Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 11, No. 1, March 2023, pp. 180~193
ISSN: 2089-3272, DOI: 10.52549/ijeei.v11i1.4295

A Review on VANET Security: Future Challenges and Open Issues

Md. Julkar Nayeen Mahi[1], Sudipto Chaki[2], Esraq Humayun[3], Hafizul Imran[4], Alistair Barros[5], Md Whaiduzzaman[6]

[1, 3,4]Department of Software Engineering, Daffodil International University, Bangladesh
[2] Department of Computer Science and Engineering, Bangladesh University of Business and Technology, Bangladesh
[5,6]School of Information Systems, Queensland University of Technology, Australia

Article Info

Article history:

Received Nov 7, 2022
Revised Dec 6, 2022
Accepted Feb 2, 2023

Keywords:

VANET
Security
UAV
DMN nodes
Heterogeneous Access
Trust Verification

ABSTRACT

Vehicular Adhoc Network (VANET) is an established technology that is well-suited for emerging technologies such as the Internet of Vehicles (IoV) and Unmanned Aerial Vehicles (UAVs). However, while VANET offers improved methods for addressing contemporary technology, it also presents significant challenges in providing adequate security measures for intended access. VANET operates on multiple execution platforms, such as roadside units, vehicle-to-vehicle, vehicle-to-device, and vehicle-to-everything (V2X) communication. As a result, VANET must establish robust security measures for future purposes and strengthen protocol authentications to ensure secure data delivery and network-wide execution. In this work, we provide an overview of some of the recent security problems faced by VANET to raise awareness among developers and engineers about the specific security needs of VANET and how to avoid errors or intrusions when deploying VANETs in cities and urban areas. We cover topics such as the classification of security attacks, standard or security protocol problems and solutions, and the best feasible security criteria for extended VANETs. Finally, we discuss open issues and future VANET security developments or concerns.

Corresponding Author:

Md Whaiduzzaman,
School of Information Systems
Queensland University of Technology, Brisbane, Australia
Email: wzaman@juniv.edu

1. INTRODUCTION

Public health and safety organizations face a formidable obstacle in the growing frequency of deadly traffic accidents. A roadway accident is featured prominently on the front page of newspapers. The leading cause of death in the current population is automobile collisions. In 2013, more than 1,37,000 individuals were killed in traffic accidents. This check is greater than the number of warriors who gave their lives on the battlefield. Numerous factors contribute to street accidents, including inappropriate roadway design and maintenance, traffic congestion, and the increasing number of vehicles on the road. In addition, drivers and other road users' lack of street awareness have compounded the matter. It is a tragedy for our nation that most youths die on the streets due to irresponsible driving, intoxicated driving, and other issues. According to the World Health Organization, traffic-related injuries caused an estimated 1.25 million deaths worldwide in 2010 (one death every 25 seconds) [1]. However, preparing for effective security participation inside VANET modular activities can save many lives. An intelligent vehicular communication network, interpreting through Figure 1, or VANET, is a mobile ad-hoc platform that reduces traffic congestion and prevents vehicular media accidents [2, 3, 4]. Typically, VANET gives vehicle driving instruction in a practical setting. Nevertheless,

discrepancies in allocating and transmitting real-time communication from device to device may result in system failure among networked devices, endangering road safety [5, 6, 7].

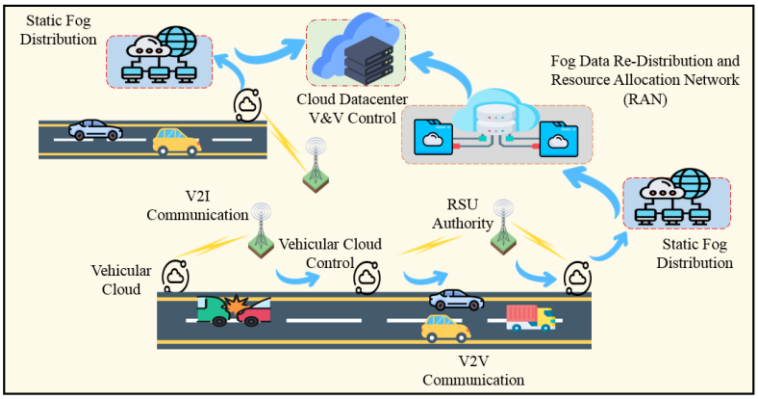


Figure 1. Vehicular fog-cloud orchestration for secured and enhanced data dissemination activities

As third-party application deployments drive it, protecting VANET connectivity is vital for enhancing functionality and vehicular device engagements. Therefore, establishing security patterns for maximal communication output in VANET has become a problem for amateur researchers. VANET operates through the management of specific permission controlling On-Board units (OBUs) and Road Side Units (RSUs). RSUs are placed on nearby roadside borders between the vehicle and the roadside control room (V2R) to increase security and decrease data offloads. VANET provides vehicle-specific network services, while OBUs are used for navigation [8, 9, 10]. While traveling on the road surface, RSUs communicate via approved controllers. Most often, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and hybrid communications are established using dedicated short-range communication (DRSC) in a multi-hop or single-hop pattern. Future VANETs will connect OBUs as an on-board wireless mechanism; global positioning system (GPS), Event Data Recorder (EDR), and sensors (radar) will be utilized as a traffic congestion control module [11, 12, 13]. In VANETs, these controllers provide correct instructions by relaying data via V2V or V2I patterns. Active road safety controls, traffic reduction, regulating infotainment, speed control checker, and cooperative navigation interpreters can be assisted by VANET [14]. Security is a concern and a necessary condition of immunity from danger or attack, yet the entire system could be compromised due to vulnerabilities and obstacles. Security provides safety precautions and protection measures [15, 16]. For example, if specific security is required for the parade route, more guards must be provided as a section of groups. Because VANET uses a wireless connection, which is more difficult to secure [17, 18], it is vital to thoroughly protect against misuse activities and design the security architecture. Security ensures people's safety by taking precautions or steps that are predictable. Various researchers have alerted VANET security breaches to feasible fixes. Some individuals have experience with security infrastructures and protocol standardizations. Nonetheless, addressing device-based theft and data security is a vast area to investigate [19, 20]. This data security pattern and threshold-based security communication expand the potential for VANET upgradability [21, 22].

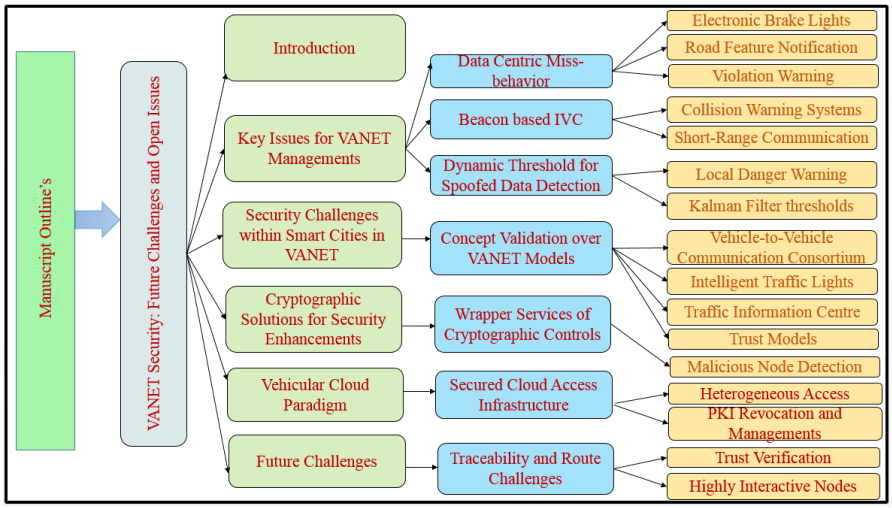


Figure 2. Paper Organization Chart

Incorporating with Figure 2, this paper investigates device-based security counterfeiting and its countermeasures, malicious node identification, PKI infrastructure-based authentication, beacon-based vehicular cloud communication, dynamic threshold-based malicious node detection, secured data execution, and spoofed identity disclosure, device-based secured trust managements, and probable security measures or related issues [23, 24]. We have concentrated on unique classifications, secured architectures of various conceivable assaults on vehicle IDs, and solutions for the related problems based on entities from the cited literature. Finally, we have demonstrated the potential future results of VANETs enabled by newly introduced technology and posed several unanswered concerns or difficulties for future research [25, 26, 27, 28].
The essential outcomes of this paper are given below –

