ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse801022021.pdf
https://doi.org/10.30534/ijatcse/2021/801022021

Cloud Based Approach to Enhance Security in VANET Communication

A.Sajithabegam[1], Karan V[2] , Nithish Kumar G[3,] Venkatesh Prasad D[4]
[1]Assistant Professor, india, sajiasad24@gmail.com
[2]Student, India, aceit294@gmail.com
[3]Student, India, mba.sheriffdeen@gmail.com
[4]Student, India

ABSTRACT

Within the last decade, there has been growing interest in transport unintended Networks (VANETs). These days automotive makers have already began to equip vehicles with subtle sensors which will give several helpful options like front collision shunning, automatic lane following, partial autonomous driving, suggestive lane dynamic , and so on. Such technological advancements are facultative the adoption of VANETs not solely driving expertise however additionally provide several different helpful services to the motive force similarly as passengers of a vehicle. However, privacy, authentication and secure message dissemination are a number of the most problems that require be completely addressing and resolving for the widespread adoption/deployment of VANETs. Given the importance of those problems, researchers have spent heaps of effort in these areas over the last decade. We have a tendency to gift a summary of the subsequent problems that arise in VANETs: privacy, authentication, and secure message dissemination. Then we have a tendency to gift a comprehensive review of assorted solutions projected within the last ten years that address these problems. Our survey sheds lightweight on some open problems that require to be addressed within the future.

Keywords
VANETs, transport networks, Securing VANETs

1. INTRODUTION

Several applications like early warning systems which may warn concerning construction, collisions, weather-related hazards, merging lanes, speed limits for curves, and crossing warnings, are prepared for the widespread readying in transport Ad-hoc Networks (VANETs). Aside from aiding drivers to drive safely, VANETs may give pica to drivers/passengers for an additional pleasant driving similarly as riding expertise. Moreover, VANETs may assist in paying for parking and tolls, finding parking places, change built-in vehicle navigation systems with period of time traffic state of affairs, and downloading music, video and software package updates [1], [2], [3]. VANETs may assist enforcement agencies in reconstructing accidents similarly as reaching the situation of the accidents quicker.

The general model of VANETs projected within the literature consists of 2 major components: On Board Units (OBUs), put in on vehicles, and Road aspect Units (RSUs) put in on edge to support the infrastructure required for the readying of VANETs. every vehicle is assumed to be equipped with a group of sensors to gather phenomena encompassing the vehicle; the OBU processes the data collected by the sensors and sends/receives them to/from different relevant vehicles directly or through near RSUs [4]. The RSUs can also connect with the web to produce the mandatory services to vehicles. A broad vary of applications may be enabled by 2 main forms of communication: (i) infrastructure-based communication (Vehicle to Infrastructure (V2I) communication) and (ii) direct communication between vehicles (Vehicle to Vehicle (V2V) communication) [5] as shown in Fig. 1. Major efforts for standardizing VANETs communication protocols are applied by the IEEE 802.11 Task cluster by process enhancements to IEEE 802.11 needed to support Intelligent Transportation Systems (ITS) applications. This change is presently called IEEE 802.11p. The wireless communication capability between moving vehicles is achieved by exploitation Dedicated Short vary Communication (DSRC). It's anticipated that DSRC are used for each V2V communication and V2I communication. The spectrum is seen as significantly helpful as a result of it will support low-latency, secure transmissions, quick network acquisition and has the power to handle fast and frequent hand-over's that are inherent in VANETs; it's additionally strong in adverse weather [6].

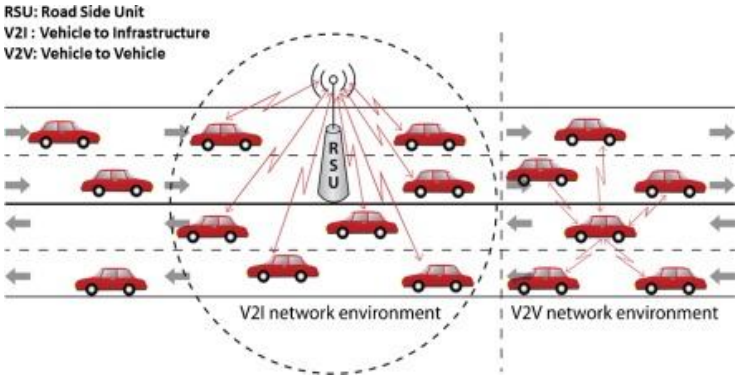

Figure. 1. VANET communication - infrastructure-based and infrastructure-less.

Although the thrill encompassing the potential advantages of VANETs is growing, the dynamic nature of VANETs (vehicles will be part of and leave at will) in conjunction with a mess of system and application connected necessities create it terribly difficult to style economical strategies for guaranteeing privacy of vehicles. Privacy refers to the privacy of the vehicles (drivers) and therefore the location of the vehicles. Once a vehicle sends a message, nobody (except relevant authorities) ought to be able to confirm the identity or location of the vehicle from the messages a vehicle sent. At a similar time, all messages sent by a vehicle ought to be attested before being processed shown in figure one till these issues are resolved to the simplest satisfaction of the users, widespread readying of VANETs cannot come about. Authentication has to be achieved at 2 levels – initial at node level, referred as node authentication and second at the message level, referred as message authentication [7]. The fundamental principle of message authentication may be simplified as sign language a message by the sender so corroboratory the credibleness and integrity of the message at the receiver's finish. Sure authentication necessities like low machine overhead, robust and climbable authentication, economical and climbable certificate revocation should be addressed and resolved to confirm secure communication in VANETs.

