to receive and validate their messages bridging the gap with the TA. OBUs present in the vehicles hide all the information and lets the vehicles connect with other agents through a wireless network. Their scheme shows its resistance to attacks like replay attack, impersonation attack and modification attack. Message authentication, identity preserving, traceability and unlinkability are all taken care by their design. Their scheme got its base from the Schnorr signature scheme. Three phases in their scheme accomplishes the complete task. The first phase begins with system initializing of various parameters, such as elliptic curve parameters, prime numbers and random numbers. The TA in this phase sends all the public parameters to RSU and vehicles. The second phase involves generation of anonymous identity.

Message signing is also a part of this phase which finally broadcasts a meesage. The last phase is message verification phase which is performed by verifying single message or even by using batch verification. The freshness of the message is checked through the timestamp values before the verification occurs.

Maximum protocols that preserve the identity conditionally either face overheads due to the presence of certificate authorities or they are time consuming when they are based on identity management. Islam *et al.* [77] proposed a password based conditional privacy preserving authentication and group key generation protocol which requires less memory usage of the TA. Their protocol even took care of a user joining or leaving a network and provided password updating facility. It assumes that a vehicle will be only communicating to the vehicles in the same RSU region using a group key, and thus, it avoids collusion attack. The protocol uses hash function instead of elliptic curve or bilinear pairings. The system model consists of the TA, vehicles and RSU. All the vehicles are installed with on OBU devices which are tampered free and have some memory which is utilized during authentication message generation and verification phases. Their scheme undergoes the system initialization phase, and RSU registration phase which registers RSUs by receiving some network information from them and allotting them with identities and secret keys for communicating in the network. In vehicle registration phase, all the important credentials are installed in OBU and are handed over to the vehicles through a secure medium. Authentication message generation phase is performed by OBU of all vehicles that generates an MAC and an anonymous identity for their corresponding vehicle which is sent to the TA. The TA verifies the received MAC in authentication message verification phase. Group-key generation phase generates a group key for all the vehicles of a particular region and is updated during the exit and entry of the vehicle to maintain forward and backward secrecy. Vehicle leaving phase, vehicle joining phase, and vehicle password change phase are also asset to the scheme making it flexible for real time application. The scheme maintains the identity, and provides authentication, forward and backward secrecy, and it is also secure against replay, impersonation, modification and offline password guessing attacks.

Vijayakumar *et al.* [78] proposed a conditionally privacy preserving scheme for IoV network along with providing a group key agreement and distribution protocol for the vehicles to broadcast their location information. Their scheme mutually authenticates the vehicles simultaneously by maintaining integrity and privacy aspects. The tracking of the malicious vehicles marks the essence to their scheme. Their scheme is implemented on a system model with three entities. The TA indulged with firewalls being a part of a public cloud becomes the most powerful computational entity in the real-time scenario. The mobile vehicles being the second entities are registered to the TA before becoming the communicating to any other entity in the network. The TA also helps RSUs in key generation and distribution phase, and hence, it is connected to RSU which is the third entity in the model. The RSUs are placed all over the network each in every domain. RSUs form the connection between the vehicle and the corresponding TA of the same domain. When the vehicle moves from one domain to another, the credentials are also passed to the TA of the current domain from the previous one. Each vehicle is provided with OBU that is tampered free to save public/private keys of the vehicles. Their scheme is executed in three phases: starting from an initialization phase where the TA chooses hash function, its public and master key, and computes public parameters that are exposed on the network. This is followed by a registration phase in which the vehicles register themselves to the TA. The third step of their scheme helps the vehicles to prove their legitimate existence to each other through anonymous identity hiding the real identity. The vehicles communicate using short term valid certificates to prove or verify the identities of each other mutually. Their scheme in spite of using anonymous identity throughout the process can even find the real identity in case of tracking a malicious attacker in the network. This scheme proves itself secure from impersonation attack and man-in-the middle attack, and it also provides user authentication, non-repudiation and conditional privacy.

D. DUAL AUTHENTICATION

Some protocols fulfil the demand by providing a dual authentication mode. Table 6 presents several characteristics of analyzed dual authentication protocols in this section.

Liu *et al.* [80] prescribed a modified ''Trusted Platform Module (TPM)'' approach that equips a root that provides integrity assessment report containing the confidential information. It avoids all sorts of issues related to distribution and management of keys. Their approach increases the security by its bifold phases of authentication involving authentication protocol along with ID based asymmetric encryption. It does not use the real identity of the vehicles, thus ensuring the permanent identity to be saved. Their scheme has three layered architecture with bottom layer consisting of vehicles with OBU. The three layers have interaction amongst themselves with RSUs (middle layer) and the TA (top layer) having wired connection. The session key is provided to the requesting vehicle by RSU after having its identity and reputation verified through the TA. The process is described in five phases: the first phase is for RSU registration, and the second phase is for vehicles registration. Third phase issues the validity of the users during their login, fourth phase monitors the authentication and the secure communication, with the last phase updating the new parameters of password and trust parameters. The first phase is progressed in two steps: step 1 initializes the whole system with the TA calculating the private master key and public parameters and step 2 allows the TA to establish public and private keys for all RSUs. The second phase accomplishes the registration of vehicle with the TA. It also calculates some parameters used in login phase and saves in the local database for further verification. The third phase takes the password and ID of a user as credentials and

TABLE 6. Summary of characteristics of dual authentication protocols.

Scheme	Year	Concept applied	Network model entities	Phases or steps	Benefits and limitations
Vijaykumar *et al.* [80]	2015	*Fuzzy inference *Biometrics *Hash function *Chinese remainder theorem	*TA *RSUs *OBUs equipped with fuzzy inference *Two cryptographic units *Decision making agent *Sensors *Event data recorder *Data collection unit *Spatial temporal reasoning unit	*Vehicles registration phase *Two authentication phases (vehicles authentication phase, TAs authentication phase)	*Secure against sybil attacks, masquerade, replay attacks, fabrication, alteration message tempering and collusion attack *Forward and backward secrecy *Low cost
Liu *et al.* [81]	2017	*Bilinear mapping *Trusted computing technology *Node repudiation evaluation	*Three layers–bottom layer (vehicles with OBU), second layer with RSUs and top layer with TA	*System initialization phase *User registration phase *User login phase *Vehicle authentication phase including session key agreement *Trust degree update phase	* Secure against man in middle, replay and password guessing attacks *Enhanced anonymity and computational cost
Lalli *et al.* [82]	2017	*Elliptic curve digital signatures *TESLA *Time frames *Beacons	*Vehicles	*Generate chained keys *Trace position *Merkle hash tree construction *Signature verification	*DoS attack *No packet loss *Increased delivery ratio *High throughput

calculates its correction by comparing it with the parameters stored in the database during the second phase by the TA. The third phase is a four-step process. Step 1 allows the vehicles to requests RSU by creating an anonymous identity to initiate a session with peer vehicles. The RSU sends the details to the TA for them to verify the actual and the created identity. Step 3 helps the TA to verify and send the session key which is delivered to the vehicles in the next step through RSU. The last phase is to keep the system progressing by rejuvenating the new values of password and trust.