- We have depicted some taxonomies of generic VANET security enhancements, causes and possible solutions.
- We have discussed here the recent emerging VANET security problems and show the possible way of managing securities through providing taxonomy insights.
  .
- Utilized and focused trust management paradigms to enhance security and threat remedy possibilities across the VANET road side units as well as authentication properties.
- Reviewed existing VANET based security properties, services and monetize the particular developments which can be a major help for reducing threat activity across the VANET modular nodes.
- Described the in-depth security attacks on VANETS and the solution to get rid of this attacks future VANETS security enhancements.

The rest of this paper is organized as follows, **Section 2** describes generic key issues and security measures for VANET Managements, **Section 3** depicts VANET security challenges on implementations around smart cities **Section4** employs cryptographic solutions for VANET security enhancements, and **Section 5** shows secured VANET communication control over a vehicular cloud platform, **Section 6** presents future challenges and issues in VANET security up-gradation possibilities, Finally, **Section 7** briefly concludes this paper.

2. GENERIC SECURITY MEASURES AND KEY ISSUES FOR VANET MANAGEMENTS

This generic taxonomy shows an optional improvement for the future VANET technologies. In Figure 3, we can see that trending elements, applications software and hardware tools have a good impact in changing VANET working patterns. Infotainments, co-operative legal services can make VANET communication up to date with the help of varying data controls [29, 30]. However, security challenges and requirements blocks have carried some important notifications that considered as a must development for the future VANET improvements.

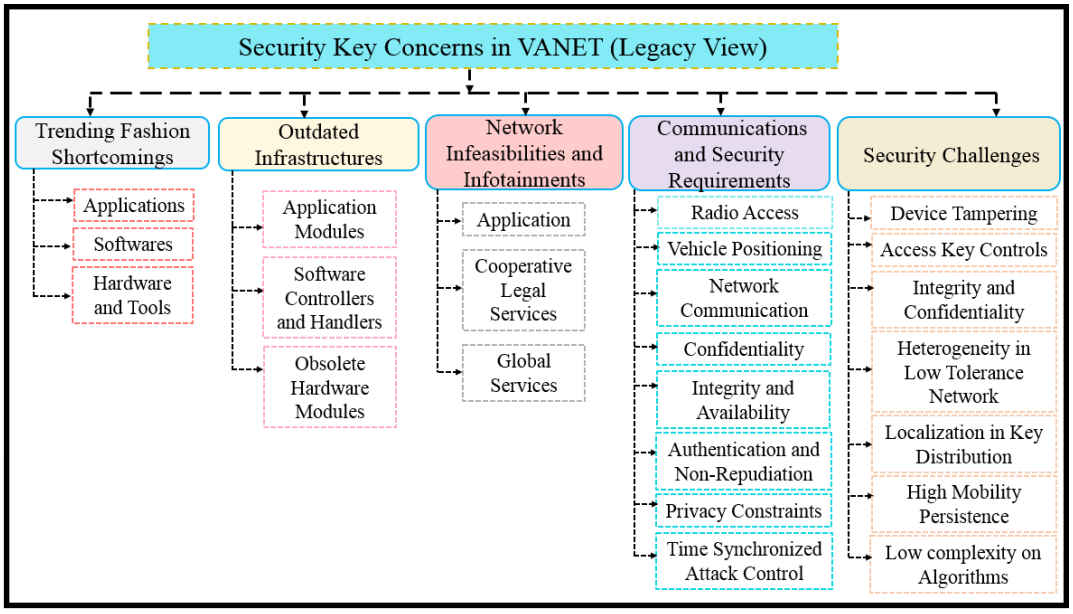


Figure 3. Device-based views and security key concerns in improving traditional VANET

2.1. Data-Centric Misbehavior Detection in VANETs:

Misconduct or transmission of erroneous information in vehicle ad hoc networks (VANETs) is a severe problem with far-reaching implications, including safety-related and traffic-avoidance applications. MDS (misbehavior detection system) focuses on detecting hostile nodes; nevertheless, its primary goal is to detect incorrect information instead of identifying misbehaving nodes [31, 32]. VANETs are ephemeral networks where the link between vehicles (nodes) is temporary. As nodes move into and out of range of one another, the network topology is regularly altered [33]. In addition, we present the detection of intrusions in mobile ad hoc networks, a topic that has been explored extensively in the context of wireless ad hoc networks [34]. Observing a node's alarms and subsequent actions enables the identification of inappropriate activity, hence decreasing the communication and processing costs involved with producing, sending, and maintaining certificate revocation lists. Additionally, erroneous location information and misleading warning signals can be identified. Emergency Electronic Brake Lights (EEBL), Post-Crash Notification (PCN), Road Hazard Condition Notification (RHCN), Road Feature Notification (RFN), Stopped or Slow Vehicle Advisor (SVA), Cooperative Collision Warning (CCW), Cooperative Violation Warning (CVW), Congested Road Notification (CRN), Change of Lanes (CL), and emergency vehicle approaching are (EVA) examples of alert messages that ensure road safety [35].

2.2. Beacon-based IVC (Inter-Vehicular Communication) Systems:

This Beacon-based IVC systems utilize Inter-Vehicle Communication (IVC) beaconing to improve motorist safety at junctions. Inter-Vehicle Communication (IVC) is largely driven by safety and efficiency applications, which both require effective management of the wireless communication channel. Dedicated Short-Range Communication (DSRC) development and standardization using IEEE 802.11p at the access level. By offering assistance technologies such as cross-traffic assistance, DSRC helps avert accidents. I Risk classification: This system examines safety measures for Intersection Collision Warning Systems (ICWS), based on which each vehicle may assess the severity of the current situation. This invention created a simulation environment that enables the collision-free road traffic simulator, Simulation of Urban Mobility (SUMO) to support cars that selectively violate traffic laws and identify future collisions or near misses. This system delivers safety messages and displays the conditions (corresponding to risk classifications) under which hazardous vehicles can exchange beacons. This system emphasizes the security features of Intersection Collision Warning Systems (ICWS). The following are examples of safe junction design: I Crash Probability Interval ii) Classification of Risk. Therefore, beacon-based [36, 37] IVC systems can improve the safety of vehicles at junctions.

2.3. Cooperative Message Authentication Distributed Key Management Framework:

In contrast to the centralized key management assumed by present group signature systems, distributed key management is anticipated to permit the revocation of risky vehicles, system repair, and various security standards. Each RSU is the group's primary distributor, and there is a growing concern that the semi-trust RSUs may be hacked. Due to its exciting and promising features, such as vehicle safety, traffic congestion avoidance, and location-based applications, vehicular ad hoc networks (VANETs) have garnered significant attention. As part of a safety driving application, each vehicle regularly communicates its current position, heading, velocity, and road data. A distributed key management structure streamlines the revocation of hazardous vehicles, system maintenance, and the implementation of varied security standards [38]. The framework's communications may be categorized into essential distribution and routine broadcasting times. This technique is based on the short group signature to offer privacy in VANETs and is augmented by a cooperative message authentication mechanism to decrease computational effort. The problem is that semi-trust RSUs are susceptible to manipulation and can potentially operate with malevolent cars.

