ISSN 2047-3338

Review of Cloud Computing Model for Vehicular Adhoc Networks

Ansab Malik[1], Reeba Zahid[2]
[1,2]Departement of Computer Science, University of Engineering & Technology, Lahore, Pakistan
[1]ansab.malik96@gmail.com, [2]reeba.zahid1998@gmail.com

Abstract— **Vehicular ad hoc networks (VANETs) have been concentrated seriously because of their wide assortments of uses and services, like traveler security, improved traffic effectiveness, & infotainment. Along the development of innovation & abrupt development in various shrewd automobiles, conventional VANETs face a few specialized provokes in deployment & management because of less adaptability, versatility, helpless network, and lacking insight. cloud computing is viewed as a method for fulfilling these requirements in VANETs. With the progress and maturity of the VANET, a major transformation in the field of wireless communication will occur in terms of fast handovers, network availability, security, and safety through the employment of advanced applications, among other things. Although VANET technology is improving with the passage of time, there are still a various challenge that must be addressed in order for the network to become more robust. In light of the foregoing, we examined and reviewed numerous research works connected to VANET applications, protocols, and security in this study. Furthermore, after reviewing the previous works, we assessed them and identified the benefits and drawbacks for future research.**

Index Terms—**VANET, Cloud Computing, Mobile Ad-Hoc Network, Architecture and Design**

I. INTRODUCTION

VEHICULAR ad hoc networks (VANETs) has acquired fame in the last few annum. Traffic mishaps, route blockage, petrol utilization, & contamination because of the huge various vehicles have become critical universal concerns. To defeat these issues and make the voyage more secure, proficient, trouble-free, & engaging, Intelligent Transportation Systems (ITS) acquainted VA-NETs with making a more secure framework for road transportation [1], [2]. Vehicular ad hoc networks (VANETs) uphold transmission among vehicles, named as vehicle to vehicle (V2V) communication, and among automobiles & the RSU framework, so-named vehicle-to-infrastructure (V2I) communication, regularly utilizing GPS gadgets to detect the location/position of vehicles [3]. It might be a safe and fasten system in favor of effective traffic control. The formation of VANET as indicated by current itches might be demanding. In an ad-hoc grid, versatile hubs self-systematize ourselves to make a grid aside from the help of any framework like base stations.

The fundamental concept of VANET is to bring the generally ratified and economical Wireless LAN automation, with a couple of changes, and introduce it on vehicles. among numerous objectives of VANET is to help the safety of traffic & induce the driving undergo too protected & convenient. In VANET, automobiles, & RSUs (Road-Side Units), for example, grid hubs, will have rigged along onboard calculations and contact modules to ensure productive transmission is conceivable particularly [4] – [7]. VANET end clients (drivers and travelers) are for the most part needed to purchase the necessary software, an applicable platform, and the relevant hardware which can all be leased from inventive vehicular cloud architecture.

Currently, Cloud computing has seen critical consideration in vehicular transmission. It has commutated the calculation and transmission outlook by dissociate computational resources from tangible network subsequently empowering dematerialization [8]. The principal rationale of distributed computing is to "precisely what you need and when you need ". In Vehicular Cloud Computing (VCC), a collection of associated automobiles shapes a cloud fully intent on sharing their plentiful assets. Vehicles using Clouds (VuC) empowers the admittance to the functions of ordinary cloud at automobiles through the Internet. It supports in acknowledging savvy ITS applications containing ongoing traffic prophecies and web services [12].

In vehicular networks, decreased delay, effectiveness, versatility, dependability, and safety are exceptionally fundamental to further develop route protection & traveler solace over intelligent transportation systems (ITS). In particular, VANET-Cloud permits aboard computing assets of automobiles to be incorporated along the customarily distributed computing context, that comprises just of fixed calculation elements. In addition, this system receives the rewards of the computing abilities of automobiles that contain processing, capacity, just as the sense to broaden conventional distributed computing capacities with versatile elements. Thusly, too adaptable outcomes might be given to support drivers & specialists conquer basic route circumstances, for example, discovering elective paths & systematizing traffic signals to diminish route blockage, managing advent and traffic mishaps, giving economic automobile operations, etc.

Our VANET-Cloud idea forms the cloud accessible to vehicular frameworks & exploits distributed computing assets to all the more likely serve VANET end-users as far as giving the least expensive without the need to purchase extra assets. 2 partial-models compose the VANET-Cloud design. The primary partial-model depends on the ordinary cloud, that propose cloud services like software, infrastructure, and platform as a service to vehicles. The subsequent one comprises vehicles that together structure another impermanent cloud. The last is intended to extend the extremely durable cloud and means to expand the computing aptitude demanded by consumers.

In this paper, objective is to analyze an ad-hoc cloud design that consolidates the idea of mobile ad-hoc, vehicular ad-hoc network, and cloud computing to give superior control of trafficking and protection on the route along the benefit of V-cloud.