Vijaykumar *et al.* [79] explained a scheme which performs dual authentication and does not allow any malicious nodes to enter the network. Authentication is followed by the multicasting of the message from the TA to all the authenticated vehicles. The multicasting of the message requires a key which is calculated by using the ''Chinese Remainder Theorem (CRT)''. Regular updation of the key is done by easy addition or subtraction method that confirms forward and backward secrecy in lesser cost. The system model is similar to as used by previous protocols. The TA is for registering RSUs and vehicles, and for transferring data; RSU is at every area filling up the communicational gap between the vehicles and TA, OBUs on each vehicle which have several components like fuzzy inference, cryptographic units, decision making agent, sensors, event data recorder, data collection unit and spatio temporal reasoning unit. The data is collected from several sources by data collection unit and used as an input to the components of RSUs to give a decision using fuzzy inference agent. The spatio temporal deals in decision making based on speed, time and road condition. The authors have modified system model by setting up a TA in every state such that a vehicle entering into a new state is initially verified by the TA of that state. It is a dual authentication method as the authentication is done twice: the first one if on TA side by using a hash function on the vehicle secret keys (VSK) and other is on vehicle's side by using biometrics or password. So even if the secret information of the user is hacked, still the attacker would not be able to attain the finger print of the user. Hence, it resists an attacker to enter into the network even if the credentials are compromised. Their scheme starts with registration phase which can be done online or offline mode with the TA choosing two prime numbers: one is for defining the group and other is for group key. Each user provides his/her credentials along with the finger print to the TA. VSK using hashing and the finger print is used for authentication process. The end of registration phase provides vehicles with VSK loaded into it. The second phase which follows the registration phase is vehicle's authentication process. Whenever a communication has to be initiated from any vehicle, the user of that vehicle validates itself by its fingerprint against the finger print that is already saved in the TPD in vehicles. The positive validation will allow the vehicles to communicate with rest of the vehicles and TA. Next is the dual authentication's second authentication phase which

TABLE 7. Summary of characteristics of hash based authentication protocols.

Scheme	Year	Concept applied	Network model entities	Phases or steps	Benefits and limitations
Cui *et al.* [64]	2018	*Cryptographic hash function *CRT	*TA *RSU *OBU	*System initialization phase *RSU registration phase *Vehicle registration phase *Authentication message generation phase *Authentication message verification phase *Group-key generation phase *Vehicle joining phase *Vehicle leaving phase	*Preserving privacy *Traceability *Authentication of the messages *Integrity *Un-linkability *Secure against replay attack, impersonation attack, modification attack *Forward and backward secrecy
Xiaodong *et al.* [84]	2018	*Bilinear pairing *Trapdoor hash function *Proxy re signature	*TA *RSU *OBU	*System initialization phase *Key generation phase *Registration phase *Resigning key generation phase *First vehicle communication *Subsequent communication *Verification of signature *Traceability of vehicle	*Unforgeable *Privacy preservation *Traceability

is trusted authority authentication process and provision of authenticated codes which includes the vehicle to select a random number applying multiple hashing to it and sending the hash code, the identities of vehicles and TA, timestamp to RSU which is then forwarded to the TA by RSU after appending its ID to the packet. The TA then verifies the ID and authenticates the user of the vehicle by matching the hashed code and producing the authenticated code which is sent in response to vehicle. Their scheme is secure against Sybil attacks, masquerade, replay, fabrication, alteration message tempering and collusion attacks. In addition, their proposal also maintains forward and backward secrecy.

Lalli and Graphy [81] proposed a dual authentication scheme for VANETs that supports the group management of the keys. This scheme turned out to be secure against DoS attack. It provided resilience against packet loss in V2V communication. Their scheme provides effective authentication which is scalable enough for practical implementation. Non-repudiation is also solved by this scheme. Their scheme is based on ''elliptic curve digital signature algorithm (ECDSA)'' [82] and TESLA. Their scheme divides the timeline into frames and into beacons. The receiving vehicle will verify the received signature by utilizing less cost and storage space using TESLA. Each vehicle will self-visualize their position with respect to the position vector, and distance vectors in corresponding beacons with respect to other vehicles. Throughput, end-to-end delay, and packet delivery ratio showed a drastic improvement as compared to other position based themes.

E. HASHCHAIN-BASED AUTHENTICATION

Hash chain based method is the mechanism that is applied to provide authentication with less computational overheads. Table 7 provides various characteristics of the hash-based authentication protocols in the IoV environment.

Cui *et al.* [63] exhibited a proposition of a conditional privacy safeguarding by using a hash function. The majority of protocols use bilinear pairing or elliptic curves, but this protocol becomes the cost efficient of all protocols by using simple hash functions. The validity of a vehicle is certified by the TA indirectly through RSU as a bridge in between. Their scheme undergoes the confidentiality mechanism through group key agreement by using the CRT. Each authentic vehicle is provided with a shared key which is further used by all the vehicles. The syntactic truth lies in the fact the key can be changed when a vehicle enters or leaves. The system model again consists of three units. TA is responsible for verifying credentials. It is the only part of the system that has the real identity of the vehicle. An RSU which works on DSRC here is looked after by the TA as it can be attacked by an attacker. The VANETs support V2V which could be done directly between the vehicles or between the vehicles through RSU or by the combination of both the strategies. OBUs of the vehicles deal with communicating a vehicle with other vehicles or RSUs. Their scheme deals with vehicles communicating with each other without using RSUs. Their scheme also wins over the issues like preserving privacy though the TA is able to trace the vehicle, detection of the malicious nodes, authenticity of the messages, integrity of message by applying simple cryptographic science using a shared group key no link between two messages, maintenance of forward and backward secrecy by using group key, replay attack, impersonation attack and modification attacks.

Xiaodong *et al.* [83] proposed a scheme by using trap-door function to authenticate the messages involving less computation overhead. Their scheme includes bilinear pairing and proxy signature. The system model used in their scheme consists of three entities. The TA is responsible for authentication, registration and traceability. The RSUs are constructed on the side of the roads responsible for forwarding the

messages from vehicles. This also helps the TA in tracing an identity. Their scheme is performed in various phases. The first phase is the initialization phase in which the system chooses the trapdoor hash function, collision resistant hash function, two groups and other parameters involved in bilinear pairing. The generation of key is the second phase in which OBU and RSU select their private keys and find the corresponding public keys to have their key pair. Third phase is the registration of the vehicles followed by the re-signing key generation which transforms the message signature of the OBU into the signature of the TA. After the set up, a vehicle is allowed to start its first communication by sending a message to another through RSU as a mediator. Verification of the message signature marks the next phase followed by traceability if required. Their scheme is unforgeable and untraceable, and it also maintains privacy.

VIII. PERFORMANCE COMPARISON OF AUTHENTICATION PROTOCOLS IN IoV ENVIRONMENT

This section evaluates the performance of discussed authentication protocols in Section VII in terms of computation and communication overheads.

The description of the notations used for various cryptographic operations in comparison of computational costs is shown in Table 8. We consider that the estimated computation time needed for T_{ecm}, T_{eca}, T_{mtp}, T_{bp}, T_{exp}, T_h and $T_{enc/dec}$ as 17.10 ms [84], 4.40 ms [85], 44.06 ms [76], 42.11 ms, 19.20 ms [84], 0.32 ms [85] and 0.32 ms, respectively (assuming $T_{enc/dec} \approx T_h$). We ignore the time to compute modular multiplication over a finite field as that is negligible in nature.

TABLE 8. Notations and computation costs.

Notation	Time needed for	Approximate time
T_{ecm}	Elliptic curve point multiplication	17.10 ms
T_{eca}	Elliptic curve point addition	4.40 ms
T_{mtp}	Map-to-point operation	44.06 ms
T_{bp}	Bilinear pairing	42.11 ms
T_h	One-way hash function	0.32 ms
T_{exp}	Modular exponentiation	19.20 ms
$T_{enc/dec}$	Symmetric encryption/decryption	0.32 ms

The communication overheads of all the discussed authentication schemes are evaluated which involve the number of messages and the number of bits of the transmitted messages. It is assumed that the one-way cryptographic hash function (using SHA-1 hashing algorithm [86]) produces an output of 160-bit hash value. Since 160-bit elliptic curve cryptography (ECC) provides same security as that of 1024-bit RSA [43], it is considered 160-bit ECC for communication and computation comparisons of the authentication schemes. With this consideration on ECC, the communication overhead to transmit an elliptic curve point $P = (P_x, P_y)$ is of $(160 + 160) = 320$ bits, where P_x and P_y are the x and y co-ordinates of the point P, respectively. It is also assumed that the vehicle's real identity, random nonce and timestamp

TABLE 9. Message fields and their sizes in bits used in comparison of communication costs.