2.4. Dynamic Threshold based Spoofed Data Detection Identities:

To improve road safety, vehicular ad hoc networks, safety-related applications, and vehicle-to-vehicle communications are provided. Because decisions are based on these signals, safety-related applications require a high level of message reception confidence. Automobiles choose to increase their credibility when a predetermined threshold is reached. The threshold is treated as a Kalman filter, and a technique for changing the threshold dynamically is provided. The verified threshold mechanism based on the Kalman filter is supported in many system models, including i) Assumptions: which use dynamic thresholds to detect fabricated data. On multilane roads, vehicles use a common V2V safety application: the Local Danger Warning (LDW). The LDW application consists of three steps: propagation of the message, detection, and evaluation. ii) Attacker model: forging is an assault when attackers transmit phony notifications to persuade others to make erroneous judgments in an effort to control traffic. An attacker who gets another's false alarm verifies the incident by sending out their own false alert. iii) Calculating distances to OBU: several lengths are taken into account by this system model, including detection, braking, information and reaction, and decision distance. iv) A state

transition diagram for an OBU: The state transition diagram of a vehicle that detects a hazard and receives a single alarm showing that the vehicle moves from an inactive state to one of alert transmission. The state transition graphic assists the vehicle in making and carrying out this decision. A dynamic threshold [39] method could boost confidence in local risk warnings by detecting fabricated data.

2.5. Dynamic Vehicular Ad Hoc Network Security Enhancements:

Such a network is intended to withstand a range of malevolent abuses and security assaults. Despite the benefits of a VANET, there are significant obstacles, especially in terms of security and privacy. As a specialized implementation of mobile ad hoc networks (MANETs), VANETs [40] inherit all the known and undiscovered security flaws of MANETs and are susceptible to various security and privacy concerns. Any malicious conduct by users, such as a modification and replay attack against the disseminated messages, may be catastrophic for the other users. As security becomes more challenging due to the unique characteristics of networks, such as the high-speed mobility of the network entity (or vehicle) and the vast number of network entities, conditional privacy preservation must be achieved in the sense that user-related privacy information, i.e., user-identifiable information, must not be disclosed unless necessary. IEEE 1609.2 covers WAVE message security against eavesdropping, spoofing, and other attacks [41, 42]. Certificate revocation is fundamental to any public key infrastructure-based security system [43] because it ties the public key to its owner's identity, which has been validated and issued by a certificate authority (CA). This certificate protects against several attacks, including man-in-the-middle and impersonation attacks [44]. Based on its traffic-related broadcast messages, the movement of a vehicle can be anticipated for security purposes [43]. Due to privacy-sensitive content, it is anticipated that the source [45] privacy of safety messages will become a major security risk in VANETs that protect privacy. Jan et al. [46] proposed anonymous credentials, a security approach based on a pair of keys.

2.6. Security Enhancements over in-bound Vehicular Networks:

A vehicular network is one of the indispensable technologies for implementing a variety of automobile, traffic, and safety-related applications. There are several obstacles to the security of automobile network infrastructure. Due to the mobility and variety of autos, protecting a vehicular network is more complex than securing other networks such as WSN. Five components comprise the security issues of car networks: secrecy, authentication, non-repudiation, localization, and data verification. Non-repudiation, for instance, ensures that entities cannot deny sending or receiving messages from them. In addition, data-centric trust and verification are employed to safeguard the vehicular network [47] against information-based threats, such as the alteration of in-transit traffic or impersonation. Several methods have been developed to meet these criteria and safeguard vehicle networks [48] against these blockages. For example, Plausibility Checks, Logic Reception Beacons, and tamper-proof GPS are three approaches for protecting vehicular networks against attackers who get the position of cars on purpose. In addition, automotive networks leverage reactive and proactive security solutions [36] to allow data-centric trust and verification.

- **Vehicular Cloud Computing (VCC):**

As the frequency of vehicle cloud computing increases, so makes the industry's demand for security. Multiple security vulnerabilities challenge the security of automotive cloud computing, which may be grouped into six groups: service denial, identity spoofing, modification repudiation, repudiation, Sybil attack, and data disclosure.

i. **Denial of service:** Denial of service is a prevalent assault against vehicular clouds and networks that aims to render the resources unavailable.
ii. **Identify spoofing:** The second issue, identity spoofing, allows an unauthorized user or program to use another individual's identity and security credentials.
iii. **Data modification (Tampering):** It is another security risk in vehicular cloud that several attackers can execute before the data are received at their destination; for instance, the Man-in-the-Middle attack is the most prevalent assault on this group.
iv. **Repudiation:** Due to the lack of proper tracking and recording mechanisms, the repudiation attacker can change or invent the identification of new actions, data, and processes. In other terms, repudiation is the capacity to reject the existence of reality or action.
v. **Sybil attack:** Sybil attack entails creating a large number of pseudonymous identities to conduct a redundant remote operation, compelling the system to pick a single remote entity several times and overcoming redundancy.

vi. **Information Disclosure:** Due to a lack of data privacy, information disclosure is acquiring a system's unique data. This attack contains Information Leakage (disclose sensitive information), Path Traversal (force access to outsourced data), and Predictable Resource Location (identify where resources are located) (finding hidden content and functions). It is hard to develop a safe cloud computing environment for the automobile sector without considering security requirements like confidentiality, integrity, and authentication.
vii. **Confidentiality:** Users without permission should not release sensitive information.
viii. **Data integrity:** The data's integrity should not be compromised or altered. The messaging must be trustworthy and genuine, and the data should be easily available.
ix. **Authentication:** It establishes if a person or thing is who or what it purports to be.

- **Real-time Constraints:**

Certain applications [49], notably accident alerts, require real-time or near-real-time communication. This illusion may result in car accidents, traffic congestion, and a decrease in VANET bandwidth performance

3. SECURITY CHALLENGES OVER VANET IMPLEMENTATIONS WITHIN SMART CITIES

3.1. Warning Messages, Intelligent Traffic Lights (ITLs):

In the traffic management of smart cities, data from TIC (Traffic Information Centre) infrastructures are accessible at all times and from any location. This work describes the creation of a warning system made of Intelligent Traffic Lights (ITLs) that alerts drivers of traffic congestion [36, 48] and weather conditions on city highways [25, 26]. The warning signals provided by VANETs offer significant benefits to road operators and drivers. Appropriate traffic warnings and current information on traffic occurrences will minimize traffic congestion, increase road safety, and enhance city driving. Vision - Driven ITS, Multisource-Driven ITS, Learning-Driven ITS, and Visualization-Driven ITS are multifunctional data-driven intelligent transportation systems that rely on vast quantities of data from numerous sources. The foundation for smart cities incorporates ITLs at particular junctions. These ITLs capture real-time traffic data from passing cars and produce traffic statistics, including the traffic density on adjacent streets. Message format details include traffic density (TDst), vehicle transmitting statistics, the number of neighbors (NoN), the time the statistics report was generated, and the IP address of the ITL. In addition, it involves the management of traffic density and written warnings.