Since info} requests uploaded by vehicles are tightly related to the in person recognizable information (PII) of individuals on-board. If an information request may be unambiguously coupled to a vehicle, some privacy-sensitive info can be disclosed (such as hospitals or churches), and people info should be strictly prohibited from unauthorized access. Even supposing incontrovertibly sensible privacy in VANETs may be achieved with pseudonyms [5], [6], associate oppose will still associate an information request with a specific vehicle, and more infer the driver's mechanical phenomenon and behavioral pattern through observation. However, once there exist a bunch of vehicles causing information requests along, it's extremely attainable that the info request uploaded by one vehicle is indistinguishable from the remainder of information requests, i.e., by disrupting the association between one vehicle and its information request.

If a bunch of information requests are processed on an individual basis, it might bring serious computation and communication prices towards the RSU, particularly once there is an outsized variety of information querying vehicles. Thus, the uploaded information requests ought to be processed aggregately, and therefore the projected theme ought to even be adaptive to the unsteady variety of querying vehicles within the spatio-temporal domain. To attain privacy-preserving information aggregation, a secure multi-dimensional information aggregation theme is projected in [6], within which every dimension of information aggregation will still be recovered once coding. Specifically, the projected theme structures the multi-dimensional information report with a super-increasing sequence, and encrypts the info with the homomorphism Paillier cryptosystem, that achieves the ciphertexts aggregation and quality reduction. To preserve the situation privacy of the taking part vehicles, a privacy preserving route reportage aggregation theme in VANET is projected in [7] that utilizes the homomorphic cryptography technique to count the quantity of vehicles in every route phase.

2. RELATED WORKS

Recent enhancements in software package, hardware and communication technologies are empowering the planning and implementation of many forms of networks deployed in numerous environments. For the previous few years, one such network that has received a lot of attention is that the transport Ad-Hoc Network (VANET) (Olariu et al., 2011; Zeadally et al., 2012). A VANET may be a set of moving vehicles in a very wireless network that apply the data Communication Technology (ICT) to produce progressive services of traffic management and transport. Presently, VANET has received important thought as a result of the prospect of facultative novel and engaging solutions in areas like vehicle and road safety, traffic potency and Intelligent Transportation Systems (ITS) (AlSultan et al., 2013; Hartenstein and Laberteaux, 2008).

The promise of transport networking has semiconductor diode to a quick convergence with ITS and to the arrival of Intelligent transport Networks (Hossain et al., 2010), that ar anticipated to rework driving designs by making a secure, safe and healthy surroundings that may ultimately cover our busy town streets and highways. Thus, the intelligent transport networks can give pic and can alter a replacement versatile system that enhances transportation potency and safety (Olariu et al., 2013).Although several efforts are created to succeed in these objectives, VANET has many drawbacks, like the high value of the service unnatural communications because of the high quality of the vehicle (Akbari Torkestani, 2012; Qin et al., 2012).

Advances in transport technology have provided resources like storage devices, higher computing power, psychological feature radios, and differing types of programmable detector nodes. By exploitation Wireless detector Networks (WSNs), intelligent applications enhance IT'S and might improve each driving safety and traffic potency (Fonseca and Vazão, 2012). The arrival of mobile net in vehicles brings along the innovative and, wide divergent advantages of the web and such developments have an amazing social impact (Goggin, 2012).Therefore, within the futures, cars and vehicles are ubiquitously furnished communication, computing and sensing devices, and universal networks can create the web out there on the move. Thus, the driving expertise is additional pleasant, comfortable, safe and environmental friendly. Eventually, the billboards of our highways are changed for in-vehicle advertising, wherever the motive force will select promotional material supported their desires. However, the outstanding array of on board computing talents gift in our vehicles is possibly not utilized by the applications mentioned above (Karagiannis et al., 2011).Mobile Cloud Computing (MCC) may be a new paradigm which will be employed by vehicle drivers to leverage services as a utility by

a pay as you go model, and might method an outsized quantity of information on demand anytime from anyplace (Abolfazli et al, 2013).

The drivers will use their mobile devices to attach to the cloud via the web. MCC provides the essential surroundings and foundation to integrate platforms and technology that may monitor road safety by process detector network information exploitation completely different mobile cloud architectures, like Platform as a Service (PaaS). However, the mobile devices suffer from computing resources limitations, battery restriction and time interval (Shiraz et al., 2012).In addition, uploading period of time info on the cloud like hold up or accident state of affairs, by exploitation the web is dear and time overwhelming (Fernando et al., 2013).Vehicular Cloud Computing may be a new technological shifting, that takes advantage of cloud computing to serve the drivers of VANETs with a pay as you go model. Thus, the objectives of VCC are to produce many machine services at low value to the vehicle drivers; to attenuate tie up, accidents, time period and environmental pollution; and to confirm uses of low energy and real time services of software package, platforms, and infrastructure with QOS to drivers (Gerla, 2012). VCC will address the convergence of IT'S and therefore the tremendous computing and storage capabilities of MCC. Moreover, VCC provides a technically possible incorporation of the ever present sensing of WSN, ITS and MCC for higher road safety and secured intelligent urban traffic systems (Tekbiyik and UysalBiyikoglu, 2011; Wang et al., 2011).