Description	Size (in bits)
Message digest (hash value)	160
Elliptic curve point	320
Random or pseudo identity	160
Timestamp	32
Random nonce	128
AES plaintext/ciphertext block	128
Message length	160

TABLE 10. Comparative computational costs analysis of light-weight authentication schemes.

Scheme	Total cost	Estimated time (in milliseconds)
Wazid *et al.* [48]	$24T_h$	$\approx$ 7.68 ms
Vasudev and Das [68]	$4T_h + 2T_{enc/dec}$	$\approx$ 1.92 ms
Jhou *et al.* [71]	$8T_h + 10T_{ecm} + 2T_{eca}$	$\approx$ 182.36 ms

TABLE 11. Comparative communication costs analysis of light-weight authentication schemes.

Scheme	Number of messages	Number of bits
Wazid *et al.* [48]	3	896
Vasudev and Das [68]	2	800
Jhou *et al.* [71]	1	992

TABLE 12. Comparative computation costs analysis of batch verification-based authentication schemes.

Scheme	Total cost	Estimated time (in milliseconds)
Gayathri *et al.* [75]	$5T_h + 7T_{ecm} + 3T_{eca}$	$\approx$ 134.5 ms
Jiang *et al.* [74]	$5T_h + 7T_{ecm} + 2T_{eca}$ $+3T_{bp} + T_{enc/dec}$	$\approx$ 256.75 ms
Bayat *et al.* [73]	$2T_{ecm} + T_{eca} + T_{mtp}$ $+3T_{bp} + 2T_h$	$\approx$ 209.63 ms

TABLE 13. Comparative communication costs analysis of batch verification-based authentication schemes.

Scheme	Number of messages	Number of bits
Gayathri *et al.* [75]	1	960 $960n^*$
Jiang *et al.* [74]	2	$1952 + 256t$
Bayat *et al.* [73]	1	512 $512n^*$

Note: *: batch verification of n messages; t: degree of a bivariate polynomial used in Jiang *et al.*'s scheme [74]

are of 160-bit, 128-bit and 32-bit, respectively. For symmetric key encryption/decryption, the Advanced Encryption Standard (AES-128) has been used [87].

In Tables 10 and 11, we have compared the computation and communication costs of the light-weight authentication schemes of Wazid *et al.* [47], Vasudev and Das [67], and Jhou *et al.* [70]. Out of the compared schemes, Jhou *et al.*'s scheme [70] needs more communication and comptational costs as compared to other light-weight schemes.

In Tables 12 and 13, the computation and communication costs of the batch verification-based authentication schemes of Gayathri *et al.* [74], Jiang *et al.* [73], and Bayat *et al.* [72] are compared. It is seen that Jiang *et al.*'s scheme [73] demands more computation cost as compared to other

TABLE 14. Comparative computation costs analysis of privacy preserving authentication schemes.

Scheme	Total cost	Estimated time (in milliseconds)
Islam *et al.* [78]	$10T_h$	$\approx$ 3.2 ms
Vijaykumar *et al.* [79]	$10T_{exp} + 3T_h + 2T_{bp}$	$\approx$ 277.18 ms
He *et al.* [77]	$6T_{ecm} + 2T_{eca} + 3T_h$	$\approx$ 112.36 ms

TABLE 15. Comparative communication costs analysis of privacy preserving authentication schemes.

Scheme	Number of messages	Number of bits
Islam *et al.* [78]	2	1632
Vijaykumar *et al.* [79]	1	7488
He *et al.* [77]	2	1824

compared schemes, whereas Gayathri *et al.*'s scheme [74] needs more communication cost as compared to other schemes where n is the number of messages in batch verification.

Table 14 shows comparative analysis on computation costs among the privacy preserving authentication schemes of Islam *et al.* [77], Vijaykumar *et al.* [78] and He *et al.* [76]. It is observed that the scheme designed by Vijaykumar *et al.* [78] demands more computation cost as compared to two other schemes. The comparison of communication costs among the schemes of Islam *et al.* [77], Vijaykumar *et al.* [78] and He *et al.* [76] is also provided in Table 15. From the results listed in this table, it is seen that Vijaykumar *et al.*'s scheme [78] also demands more communication cost as compared to two other schemes.

TABLE 16. Comparative computation costs analysis of hash based authentication schemes.

Scheme	Total cost	Estimated time (in milliseconds)
Cui *et al.* [64]	$5T_h$	$\approx$ 1.60 ms
Xiadong *et al.* [84]	$2T_h + 8T_{exp} + 5T_{bp}$	$\approx$ 364.79 ms

TABLE 17. Comparative communication costs analysis of hash based authentication schemes.

Scheme	Number of messages	Number of bits
Cui *et al.* [64]	2	1312
Xiadong *et al.* [84]	4	4992

In Tables 16 and 17, the comparative analysis on computation and communication costs for the schemes of Cui *et al.* [63] and Xiadong *et al.* [83] is shown. From the analysis, it is worth noticing that the scheme proposed by Xiadong *et al.* [83] more computation and communication costs as compared to those for the scheme of Cui *et al.* [63].

Finally, in Tables 18 and 19, the comparative analysis on computation and communication costs for the schemes of Liu *et al.* [80] and Vijaykumar *et al.* [79] is illustrated. From the analysis, it is observed that the scheme of Liu *et al.* [80] more computation and communication costs as compared to those for the scheme of Vijaykumar *et al.* [79].

TABLE 18. Comparative computation costs analysis of dual authentication schemes.

Scheme	Total cost	Estimated time (in milliseconds)
Liu *et al.* [81]	$9T_h + 3T_{exp} + 5T_{bp}$	$\approx$ 271.03 ms
Vijaykumar *et al.* [80]	$2T_h + 4T_{exp} + 6T_{enc/dec}$	$\approx$ 79.36 ms

TABLE 19. Comparative communication costs analysis of dual authentication schemes.

Scheme	Number of messages	Number of bits
Liu *et al.* [81]	1	8000
Vijaykumar *et al.* [80]	3	3168

IX. TESTBEDS AND THEIR EVOLUTIONS IN IoV DEPLOYMENT

Deployment of any implementation practically requires a lot of testing beforehand to avoid loss in terms of both time and money. Moreover, IoV and VANETs are extremely real time based applications that cannot afford to have mistakes or risks leading to danger situations. Various wireless simulators, like NS2, NS3 and vehicular movement simulators, like SUMO are used for simulation are still open to errors because of various factors like more number of simulating parameters make it prone to human errors, interference in signals and physical obstacles. So, when it comes to simulation of VANETs, there comes out a difference between the results during simulations and hardware implementation. Thus, this gap was bridged by creating testbeds or emulating hardware implementations along with simulating the environment. Moreover, these give opportunity to test the models against the appreciable number of nodes to get the real time results. These testbeds are prepared by excessive number of wireless devices which are non mobile placed indoors at a single place connected to some physical infrastructure. Hence, verifying the results of simulation against certain hardware implementation becomes necessary by considering various factors like vehicular density, packet size and relative speed of the vehicles [88]. Designing the testbeds turns out to be favourite research area for both academia and industry. The testbeds overcome the limitation of simulators by emulating hardware components [89], [90]. In addition, the testbeds give exact user's experience and feedbacks.

A. TESTBED REQUIREMENTS

Generally, a testbed should support the IEEE 802.11p protocol, larger packet size, more number of nodes at an instance, multihop topologies, and degraded and upgraded quality of links. Elaboration on the requirements is presented as follows [89]:

- *Configuration input*: The data from the sensors and smart devices is collected and is saved explicitly in the data type supported by the corresponding data structure

in the database, which makes inserting, deleting, searching of the data easier. This data type conversion is done by the data mapping layer, which is a part of the architecture. The input data is classified into four types: location and mobility of the vehicles and their surrounding neighbors are provided in the simplest form in terms of latitudes and longitudes as supported by the GPS services. The other important input that a testbed needs to store is the default configuration of the devices like their interfaces and sensors. Then, this configuration is matched with the corresponding device on the database.