3.2. Enhanced Secured RSU Communication over VANETs:

VANETs consist of vehicle-to-vehicle and vehicle-to-infrastructure wireless local area network connections. VANETs allow a direct link between vehicles and RSUs and may broadcast and receive traffic or danger alerts with little delay. Studies on unicast routing were commonly related to ad hoc networks and useful for VANET integrated developments. Applications and requirements for VANET developments include the following references [19, 20, 21, 22]:

i. Countless programs and coalitions have developed and evaluated vast lists of potential uses. These applications are categorized as safety, efficiency in transportation, cooperative information and user enjoyment.
ii. The Vehicle-to-Vehicle Communication Consortium (V2VCC) analysed superior enhanced route directing and navigation having green light optimal speed advising and lane merging aid for applications enhancing transportation efficiency.
iii. Cooperative information and entertainment applications include tolling, point-of-interest alerts, fuel consumption control, podcasting, and multichip wireless internet access.
iv. In VANETs, a communication coordinator cannot be assumed, which presents a substantial issue. Despite the probability that certain applications would require infrastructure (e.g., traffic signal violation warning, toll collection).
v. Specifications of APIs managed for coupling traffic flow and networking simulators models how drivers respond to the additional information offered by VANETs, as well as benchmark definitions for comparing simulation study results.

Concerns regarding the authenticity of the data are raised because security and privacy enhance the efficiency and reliability of a system in which information is gathered and exchanged among autonomous entities.

3.3. Secured Trust Management for VANET Modifications and Up-gradations:

Due to the catastrophic consequences of acting on misleading information given by malicious peers in this context, VANETs require robust trust management.

i. **Trust Emerging from Multiple Direct Interactions among Agents:** Numerous trust models established in multi-agent systems are built on the idea that agents interact with one another on multiple occasions.
ii. **Degree of Environment Knowledge:** The vast majority of learning models of trust presented in the literature for multi-agent systems, such as multi-agent environments where there is some degree of uncertainty regarding other agents and the environment, also include the Role of Central Entities and Collusion and Strategic Lying [23, 24].

Trust Models in MANETs and VANETs share comparable properties, such as decentralization, mobility, openness, etc., because they are both applications of mobile ad-hoc networks. However, there are also differences between them. On Trust Models in VANETs, security and privacy researchers have expended much effort, for example, to design a system that relies on a secure infrastructure and regularly uses digital certificates. VANETs desire the following trust management characteristics: decentralized trust establishment, coping with sparsity, event or task and location or time specificity, scalability, integrated confidence measurement, system-level security, and sensitivity to privacy concerns. Trust management may become the target of attacks and be compromised; such attacks include the Sybil Attack, the Newcomer Attack, the Betrayal Attack, the Inconsistency Attack, the Bad-mouthing or Ballot-Stuffing Attack, and the Collusion Attack [25, 26].

4. CRYPTOGRAPHIC SOLUTIONS FOR SECURITY ENHANCEMENT IN VANETS

VANETs feature various distinguishing qualities, including the high mobility of their nodes and short connection times. Standard security measures are rarely successful. It focused all of its research on relating the security challenges of VANETs to cryptographic solutions that can eliminate or mitigate problems and their impact. People were intrigued by the classification of attacks, the presentation of the attacker model, and the inclusion of previously unknown attacks such as the disguised vehicle, tunnel, wormhole, and Bush Telegraph. VANETs permit two types of communication: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) (V2I). Security issues and potential cryptographic solutions require an understanding of the characteristics of VANETs, such as their high mobility, dynamic topology, frequent disconnections, availability of the transmission medium, the anonymity of the support, and limited bandwidth, attenuations, limited transmission power, energy storage, and computing. Confidentiality guarantees that only authorized parties can access communications, and authentication allows the recipient to authenticate the data's origin and the sender's identity. Integrity signifies that the recipient can confirm that the communication received is identical to the message sent and has not been altered en route. An attacker should be incapable of altering messages. Cryptographic primitives and tools define encryption or decryption, symmetric cryptography, and asymmetric cryptography. All contemporary assaults on VANETs are wrapped by cryptography and its potent primitives and services. We analyze the affected services and suggest cryptographic countermeasures for each attack [26, 27, 28].

4.1. Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks:

DMN-Detection of Malicious Nodes is a technique in VANETs that can enhance the DMV Algorithm in terms of the efficient selection of verifiers for detecting malicious nodes and the network performance. There are two types of systems in existence. Schemes consist of (1) Node-Centric Misbehavior Detection Schemes: This technique must distinguish between distinct nodes employing authentication. Message transfer authentication is carried out using security credentials and digital signatures. These approaches give the nodes transmitting messages precedence over the data transmitted. (2) Data-Centric Misconduct Detection Strategies This method checks the data transmitted between nodes to identify inappropriate behavior. It emphasizes the relationships between messages rather than the identities of individual nodes. The information of the network nodes is analyzed and compared to the information received by the other network nodes to verify the accuracy of the received warning signals. In addition to isolating nodes with abnormal behavior, the DMN technique aims to enhance network performance [14, 15, 16, 48].

5. SECURED VEHICULAR CLOUD (VC) PARADIGM FOR VANET CONTROL

5.1. Secured Access Control in Heterogeneous Networks:

VC provides an efficient method for exploiting vehicles' processing and storage capability. Unrestricted access to and modification of the data stored on other cars by the vehicles. Each vehicle's sensitive data should be encrypted to prevent unauthorized access (using the vehicle's private key, for example). Alternately, when automobiles parked in a shopping mall are utilized as a data center, it is feasible to store sensitive customer information in a vehicle temporarily. This data must be erased from the devices before the car leaves the parking lot. A virtual machine is necessary for the VC to manage the assignment of physical

devices that have been used to compute or store sensitive data. (1) the host vehicle or other VMs cannot interfere with applications and services operating within a VM, ensuring isolation; (2) to be replicated, transferred, or reassigned among host servers, maximizing hardware resource utilization; and (3) to ease data backup and recovery. GPS, wireless transceivers, and onboard radar systems are common onboard technology found in automobiles. Each vehicle can have a unique combination of onboard technology with various capabilities, including processing speed, memory size, storage space, and CPU capacity. Consequently, it is difficult to provide security for these heterogeneous cars in a VC setting, as most cryptographic techniques are onerous, and the vehicles must comply with specified hardware standards. Access control is a difficult component of the VC that checks the user's identity before granting access to a resource. Multiple levels of access restriction are established in the VC, and each user is allocated to a distinct cluster based on their network function [28, 32, 33].

5.2. Public key Security Managements in VANET (PKIVAN):

Multiple types of autos registered in various nations can travel outside their respective regions, necessitating a complex key management system. The Vehicular Public Key Infrastructure consists of the three phases indicated in [28]; it is one of the primary systems for key management between autos.

The primary duty of Certificate Authorities (CAs) is to: During this stage, public and private keys are issued for each vehicle. A key is assigned based on a unique identification with an expiration date. Key Verification Authentication: CAs can validate the vehicle's public key in this step. CAj will issue Pui as the car's public key when vehicle i) requests a public key. Using the car's public key and identifier, CAj computes a certification (Ceri [Pui]) for this vehicle i. Here, Ceri [Pui] is the public key vehicle issued by CAj, and CAj created its public key. (Pui | ID CAj) is signed by CAj's private key.

5.3. Public Secured Revocation Method:

Certificate revocation is one of the most effective methods for safeguarding data against attack. When an attacker's certification is identified or when an attacker exposes a node's certification, the certificate should be revoked. Certificate's Revocation List (CLR) is the important revocation mechanism in a vehicle network, according to Housley et al. The CRL is an instantaneously delivered list of recently revoked certificates. CLRs have various drawbacks, including a potentially lengthy list and a limited certificate validity period. When the CA decides to destroy the pairing key of each car using RTPD, the vehicle receives a revocation message encrypted with its public key (PuVi). All key pairs will be revoked after the tamper-resistant device (TPD) verifies this message. Finally, a message of acknowledgment will be sent to the CA. Vi's current location must be communicated to the CA; otherwise, the revocation message must be broadcast to all cars. In accordance with the RTPD model, the CA must revoke all M keys for private and public vehicles. RC2RL is utilized if the CA wishes to revoke a subset of vehicle keys or if the TPD of Vi is unavailable. Lastly, the DRP approach is utilized when cars collect complaints about the misconduct of other vehicles and the neighbors of the guilty vehicle (Vi) remove their keys. Consequently, while employing these technologies, the automobile cloud computing communication lines may be relied upon.