We are driven as a result of the communication, storage and computing resources offered within the vehicles are usually underutilized. Combining these resources meaningfully can have a significant influence on society. Per se the underutilized transport resources together with computing power, internet connections and storage facilities are often pooled with those of alternative drivers on the road or rented to customers, like the means within which the resources of the current typical cloud are provided. With current technology, transport Clouds are technologically possible and economically viable and can be consequent paradigm shift. They'll give several advantages, together with social and technological impacts. the concept of a transport Cloud is recent (Olariu and Weigle, 2009) and our stress is on the possible applications and important aspects of analysis challenges.In this paper, we have a tendency to highlight transport Clouds (Olariu et al., 2013; Olariu et al., 2011), Associate in Nursing extension of typical Cloud Computing with many new dimensions. Our aim during this paper is to assist readers higher perceive the elemental transport cloud computing mechanisms and suggests the potential applications for up transport network and road safety. We have a tendency to gift a comprehensive taxonomy of transport networking and a comparative study between CC and VCC. Additionally, we have a tendency to justify the VCC design, autonomous cloud formation and therefore the in depth application situation. Every vehicle in VCC will communicate to the opposite vehicles or the network infrastructures by victimization the vehicle to vehicle or the vehicle to infrastructure network communication. We have a tendency to describe a key management methodology to supply a secure communication within the transport network. What is more, we have a tendency to reason the transport networks supported the safety problems and solutions. The safety and privacy of VCC, the analysis challenges and open problems also are mentioned.

3. PROPOSED METHODOLOGY

Within the thesis, secure and privacy-preserving schemes are designed in transport networks, and therefore the specific details of the finished works are shown as follows. Because of the increasing quality of intelligent vehicles and therefore the recent flourishing of cloud computing, it becomes a recent analysis trend of extending cloud computing to vehicles by investing under-utilized on-board capabilities of vehicles. In transport cloud, 3 security schemes are designed during this thesis. Within the 1st theme, a unique location privacy-preserving information question theme is projected, with the projected theme; an information requester will retrieve the information generated by transport sensors from the distributed transport on-board storage with high accuracy. Since the bulk of intelligent vehicles are usually thought of as not absolutely used, these vehicles are candidates to supply distributed information assortment and storage services. By exploiting the homomorphic Paillier cryptosystem technique and therefore the structured binary scalars to represent the positions {of information|ofknowledge|of information} requesters and therefore the data generating vehicles, the projected theme are able to do the placement matching of the concerned entities with privacy-preservation. Within the second theme, Associate in nursing economical information sharing theme and site privacy-preservation in web of vehicles (IoV) is projected, that permits the gathering and distribution of the information captured by transport sensors. The information captured by transport sensors records a myriad of physical phenomena regarding the encompassing environments that permits the information sharing among vehicles and deployed edge infrastructures to more improve traffic safety and on-board expertise within the intelligent transit. With the projected theme, the multi-dimensional sensory information captured at totally different locations are 1st structured by the Chinese Remainder Theorem, then the changed Parlier cryptosystem is exploited to realize the placement privacy-preserving sensory information aggregation. Meanwhile, the projected theme exploits the proxy re-encryption technique to realize the sensory information acquisition at the network edge, while not the involvement of the trustworthy central entity. Within the third theme, a secure request-response primarily based transport information dissemination theme within the car parking zone situation is projected. The edge units (RSUs) deployed in transport unexpected networks (VANETs) will act as info servers to supply info to vehicles underneath their coverage space. The projected theme exploits Associate in Nursing invertible matrix to structure multiple information requests,

and encrypts the information requests with the homomorphic Paillier Cryptosystem technique. Supported the information requests aggregation, the RSU will recover the individual information request whereas protective the unlink ability between the information question and its origin. additionally, the RSU will verify the correctness of the recovered information requests while not privacy speech act by exploiting Associate in Nursing identity-based batch verification technique. To enhance the standard of the vehicle-to-infrastructure (V2I) communications, the LTE-A network is delivered to transport network for its dense preparation, high information measure and high-speed movement support. Specifically, 2 secure relinquishing key institution schemes are designed during this thesis. Within the 1st theme, a secure relinquishing session key management theme is meant in mobile relay LTE-A network. To be a lot of specific, a session key between the on-board user instrumentalities (UE) and therefore the Donor evolved Node B (DeNB) is 1st made by the UE so firmly delivered to the DeNB. It is able to do the safety goal of forward and backward key separations. Meanwhile, to decrease the communication and procedure burden of the projected theme, the proxy re-encryption technique is additionally used, i.e., the session keys are ab initio encrypted by the general public key of the quality management entity (MME) so re-encrypted by the mobile relay node (MRN), so the target DeNB will recover the worth of the session key with its personal key while not involving the core entity MME. within the second theme, a unique secure coordinated multi-point (CoMP) joint transmission relinquishing key institution theme in LTE-A transport networks is projected. Specifically, to realize the variety gain brought by the CoMP joint transmission and accommodate to shield the backward/forward key separation, the session key's ab initio made by the vehicle so firmly delivered towards the cooperating eNBs, so decrypted by every cooperating eNB severally.

