International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Survey of Vehicular Cloud Netwok (VCN) - Architecture, Operations, Threats and Security

R. Suganya[#1], I. Mumtaj Begam[*2], M. Anisha Montina[*2], S. Maduvanthi[*2]
[#1]Assitant Professor,[*2] UG Scholar, Department of CSE, RAAK College of Engineering and Technology, Pondicherry, Tamil Nadu, India

ABSTRACT

Vehicular Ad-hoc Networks (VANET) is that the unit of measurement of thelargest reality application of circumstantial networks where nodes space unitrepresented via quick paced vehicles. This paper introduces thefuture rising technology, i.e., conveyance Cloud Networking(VCN) where vehicles and adjacent infrastructure merge withtraditional internet clouds to produce altogether completely different applications move from low sized application to really difficult applications.VCN consists of three forms of clouds: conveyance cloud, Infrastructure cloud and Ancient Back-End (IT) cloud. we tend to introduced these clouds via a three tier style onwith their operations and characteristics. we have planned use cases of each cloud tier that designate but it's a lot of created and utilised whereas taking the conveyance quality thoughtlessness. Moreover, it's crucial to substantiate security, privacy and trust of VCN network and its assets. Therefore, to clarify the safety of VCN, we have provided associate full analysis of various threats related to each tier of VCN. The threats connected to conveyance cloud and infrastructure cloud unit of measurement classified in step with their assets, i.e., vehicles, adjacent infrastructure, wireless communication, conveyance messages, and conveyance cloud threats. Similarly, the Back-End cloud threats unit of measurement classified into data and network threats. The implications of thosethreats and their effects on varied components of VCN square measure explained fine.

Keywords : Vehicular Ad-hoc Networks, Cloud Networking, Ancient Back-End, vehicle-to-infrastructure, vehicle-to-vehicle, RSU

I. INTRODUCTION

With large amount of vehicles distributed around the world,Vehicular Networks (VANET) [1] square measure thought of because the basisof Intelligent Transport Systems(ITS).Successive generationof vehicles are going to be equipped with completely different sensible sensors,wireless communication modules, machine and storage capabilities [2].The sensors can collect necessary datafrom surroundings and share it with neighbouring vehicles and adjacent road side units (RSU) via vehicle-to-vehicle(V2V) or vehicle-to-infrastructure (V2I) communication. Thefact that every vehicle has hardware constraints leads to the limited applications offered by these machine and storageresources. As an example, so as to produce invehicle diversionto users high storage and machine capabilities are needed which cannot be supported by individual vehicle.

To support information measure hungry applications with advanced computation, the vehicles and adjacent RSU should join forces together to share their machine and storage resources,resulting in a short lived cloud with a lot of resources.

Similarly,merging ancient cloud . With these temporary clouds will further enhance the network potency. This introduces the concept of recently rising technology referred to as "Vehicular Cloud Networking (VCN)". The temporary clouds will be usedfor low-sized applications like traffic management, safety applications and sharing traffic conditions whereas the resources of ancient clouds will be used for advanced applications like providing in-vehicle diversion to the conveyance user.

II. VANET

Emerging Applications On Wheels:
Applications in vehicle communications have ranged from safety and convenience to recreation and business services. This segment discusses 3 noticeable characteristics observed in rising VANET applications.

Application Content Time-Space Validity: Vehicles manufacture a good quantity of content, while at a similar time overwhelming the content. That is, they become made information "presumes." Such contents show many common properties of native connexion native validity, explicit lifetime, and native interest. Inherent validity indicates that vehicle-generated content has its own spatial scope of utility to shoppers. In safety applications, as an example, a speed warning message near a pointy corner is merely valid to vehicles approaching the corner, say among a hundred m. Explicitlifetimereflects the very fact that vehicle content has its own temporal scope of validity. This also implies that the content should be accessible throughout its entire life. As an example, road congestion information could also be valid for thirty min, while the validity of a roadwork warning should last till the work is finished. Native interest indicates that nearby vehicles represent the majority of potential content shoppers. This idea is any extended thus on distinguish the scope of shoppers. For instance, all the vehicles within the locality wish to receive safety messages, while only a fraction of vehicles have an interest in business advertisements. Table one shows Associate in Nursing overview of auto applications and their content properties.

Content-Centric Distribution: Vehicleapplications area unit chiefly inquisitive about content itself, not its root. This memory less property is characteristic of VANETs. Within the mounted Internet, once one needs to examine holdup, one visits a favourite service website. That is, the explicit site's address guarantees access to sample reliable info. In distinction, vehicle applications flood question messages to area, to not a selected vehicle, accretive responses regardless of the identity of the content suppliers. In fact, the response could return from a vehicle within the locality that has successively received such traffic info indirectly through neighbouring vehicles. During this case, the vehicle doesn't care WHO started the printed. This characteristic is mainly because of the very fact that the sources of information (vehicles) area unit mobile and geographically scattered.