To ensure the security of vehicular communication, all nodes, including autos and roadside infrastructures, can link via V2V or V2I communication models in vehicular cloud computing. In addition, vehicles and roadside infrastructure must connect to the cloud to store or analyze their data. The OBU is responsible for establishing communication between cars or vehicles and infrastructures. This communication takes place inside an OBU. An RSU is an access point connected to a location server that stores or processes all location data transmitted by RSUs. The location server sends the data to the cloud for processing or storage. In addition, a trustworthy certificate authority (CA) is responsible for providing authentication services to automobiles and location-based service providers. The message from the VC has the fields vehicle id or a pseudonym to identify the driver, timestamp, message type, message length, data, geographic position, direction, and an error checking field [28]. The message type may consist of the following:

i. **Short Message:** to send an alert or warning message.
ii. **Media Message:** to obtain environment services from other vehicles or a cloud,
iii. **Priority Message:** to cease sending an alert or urgent messages.
iv. **Error Message:** to send an error message to the sender.
v. **Recognize Message:** It is the confirmation of communication reception. The value of secure communication in a vehicular cloud lies in its ability to make driving safer and more efficient. Several security flaws in vehicular communication make it susceptible to attack, including preventing communication (jamming), forging messages, transmitting false hazard warnings by the attacker (forgery), dropping or modifying a message by intermediate nodes (traffic tampering), and privacy breaches. Figure 4 demonstrates VANET security breaches and prospective threats. A cryptographic strategy is required to safeguard vehicle communication against various attacks.

vi. ElGamal is a method for securing communications inside a VC set. Each vehicle has its public and private key (**Kpu, Kpr**), where **Kpu = gKpr** modulo p, g is a multiplicative group generator, and p is a huge prime integer.

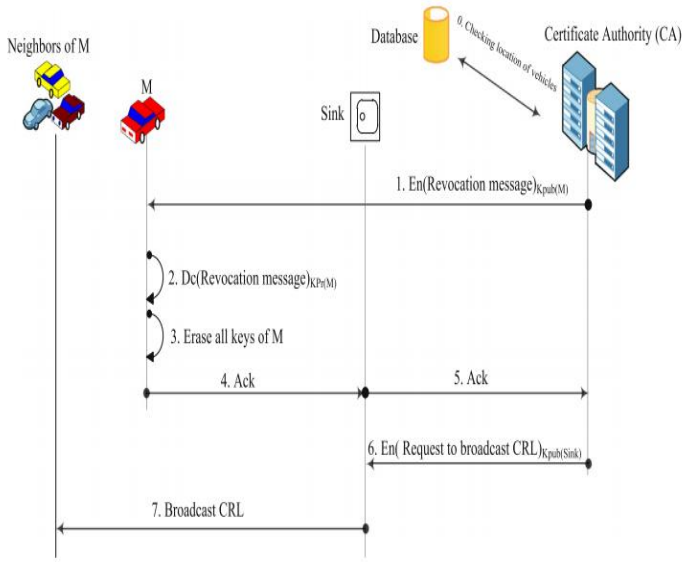


Figure 4. Revocation protocol of the tamper-proof device (RTPD) [28]

Prior to transmitting a message, its private and public keys are calculated (**Kmpr, Kmpu = gKmprmod p**), and the message digest dm is generated by hashing the message and its public key (**dm = H(m|Tm)**). The receiver receives the message, public key, and a signature created using the following formula. ***Sm = Kmpr + dmKpr mod (p-1)*** upon receiving the message, the signature should be validated by comparing $gx = K_{mpu}K_{pu}^{dm}$. Key management is the most challenging aspect of each cryptographic technique in the vehicular cloud. The Vehicular Public Key Infrastructure (VPKI) is a popular key management approach that ensures the message's integrity and privacy in vehicular clouds.

5.4. Possible Threat and Solution for Device based Counterfeiting in VANET:

In this section we have generalized the device based plausible threat execution and solution for the device counterfeiting across the active VANET nodes. The taxonomies (Part-I, Part-II, Part-III) show device based threat that occurred usually within the active VANET nodes, as shown in Figure 5(a), (b) and (c).

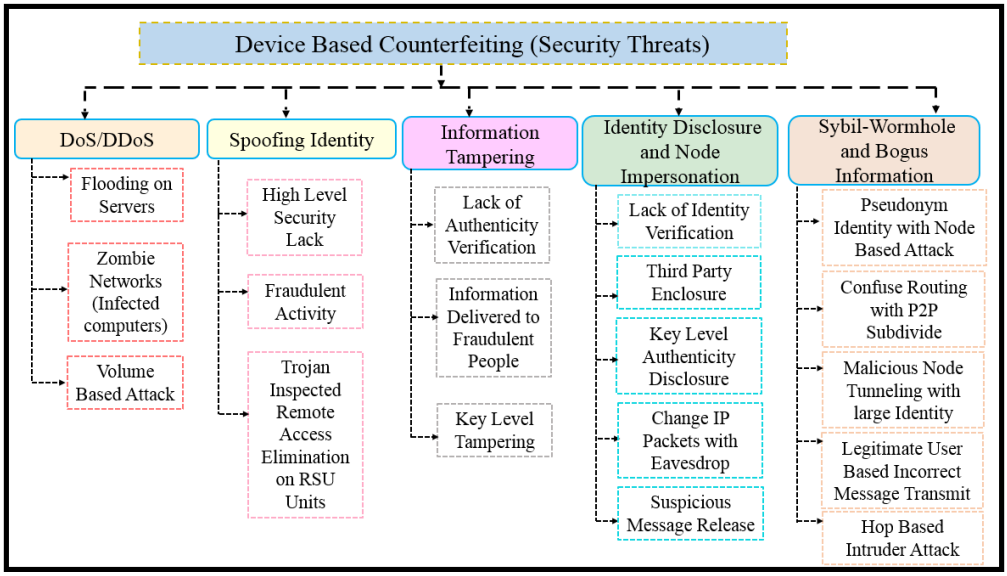


Figure 5 (a). VANET Security attacks and possible threats (Device Based Counterfeiting), [Part-I]

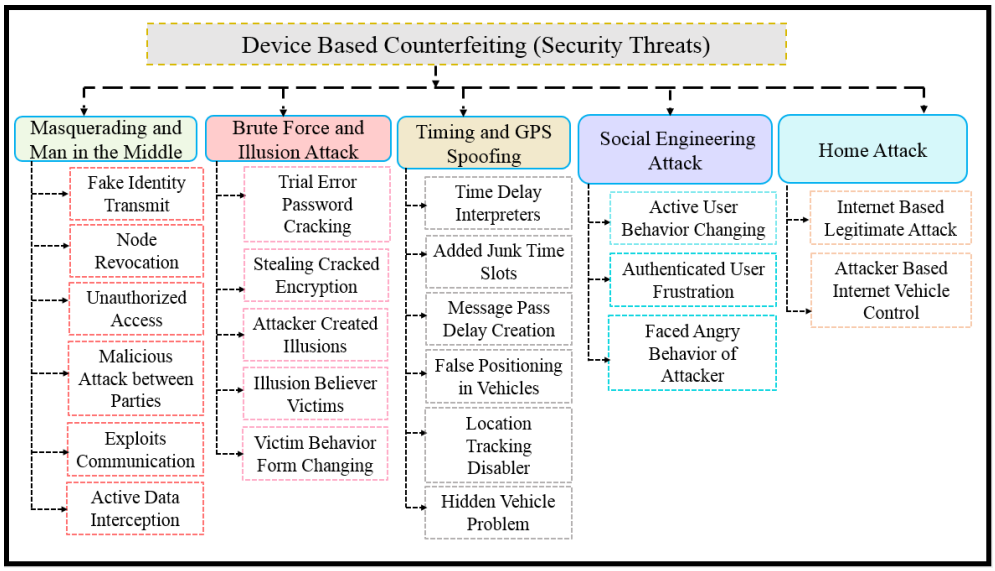


Figure 5 (b). VANET Security attacks and possible threats (Device Based Counterfeiting), [Part-II]