In this paper, we have a tendency to highlight transport Clouds (Olariu et al., 2013; Olariu et al., 2011), Associate in Nursing extension of typical Cloud Computing with many new dimensions. Our aim during this paper is to assist readers higher perceive the elemental transport cloud computing mechanisms and suggests the potential applications for up transport network and road safety. We have a tendency to gift a comprehensive taxonomy of transport networking and a comparative study between CC and VCC. Additionally, we have a tendency to justify the VCC design, autonomous cloud formation and therefore the in depth application situation. Every vehicle in VCC will communicate to the opposite vehicles or the network infrastructures by victimization the vehicle to vehicle or the vehicle to infrastructure network communication. We have a tendency to describe a key management methodology to supply a secure communication within the transport network. What is more, we have a tendency to reason the transport networks supported the safety problems and solutions. The safety and privacy of VCC, the analysis challenges and open problems also are mentioned.

Vehicular cloud (VC) extends cloud computing to vehicles taking part in transport unexpected networks, getting to give computing and storage services at low value to vehicles, improve traffic potency and safety, guarantee period of time services, etc. because of the extremely dynamic nature of VC, it's difficult to expeditiously kind a dynamic VC firmly and anonymously or to firmly deliver messages to the dynamic VC while not doubtless violating the privacy of cloud users. During this paper, we have a tendency to gift a concrete secure and privacy-preserving communication theme for VC institution and information dissemination. Our theme permits a gaggle of vehicles that are geographically getting ready to one another to make a VC firmly, anonymously and dynamically. This enables vehicle resources to be integrated and shared firmly. Once a VC is created, any cloud user could deliver messages to be firmly and anonymously processed within the VC.

3.1 BLOCK DIAGRAM

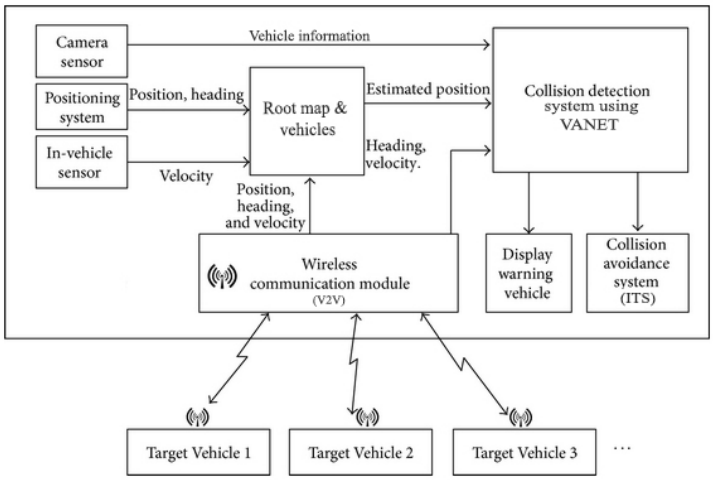

Figure 2: Block diagram

4. RESULT DICUSSION

4.1 Vehicular cloud (VC)

Vehicular cloud (VC) extends cloud computing to vehicles taking part in transport unexpected networks, getting to give computing and storage services at low value to vehicles, improve traffic potency and safety, guarantee period of time services, etc. because of the extremely dynamic nature of VC, it's difficult to expeditiously kind a dynamic VC firmly and anonymously or to firmly deliver messages to the dynamic VC while not doubtless violating the privacy of cloud users. During this paper, we have a tendency to gift a concrete secure and privacy-preserving communication theme for VC institution and information dissemination. Our theme permits a gaggle of vehicles that are geographically getting ready to one another to make a VC firmly, anonymously and dynamically. This enables vehicle resources to be integrated and shared firmly shown in figure 2 .Once a VC is created, any cloud user could deliver messages to be firmly and anonymously processed within the VC.

4.2 THE INTELLIGENT TRANSPORTATION SYSTEM

Vehicular networks have become a distinguished analysis field within the intelligent transit (ITS) because of the character and characteristics of providing high-level road safety and optimized traffic management. Vehicles are equipped with the significant communication system which needs a high power offer, on-board computing machine, and information storage devices. Several wireless communication technologies are deployed to take care of and enhance the traffic management system. The ITS is capable of providing services to the traffic authorities and preventative measures to the drivers and passengers. Many strategies are projected for discussing the safety and privacy problems for the transport unexpected networks (VANETs) and transport cloud computing (VCC). They receive an excellent deal of attention from researchers round the world since they're new technologies and that they will improve road safety and enhance traffic flow by utilizing the vehicles resources and communication system. Firstly, the VANETs are bestowed, together with the essential summary, characteristics, threats, and attacks. The placement privacy methodologies are careful, which might shield the wind of the vehicle, like the placement detail and driver info. Secondly, the trust management models within the VANETs are comprehensively mentioned, followed by the comparison of the cryptography and trust models in terms of various sorts of attacks. Then, the simulation tools and applications of the VANETs are mentioned, and therefore the evolution is bestowed from the VANETs to VCC within the transport network. Thirdly, the VCC is mentioned from its design and therefore the security and privacy problems. Finally, many analysis challenges on the VANETs and VCC are bestowed. In sum, this survey comprehensively covers the placement privacy and trust management models of the VANETs and discusses the safety and privacy problems within the VCC that fills the gap of existing surveys. Also, it indicates the analysis challenges within the VANETs and VCC.