- *Frame of reference*: Each application in a real time IoV depends on the situation and surrounding to provide the best services. IoV being a real time application depends mainly upon the surrounding sensed by sensors and other entities. This context is provided to the application either by users or some third party entity. Hence, the emulator should be able to create context by detection or manually.
- *Assimilation of hardware*: Hardware is an important part of an IoV Network. So, the validation of the network against bugs and errors should be done against all real time hardwares.
- *Platform independence*: The designed/implemented testbeds should be independent of the operating system. Moreover, the testbeds should be designed in such a way that they should be able to overcome the weaknesses of an operating system.
- *Transparency*: The transparency of a testbed makes the experience of a user while using a testbed or a real time hardware indistinguishable. A testbed should not modify the network parameters during the test.
- *Use of virtualization*: The testbeds should support the use of virtual machines in order to test the network under tough conditions.
- *Scalable to inventions*: A testbed should be developed in a such a way that even if it is made for a specific application, it can be scalable and abstracted towards the changes in technologies. The working of testbeds should not interfere with the internal specifications of protocols and stacks.
- *V2V link emulation*: The testbed should be able to identify the quality of link between the vehicles in order to make an improvement in jitter, delay, packet lost, drop and throughput.
- *Reputable and traceable*: A testbed is generally used to find the result of an application under real conditions. Hence, an experiment can be done multiple number of times on a single network using different parameters everytime. The result of every experiment should be traceable and recorded to understand the scope of improvement to enhance the quality of IoV.
- *Data source autonomy*: A testbed should give enough liberty to emulate any data source while testing. The test cases involved for experimenting a network should be easily computable and adaptable to the requirements.
- *Minimum overheads*: The working of a testbed should generate minimum overheads on the system in order to maintain the complexities.

B. EXISTING TESTBEDS AND THEIR DISCUSSIONS

Ahmed *et al.* [89] presented a testbed for real time VANETs application that is a layered architecture using various existing simulators and database sensors. The architecture is designed by adding some functionalities to the existing operating system (Android OS) along with timestamps for time synchronisation to have a real time result in addition to use of some virtual machines, hardwares and emulating devices. Android being an open source software makes scalability and customization for the developers a bit easier. The authors make the development of the testbed inter-operable by using Software Development Kit (SDK) along with Android Development Kit (ADT). Android X-86 project that imitates Android and runs in any X-86 architecture, making the user to run this on their system as a primary OS or in dual mode. An orthodox evergreen concept of database and "Structured Query Language (SQL)" are applied to save data of the testbed implementation. The architecture of their testbed is in three layers. First layer is the input layer, second layer is the core layer that consists of a database, and third layer is the client framework. The configuration data includes the IP of the server, polling intervals and the maximum amount of cache. An algorithm for location interpolation is also implemented. The result of the successful emulation of data is projected in the form of a graph depicting selected metric. The authors created a simple WiFi application that finds the strongest WiFi around and lets it connect makes the testbed allowing WiFi interface emulation. The testbed also supports point to point communication by using an application, called WiFi direct. To reduce the time taken in receiving, the emulated data caching is applied. The language of implementation is Java which makes it portable. The authors have used NS2 and SUMO simulators to validate their testbeds. Since IoV and VANETs are all smart applications, so wireless data must be included. This adds on flexibility, scalabilty, versatility to the testbed. This layered model can emulate sensor nodes, road topology, and also the parameters of wireless network, such as jitters, bandwidth, latency and packet loss.

Vandenberghe *et al.* [88] amended the already in the market **w-iLab.t** wireless testbed developed by iMinds (formerly known as IBBT) to use it for validating VANETs research. This testbed is suitable for wireless sensor and wireless mobile networks. It is a three-floor project in Ghent, Belgium. It can afford upto total of 200 easily configurable nodes with wireless cards in support with Intel x86. There is no inter floor communication amongst the nodes. The earlier configuration was not supporting the IEEE 802.11p standard, but the authors thought to install the Unex DCMA-86P2 mini-PCI card to support IEEE 802.11p standard. However, this would made the set up restrict to work only on the IEEE 802.11p standard. So, a new solution of implementing a standard relative to the IEEE 802.11p standard with

compromised bandwidth and radiated power is suggested. In order to support high density networks, the third floor of the testbed is surrogated by performing an experiment where all the nodes listen to broadcast messages and respond back to find the transmission domains of each node. A maximum transmission power of 23 dBm with transmission domain of nodes containing 75 approximate nodes was suggested to scale the existing testbed. The authors then interrupted the testbed to make it effective for multi-hop topologies. Based on the similar experiment, selecting some nodes from the grid distribution with transmission power of not more than 2 dBm was found to be appropriate. The last epitome that is delivered was emulating the movement of nodes by using MATLAB model that can simulate the physical layer and then is converted into link impairment techniques.

Amoroso *et al.* [90] designed a testbed to test the protocols and standards by waffling the number of hops that is traversed by a packet, the density and the channel conditions by keeping the number of nodes within the tesbed constant. The authors superimposed a virtual network by introducing relays in the vehicles and interferes. This testbed can be varied in terms of number of hops, channels and neighbors without changing the real number of vehicles. They performed an experiment to circulate an accident warning that involved only three real cars, but can be successfully used for testing real IoV network in any condition. This involved extracting unicast path between two nodes which is a part of multi-hop topology. The testbed is implemented using various items like intermediate relays that are responsible for creating a path for transferring information between two indirect connected vehicles, transmission events that are to indicate transmission events occurring after every relay and interferer that indicates the vehicles that transfer the information using the same path that is under study. At last, the implementation of experiment under more number of wireless channels requires mapping of the virtual hops and vehicles to real time vehicles. The testbed has no limit to number of hops in between the sender and the receiver, and hence it can be used to implement any real time scenario instead of limited resources under any physical channel conditions. The testbed can be effectively used for routing discovery phases, broadcast events, end-to-end exchanges at the transport layer, and peer-to-peer and opportunistic dissemination of information.

Afonso *et al.* [91] created a testbed for real time vehicular emulation and simulation that has 500 vehicles. They upgraded the tradition ''Control and Management Framework (OMF)'' that supports dynamic IP addresses for a cellular network and implements watch dog that lets the vehicles have connection every time they loose one. The combination of watchdog and ''Internet Control Message Protocol (ICMP)'' message is able to recover and bring out of failure. A node, which gets disconnected, sends an ICMP message to the aggregate manager and reboots itself if there is no response. This also maintains the state of the nodes and keeps informing to the users accordingly. The nodes are installed with dual boot system in which the operating system is divided into two halves: one half executes the normal operation, while the other half holds the result of the experiment. This helps the nodes always to recover the failures. This partition of nodes helps in copying disc image by creating a secure shell connection among the nodes. The disc from the updated partition is copied to the other partition. In order to reduce the size of disc so as to involve less time in transferring it, they used Buildroot which transfers only minimal configuration. The issue of the reduced bandwidth is solved by using IEEE 802.11p standard. They proved the flexibility and efficiency of the ''OMF Measurement Library (OML)'' by analysing real time ''User Datagram Protocol (UDP)'' send and receive messages on the testbed.

Gerla *et al.* [92] showcased a whole procedure of validating a vehicular model: first through an emulator and then through a real time testbed. The testbed for validation used is based on the campus testbed architecture, called C-VeT, deployed at University of California, Los Angeles (UCLA), which is a combination of VANET and wireless mesh network. The testbed provides both V2V and V2I communication as it allows the vehicles to freely loco-mote in the network. The campus consists of 30 well-equipped vehicles with C-VeT hardware and software facilities. It works on both Linux and Windows. The testbed consists of C-VeT mobile nodes with 2.5 GHz processor, a campus wide mesh network that provides internet access from the vehicles giving them a control channel, an emulator that helps to validate protocols and standards, a web interface that abstracts the implementation of the testbed and a database to store data which is made available to the researchers. An experiment corner was performed to check the accessibility around the corners was carried out that used two cars with a node installed with Linux OS, GPS server and IEEE 802.11p standard. One car was freely allowed to move around the corners and the other was fixed. The packet rate of 10 bps was fixed which was periodically broadcasted from the fixed node and successfully received by the other node. The simulating and real time result have a little difference due to interference caused. The other experiment was to compare two VANET routing protocols. The protocols ''Ad Hoc On-Demand Distance Vector (AODV)'' and ''Optimized Link State Routing Protocol (OLSR)'' were compared on the basis of topology changement, packet hop count and optimal shortest path.