Vehicle Collaboration Sharing Sensory information: rising vehicle applications consume ahuge quantity of device information during a cooperativemanner. That is, multiple sensors, put in onvehicles, record a myriad of physical phenomena.Vehicle applications collect such devicerecords, even from neighbouring vehicles, to producevalue-added services. In MobEyes, forexample, vehicles use many sensors (including avideo camera) to record all close eventssuch as automotive accidents whereas driving. Thereafter,Internet agents and/or mobile agents (e.g.,police) search the transport network for witnessesas a part of their investigation. The CarSpeakapplication permits a vehicle to access sensorson neighbouring vehicles within the same mannerin which it will access its own. The vehicle thenruns Associate in Nursing autonomous driving application victimisationthe device assortment while not knowing WHO createdwhat.

Networking:

The existing VANET networking model hasbeen derived primarily from ancient wirednetworking protocols, as illustrated on the left side. However, because of the massive distinctionbetween the web and also the infrastructurelessad hoc condition, the model showsseveral intrinsic limitations.First, the VANET protocol still assumesusing scientific discipline address to represent a bunch. AssigningIP addresses to moving nodes isn't trivial in adhoc environments. The assignment task usuallyrequires infrastructure support like a centralDynamic Host Configuration Protocol (DHCP)server, that directly conflicts against the philosophyof ad-hoc networks that operate during aselforganizedmanner with none infrastructure.Second, it's hard to find the scientific discipline addressof the publisher of specific content in an adverthoc network. Nodes be a part of and leave the networkfrequently, and any node will become a replacementpublisher of the content. Thus, the content ofinterest cannot be systematically certain to a singular IP address. Last, the VANET protocol merelyperforms IP-based end-to-end communications.During a routing procedure, a router merelyrelays so deletes content. though thecontent is thus well-liked that a lot of nodes conjointly wishit, the router cannot directly send it to thembecause the router doesn't put it aside.

Figure 1. Architecture of Vehicular Cloud Network(VCN).

III. VEHICULAR CLOUD NETWORKING (VCN) ARCHITECTURE:

Theproposed architecture contains the three tier architecture consisting of three levels:

A. Tier-1 cloud: Vehicular Cloud (VC).
B. Tier-2 cloud: Infrastructure Cloud (IC).
C. Tier-3 cloud: Back-End Cloud (BEC).

A. Vehicular Cloud (VC):

In VC, the physical sources (storage and computation)of automobiles are shared between group of automobiles only.Thiseffects in excessive normal efficiency of the network. The scope of VC is nearby within the context of VANET where the statisticsis shared among the automobiles through V2V conversation. Becausethe community usually experience cars with each high andlow mobility, the technical trouble of the formation of VCvaries for exceptional context of VANET. Following use instances ofVC are viable:

- ✓ **Urban areas:** usually, mobility of the motors inurban areas (e.g., metropolis middle) is low as compared tohighways, ensuing in collaboration amongst motorsfor a longer time period. This permits the opportunityof formation and life of VC in urban areas whichmay be used in specific packages inclusive of videosurveillance of public transport.
- ✓ **Rural regions**: Rural regions broadly speaking experience high speedautomobiles where exceptional automobiles collaborate for a completelyshort span of time ensuing in a totally quick existence cycle of VC. The opposite essential issue in rural place is thelow frequency of automobiles which makes it even harderfor VC to be created and implemented.
- ✓ **Parking:** Parking is the nice state of affairs to enforce VCdue to 0 or negligible mobility of motors. The lifecycle of VC in parking is lengthy in comparison to rural andcity regions. The computation and storage resourcesof parked vehicles may be used to create a VC whichcan doubtlessly be used to serve users in that precisegeographical vicinity, e.g., VC created in vehicle park ofthe shopping center may be used to serve users of thatparticular place.

B. Infrastructure cloud(IC):

IC is on the whole initiated by using adjoining RSU alongside the roadwherein vehicles request to get admission to the offerings provided bycloud. The scope of this cloud is local to small geographicallocation where RSU is positioned [12]. verbal exchange betweenunique ICs is finished via dedicated nearby servers.Given that each static (RSU) and mobile (vehicle) entities areworried in IC, the technical trouble of formation of IC variesfor one-of-a-kind eventualities of VANET.

- ✓ **Urban areas:** As city regions mostly includes automobileswith low mobility and immoderate adjacent infrastructure,the formation and lifestyles of IC is viable forcity scenarios due to the availability of sizeablequantity of RSU. IC in urban areas may be used invarious applications which includes faraway navigation and site visitors management.
- ✓ **Rural regions**: The opportunity of formation of IC is lowin rural areas because of absence of adjacent infrastructureand excessive mobility of motors. in this scenario, thetemporary cloud is shaped between RSU and carfor a totally quick span of time.
- ✓ **Parking**: If the motors have negligible mobility andadjoining infrastructure which include RSU is to be had, thenthe formation, lifestyles and implementation of ICin the vicinity of respective RSU is noticeably possible.The aggregate of each VC and IC can serve bettervariety of customers, resulting in very high efficiency ofthe community.