4.3 VEHICLE-TO-VEHICLE (V2V) TECHNIQUE

VANETs square measure the kind of mobile unintended network (MANET), which might give the communication between the vehicles and infrastructures [3, 4]. The vehicle manufacturer and telecommunication industries square measure cooperating along to assemble every vehicle with the on-board unit (OBU) communication device, that square measure able to communicate with alternative vehicles by exploitation the vehicle-to-vehicle (V2V) technique and at the same time with the infrastructures by exploitation the vehicle-to-infrastructure (V2I) technique. The VANETs provides several blessings in terms of reducing road accidents, snug and pleasant driving, automobile parking, etc. moreover, it will serve the driving force and traveler with the weather data, music, picture, etc. [5]. The VANETs provides sturdy solutions in terms of road and vehicle safeties and improves the traffic flow and potency [6]. It conjointly provides the quick convergence of conveyance network with the IT'S to explore the advanced development of the intelligent conveyance network [7]. These advancements square measure expected to remodel driving options and experiences by making secure traffic surroundings as well as the town traffic and main road traffic. The conveyance network provides the picture services and enhances the potency of the ITS. Several contributions are created to get these goals. However, the demerits of VANETs conjointly seem, like the transmission overhead caused by the high-mobility vehicles [8]. Secure communication in VANETs is difficult thanks to completely different styles of threats and attacks [9]. Recently, analysis works are done to beat these problems and supply security solutions to tackle these attacks. within the VANETs, several existing security solutions associated with the cryptography technique give the secure communication by exploitation completely different security certificates [10], public key infrastructures (PKIs) [11], signatures [12], and trusty third parties [13]. In distinction, some high-mobility situations can't be performed well while not the infrastructure; therefore, the cryptography answer is restricted that isn't able to give secure communication within the VANETs. Once a trustworthy user becomes a malicious node or additional prone to be attacked, then the upper likelihood of cryptography answer is being compromised and will be overtaken [14]. Within the VANETs, the trust management relies on the direct interactions and indirect recommendation between vehicles. Therefore, the analysis of trust depends on this scenario in terms of knowledge exchanges [14]. Trust models within the VANETs square measure classified into 3 types: entity-oriented model, data-oriented model, and hybrid trust model [15]. The trust model is capable of addressing the within attackers wherever the cryptography is unable to handle these attacks within the VANETs. However, the cryptography is in a position to handle outside unauthorized attacks. Shown in figure 3.

Recent development and advances within the conveyance technology give several resources like storage devices, radio network, sturdy process power, and completely different styles of vehicle sensors. Challenges and advantages within the ITS have driven the researchers to introduce and promote the conveyance cloud computing (VCC) [16]. It aims to produce the services to the drivers, improve the traffic flow, scale back the holdup and accident, and make sure the usage of the period software system and infrastructure with the standard of service (QoS) to drivers [17]. Specifically, the VCC will be the platform for the convergence of the IT'S and therefore the computing and storage capabilities of the mobile cloud computing (MCC). Moreover, the VCC will incorporate the options of ITS, WSN, and MCC for providing a much better road safety, up the driving conditions and therefore the secured traffic management system [18].

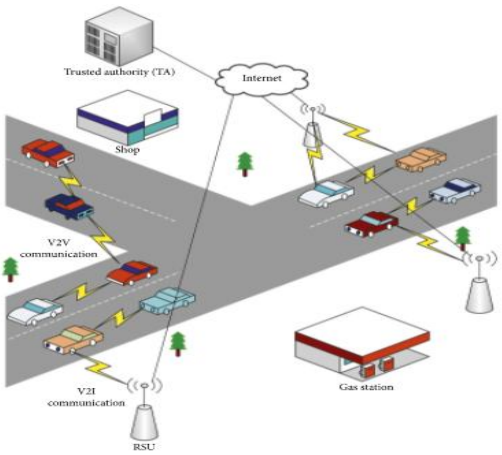

Figure 3:V2V Communication

4.4 VANETs CHARACTERISTICS

The VANETs square measure extremely dynamic unintended networks with high reliableness, giving multiple services, however have restricted accesses to the network infrastructure. VANETs have characteristics of high quality and frequent modification in topology as compared to the MANETs [1, 46], and might be any classified into the topology and communication mode also because the vehicle and driver mode. The characteristics of the VANETs square measure as follows:

i)High quality: VANETs have high mobility as compared with the MANETs. The high quality is one amongst the most options and plays an awfully vital role within the modeling of VANET protocol. Each node within the VANET moves on terribly high speed. Therefore, the high quality of nodes reduces the communication time within the network [5].

(ii)Driver safety: VANETs will improve the driving force safety, enhance the traveler comfort, and improve the traffic flow. The most advantage of VANETs is that the vehicles will communicate directly with one another. It permits variety of applications to speak among completely different nodes like the RSUs and OBU.

(iii)Dynamic network topology: the topology of VANETs varies speedily supported the vehicle speed and high quality. The speedy changes in vehicle quality create VANETs additional prone to attacks and conjointly terribly tough to acknowledge the suspected vehicles.

(iv)Frequent network disconnection: the frequent disconnection of the VANETs square measure thanks to the high-speed movement among vehicles and alternative problems like the atmospheric condition. An oversized variety of vehicles on the road can even result in the repeated disconnection.

(v)Transmission medium: the transmission medium is that the air within the VANETs, and therefore the universal accessibility of the wireless medium will be a sturdy advantage within the intervehicle communication (IVC), however there still square measure some security issues that rely on the character of transmission and therefore the security of communication by exploitation associate open support [1].