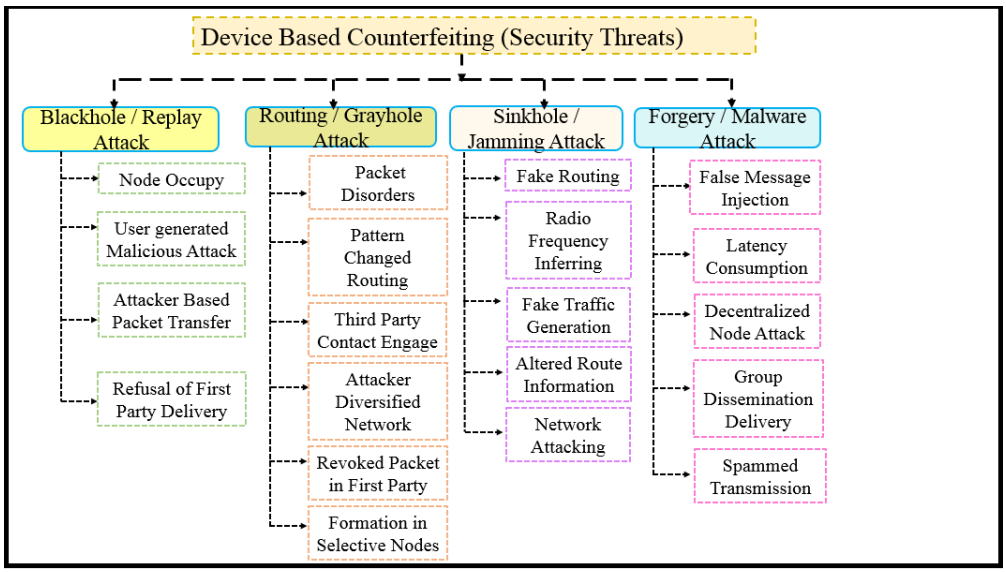


Figure 5 (c). VANET Security attacks and possible threats (Device Based Counterfeiting), [Part-III]

Checking and validating the taxonomies we can reduce the attacks in future VANET architectures as well as make additional alignments towards security enhancements. The taxonomies related to Figures 5 (a), (b) and (c) describe possible security attack problems and remedies in terms of device based counterfeiting within VANET modular activities.

6. FUTURE RESEARCH CHALLENGES AND OPEN ISSUES IN VANET SECURITIES

6.1. Cryptographic approaches for security, privacy, and non-traceability assurance:

Cryptographic approaches for ensuring security, privacy, and non-tracking: Key distribution patterns must exclude the government and automobile manufacturers. Secured authentication patterns, key sizes, and hashing mechanisms require certain protocols to be specified by the guaranteed authority; otherwise, they are susceptible to forgery by third-party eavesdroppers. Network data overhead may result from excessive key exchange delay; hence, switching certificate privacy may include authenticated servers known to the authority and published to all VANET users. Non-traceability and privacy assurance are greatly desired as a network grows in size and number of active users. In this scenario, partial pseudonym distribution and butterfly encryption strategy could be employed for resource-constrained VANET node execution to improve linkage values. Frequent IP switching within the DHCP protocol to reduce security counterfeiting or time threshold-based MAC initialization by VANET-networked cars to reduce position tracking or traceability of hashed IP utilizing trust functions could be a promising future development [28, 36, 48].

6.2. Trust and verification in Data Management:

Vehicle ad hoc networks (VANET) were created to improve their security. It administers a cooperative driving strategy that eliminates theft, impersonation, and accidents that endanger human life. This frequently necessitates self-organizing nodes to alert the drivers of any impending danger in the vehicle. The information exchanged through VANET must be protected and regulated by a verified source to destination media. For unneeded accident warnings, further study is required into data-centric verification and trust employing robust hardware. Deploying an intrusion detection system within a VANET-encompassed vehicle fleet necessitates context verification while examining and comparing environmental states and utilizing available personal data. Future trust-based data verification and management requires strengthening proactive and reactive security measures [28, 36, 48, 47].

6.3. Highly interactive mobile network environment for autonomous VANET nodes:

To reestablish data communication between group-organized nodes utilizing partition-based localization in a VANET-controlled region with a rapidly expanding user population. The key management inside the group formation is complex due to the usage of a central server [49], which may cause additional delays across the networks for security validations and requires proper authentication to prevent third-party access. Since the central server manages all the nodes for security validations, load reduction is crucial. He is in charge of key management and fundamental communication. After adhering to security configurations, each node must depart the contact pattern, and pair with another VANET node before security key verification and backup key restoration may be performed. The verification leave for pairing VANET devices is not completely obfuscated. This policy must be revised for the foreseeable future [28, 36, 48].

6.4. Highly interactive mobile network environment for self-organizing VANET nodes:

If any misbehavior is identified among the VANET-connected devices, the revocation procedure must be managed, and instructions must be sent. A certificate revocation list-based strategy requires more development. Certificate through cryptographic hash changing policies and short time generated certificates utilizing certificate revocation list yet not fully determined and poses an issue of infrastructure vulnerability [28, 27, 36, 48].

6.5. Trust-based secured Management in VANET:

i. The evaluation of the reliability of VANETs is a long-term concern. In VANET, any miscommunication between devices may endanger human life. We must develop an appropriate metric for evaluating the node-based trustworthiness of active VANET nodes. For confidence, we must examine and validate if a reliable count is scheduled as part of the essential message distribution plan for the roadside unit authorized center [20, 26, 46, 47].

ii. Detecting misbehaving activity across VANET nodes may be a crucial parameter for enhancing the security of vehicle IDs and backend services. To protect future VANET communications, the approximate actions for regulating hostile nodes and disinfected information delivery behavior must permit certain specific and appropriate measures (punishment or encouragement). These incentives may assist us in mitigating the growing threat posed by malicious node activity across VANET modules [28, 36, 48].

7. CONCLUSION AND REMARKS

We presented a comprehensive taxonomy of generic security enhancements, device-based counterfeiting, and cryptographic revocation structures essential for supporting existing and emerging systems in the VANET. The taxonomies developed in this work can serve as a valuable reference for future VANET technology and development researchers. Additionally, we discussed various RSU security improvements necessary for enhancing the security of VANET in smart cities. However, we also acknowledged that various challenges, such as cryptographic behavior, protected vehicular cloud computing, and rogue nodes' detection, significantly impact the ability to identify vehicle unawareness in urban and pre-urban settings. The taxonomy of generic security enhancements presented in this study includes various methods such as secure communication protocols, secure routing protocols, secure positioning protocols, and secure data dissemination protocols. These enhancements aim to provide secure communication between vehicles, vehicles and roadside units, and vehicles and other network entities. Finally, we also highlighted the challenges that need to be addressed to improve the security of VANET in smart cities.

ACKNOWLEDGMENTS

This research is partially supported through the Australian Research Council Discovery Project: DP190100314, "Re-Engineering Enterprise Systems for Microservices in the Cloud."

