Vehicular Cloud Computing Exposures

Pallavi B. Tembhurnikar (SKNCOE,Pune)[a], Prof. S.S.Barde(SKNCOE,Pune)
[a] now at Borehole Geophysics Research laboratory,karad,Maharashtra,India

Abstract— Vehicular systems administration has turned into a mainstream research zone in light of its particular gimmicks and applications, for example productive movement administration, road security and business perspectives. Vehicles are relied upon to convey generally more correspondence frameworks, ready for offices, stockpiling and expanded sensing force. Consequently, numerous advances have been sent to keep up and advance Intelligent Transportation Systems (ITS). As of late, various arrangements were proposed to address the difficulties and issues of vehicular systems. Vehicular Cloud Computing (VCC) is one of the arrangements. VCC is another engineering that has a recognizable effect on activity administration and road security by in a flash utilizing vehicular assets, for example, figuring, stockpiling and web for choice making. This paper shows the condition of the overview of secure communication in vehicular cloud computing. In addition, we exhibit a scientific categorization for vehicular cloud in which extraordinary consideration has been dedicated to the broad applications, cloud developments, key administration, protection and security issues. Through a far reaching survey of the writing, we outline building design for VCC, organize the properties needed in vehicular cloud that help this model. We contrast this system and typical Cloud Computing (CC) and talk about open exploration issues and future headings. By evaluating and examining writing, we found that VCC is an innovatively beneficial and monetarily reasonable innovative moving standard for joining canny vehicular systems towards self-ruling movement, vehicle control and recognition frameworks.

Index Terms—Vehicular cloud,V2V,V2I,CBRF,VANET,RSU,CLGF.

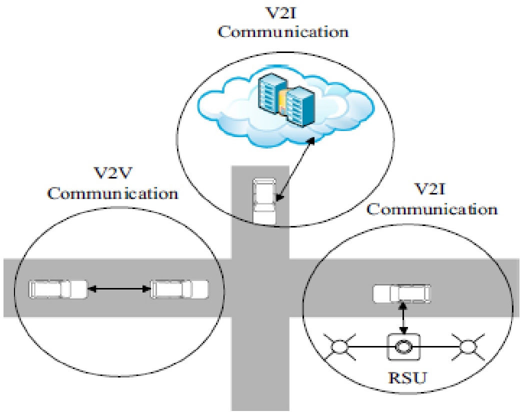
1 Introduction

Endeavors are routinely hunting down another and change strategy to build their profit and diminish their expenses. Those creativities need diverse advances that let them develop and don't strain them fiscally. From the present advancements, Cloud registering has risen as a promising arrangement giving on interest access to powerful figuring assets, stages, and applications in a pay-as-you-go way. Cloud administration clients can utilize what they require and pay just for what they utilize. As a consequence of this, Cloud registering has raised the conveyance of IT administrations to another level that brings the solace of conventional advantages, for example, water and power to its clients. There are different points of interest of Cloud processing, for example, cost value, versatility, and effortlessness of administration, empower more organizations and administration suppliers to adjust it and over their answers through Cloud registering models. Vehicular cloud figuring additionally builds its notoriety. Individuals use Laptops and other cell phones to get to the administrations of cloud. So the security issue increments and the information does not stay safe the aggressor assaults the information and misuse it. So to Investigate the fresh out of the plastic new zone and outline answers for every individual test in particular for authentication, Authorization, truth relationship, scalability and so on.

2 Related Work

All hubs, for example, vehicles and street side bases have the capacity correspond with one another focused around the V2V or V2I correspondence models in vehicular distributed computing. Besides, the vehicles and street side bases are obliged to speak with the cloud to store or methodology their information.

Area data assumes a crucial part in VC to transmit information and make associations on the grounds that most applications in vehicular frameworks depend on area data, for example, activity status reports, impact evasion , crisis cautions ,and helpful driving. In this way , the security of area data and restriction ought to be given among vehicles.



.

3 Proposed Work

1 VANET uses moving cars as node in network to create a mobile network which turns every participating car into a wireless router or node, allowing cars approximately 100 to

300 meters of each other to connect and, in turn , create a network with a wide range.

2 as cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

3 Each VANET car communicates with the VANET base station and other VANET cars using various protocols which are within its range.

4 VANET users vehicular mobility that take into consideration a number of parameters such as the speed of the vehicle, number of intersections on the road etc.

Small Scale VANETs

Small Scale VANETs- These are compatible for small areas which are less than 1 square miles. Special routing protocols are used in these VANETs which are different than the traditional MANETs.

Routing in small scale VANETs- Two routing techniques are used in small scale VANETs:- connection-based restricted forwarding (CBRF) and connectionless geographic forwarding (CLGF)

A. Proposed Schemes

1)Connection-based restricted forwarding (CBRF) : -It builds routes using a route request (RREQ)/route reply (RREP) query cycle. First RREQ packets are broadcast across the network to discover a route from the source to the destination. A node receiving an RREQ packet sends RREP packets back to the source if it has a route to the destination or is the destination itself; otherwise, it will rebroadcast the RREQ. Data packets are sent to the destination after the source node receives the RREP. The routing information is updated to ensure that the best route is chosen. If a link breaks while the route is active, a route error (RERR) message is sent to the source node. The source node may then reinitiate a route discovery process.