(vi)No power constraints: there's no power constraint in VANETs as compared to MANETs; therefore, the vehicle provides continuous power to the OBU through the durable battery.

(vii)Limitation of transmission power: the transmission power is unnatural within the wireless access of conveyance surroundings (WAVE) that ranges from zero to twenty-eight.8 dBm with the associated coverage distance ranges from 10 m to 1 km. Thus, the restricted power transmission will have an effect on the coverage distance of VANETs.

Secure content distribution and promotional material dissemination in VANETs

RSUs offers numerous services like net access, real time traffic information access, maps, and media files transfer and software system updates transfer through high speed networks. Vehicles will create use of those services by connecting to the RSUs through VANET. Several of the analysis works on this sort of service-oriented conveyance communication failed to take information security and placement privacy of the users into thought. Recently, advertisements of business product to vehicles have been known as a promising application for VANETs. However dissemination of advertisements will be ineffective and insecure within the presence of non-cooperative ungenerous vehicles and malicious vehicles. During this section, we have a tendency to discuss the protocols designed for secure content distribution/downloading and promotional material dissemination in VANETs.Huang et al. propose associate Anonymous Batch Authentication and Key Agreement (ABAKA) theme to facilitate the readying of added services in VANETs. To support added services provided by Service suppliers (SPs), communication between vehicles and SPs ought to be secure and therefore the message authentication method ought to be economical. ABAKA addresses this issue and permits multiple vehicles to be documented in batches, instead of one vehicle at a time. It permits the creation of pseudonyms and therefore the individual personal keys for every vehicle to confirm conditional privacy. The same as the approach taken by metal et al. [30], the Tamper-Proof Device (TPD) will generate personal keys supported Elliptic Curve Cryptography (ECC) and therefore the associated pseudonyms and store them. Requiring each vehicle to possess a tamper-proof device put in could limit the participation of vehicles in VANET. Moreover, TPDs factory-made is also able to resist well-known attacks, however not essentially all future attacks; TPDs may even be vulnerable to side-channel attacks mentioned in.

Lee et al. Propose a Signature-Seeking Drive (SSD) that makes the dissemination of advertisements (ads) secure however conjointly counsel providing incentives within the type of virtual money to encourage non-cooperative vehicles to participate in ad dissemination. Several of the prevailing incentive schemes suppose tamper-proof hardware, however this theme leverages on the general public key infrastructure to produce incentives firmly for cooperating nodes in each single level and construction transactions. During this theme,

the conveyance Authority (VA) is accountable of promotional material authorization and maintenance. The VA conjointly maintains the records of all the transactions. Once a vehicle receives a poster, it verifies the credibility of the received ad and sends back its signed receipt to the sender of the add Thus, this theme prevents the dissemination of false or dummy ads. However, once the quantity of co-operating vehicles will increase, this could lead to overspending on incentives and thence this approach might not be profitable to advertisers.

The Trajectory-aware Content distribution strategy (TraC), planned by timber et al, uses Content-Centric Networks (CCN) to create persistent proactive caches in RSUs. TraC relies on users' mechanical phenomenon to extend the likelihood of content delivery, that wasn't antecedently taken into consideration within the CCN based mostly analysis works in VANET situations. During this theme, RSUs will pro-actively transfer the content requested from the web even before the arrival of a vehicle at intervals the zone of associate RSU. Therefore the vehicle doesn't have to stay up for the content to be downloaded once it arrives within the zone of associate RSU. Triangular space Forwarding (TAF) and Distance step-down Forwarding (DMF) techniques, and {a neighborhood|ansquare measurea|adistrict|aregion|alocality|avicinity|apart|a section} discovery protocol are wont to forward interest of vehicles to RSUs. The performance of Trace with relevancy the content delivery magnitude relation, and the way quick content and interest's square measure glad is evaluated within the urban, main road and a practical rush-hour (using Cologne dataset [39]) situation. Their analysis shows that Trace satisfies additional users' interests and quicker compared to typical CCNs normally, and satisfies five hundredth additional interests within the urban situation. The screenshot of message transfer is shown in figure 3, 4,5,6,7.

Ramakrishnan et al. gift a cluster-based rule for broadcasting emergency messages in VANETs. They initial type clusters and therefore the cluster-heads square measure to blame for intra-cluster management. They conjointly use macintosh layer broadcast protocols for increasing the reliableness of emergency message dissemination. Nkenyereye et al. gift a conveyance cloud based mostly traffic information dissemination protocol. He et al. gift a dropbox based mostly approach for dispersive messages in VANETs. The dropbox based mostly approach will cause delay in message dissemination and thence the receiver might not be able to get the messages on time. To deal with this drawback, the authors initial gift a theoretical framework for estimating the delay; then they gift a dropbox readying rule. They use dimension enlargement and dynamic programming to style drop box readying rule.