REFERENCES

[1] Road accidents biggest killer of young people – WHO: 2018. https://www.bbc.com/news/world-africa-46486231
[2] Nadeem Ahmed, Zhongliang Deng, Imran Memon, Fayaz Hassan, Khalid H. Mohammadani, and Rizwan Iqbal, "A Survey on Location Privacy Attacks and Prevention Deployed with IoT in Vehicular Networks." Wireless Communications and Mobile Computing, Article ID 6503299, 2022.
[3] Ghassan Samara and Mohammad Rasmi. "Deploying an Efficient Safety System for VANET." World of Computer Science & Information Technology Journal Vol. 5, No. 3, 2015, pp. 41-50.
[4] Christian Lochert, Björn Scheuermann, Christian Wewetzer, Andreas Luebke, and Martin Mauve. "Data aggregation and roadside unit placement for a vanet traffic information system." In Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking, pp. 58-65. 2008.
[5] Dongliang Su and Sanghyun Ahn. "Autonomous platoon formation for VANET-enabled vehicles." In 2016 International Conference on Information and Communication Technology Convergence (ICTC), pp. 247-250, 2016.
[6] C. P. U. Berkeley: 1986 California Partners for Advanced Transportation Technology (PATH). https://path.berkeley.edu/research/connected-automated-vehicles-and-active-safety
[7] P. d. T. NewCom: 2001 Institut Eurecom. Vanetmobisim. http://vanet.eurecom.fr/
[8] Felipe Cunha, Leandro Villas, Azzedine Boukerche, Guilherme Maia, Aline Viana, Raquel AF Mini, and Antonio AF Loureiro. "Data communication in VANETs: Protocols, applications and challenges." Ad Hoc Networks vol. 44, 2016, pp. 90-103..
[9] Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. Shen, "Software Defined Space-Air-Ground Integrated Vehicular Networks: Challenges and Solutions," IEEE Communications Magazine, vol. 55, no. 7, pp. 101−109, 2017.
[10] Kan Zheng, Hanlin Meng, Periklis Chatzimisios, Lei Lei, and Xuemin Shen. "An SMDP-based resource allocation in vehicular cloud computing systems." IEEE Transactions on Industrial Electronics vol 62, no. 12, 2015, pp. 7920-7928.
[11] H. Zhang, Q. Zhang, and X. Du, "Toward vehicle-assisted cloud computing for smartphones,"IEEE Transactions on Vehicular Technology, vol. 64, no. 12, 2015, pp. 5610−5618,.
[12] Clara Marina Martinez, Mira Heucke, Fei-Yue Wang, Bo Gao, and Dongpu Cao. "Driving style recognition for intelligent vehicle control and advanced driver assistance: A survey." IEEE Transactions on Intelligent Transportation Systems vol. 19, no. 3, 2017, pp. 666-676.
[13] Nabeel Akhtar, Sinem Coleri Ergen, and Oznur Ozkasap. "Vehicle mobility and communication channel models for realistic and efficient highway VANET simulation." IEEE Transactions on Vehicular Technology vol. 64 No.1, 2014, pp. 248-262.
[14] Clayson Celes, Fabricio A. Silva, Azzedine Boukerche, Rossana Maria de Castro Andrade, and Antonio AF Loureiro. "Improving vanet simulation with calibrated vehicular mobility traces." IEEE Transactions on Mobile Computing vol.16, no. 12, 2017, pp. 3376-3389.
[15] Xiaoxiao Jiang, and David HC Du. "PTMAC: A prediction-based TDMA MAC protocol for reducing packet collisions in VANET." IEEE Transactions on Vehicular Technology vol. 65 No. 11, 2016, pp. 9209-9223.
[16] Yuanguo Bi, Haibo Zhou, Wenchao Xu, Xuemin Sherman Shen, and Hai Zhao. "An efficient PMIPv6-based handoff scheme for urban vehicular networks." IEEE Transactions on Intelligent Transportation Systems vol. 17, no. 12, 2016, pp. 3613-3628.
[17] Omar Sami Oubbati, Abderrahmane Lakas, Fen Zhou, Mesut Güneş, Nasreddine Lagraa, and Mohamed Bachir Yagoubi. "Intelligent UAV-assisted routing protocol for urban VANETs." Computer Communications vol. 107, 2017, pp. 93-111.
[18] Lucas Mearian, "Self-driving vehicles could create 1GB of data a second", Computerworld, 2013. https://www.computerworld.com/article/2707396/self-driving-cars-could-create-1gb-of-data-a-second.html.
[19] Raul Mur-Artal, Jose Maria Martinez Montiel, and Juan D. Tardos. "ORB-SLAM: a versatile and accurate monocular SLAM system." IEEE Transactions on Robotics vol. 31 No. 5, 2015, pp. 1147-1163.
[20] Google's self-driving vehicle: 2022. https://www.theguardian.com/technology/2022/mar/30/waymo-self-driving-ride-hailing-service-san-francisco-alphabet-google
[21] Li Li, Wu-Ling Huang, Yuehu Liu, Nan-Ning Zheng, and Fei-Yue Wang. "Intelligence testing for autonomous vehicles: A new approach." IEEE Transactions on Intelligent Vehicles vol. 1, no. 2, 2016, pp. 158-166.
[22] Mobileye autonomous driving: 2020. https://www.mobileye.com/solutions/super-vision/
[23] M. Bojarski, D. Testa, D. Dworakowski, B. Firner, B. Flepp, P. Goyal, L. D. Jackel, "End to end learning for self-driving vehicles," arXiv preprint arXiv:1604.07316, 2016.
[24] Chenyi Chen, Ari Seff, Alain Kornhauser, and Jianxiong Xiao. "Deepdriving: Learning affordance for direct perception in autonomous driving." In Proceedings of the IEEE international conference on computer vision, pp. 2722-2730, 2015.
[25] Heiko G. Seif and Xiaolong Hu. "Autonomous driving in the iCity—HD maps as a key challenge of the automotive industry." Engineering 2.2 (2016): 159-162.
[26] Autonomous Automotive Cybersecurity: 2022. https://cyberstartupobservatory.com/cyber-security-connected-autonomous-vehicles/
[27] Joshua Joy, Vince Rabsatt, and Mario Gerla. "Internet of Vehicles: Enabling safe, secure, and private vehicular crowdsourcing." Internet Technology Letters vol.1 No. 1 2018, e16.