A literature review is presented in Section II. Design architecture of cloud computing in VANET is thoroughly examined in Section III. Section IV examines the limitations of VANET in cloud computing. Finally, Section V brings the conclusion of the article.

II. RELATED WORK

Several research papers has been written related to VANET (Vehicular ad-hoc Network) cloud computing in the recent era. But still before 2012 there was no generic model to configuration a cloud system for VA-NET. Through all the extant research models of ad hoc cloud network design named “cloud on the run” is of great importance as it focuses more on vehicles and includes wireless devices, attached to vehicles, work as a mobile multi-hop network and a vehicular cloud (VC) which is created by the vehicles publicly or privately [9].

Oralia and his colleagues proposed merging VA-NET and cloud computing in their researches in recent times [10, 11]. Autonomous Vehicular Clouds (AVC) was proposed by them, which could be helpful for VANET users. In addition, the authors concisely considered research issues in vehicular clouds. Abuela et al [11] proposed that the traditional VANETs be moved to the cloud, and that in the imminent, underutilized VA-NET methods might be used by integrating VA-NET and cloud computing [10].

Some authors reflected that VC is a cluster of mainly autonomous motorcars. The computing ability, communication capability, sensing, and tangible materials of vehicular clouds (VC) can be corresponded and given to client dynamically [12].

Some authors also highlighted the enabling issue of automobiles in a VA-NET so that their required services from mobile cloud servers that are shifting close can be discovered. An Road side Units, that serve cloud catalogues and structure, a dependent system named CROWN is also proposed. To attain this, RSUs documented data is available to allow the automobiles to locate the needed cloud benefits within the region surrounded [13].

In a paper, the authors state a solid classifications of VA-NET based cloud computing. Moreover, VA-NET clouds are divided into 3 different architectural scheme namely Vehicular Clouds (VC), Vehicles using clouds (VuC), and Hybrid Vehicular Clouds (HVC). They also put stress on the VANET clouds research challenges and security and privacy issues [14].

In a paper classic cloud created by vehicles has been presented which is a unique service paradigm which is understood as Sensor-as-a-Service (SenaaS) that makes public automobile sensors and devices to third-party automobile monitoring operations, as cloud computing services called sensor-cloud benefit [15].

Bernstein et al. [16] went a step further and presented a Platform-as-a-Service (PaaS) paradigm for the mobile vehicular sector, with attainable applications. The privacy and security problems in vehicular clouds were highlighted by Yan et al [17]. They explored the issues posed by vehicular cloud characteristics, such as high-mobility automobiles authentication and the intricacy of multiplayer belief generated by fitful tactical transmission. All things considered, the tiny automobiles clouds will require much analysis to create it over the deployment stage. One benefit is that because the infrastructure is already in place, no extra infrastructure is required for implementation. In [18] focused their research mostly on applications.

Table I summarizes the aforementioned literature study on architectural design. Contribution, kind of architecture, technique, implementation, and remarks are among the parameters used to create the summary. The contribution emphasizes the articles' progressive impact on the CC-V research issue of architecture design. The architecture chooses between the three forms of vehicular cloud: VuC, VCC, and hybrid vehicular cloud (HVC). The approaches used to address the problem are identified by the techniques.

Table I: Aforementioned literature study

Protocols	**Contribution**	**Architectures & Techniques**	**Implement-ation**	**Remarks**
Tlaas [18]	Location privacy scheme	VuC & Location based encryption	No	Crypto overhead
TCBI [19]	incentive mechanism	VCC & Framework design	Custom simulator using JAVA	System complexity issue
ICDI [20]	Adaptive intrusion detection	VCC & Pseudo-dynamic clustering	NS-2 and SUMO	Adaptivity processing overhead
VCC-SSF [21]	Authentication scheme	VuC & Cryptography based design	NO	Cryptography overhead
PVCM [22]	Zone based revocation system	VCC & Algorithm development	MatLab	Complexity Analysis issue
DPK-LS [23]	Dual registration detection	VCC & Privacy preserving detection	Custom simulator	Privacy level not defined

III. CLOUD COMPUTING IN VANETs

Cloud computing is an arising search topic in VA-NETs. It is because of the demand to grow the different business benefits at present accessible on the Internet to VANETS. It is just pay-as-you-go service in which the bill is to be paid at the month ending for precisely what has been used by the user. The cloud services' core consists of 3 primary delivery networks with first layer named as Software-as-a-Service (SaaS), mid layer named as Platform-as-a-Service (PaaS) and last layer named as Infrastructure-as-a-Service (IaaS). SaaS distributes applications to consumers in a cross functional style. PaaS allows client to adopt modern development context as a service remotely rather of establish them on multitude computers. In IaaS physical resources like servers, connections, and related tools are released to clients as a service. In [19], Cloud computing in VANET has 3 significant issues, Architecture design, data dissemination, and security. Every issue has been researched in a few ways and will be evaluated in the accompanying sections.