4.5 SCREEN SHOTS

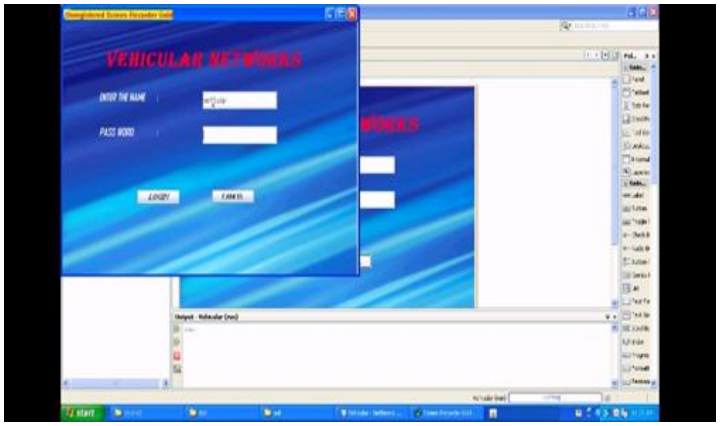

Figure 3: Admin Login

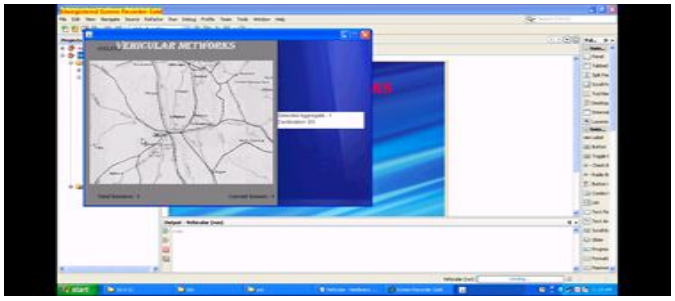

Figure 4:Route Map

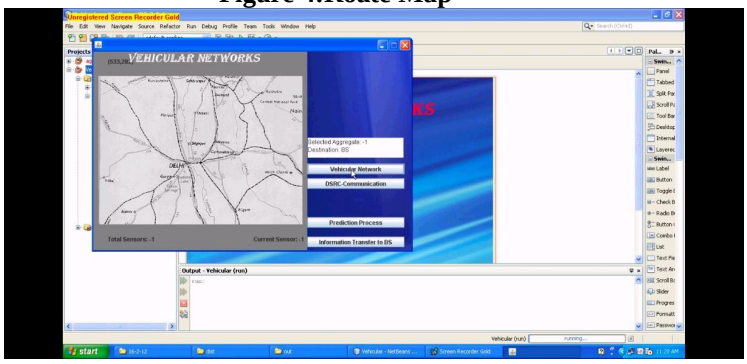

Figure 5:Vechicular Network

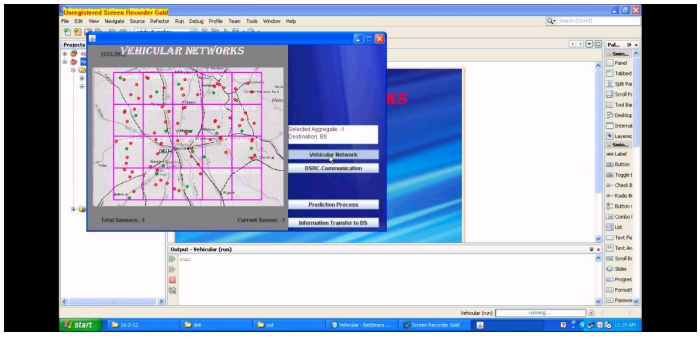

Figure 6:Message Transfer

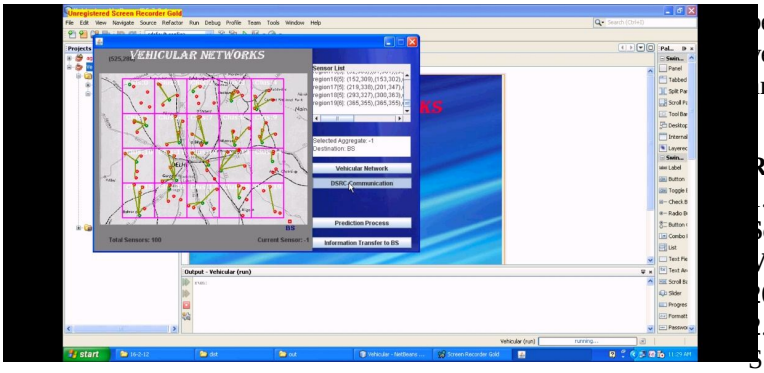

Figure 7: Transfer to nearest system

5. CONCLUSION

In this paper, we tend to given a survey of papers revealed within the last ten years that address privacy, authentication and secure message dissemination in VANETs. Supported the tools and techniques utilized in the papers, we have a tendency to classified the papers into numerous classes. We have a tendency to create a comparative study of the protocols in every class and mentioned their strengths and weaknesses. Then, we have a tendency to mention a number of the open problems that stay to be self-addressed. We have a tendency to hope this survey can function prepared reference for alternative researchers operating in these areas and conjointly facilitate in addressing a number of the open problems.