Wu *et al.* [93] proposed a testbed used for evaluating ''Media Access Control (MAC)'' protocols under real time conditions. It is based on Xilinx Zynq-7015 SoC, Linux and ''Field-Programmable Gate Array (FPGA)'' as software and hardware combination based on off-the-shell Atheros AR9462 NIC where the FPGA handles high priority task while the Linux handles normal tasks. NICs are configured in a way that they can handle error free sending and receiving of the packets using some descriptors. FPGA contains the ''Cascaded Processing Module (CPM)'' and the ''Slot Access Controller (SAC)'' module. This set up makes ''Time-Division Multiple Access (TDMA)'' protocols evaluation under the real time possible in support from two synchronised

TABLE 20. Testbeds and their goals.

Reference	Year	Framework	Place	Experiment entities	Purpose
Afonso *et al.* [92]	2014	Control and management framework (OMF)	Universidade de Aveiro, Portugal	500 vehicles (2 vehicles during experiment)	*Montoring UDP transmission *Traffic analysis
Amoroso *et al.* [91]	2012	Creative augmentation and 3D space of study	Los Angeles area, USA	Experiment with three cars	Circulation of warning alerts Broadcasting End-to-end exchange
Gerla *et al.* [93]	2012	Campus testbed architecture (C-VeT)	University of California, Los Angeles (UCLA), USA	Two cars: one fixed and other moving	*Validation of models *Correctness of protocols
Vandenberghe *et al.* [89]	2011	w-iLab.t wireless testbed	Ghent, Belgium	200 real vehicles deployed on three floors	*Targeting the validation of research obtained in simulation *Field operation test *Used as additional tool in VANETs research
Wu *et al.* [94]	2019	*Xilinx Zynq-7015 SoC *Linux *FPGA	Beijing, China	Yet to perform	*Evaluation of MAC protocols *Calculating round trip time *High priority data delivery
Ahmed *et al.* [90]	2017	Android OS	Montreal, Canada	Yet to perform	*Proposed architecture for testbed location *Wireless emulation in reduced time

time pulses: *Tp1* represents the start of GPS and *Tp2* is for the start of time slot. *Tp2* and the frame length are set in alignment to each other. SAC provides the time slots to any node which wishes to acquire it. FPGA is also installed with a memory-mapped interface. Mobility is one of the most important features of VANET, which is missing in most of the testbeds. Unmanned Ground Vehicle (UGV) was used to have a check on mobility of the nodes depending on the GPS. UGVs are trained to follow the nodes trajectory motion with a constant speed, and hence, we can fix the communication range. The testbed supports to evaluate round trip time utilised for delivering real time data based on GPS.

In a nutshell, Table 20 summarizes few available testbeds along with their descriptions and purposes that can be used in IoV environment.

X. OPEN RESEARCH ISSUES AND CHALLENGES

In this section, some potential future research directions and challenges that need to be addressed in IoV security are discussed.

A. BLOCKCHAIN-BASED AUTHENTICATION IN IoV

The combination of VANETs and IoT led to the evolution of IoV. Now-a-days the value-added services are provided to the entities of IoV by adding up social relationship among the potential fellow vehicles or owners based on the trust of the already established relationship to share information and services, which develop the concept of Social IoV (SIoV). This increases the quality and level of services, but also leads to various threats on the paradigm and mainly on the privacy of the users. In order to provide data and current information, SIoV allows new relations to form among the vehicles known or unknown increasing the chance of threats and attacks. The risk on the privacy is more because of no involvement of users, multivariate data forwarding, storing and reusing. Hence, SIoV provides high range of data but can only be of wide acceptance if privacy preservation of an individual's identity, location, social data and destination are secured and safeguarded. The need of an hour is to determine a privacy mechanism on SIoV that guards various dimensions of privacy of user, his/her behaviour, habits or actions, location and space, thoughts and feelings, data generated by himself/herself, communication and association considering the factors like communication technologies, architecture of the paradigm, preferences of the users, social relationships, inter operability and mobility. The authors in [94] presented and analyzed all the layers of the paradigm including their issues and solutions to preserve privacy throughout SIoV. Their work provided blockchaining as the concept to safeguard privacy in SIoV to protect several dimensions of privacy.

Blockchain has made the technology decentralized by removing the need of any trusted third party. Blockchain is used in the files of money transfer, financial application, and the areas of government science. Hence, this flexibility can be also implemented in IoV deployment. A considerable amount of efforts is needed to improve transparency, efficiency, reliability, resilience, fraud prevention and quality of services in IoV environment. Blockchain-based IoV is one of the prominent technologies that can provide the solution for current centralized infrastructures [95]. There are several intrinsic applications in the Blockchain of Things (BCoT) [96]. Some of the potential applications include the following: a) smart grid [97], [98], b) healthcare [99], [100], c) Internet of Vehicles (IoV) [95], d) smart manufacturing [101], e) IoT [102], f) Industry 4.0 [103], g) smart transportation [104], and h) supply chain [105]. Fig. 5 illustrates several applications of BCoT that have gained popularity recently in the research community.

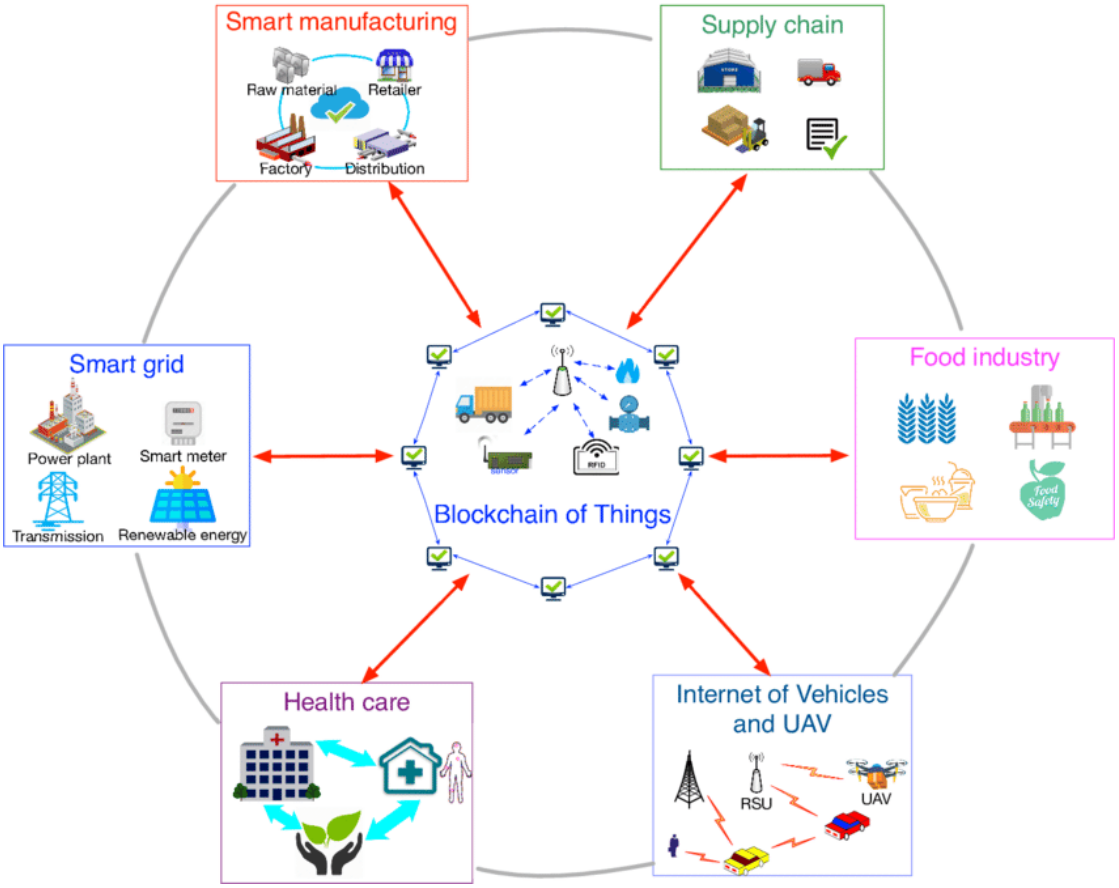

FIGURE 5. Potential applications of Blockchain of Things (BCoT) [96].