A. *Design of Architecture*

The difficulties of subsidiary usage of VANETs resources & unnormalized architecture of Cloud computing inside VANET are the fundamental concentration.

In Fig. 1, the architecture design has been isolated into 3 classes containing services, computation, & communication. Architectures concentrating on the most proficient method to use vehicular resorts as cloud resorts have been classified in services.

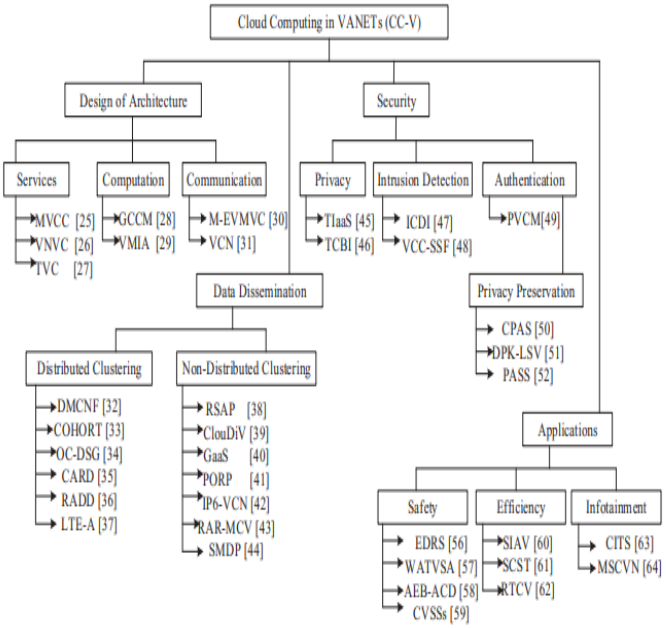

Fig. 1: Scientific classification of CC-V

1) *Service*: In [20], An idea which combines VANETs and cloud has been proposed to describe the under usage of vehicles' locally available gadgets & devices.

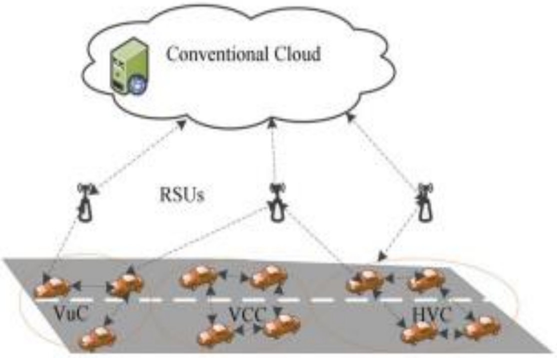

Fig. 2: The 3 architectures for cloud in VANET

The significant commitment of VNCN is traffic data as a service, which deal with convolute traffic data calculations utilizing the cloud. It additionally offers services including enormous traffic information examination, online configuration, vehicle execution checking, and area-based promotions.

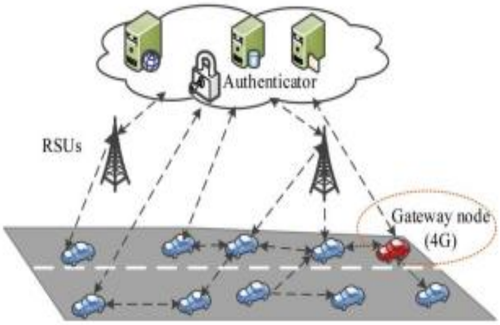

Fig. 3: Network for traffic data

One more thought of enchanting VANET to the cloud has been recommended by Olariu-et-al. The design incorporates two distinct services, specifically, NaaS and STaaS. NaaS is too appropriate for distributed network computing in vehicular correspondence because of the thought of 3G & Wi-Fi placed Internet association in automobile or vehicles. These automobiles can distribute their storage, & processor for capacity, & calculation of huge information.

2) *Computation:* In [21], A conventional distributed network computing model for VANET has been recommended to improve the accessibility of the locally available frameworks for other customer vehicles. The framework parts are assembled into 3 layers which contain customer, correspondence, & cloud. To give driving help, a worldview called traffic-aware portable geological data framework with traffic cloud emotionally supportive network has been talked about.

3) *Communication*: In [22], the thought of whether or not to move has been examined, by investigating virtual machine relocation in the side of the road cloudlet-based vehicular cloud. The presentation of the 2 algorithms has been assessed to analysis the impact of amount on the thickness & resources necessity of virtual devices.

B. Data Dissemination

In Cloud computing VANET, clustering is the favored choice for information spread between vehicles. This is because of the greater chance of cloud-based resource distributing while at the same time scattering information. In this part, related writing on configuring clustering schemes for communicating information in Cloud computing VANET is fundamentally investigated & surveyed.