6. FUTURE IMPROVEMENT

Vehicular fog has attracted sizeable attention recently, because the densely deployed fog devices square measure in proximityto conveyance end-users, and that they square measure significantly appropriate for the latency-sensitive and location-aware conveyance services. During this paper, we have a tendency to propose a secure querying theme in conveyance fog information dissemination, within which the wayside units (RSUs) act as fog storage devices to cache information at network edge and disperse information upon querying. To disrupt the association between a particular information request and its origin vehicle, the planned theme exploits associate invertible matrix to structure multiple information requests from completely different vehicles, and aggregates the cipher texts of knowledge requests at the RSU aspect with the homomorphic Paillier cryptosystem. Meanwhile, given the invertible matrix and cryptography result, the RSU will recover every individual information request while not distinguishing its origin vehicle. Additionally, the RSU will verify the correctness of the recovered information requests with associate identity-based batch verification theme. Through security analysis, we have a tendency to demonstrate that the planned theme are able to do the safety goals of unlink ability, confidentiality, and verifiability. Performance evaluations are also conducted, in which the obtained results show that the proposed scheme can be adaptive to the fluctuating number of the data querying vehicles, and significantly reduce the computation complexity and communication overhead.

REFERENCES

1. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. **A Scalable Robust Authentication Protocol for Secure Vehicular Communications.** IEEE Trans. Veh. Technol. 2010, 59, 1606–1617.

2. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. **Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure**. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–6.

3. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: **An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs**. IEEE Trans. Intell. Transp. Syst. 2011, 12, 736–746.

4. Yao, Y.; Chang, X.; Miši´c, J.; Miši´c, V.B.; Li, L. BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. IEEE Internet Things J. 2019, 6, 3775–3784.

5. Tan, H.; Chung, I. **Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor.** IEEE Access 2019, 7, 151459–151474.

6. Li, J.; Lu, H.; Guizani, M. ACPN: **A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs**. IEEE Trans. Parallel Distrib. Syst. 2015, 26, 938–948.

7. He, D.; Zeadally, S.; Xu, B.; Huang, X. **An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks.** IEEE Trans. Inf. Forensics Secur. 2015, 10, 2681–2691.

8. Lo, N.; Tsai, J. **An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings**. IEEE Trans. Intell. Transp. Syst. 2016, 17, 1319–1328.

9. Lu, R.; Lin, X.; Liang, X.; Shen, X. **A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs.** IEEE Trans. Intell. Transp. Syst. 2012, 13, 127–139.

10. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. **Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs.** Wirel. Commun. Mob. Comput. 2018, 2018, 1–13.

11. Shao, J.; Lin, X.; Lu, R.; Zuo, C. **A Threshold Anonymous Authentication Protocol for VANETs.** IEEE Trans. Veh. Technol. 2016, 65, 1711–1720.

12. Zhang, Q.; Gan, Y.; Zhang, Q.; Wang, R.; Tan, Y**. A Dynamic and Cross-Domain Authentication Asymmetric Group Key Agreement in Telemedicine Application.** IEEE Access 2018, 6, 24064–24074.

13. Tian, Z.; Shi, W.; Wang, Y.; Zhu, C.; Du, X.; Su, S.; Sun, Y.; Guizani, N. **Real-Time Lateral Movement Detection Based on Evidence Reasoning Network for Edge Computing Environment.** IEEE Trans. Ind. Inform. 2019, 15, 4285–4294.

14. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. **An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection.** J. Internet Technol. 2018, 19, 481–488.

15. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. **Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network.** IEEE Access 2019, 7, 71424–71435.

16. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. **A Distributed Key Management Framework with Cooperative Message Authentication in VANETs.** IEEE J. Sel. Areas Commun. 2011, 29, 616–629.

17. Wasef, A.; Shen, X. EMAP: **Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks.** IEEE Trans. Mob. Comput. 2013, 12, 78–89.

18. Tan, H.; Chung, I**. A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs.** Sensors 2018, 18, 3930.

19. He, D.; Kumar, N.; Wang, H.; Wang, L.; Choo, K.R.; Vinel, A. **A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network**. IEEE Trans. Dependable Secur. Comput. 2018, 15, 633–645.

20. Chuang, M.; Lee, J. TEAM: **Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks.** IEEE Syst. J. 2014, 8, 749–758.

21. Zhu, X.; Jiang, S.; Wang, L.; Li, H. **Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks.** IEEE Trans. Veh. Technol. 2014, 63, 907–919.

22. Shen, J.; Tan, H.; Ren, Y.; Liu, Q.; Wang, B**. A Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangement With Adequate Security Assurance.** In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31 January–3 February 2016; pp. 693–699.

23. Tan, H.; Chung, I. **A Secure Cloud-Assisted Certificateless Group Authentication Scheme for VANETs in Big Data Environment.** In Proceedings of the 2019 International Conference on Big Data Engineering (BDE2019), Hong Kong, China, 11–13 June 2019; pp. 107–113.

24. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: **A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET.** IEEE Trans. Veh. Technol. 2016, 65, 896–911.

25. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. **Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis.** Symmetry 2018, 11, 969.

26. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: **Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks.** IEEE Trans. Ind. Inform. 2020, 16, 4146–4155.

27. Zhou, T.; Shen, J.; Li, X.; Wang, C.; Tan, H. Logarithmic **Encryption Scheme for Cyber-Physical Systems Employing Fibonacci Q-matrix.** Future Gener. Comput. Syst. 2020, 108, 1307–1313.

28. Tan, H.; Xuan, S.; Chung, I. HCDA: **Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs.** Symmetry 2020, 12, 1003.

29. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. **A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs.** IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2019, 27, 2792–2801.

30. Li, Y.; Chen, W.; Cai, Z.; Fang, Y. CAKA: **A Novel Certificateless-Based Cross-Domain Authenticated Key Agreement Protocol for Wireless Mesh Networks.** Wirel. Netw. 2016, 22, 2523–2535.