C. Back-end cloud (BEC):

BEC is the biggest traditional cloud in vehicular environmentwhich exists in the net domain. BEC has extrasources which may be used by cars for full-size facts garage and high computation. The scope of BEC is spreadover the massive geographical place to serve the motors. BEC canplay a critical function for the duration of bandwidth management programswherein it serves the customers with excessive bandwidth requirementsconsisting of to provide in-automobile multimedia.

Vehicular Cloud Networking (Vcn) Operation:

To create and initiate a cloud in vehicular networks, itdemands a cloud leader which can be either automobile or adjoiningRSU. If the leader is a automobile to provoke the cloud andno adjoining RSU participates in cloud formation, then theresulting cloud is VC. But, if the request for cloudis initiated by using RSU as a frontrunner and neighbouring motorsresponds to its request consequences inside the formation ofIC.The cloud leader invitations cloud members i.e. cars andadjacent RSUs in its location with the aid of transmitting resource requestmessages (REQs) to shape a cloud. Any automobile desires toenrollinthe cloud responds back to the cloud chief with resourcerespond messages (REPs). Whilst cloud chief receives theaffirmation via REP messages, it keeps its contributors' identity andassign one-of-a-kind responsibilities and packages with them for this reason.

The contributors speak continuously with its cloud chief. Based at the permission from cloud leader, the members canpublish and percentage the content material received from leader with othermotors.Cloud leader is accountable for the renovation of thecloud it created. however, if any cloud member, who desiresto leaves the cloud requests the useful resource leaving message tocloud chief. in that case, the cloud leader confirms the dischargeof its member and recruits new members with the aid of broadcasting REQmessages. however, in case if the cloud chief itself now not need to hold the cloud, it pronounces the cloud release messageand leaves the cloud.

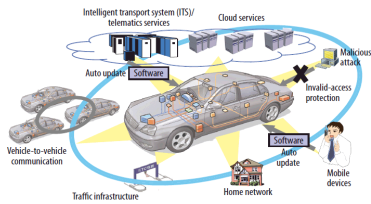

Figure 2. Operation of Vehicular Cloud Network(VCN)

Security and Privacy:

Since VCNencourages sharing resources, the foremost crucial security issue would be a threat targeting the cloud platform itself. Associate degree mortal might launch a DoS attack like jamming . Or, it should try and inject malware into the platform to use the platform's resources or to choose the platform into a botnet. An intrusion detection system or system integrity checking will facilitate mitigate injury. Privacy is also vital in VNC as a result of the contents each vehicle generates tend to disclose personal information. Associate

degree anonymization theme will facilitateresolve th e difficulty.Future analysis should conjointlyaddress the privacy considerations of service customers. They actively obtain resources and contents on the cloud. Watching such activities willreveal consumers' use patterns of specific applications. A secure search theme should create these activities invisible victimisation correct cryptosystems.

IV. CONCLUSION

Vehicular Cloud Networks (VCN) is that the merging ofVANET technologywith cloud computing that changes approach ofnetwork service provisioning and helps conveyance users to usecloud in step with their necessities. VCN helps the conveyanceusers by providing them ancient safety options of VANETsas well because the further options to share tiny conveyanceresources or acquire high process capabilities. In thispaper the various classes of clouds concerned in VCN areexplained by dividing them in a very 3 tier design. Thisarchitectureexplains the mechanisms through that conveyanceusers will use completely different VCN clouds together with conveyance cloud,infrastructure cloud and back-end cloud. The employment cases givenin the paper make a case for the formation of every cloud tier fordifferent eventualities like urban areas, rural areas and parking.This paper conjointly provides associate degree in-depth analysis of varioussecurity threats in every tier of VCN cloud. For tier-1 and tier-2clouds, the threats are known in step with vehicle, adjacentinfrastructure, wireless communication, necessary messages,vehicular clouds and infrastructure clouds. Similarly, for tier-3cloud threats are known as information andnetwork threats. In our future work, we are going to analyse the attainable security solutionsthat secure the VCN technology by mitigating the attainable threats.

V. REFERENCES

[1]. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011.

[2]. Cloud Computing-The complete cornerstone guide to cloud computing best practices.pp-18.

[3]. Rajkumar Buyya , Chee Shin Yeo , Srikumar Venugopal, James Broberg , Ivona Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, Elsevier,2008.

[4]. Jeremy Geelan. Twenty one experts define cloud computing. virtualization, August 2008. Electronic Magazine, article available at http://virtualization.sys con.com/node/612375.

[5]. Luis M. Vaquero , Luis Rodero Merino , Juan Caceres , Maik Lindner: A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review. Vol 39, Jan 2009.

[6]. Anthony T. Velte, Toby J. Velte, Robert Elsenpeter : Cloud Computing-A Practical Approach. McGraw-Hill.

[7]. A white paper produced by the Cloud Computing Use Case Discussion Group Cloud Computing Use Cases. Version 3.0, February 2010.

[8]. Introduction to Cloud Computing. https://www.priv.gc.ca/resource/fsfi/02_05_d_51 _cc_e.pdf.

[9]. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, unho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia: Above the Clouds: A Berkeley View of Cloud Computing.