1) Distributed Clustering: A dispersed compound bounce algorithm for clustering dependent on area follow have been introduced to improve strength in algorithm for clustering [23]. A group-form vehicular-cloud framework along (COHORT) knowledge based manage resource has additionally been talked about. The co-hort can be best identified with computerized reasoning and the shrewd applications layer of the suggested Cloud computing VANET layered design.

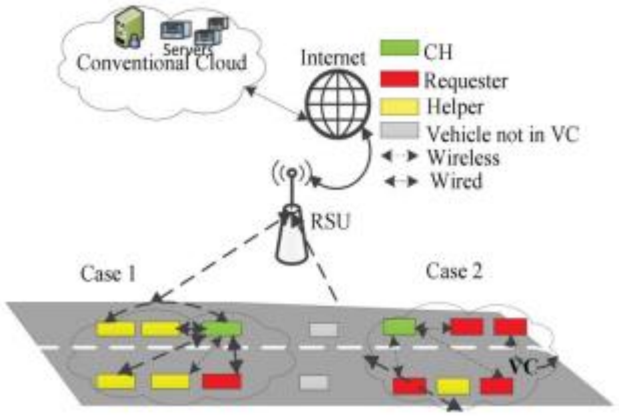

Fig. 4: Cluster VCC

2) Non-Distributed Clustering: A data circulation network for cloud-empowered VA-Nets utilizing an in-vehicular resources framework dependent on the side of the road access points (RSAP) has been recommended [24]. ClouDiV has given versatile dispersal of security and non-wellbeing messages through distributed computing design. Cloud-upheld consistent Internet access in ITS is suggested for getting to top-notch ITS services [25].

In static doors, RSUs fill in as a passage, and RSUs are utilized as an entryway for vehicles to interface with the Internet. Connection lifetime forecast conspire thinks about the hour of entering or leaving from the gateway. PORP convention can be observed under the elements of coordination & AI reasoning layer as far as the Cloud computing VANET layered design.

C. Security

Security difficulties of shrewd applications are validation concerns containing programmed safety, data management, & services authentication. For AI, the significant security issue is in interruption discovery of servers & server farms or vehicles which structure a cloud. With the execution of the Cloud computing VANET-layered design, a more secured AI can be accomplished.

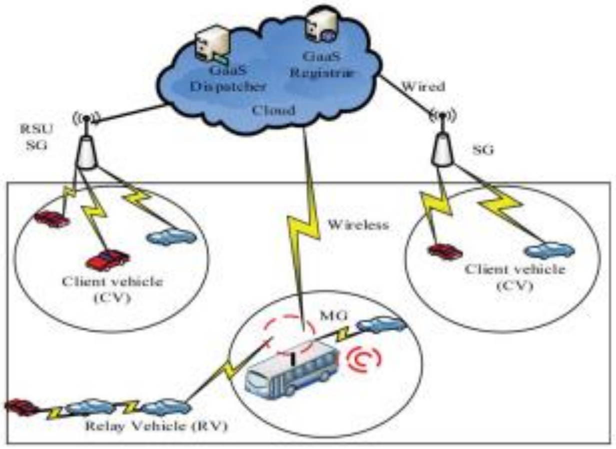

Fig. 5: GaaS system

1) Privacy: Security issues cause lower use of VANETs foundation including correspondence, calculation, and installed stockpiling. In [26] proposed a protected and security mindful traffic data as assistance (T-IaaS) for V-N-V-C to sermon the vehicle client protection problems. In figure 6 a repudiation system, TIaaS meager customer idea for vehicles, and proficient portability vectors structure have been planned. In spite of its solidarity in hiding area data, it may take longer handling time because of the encryption conspire embraced.

A safe and protection-saving convention for vehicular which based on cloud defers resistance organizations (D-T-Ns) have been introduced to resolve the problem of security in motivation framework & parcel sending convention. TCBI urges vehicles to help out one another by computing security and protection and sharing assets. In TCBI [27], the vehicular protection is all around got from both the cloud and transportation chief for playing out any single direction secret entrance work. Execution is needed to test the possibility of the plan.

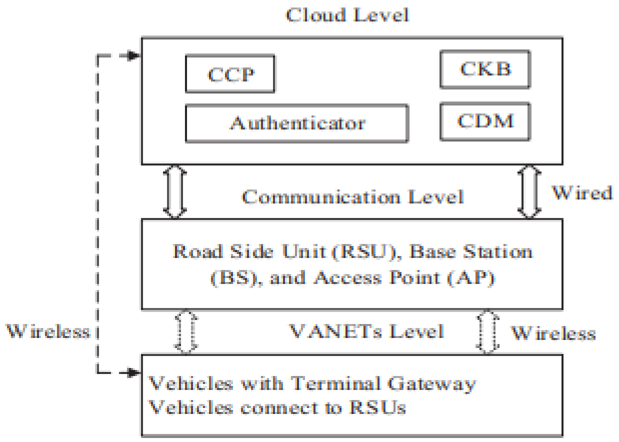

Fig. 6: Tlaas Model

2) Detection Intrusion: A digital clustering plan for appropriated detection of intrusion in Vanet cloud network computing has been proposed. The framework depends on grouping, standard cryptographic procedures, and prize punishment stochastic plan. The structure has given encryption, confirmation, access control, secrecy, trustworthiness, and security assurance of individual data identified with clients and vehicles [28]. Notwithstanding, this system probably won't be financially practical because of the greater prerequisites and intricacy.