[28] Md. Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya. "A survey on vehicular cloud computing." Journal of Network and Computer applications vol. 40, 2014, pp. 325-344.
[29] Md. Whaiduzzaman, Anjum Naveed, and Abdullah Gani. "MobiCoRE: Mobile device based cloudlet resource enhancement for optimal task response." IEEE Transactions on Services Computing vol. 11 No. 1, 2016, pp.144-154.
[30] Abdullah Gani, Golam Mokatder Nayeem, Muhammad Shiraz, Mehdi Sookhak, Md Whaiduzzaman, and Suleman Khan, "A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing." Journal of Network and Computer Applications vol. 43, 2014, pp. 84-102.
[31] Md Whaiduzzaman, Abdullah Gani, Nor Badrul Anuar, Muhammad Shiraz, Mohammad Nazmul Haque, and Israat Tanzeena Haque "Cloud service selection using multicriteria decision analysis." The Scientific World Journal 2014, Article ID 459375.
[32] Deba Prasead Mozumder, Julkar Nayeen Mahi, Md Whaiduzzaman, and Md Julkar Nayeen Mahi. "Cloud computing security breaches and threats analysis." International Journal of Scientific & Engineering Research vol. 8, no. 1, 2017, pp. 1287-1297.
[33] Md. Whaiduzzaman, Julkar Nayeen Mahi, Alistair Barros, Md Ibrahim Khalil, Colin Fidge, and Rajkumar Buyya. "BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture." IEEE Access vol. 9, 2021, pp. 106655-106674.
[34] Md. Whaiduzzaman, Khondokar Oliullah, Md Julkar Nayeen Mahi, and Alistair Barros. "AUASF: An anonymous users authentication scheme for fog-IoT environment." In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-7. 2020.
[35] Farjana, Nishat, Shanto Roy, Md Julkar Nayeen Mahi, and Md Whaiduzzaman. "An identity-based encryption scheme for data security in fog computing." In Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018, pp. 215-226.
[36] Md. Whaiduzzaman, Nishat Farjana, Alistair Barros, Md Mahi, Julkar Nayeen, Md Satu, Shanto Roy, and Colin Fidge. "HIBAF: A data security scheme for fog computing." Journal of High Speed Networks vol. 27, no. 4, 2021, pp. 381-402.
[37] Shanto Roy, Ahmedur Rahman Shovon, and Md Whaiduzzaman. "Combined approach of tokenization and mining to secure and optimize big data in cloud storage." 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). IEEE, 2017.
[38] Shanto Roy, Md Ashaduzzaman, Mehedi Hassan, and Arnab Rahman Chowdhury. "Blockchain for IoT security and management: Current prospects, challenges and future directions." In 2018 5th International Conference on Networking, Systems and Security (NSysS), pp. 1-9. IEEE, 2018.
[39] Ahmedur Rahman Shovon, Shanto Roy, Tanusree Sharma, and Md Whaiduzzaman. "A restful e-governance application framework for people identity verification in cloud." In Cloud Computing–CLOUD 2018: 11th International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25–30, 2018, Proceedings 11, pp. 281-294. Springer International Publishing, 2018.
[40] Md Torikur Rahman, and Md Julkar Nayeen Mahi. "Proposal for SZRP protocol with the establishment of the salted SHA-256 Bit HMAC PBKDF2 advance security system in a MANET." 2014 International Conference on Electrical Engineering and Information & Communication Technology. 2014.
[41] Md. Mahi, Julkar Nayeen, Milon Biswas, Obonee Kushum, Md Whaiduzzaman, and Shamim Al Mamun. "A new unified communication approach to comply bandwidth optimization technique using dynamic channel allocation." International Journal of Computing and Network Technology vol. 6, no. 01, 2018, pp. 1-11.
[42] Md. Mahi, Julkar Nayeen, Sudipto Chaki, Shamim Ahmed, Iffat Tamanna, and Milon Biswas. "LCADP: a low-cost accident detection prototype for a vehicular ad hoc network." In Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021, pp. 391-403.
[43] Xin Liu, Dongyue He, and Hua Ding. "Throughput maximization for UAV-enabled full-duplex relay system in 5G communications." Physical Communication vol. 32, 2019, pp. 104-111.
[44] Said Ghendir, Salim Sbaa, Ali Al-Sherbaz, Riadh Ajgou, and Ali Chemsa. "Towards 5G wireless systems: A modified Rake receiver for UWB indoor multipath channels." Physical Communication, vol. 35, 2019, pp. 100715.
[45] Rakib Hossen, Md Whaiduzzaman, Mohammed Nasir Uddin, Md Jahidul Islam, Nuruzzaman Faruqui, Alistair Barros, Mehdi Sookhak, and Md Julkar Nayeen Mahi. "BDPS: An efficient spark-based big data processing scheme for cloud fog-iot orchestration." Information vol. 12, no. 12, 2021, pp. 517.
[46] Sagheer A. Jan, Noor Ul Amin, Mohamed Othman, Mazhar Ali, Arif Iqbal Umar, and Abdul Basir. "A survey on privacy-preserving authentication schemes in VANETs: attacks, challenges and open issues." IEEE Access vol. 9, 2021, pp. 153701-153726.
[47] Bhanu, Chander. "Challenges, Benefits and Issues: Future Emerging VANETs and Cloud Approaches." Cloud and IoT-Based Vehicular Ad Hoc Networks, 2021, pp. 233-267.
[48] Md. Mahi, Julkar Nayeen, Sudipto Chaki, Shamim Ahmed, Milon Biswas, Shamim Kaiser, Mohammad Shahidul Islam, Mehdi Sookhak, Alistair Barros, and Md Whaiduzzaman. "A review on VANET research: Perspective of recent emerging technologies." IEEE Access vol. 10, 2022, pp. 65760-65783.
[49] Hossain, Md Razon. "A scheduling-based dynamic fog computing framework for augmenting resource utilization." Simulation Modelling Practice and Theory vol. 111, 2021, pp. 102336.

BIOGRAPHY OF AUTHORS

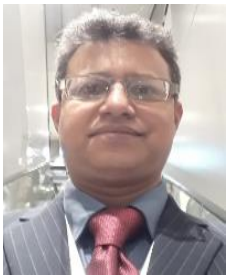
Md. Julkar Nayeen Mahi has successfully completed his B.Sc. and M.Sc. degree from IIT, Jahangirnagar University, Bangladesh. He is serving as a `Lecturer' in Daffodil International University, Bangladesh. His current research interests are mainly in Distributed computer networks, Embedded systems, IoT, Data mining, Cloud computing, Operating Systems Scheduling approach, Network securities and Bio informatics. Recently he has published a paper in IEEE Access regarding VANET up gradation through emerging technologies.

Sudipto Chaki received his B.Sc degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh. He is currently working as a full-time "Lecturer" in Bangladesh University of Business and Technology (BUBT), Dhaka, Bangladesh. His current research interests include machine learning (ML), computer vision (CV), digital image processing (DIP), computer networks (CN), and Internet of Things (IoT). He has multiple publications in different research fields. He received the best paper award from the conference of Trends in Electronics and Health Informatics, Springer

Esraq Humayun received his B.Sc. and M.Sc. degree in Software Engineering from American International University of Bangladesh. He is currently working as a lecturer in Daffodil International University Software Engineering Department. His current research interest includes Machine Learning, Cyber Security, Big Data and Internet of Thing. He previously worked as a software developer in A2I ICT Division and also as a Team Leader in OK Technology Sydney.

Hafizul Imran received his B.Sc in Electrical and Electronic Engineering degree from Daffodil International University, Bangladesh. He is currently working as a full-time "Sr.Lecturer" in Daffodil International University, Dhaka, Bangladesh. His current research interests include machine learning (ML), Robotics, Embedded Systems and Internet of Things (IoT). He has multiple publications in different research fields. He received the national hackathon award from Start-Up Village 2018, Skolkovo, Moskow, Russia. Recently he published in an article named - Nishash: A Reasonable Cost-Effective Mechanical Ventilator for COVID Affected Patients in Bangladesh in 'Heliyon' ISI indexed journal from Elsevier, Press, Netherlands.

Dr. Alistair Barros is a Professor of Information Systems and Head of the Services Computing Program, at QUT's Information Systems School. He has 32 years ICT experience across industry, industrial R&D and academic roles, including Global Research Leader and Chief Development Architect at SAP AG and his research interests include Cloud, enterprise systems and microservices engineering, evolution and provisioning using model-based techniques.



Dr. Md Whaiduzzaman completed his undergraduate degree in Electronics & Computer Science and M.Sc. in Telecommunication & Computer Network Engineering from London, UK. He also completed his PhD degree, at University of Malaya, Malaysia. He serves as a Professor in the Institute of Information Technology (IIT), Jahangirnagar University. Presently, he works in an ARC funded projects at Queensland University of Technology, Australia. His research interests are Mobile Cloud Computing, Vehicular cloud computing, Fog Computing, Microservices, IoT and Cyber Security. Recently, he received the Elsevier JNCA best paper award in Paris, France.