Blockchain is classified into three categories: a) public blockchain, b) private blockchain and c) consortium blockchain. The public blockckchain is open to anybody to join, access, send, verify and receive transactions of the blocks in the network. Some applications of using public blockchain are cryptocurrency (Bitcoin) [106] and Ethereum. In a private blockckchain, which is a fully trusted network, the access is only permitted to a particular entity or a group of trusted entities. In such case, the owner of the network mainly decides which entity will perform a specific task. On the other side, a consortium blockchain is combination of both public and private blockchains. Various consensus mechanisms can be used to achieve consensus among the nodes involved in a peer-to-peer (P2P) blockchain network. Some widely-accepted consensus mechanisms include "Proof-of-Work (PoW)", "Proof-of-Stake (PoS)", "Byzantine Fault Tolerance (BFT)", and "Practical Byzantine Fault Tolerance (PBFT)". The advantages of using blockchain-based IoV system is to support decentralization, immutability, transparency, confidentiality and trust like smart grid systems [107]. By transparency, it is meant that when an entity's real identity is made secure, one can still view all the transactions that were done by their public addresses. Immutability property allows once a block containing the information is added into the private/public blockchain, it can not be tampered with later. Thus, a blockchain-based authentication mechanism for securing data in the IoV environment is another potential research challenge.

B. PHYSICALLY SECURE AUTHENTICATION IN IoV

A "Physically Unclonable Function (PUF)" is a one-way function that maps a set of challenges to another set of responses based on the unique physical micro structure of a device. PUF is considered as a crucial primitive to in order to achieve various goals like authentication, access control, and untraceability. It is also extremely useful for secure and low-cost authentication [108]. An ideal PUF consists of the following potential properties:

- The output of the PUF always depends on a physical system.
- Evaluation and construction of the PUF is easy.
- The output of the PUF is unpredictable and it works as a random function.
- Furthermore, PUF is uncloneable.

Designing a lightweight privacy-preserving authentication mechanism in the IoV deployment as in the IoT system [109] by taking into consideration of the PUF is also an interesting research direction.

C. EFFICIENT DESIGN OF AUTHENTICATION PROTOCOLS

In an IoV environment, the smart devices are installed in each vehicle. These devices are resource constrained as the devices have limited computation capability, low storage size, and limited battery capacity. Hence, computation and communication intensive operations are not viable using these devices. Furthermore, it is not commendable to use bulky messages in the authentication and key establishment process. The reason is that it consumes other resources of the environment (i.e., battery of the resource constrained devices). Hence, it is recommended to design an authentication protocol in such a way that the protocol should exhibit less computation, communication and storage costs without compromising the security. Moreover, it is also depended on the application that is neede real-time ultra-fast authentication. This is another challenge for such kind of resource-constrained devices. More deep investigation is needed to explore the new security schemes (both traditional cryptographic methods along with new emerging methods) are important. Such kind of authentication methods are more useful for mobile applications associated with IoV. For example, in transportation systems applications and other body area network (BAN) applications [110]. Hussain *et al.* [111] designed and presented a fast authentication method for moving electric cars to perform authentication with the road segment while charging with the movement. But, in future there is an essential requirement to design the ultra-fast authentication schemes which accomplish the underlying needs of both the network and different users.

D. SECURE COMMUNICATION IN HETEROGENEOUS ENVIRONMENT

The IoV communication environment consists of different communicating parties (for example, vehicles, RSUs, different users and cloud servers). In such an environment, the vehicles and users may be in moving states. Therefore, it is important which kind of wireless communication technology can be used. For instance, one can use the Dedicated Short-Range Communication (DSRC) [64] for communication among various moving vehicles, whereas if a vehicle wants to communicate with the cloud server, then that can be done through the Internet connectivity. Hence, it is essential to maintain where DSRC can be applied and where the Internet connection can be used for the communication, so that we can design security protocols (i.e., authentication) accordingly. Both kinds of communication technologies have their own characteristics and limitations. Therefore, designing of such kinds of security protocols is a challenging research topic in the IoV deployment.

E. SECURE BIG DATA ANALYTICS

Various data science algorithms (data mining methods) play an important role in the big data analytic which is used to identify the patterns from the big data (for example, chances of road accidents in a particular region of a city in future). Thus, it is essential to ensure that the data mining methods which should be secure against both external threats as well as insider threats, who can misuse their network privileges to compute the sensitive information. Henceforth, designing of a secure big data analytic method for IoV data could be another challenging problem in future [112]–[114], which also requires authentication.

F. GRANULAR AUDITING

Granular auditing is an essential mechanism which helps to determine the attacks which can occur on the data (i.e., big data) stored over the cloud server of IoV environment. For example, when the attacks happened and what were the emanations. By conducting the auditing, it can be figured out what is required to improve the security and prevent the future attacks [115]. Thus, it is also a very important to provide new methods for granular auditing for IoV environment which will further help in detection and prevention of future attacks.

G. LESSONS LEARNED

Despite the remarkable advancements to date with IoV technology, it is still too early to hypothesize about the practical deployment of security protocols for the IoV environment due to several security flaws exist in the proposed schemes designed by the researchers so far. We then believe that more research analysis of security protocols will lead the IoV towards commercialization in near future. Thus, it is a hope that this survey paper will provide some baseline for the researchers and practitioners who are interested in applying the authentication protocols in the field of IoV security.

XI. CONCLUSION

In this survey paper, an emerging trend of technology, Internet of Vehicles (IoV), is discussed which has changed the entire paradigm of transportation systems as it impacts a lot on the day-to-day life of the people. But at the same time, IoV communication is also vulnerable to various known attacks, such as impersonation attack, replay attack, man-in-the-middle attack, guessing attack, hijacking attack, etc. In addition, IoV environment should be privacy-preserving, and anonymity and untraceability properties need to be maintained. Therefore, it is needed for strong authentication, access control, privacy preservation and intrusion detection protocols to secure the communication happens in IoV environment. This paper highlights the benefits and the security aspects of IoV communication. Moreover, brief details of various threats and attacks of IoV are provided. The two system models, such as network model and threat model are explained in details. A taxonomy of security protocols for IoV communication was also added with different sections, such as key management, authentication, access control, intrusion detection, privacy preservation and routing protocols. A comparative study of different authentication protocols for IoV communication was then provided. The importance of testbed for IoV simulations and implementations was also highlighted.

Finally, several future research challenges in IoV domain are highlighted that are important in the IoV security.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for their valuable feedback on the paper which helped us to improve its quality as well as presentation.

REFERENCES

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[2] J. Joy, V. Rabsatt, and M. Gerla, "Internet of vehicles: Enabling safe, secure, and private vehicular crowdsourcing," *Internet Technol. Lett.*, vol. 1, no. 1, pp. 1–6, Jan. 2018.

[3] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-vehicles communication security," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 12, pp. 1–21, Dec. 2018.