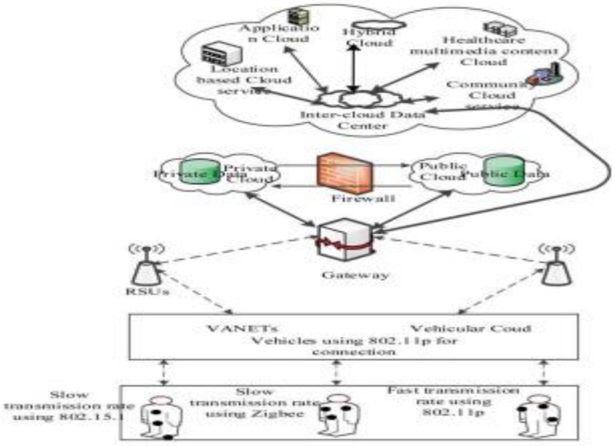
Application Cloud
Hybrid Cloud
Healthcare multimedia content Cloud
Location based Cloud service
Community Cloud service
Inter-cloud Data Center
Private Data
Private Cloud
Firewall
Public Cloud
Public Data
Gateway
RSUs
VANETs
Vehicular Coud
Vehicles using 802.11p for connection
Slow transmission rate using 802.15.1
Slow transmission rate using Zigbee
Fast transmission rate using 802.11p

Fig. 7: ICDI Model

3) Security challenges in VANET Cloud: As VANET cloud is a scattered system, so one of the major challenges for the VC are privacy and security. Leasing virtual assets in cloud climate implies many dangers or putting away information in cloud brings about delivering command over information. One of the principal concerns is protection misfortune and information stockpiling security [29], [30]. Coherently VANET mists incorporates both VANET and distributed computing consequently acquire security and protection issues [31] – [34] of both. In such a framework, clients input their information and run their applications at server farms oversaw by others. The issue turns out to be considerably really testing when impermanent VANET-Cloud locally available PCs are considered as servers. Therefore, security and security issues should zero in on guaranteeing information respectability, controlling information access, forestalling information misfortune, ensuring the classified information of clients, etc.

Many creators examined diverse street towards security issues in VANET mists.

In a paper Yan et. al., plot [30], the creators talked about mocking of characters, disavowal issues, DoS, etc. In one more paper the writers accepted that expected answers for such issues have been advanced by VANET people group as of now. These issues should be taken up with the VANET people group and distributed computing local area whichever vital. A similar contention holds for conventional cloud building issues. The security and protection challenges looked by independent VANET and distributed computing will stay unaltered regardless of whether the two advancements are converged to shape VANET mists. The primary difficulties for VANET mists are relied upon to be tattle stretch, versatile validation, contingent namelessness and virtualization, insiders and pariahs, leasing assets, independence, control, and collaboration middleware.

Validation and approval of the hubs precisely in the discontinuous short-range correspondence connects with the honesty of information [35]. The intricacy increments with the increment of hubs. Client character parodying and treating information could be the primary danger to the organization where the assailant claims to be one more client of same need level. An answer for this issue is proposed in [36] where halfway doled out advanced alias by the authority ought to be utilized.

Numerous analysts researched the assaults in VANETs. The grouping of these assaults is valuable on the grounds that the idea of VANET brings weaknesses and imperatives that require arrangements [37], [38]. By partitioning, we can more readily control. Assaults can be sorted into four fundamental gatherings: (1) those that represent a danger to remote connection point, (2) those that represent a danger to equipment and programming, (3) those that represent a risk to sensors input in vehicle and (4) those that represent a risk behind remote access, which implies in the framework (CAs or vehicle maker).

IV. LIMITATIONS OF CLOUD IN VANET

Ongoing year's specialists has been worried for the cloud network security in the execution of vehicular-cloud organizations. Notwithstanding, there are different difficulties e.g., big portability of hubs, signal lessening, versatility of network.

A. Cloud Security

Verification and approval of the hubs precisely in the discontinuous short-range correspondence identify with the Trustworthiness of information. The intricacy increments with the increment of hubs. Client character ridiculing and treating information could be the fundamental danger to the organization where the aggressor professes to be one more client of a similar need level. An answer for this issue is proposed where a halfway doled out computerized alias by the power ought to be utilized.

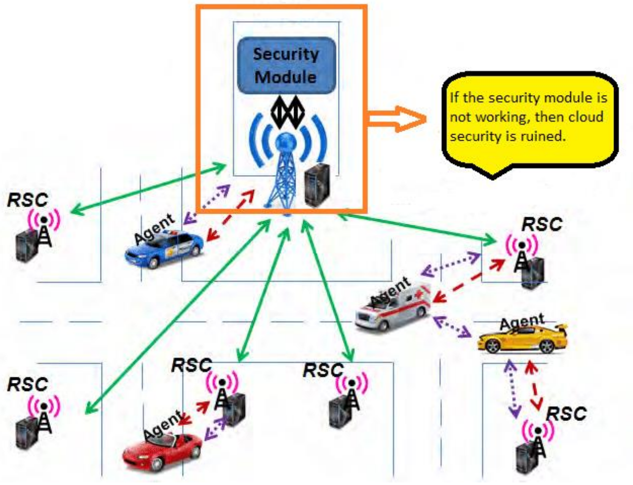
Security Module
If the security module is not working, then cloud security is ruined.
RSC
RSC
RSC
RSC
RSC
RSC
Agent
Agent
Agent
Agent

Fig. 8: Cloud Security

B. Hubs Versatility

Interference of information communication between quicker changing hubs in the expressways turns into unavoidable as the availability endures just for a couple of seconds. Despite what might be expected, during gridlock blockage of the transmitter, hubs will make commotion and impedance.

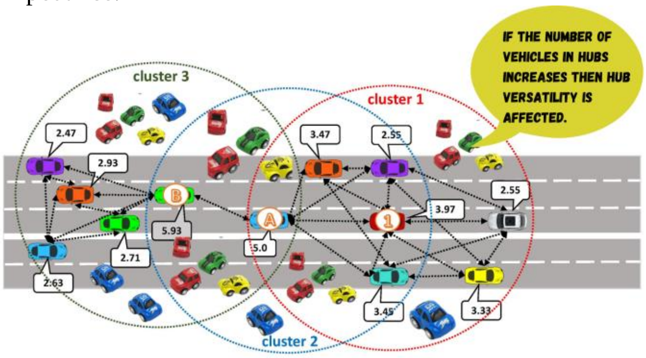
IF THE NUMBER OF VEHICLES IN HUBS INCREASES THEN HUB VERSATILITY IS AFFECTED.
cluster 3
cluster 1
cluster 2
2.47
2.93
3.47
2.55
2.55
3.97
5.93
5.0
2.71
2:63
3.45
3.33
B
A
1

Fig. 9: Hubs Versatility

C. Signal Fading

Impeded by enormous structures and different foundations in the urban regions the sign weakens at a high rate. Bringing about both disintegration sign power & sign trait.

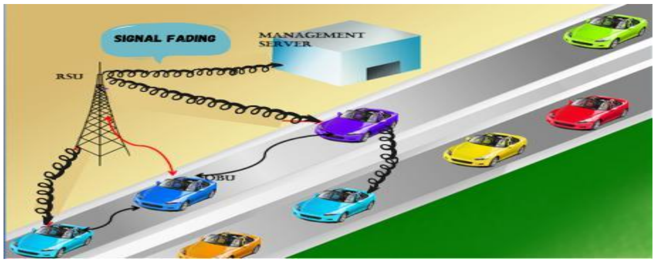

Fig.10: Signal Fading

D. Scalability of Network

For an expanding 850 billion vehicles overall & seeing the shortfall of a worldwide power that will administer the organization the adaptability of the organization is addressed. The correspondence among vehicles-2-vehicle is traded through DSRC-standard & DSRC-standard in North America is unique in relation to the DSRC principles in Europe.

E. Echo-location

In the VCC, vehicle position data assumes a significant part, which can communicate information and foster association on the grounds that numerous applications rely upon the traffic-related data, for example, concussion notice, path evolving cautioning, and crisis cautioning [39]. VCC has 3 models to assess and coordinate the position data. The first is the Active Position model, and it can adapt to automobile positions by utilizing position gadgets such as GPS and radar. The latter is a passive position model, in which it is extremely difficult to access the position of an automobile without the use of radar. The third is the extensive position model which filters the incorrect position in VC and estimates the undeniable level of position accuracy from the lower-level accuracy [40].