[4] S. Nagtilak, R. Sunil, and K. Rohini, "Internet of vehicles: Motivation, layered architecture and research challenges," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Lonavala, India, Nov. 2018, pp. 54–58.

[5] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of vehicles," *China Commun.*, vol. 11, no. 10, pp. 1–15, Oct. 2014.

[6] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[7] R. Hussain, D. Kim, J. Son, J. Lee, C. A. Kerrache, A. Benslimane, and H. Oh, "Secure and privacy-aware incentives-based witness service in social Internet of vehicles clouds," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2441–2448, Aug. 2018.

[8] L. Gafencu and L. Scripcariu, "Security issues in the Internet of vehicles," in *Proc. Int. Conf. Commun. (COMM)*, Bucharest, Romania, Jun. 2018, pp. 441–446.

[9] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, "Security and privacy in the Internet of vehicles," in *Proc. Int. Conf. Identificat., Inf., Knowl. Internet Things (IIKI)*, Beijing, China, Oct. 2015, pp. 116–121.

[10] 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.

[11] Deeksha, A. Kumar, and M. Bansal, "A review on VANET security attacks and their countermeasure," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Solan, India, Sep. 2017, pp. 580–585.

[12] A. Samad, S. Alam, M. Shuaib, and M. Bokhari, "Internet of vehicles (IoV) requirements, attacks and countermeasures," New Delhi, India, Tech. Rep., Mar. 2018.

[13] M. A. Shahid, A. Jaekel, C. Ezeife, Q. Al-Ajmi, and I. Saini, "Review of potential security attacks in VANET," in *Proc. Majan Int. Conf. (MIC)*, Muscat, Oman, Mar. 2018, pp. 1–4.

[14] N. Sharma, N. Chauhan, and N. Chand, "Security challenges in Internet of vehicles (IoV) environment," in *Proc. 1st Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, Jalandhar, India, Dec. 2018, pp. 203–207.

[15] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[16] D. B. Rawat, M. Garuba, L. Chen, and Q. Yang, "On the security of information dissemination in the Internet-of-vehicles," *Tsinghua Sci. Technol.*, vol. 22, no. 4, pp. 437–445, Aug. 2017.

[17] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

[18] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wireless Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018.

[19] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.

[20] J. Joy and M. Gerla, "Internet of vehicles and autonomous connected car-privacy and security issues," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, Jul. 2017, pp. 1–9.

[21] R. Abassi, "VANET security and forensics: Challenges and opportunities," *Wiley Interdiscipl. Rev., Forensic Sci.*, vol. 1, no. 2, p. e1324, Mar. 2019.

[22] G. U. Devi and M. K. Priyan, "A survey on Internet of vehicles: Applications, technologies, challenges and opportunities," *Int. J. Adv. Intell. Paradigms*, vol. 12, nos. 1–2, pp. 98–119, 2019.

[23] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-9, no. 2, pp. 198–208, Mar. 1983.

[24] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[25] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[26] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, Nov. 2002, pp. 41–47.

[27] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Berkeley, CA, USA, May 2003, pp. 197–213.

[28] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. 23rd Conf. IEEE Commun. Soc. (Infocom)*, Hong Kong, vol. 1, Mar. 2004, pp. 586–597.

[29] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, Oct. 2003, pp. 42–51.

[30] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, Aug. 1993, pp. 471–486.

[31] Y. Cheng and D. P. Agrawal, "Efficient pairwise key establishment and management in static wireless sensor networks," in *Proc. 2nd IEEE Int. Conf. Mobile Adhoc Sensor Syst. Conf.*, Washington, DC, USA, Nov. 2005, p. 550.

[32] D. Liu, P. Ning, and W. Du, "Grid-based key pre-distribution in wireless sensor networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, Sep. 2005, pp. 11–20.

[33] Q. Dong and D. Liu, "Using auxiliary sensors for pairwise key establishment in WSN," in *Proc. IFIP Int. Conf. Netw. (Networking)*, in Lecture Notes in Computer Science, vol. 4479, 2007, pp. 251–262.

[34] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[35] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[36] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, Feb. 2005.

[37] A. K. Das, "An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *Int. J. Netw. Secur.*, vol. 6, no. 2, pp. 134–144, 2008.

[38] A. K. Das, "ECPKS: An improved location-aware key management scheme in static sensor networks," *Int. J. Netw. Secur.*, vol. 7, no. 3, pp. 358–369, 2008.

[39] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *Int. J. Inf. Secur.*, vol. 11, no. 3, pp. 189–211, Jun. 2012.

[40] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[41] N. Koblitz, A. Menezes, and S. A. Vanstone, "The state of elliptic curve cryptography," *Des., Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, 2000.

[42] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[43] E. Barker, "Recommendation for key management," NIST, Gaithersburg, MD, USA, Special Publication 800-57, Rev. 4, Jan. 2016. Accessed: May 2018.

[44] C. Li, S. Ji, X. Zhang, H. Wang, D. Li, and H. Liu, "An effective and secure key management protocol for message delivery in autonomous vehicular clouds," *Sensors*, vol. 18, no. 9, p. 2896, 2018.

[45] 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)*, New York, NY, USA, Oct. 2017, pp. 478–483.

[46] K. K. Chauhan, S. Kumar, and S. Kumar, "The design of a secure key management system in vehicular ad hoc networks," in *Proc. Conf. Inf. Commun. Technol. (CICT)*, Gwalior, India, Nov. 2017, pp. 1–6.

[47] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[48] X.-Y. Guo, C.-L. Chen, C.-Q. Gong, and F.-Y. Leu, "A secure official vehicle communication protocol for VANET," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Fukuoka, Japan, Jul. 2016, pp. 482–485.

[49] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[50] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[51] M. Erritali and B. El Ouahidi, "A review and classification of various VANET intrusion detection systems," in *Proc. Nat. Secur. Days (JNS)*, Rabat, Morocco, Apr. 2013, pp. 1–6.

[52] W. Fu, X. Xin, P. Guo, and Z. Zhou, "A practical intrusion detection system for Internet of vehicles," *China Commun.*, vol. 13, no. 10, pp. 263–275, Oct. 2016.

[53] S. Yadav, N. K. Rajput, A. K. Sagar, and D. Maheshwari, "Secure and reliable routing protocols for VANETs," in *Proc. 4th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Greater Noida, India, Dec. 2018, pp. 1–5.

[54] A. D. Devangavi and R. Gupta, "Routing protocols in VANET—A survey," in *Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon)*, Bangalore, India, 2017, pp. 163–167.

[55] A. Slama, I. Lengliz, and A. Belghith, "TCSR: An AIMD trust-based protocol for secure routing in VANET," in *Proc. Int. Conf. Smart Commun. Netw. (SmartNets)*, Yasmine Hammamet, Tunisia, Nov. 2018, pp. 1–8.

[56] S. K. Bhoi and P. M. Khilar, "A secure routing protocol for vehicular ad hoc network to provide ITS services," in *Proc. Int. Conf. Commun. Signal Process.*, Melmaruvathur, India, Apr. 2013, pp. 1170–1174.

[57] K. Logeshwari and L. Lakshmanan, "Authenticated anonymous secure on demand routing protocol in VANET (vehicular adhoc network)," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Chennai, India, Feb. 2017, pp. 1–7.

[58] M. Kou, Y. Zhao, H. Cai, and X. Fan, "Study of a routing algorithm of Internet of vehicles based on selfishness," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Los Alamitos, CA, USA, Aug. 2018, pp. 34–39.

[59] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl. (WMCSA)*, New Orleans, LA, USA, Feb. 1999, pp. 90–100.

[60] D. K. Sandou, N. Jothy, and K. Jayanthi, "Secured routing in VANETs using lightweight authentication and key agreement protocol," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2018, pp. 1–5.

[61] R. J. Hwang, Y.-K. Hsiao, and Y.-F. Liu, "Secure communication scheme of VANET with privacy preserving," in *Proc. IEEE 17th Int. Conf. Parallel Distrib. Syst.*, Tainan, Taiwan, Dec. 2011, pp. 654–659.