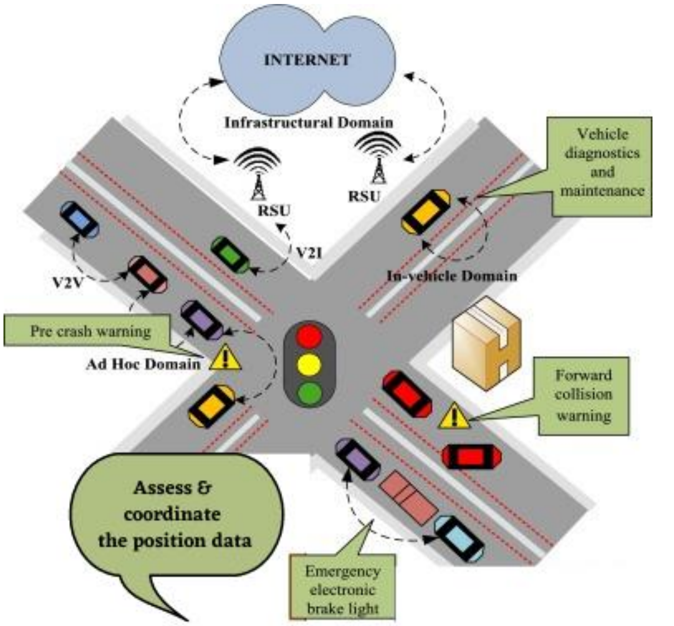
INTERNET
Infrastructural Domain
RSU
RSU
V2I
V2V
Vehicle diagnostics and maintenance
In-vehicle Domain
Pre crash warning
Ad Hoc Domain
Forward collision warning
Assess & coordinate the position data
Emergency electronic brake light

Fig. 11: Echolocation with warnings

F. Access Control

One difficult issue in VANET cloud computing is access control, which involves checking the client before accessing network assets. Different access control levels are default, in which each client connects to its devoted cluster in light of its merits in the network [41].

V. CONCLUSION

Users are more concerned about safety and security on the road, as many people's lives are lost as a result of others' misbehavior and malice. To achieve a secure VANET system, additional effort will be required in the future to overcome these issues. This study provided a comprehensive analysis of the majority of VANET security concerns and their causes, as well as known remedies. We go over the latest security architectures as well as well-known security standards and protocols in detail. We concentrated on the classification and solutions to the various attacks described in the literature. Finally, we've identified certain research issues and open topics that could lead to future study. As a result, VANET will be able to rapidly construct a system for trusting vehicles while also protecting itself from malicious nodes.

REFERENCES

[1] R. I. Meneguette, Intelligent transport systems (ITS), “Framework for public mobile networks in cooperative its (c-its)s,” Tech. Rep., European Telecommunications Standards Institute (ETSI), Palo Alto, Calif, USA, April 2012.

[2] E. Hossain, G. Chow, V. C. M. Leung et al., "Vehicular telematics over heterogeneous wireless networks: a survey," Computer Communications, vol. 33, no. 7, pp. 775–793, 2010.

[3] S. Zeadally et al., "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges," Telecommun. Sys., vol. 50, no. 4, 2012, pp. 217–41.

[4] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, vol. 15, no. 1, 2007, pp. 39-68.

[5] T. Leinmuller, E. Schoch and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," Proc. Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on, 2007, pp. 84-91.

[6] D. Antolino Rivas, J.M. Barcelo-Ordinas, M. Guerrero Zapata and J.D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation," Journal of Network and Computer Applications, vol. 34, no. 6, 2011, pp. 1942-1955; DOI 10.1016/j.jnca.2011.07.006.

[7] R. Hussain, S. Kim and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET," Information Security Applications (WISA'09), Lecture Notes in Computer Science 5932, H. Youm and M. Yung, eds., Springer Berlin / Heidelberg, 2009, pp. 268-280.

[8] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, 2010, pp. 50-58; DOI 10.1145/1721654.1721672.

[9] Md Ali Al Mamun, Khairul Anam, Md Fakhrul Alam Onik, A M Esfar- E- Alam, "Deployment of Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture", Proceedings of Congress on Engineering and Computer Science 2012 Vol I WCECS 2012, October 24-26, 2012, San Francisco, USA.

[10] S. Olariu, M. Eltoweissy and M. Younis, "Towards Autonomous Vehicular Clouds," ICST Transactions on Mobile Communications and Applications, vol. 11, no. 7-9, 2011, pp. 1-11.

[11] M. Abuelela and S. Olariu, "Taking VANET to the clouds," Book Taking VANET to the clouds, Series Taking VANET to the clouds, ed., Editor ed.ˆeds., ACM, 2010, pp. 6-13.

[12] S. Olariu, T. Hristov, and G. Yan, "The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds," Developments in Mobile Ad Hoc Networking: The Cutting Edge Directions, Wiley, 2012.

[13] K. Mershad and H. Artail, "Finding a STAR in a Vehicular Cloud," IEEE Intelligent Transportation Systems, vol. 5, no. 2, 2013, pp. 55–68.

[14] Rasheed Hussain, Junggab Son, Hasoo Eun, Sangjin Kim and Heekuck Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing, 2012 IEEE 4th International Conference on Cloud Computing Technology and Science

[15] N. Zingirian and C. Valenti, "Sensor Clouds for Intelligent Truck Monitoring," Proc. IEEE Intell. Veh. Symp., 2012, pp. 999–1004.

[16] D. Bernstein, N. Vidovic and S. Modi, "A Cloud PAAS for High Scale, Function, and Velocity Mobile Applications - With Reference Application as the Fully Connected Car," Proc. Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, 2010, pp. 117-123.

[17] G. Yan, D.B. Rawat and B.B. Bista, "Towards Secure Vehicular Clouds," Proc. Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on, 2012, pp. 370-375.

[18] R. Hussain, Z. Rezaeifar, Y. H. Lee and H. Oh. (2015). "Secure and privacy-aware traffic information as a service in VANET-based clouds," Pervasive Mob. Comput. 24, pp. 194—209

[19] J. Jun Zhou, X. Dong, Z. Cao and A. V. Vasilakos. (2015). "Secure and privacy preserving protocol for cloud-based vehicular DTNs," IEEE Trans. Inform. Forensic Secur. 10 (6), pp. 1299–1314

[20] N. Kumar, J. P. Singh, R. S. Bali, S. Misra and S. Ullah. (2015). "An intelligent clustering scheme for distributed intrusion detection in vehicular cloud computing," Clus ter. Comput. 18 (3), pp. 1263–1283

[21] W. M. Kang, J. D. Lee, Y.-S. Jeong and J. H. Park. (2015). "VCC-SSF: Service-oriented security framework for vehic ular cloud computing," Sustainability 7 (2), pp. 2028–2044.

[22] I. M. Abumuhfouz and K. Lim. (2015). "Protecting vehic ular cloud against malicious nodes using zone authori ties," IEEE SoutheastCon., pp. 1–2.

[23] R. Lu, X. Lin, X. Liang and X. Shen. (2012). "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transport. Syst. 13 (1), pp. 127–139.

[24] R. Hussain, J. Son, H. Eun, S. Kim and H. Oh, "Rethinking vehicular communications: Merging VANET with cloud computing," in IEEE 4th International Conference, Cloud Computing Technology and Science (CloudCom), 2012, pp. 606–609.

[25] S. Bitam, A. Mellouk and S. Zeadally. (2015). "VANETcloud: A generic cloud computing model for vehicular ad hoc networks," IEEE Wireless Commun. 22 (1), pp. 96– 102.

[26] H. Yao, C. Bai, D. Zeng, Q. Liang and Y. Fan. (2015). "Migrate or not? Exploring virtual machine migration in roadside cloudletbased vehicular cloud," Concurrency Comput. Pract. Experience 27 (18), pp. 5780–5792.

[27] Y. Chen, M. Fang, S. Shi, W. Guo and X. Zheng. (2015). "Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow," EURASIP J. Wireless Commun. Netw. 2015 (1), pp. 98–110.

[28] M. U. Farooq, M. Pasha and K. U. R. Khan, "A data dissemination model for cloud enabled VANETs using invehicular resources," in IEEE International Conference Computing for Sustainable Global Development (INDIACom), 2014, pp. 458–462.

[29] S. Bitam and A. Mellouk, Cloud Computing-Based Message Dissemination Protocol for Vehicular Ad Hoc Networks. Wired/Wireless Internet Communications. Springer International Publishing, 2015, pp. 32–45.

[30] Y. W. Lin, J. M. Shen and H. C. Weng. (2013). "Cloudsupported seamless Internet access in intelligent transportation systems," Wireless Pers. Commun. 72 (4), pp. 2081– 2106.

[31] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud," SIGACT News, vol. 40, no. 2, 2009, pp. 81-86.

[32] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," Proc. Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, 2010, pp. 693-702.

[33] R. Hussain, S. Kim and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET," Information Security Applications (WISA'09), Lecture Notes in Computer Science 5932, H. Youm and M. Yung, eds., Springer Berlin / Heidelberg, 2009, pp. 268-280.

[34] S. Jinyuan, Z. Chi, Z. Yanchao and F. Yuguang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 21, no. 9, 2010, pp. 1227-1239.

[35] A. Bessani, M. Correia, B. Quaresma, F. Andr, and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds," Proc. Sixth conference on computer systems (EuroSys'11), ACM, 2011, pp. 31-46.

[36] G. Yan, D.B. Rawat and B.B. Bista, "Towards Secure Vehicular Clouds," Proc. Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on, 2012, pp. 370-375.

[37] Grilli,G., “Data Dissemination in Vehicular Networks”, PhD dissertation in Computer Science and Automation Engineering, June 2010.

[38] Doetzer,F.,”Privacy Issues in Vehicular Ad Hoc Networks”, Proceedings of The 5th International Workshop, PET 2005, Cavtat, Croatia 2005, pp.192-209, 2005.

[39] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, “A survey on vehicular cloud computing,” *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 325–344, 2014.

[40] G. Yan, S. Olariu, and M. Weigle, “Providing location security in vehicular Ad Hoc networks,” *IEEE Wireless Communications*, vol.16, no. 6, pp. 48–55, 2009.

[41] G. Yan, D. Rawat, and B. Bista, “Towards secure vehicular clouds,” in *Proceedings of the 6th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pp. 370–375, Palermo, Italy, July 2012.