[62] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[63] 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.

[64] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[65] L. Zhu, C. Zhang, C. Xu, X. Du, R. Xu, K. Sharif, and M. Guizani, "PRIF: A privacy-preserving interest-based forwarding scheme for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2457–2466, Aug. 2018.

[66] N. Vijayalakshmi and R. Sasikumar, "An ID-based privacy preservation for VANET," in *Proc. Int. Conf. Comput. Commun. Technol. (ICCCT)*, Chennai, India, Feb. 2015, pp. 164–167.

[67] H. Vasudev and D. Das, "A lightweight authentication protocol for V2V communication in VANETs," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, Oct. 2018, pp. 1237–1242.

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

[69] 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 Express*, vol. 4, no. 4, pp. 221–227, Dec. 2018.

[70] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang, "An efficient V2I authentication scheme for VANETs," *Mobile Inf. Syst.*, vol. 2018, pp. 4070283:1–4070283:11, Mar. 2018.

[71] A. Perrig and J. D. Tygar, *TESLA Broadcast Authentication*. Boston, MA, USA: Springer, 2003, pp. 29–53, doi: 10.1007/978-1-4615-0229-6_3.

[72] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Jul. 2015.

[73] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[74] N. B. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. U. Rahman, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.

[75] A. A. Celes and N. E. Elizabeth, "Verification based authentication scheme for bogus attacks in VANETs for secure communication," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2018, pp. 0388–0392.

[76] 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.

[77] 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.

[78] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, Sep. 2017.

[79] 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.

[80] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[81] M. Lalli and G. S. Graphy, "Prediction based dual authentication model for VANET," in *Proc. Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Erode, India, Jul. 2017, pp. 693–699.

[82] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[83] Y. Xiaodong, A. Faying, Y. Ping, X. Likun, L. Yutong, M. Tingchun, and W. Caifen, "A message authentication scheme for VANETs based on trapdoor hash function," in *Proc. IEEE 3rd Int. Conf. Big Data Anal. (ICBDA)*, Shanghai, China, Mar. 2018, pp. 279–282.

[84] C.-C. Lee, P.-H. Wu, T.-Y. Chen, and C.-T. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," *IET Comput. Digit. Techn.*, vol. 7, no. 1, pp. 48–55, Jan. 2013.

[85] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[86] *Secure Hash Standard*, U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Apr. 1995. Accessed: Jan. 2019.

[87] National Institute of Standards and Technology, U.S. Department of Commerce. (Nov. 2001). *Advanced Encryption Standard*. Accessed: Jun. 2019. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[88] W. Vandenberghe, I. Moerman, P. Demeester, and H. Cappelle, "Suitability of the wireless testbed w-iLab.T for VANET research," in *Proc. 18th IEEE Symp. Commun. Veh. Technol. Benelux (SCVT)*, Nov. 2011, p. 6.

[89] H. Ahmed, S. Pierre, and A. Quintero, "A flexible testbed architecture for VANET," *Veh. Commun.*, vol. 9, pp. 115–126, Jul. 2017.

[90] A. Amoroso, G. Marfia, M. Roccetti, and G. Pau, "Creative testbeds for VANET research: A new methodology," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2012, pp. 477–481.

[91] J. Afonso, A. Cardote, and S. Sargento, "Vehicular testbed management," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2014, pp. 1–7.

[92] M. Gerla, J. Weng, E. Giordano, and G. Pau, "Vehicular testbeds—Validating models and protocols before large scale deployment," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Maui, HI, USA, 2012, pp. 665–669.

[93] J. Wu, H. Lu, and Y. Xiang, "A hard real-time testbed for distributed TDMA-based MAC protocols in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–7.

[94] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet of vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[95] J. Hu, D. He, Q. Zhao, and K.-K.-R. Choo, "Parking management: A blockchain-based privacy-preserving system," *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 45–49, Jul. 2019.

[96] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[97] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018.

[98] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, pp. 955–967, Aug. 2019.

[99] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.-R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[100] T. McGhin, K.-K.-R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[101] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K.-R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, Oct. 2019.

[102] M. Banerjee, J. Lee, and K.-K.-R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[103] C. Lin, D. He, X. Huang, K.-K.-R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.

[104] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K.-R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, Aug. 2019.

[105] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans Ind. Informat.*, to be published, doi: 10.1109/TII.2019.2942389.

[106] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://downloads.coindesk.com/research/whitepapers/bitcoin.pdf

[107] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid-review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[108] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[109] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.

[110] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K.-R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[111] R. Hussain, J. Son, D. Kim, M. Nogueira, H. Oh, A. O. Tokuta, and J. Seo, "PBF: A new privacy-aware billing framework for online electric vehicles with bidirectional auditability," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–17, Oct. 2017, doi: 10.1155/2017/5676030.

[112] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, "SecSVA: Secure storage, verification, and auditing of big data in the cloud environment," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 78–85, Jan. 2018.

[113] A. Jindal, A. Dua, N. Kumar, A. K. Das, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Providing healthcare-as-a-service using fuzzy rule based big data analytics in cloud computing," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 5, pp. 1605–1618, Sep. 2018.

[114] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi, "A random decision tree framework for privacy-preserving data mining," *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 5, pp. 399–411, Sep. 2014.

[115] G. Gross. *9 Key Big Data Security Issues*. Accessed: Sep. 2019. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/9-key-big-data-security-issues

PALAK BAGGA received the M.Tech. degree in computer science and engineering from Uttar Pradesh Technical University, India. She is currently pursuing the Ph.D. degree in computer science and engineering with the Center for Security, Theory and Algorithmic Research, IIIT Hyderabad, India. Her research interests include network security, and security in the Internet of Things and the Internet of Vehicles. She has published three journal articles in her research areas. She was a gold medalist in academics and also awarded by a Certificate of Merit.

Ashok Kumar Das (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad, India. His current research interests include cryptography, network security, blockchain, security in the Internet of Things (IoT), the Internet of Vehicles (IoV), the Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, and intrusion detection. He has authored over 210 articles in international journals and conferences in the above areas, including over 183 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON SMART GRID, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), IEEE CONSUMER ELECTRONICS MAGAZINE, IEEE ACCESS, IEEE COMMUNICATIONS MAGAZINE, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards and Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and the *Journal of Network and Computer Applications*. He has served as a Program Committee Member in many international conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019. He is on the editorial board of *KSII Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *IET Communications*. He is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare and for ICT Express (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT.

MOHAMMAD WAZID (Senior Member, IEEE) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology Hyderabad, Hyderabad, India. He was an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. He was also a Postdoctoral Researcher with Cyber Security and Networks Lab, Innopolis University, Innopolis, Russia. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Graphic Era University. He is also the Head of Cybersecurity and IoT research group, Graphic Era University. His current research interests include security, remote user authentication, the Internet of Things (IoT), and Cloud computing. He has published more than 70 articles in international journals and conferences in the above areas. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently a Professor with the Federal University of Piauí, Brazil, a Senior Researcher with the Instituto de Telecomunicações, Portugal, and Collaborator of the Post-Graduation Program on Teleinformatics Engineering with the Federal University of Ceará (UFC), Brazil. He has authored or coauthored over 850 articles in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. Prof. Rodrigues is also a member of the Internet Society and a Senior Member ACM. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. He is also the Leader of the Next Generation Networks and Applications research group (CNPq), the Past-Director for Conference Development - IEEE ComSoc Board of Governors, a IEEE Distinguished Lecturer, a Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the scientific council with ParkUrbis - Covilhã Science and Technology Park, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-chair of the IEEE ComSoc Technical Committee on Communications Software, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He has been a General Chair and a TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He is the Editor-in-Chief of the *International Journal on E-Health and Medical Communications* and an editorial board member of several high-reputed journals.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. In 1996 and 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. In 2003 and 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.