2) Connection-less geographic forwarding (CLGF) :- it is a location- based routing protocol that exploits the correspondence between geographic position and connectivity in a wireless network by using the postionsof the nodes to make packet-forwarding decisions. However, CLGF is greedy, because it always forwards packets to nodes that are progressively closer to the destination, if such a node exists.

Block Diagram

<u>Connection-based restricted forwarding (CBRF)</u>

1. There would be a Base Vanet Server (BVS) program running on a computer, responsible for communication between various Roadside Vanet Servers (RVS). This computer will hold the information of each RVS and also the no of connected vehicles to that RVS.

BVS is also responsible for suggesting the congestion less routing to vehicles from source to destination. BVS is capable of finding the congestion less routing because of the interconnection of RVS through BVS.

2. Each vehicle will be holding a unique identification number, so that once it leaves any one RVS and joins another RVS, then BVS can easily track the vehicle location based on the RVS details to which the vehicle is connected.

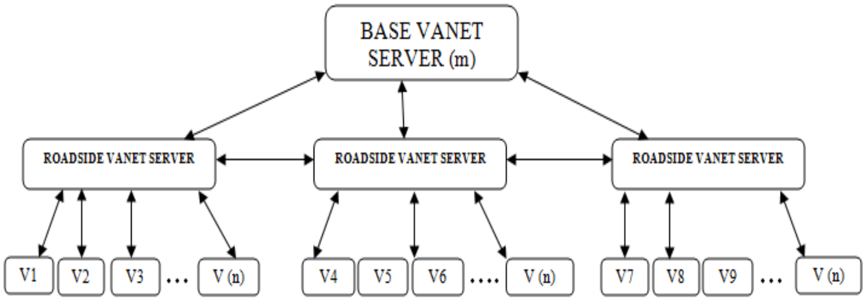
3. Each vehicle will also have properties like Id, Speed, Fuel Level, Driving Mode (Auto/Manual), GPS (enabled / disabled) & Destination. This information will be used to track and proximate the situation of the vehicle in RVS. Speed will be important to understand the system to understand or approximate its future location depending upon the speed. Destination parameter will be used to suggest the substitute path in case the approaching RVS is already flooded.

4. If any vehicle tries to join a RVS which is already congested with the max limit of vehicles allowed, then RVS will communicate with the vehicle to indicate the congestion & request to seek another path / route. It may or may not suggest a substitute path depending up on the availability of destination parameter.

5. The data communication in this model will use RSA encryption technique to make it more secure and safe to implement.

.

B) Actual Working



Notations:
m – Max Limit of Road Side Vanet Servers
n- Max Limit of Vehicles allowed / Road Side Vanet Server.

Encryption algorithm

Step 1:- Finding Hash of message (mh) using SHA-2 (H)

Step 2:- Encryption of message with Secret key (sk)

Step 3:- Perform XOR operation on mh and ks

Step 4:- Using RSA Encrypting the secret key and mhk (output of step 3) with Public key PU= {e, n} .

Step 5:- Using RSA, Decryption of mhk and encrypted secret key using Private Key PR= {d, n}

Step 6:- Perform XOR operation on sk and mhk to get mh

Step 7:- Decryption of Message using with sk

Step 8:- Finding the Hash of decrypted message and comparing it with mh (output of step 6) to authenticate the message.

Key Generation

1.Choose two distinct large random prime numbers and

2. Compute their multiplication, a= b*c, a is used as the modulus for both the public and private keys

3. Compute the totient: f (a)=(b-1)(c-1).

4. Choose an integer e such that 1 < e <f (a) , and share no factors other than 1 (i.e. e and φ(a) are co-prime) e is released as the public key exponent

5. Compute d to satisfy the congruence relation de=1(mod f (a)); i.e. de=1+kf (p) for some integer. d is kept as the private key exponent.

6.The public key consists of the modulus and the public (or encryption) exponent. The private key consists of the modulus and the private (or decryption) exponent which must be kept secret.

7.Recipient after calculating public key PU= {e , a} and private key PR= {d, a} sends the public
key value i.e., PU= {e ,a} value to sender.

4 Research Challenges

Security and protection concerns: The driver's security and security is dependably a testing examination issue in V-Cloud administrations. This can be managed by executing a module with approval what's more, validation functionalities etc.

Authentication: Security confirmation in the VC incorporates checking client character and message respectability. To direct validation, a few measurements can be received. Proprietorship: A client possesses some exceptional character (e.g.,identity card, security token, and programming token).

5 Conclusion

Security and protection are imperative viewpoints for the securing and keeping up the trust of clients in VC. Protection measures are obliged to guarantee the VC correspondence and data in the secluded and dependable environment. while security systems are expected to ensure against system dangers. Creating trust connections between a few members is an essential piece of reliable correspondence and processing. As a portion of the vehicles identified with VC may have met already ,the proactive undertaking of propelling a crucial trust relationship among vehicles is alluring and conceivable. Hence this paper gives the secure communication method to vehicular cloud computing which prevents the attacks at the time of message transfer.

.

6 Acknowledgment

This work is supported by Smt. Kashibai Navale College of Engineering,Pune under the Savitribai Phule Pune University,Pune. This project work is supported by Dr. A. V. deshpande, Dr. P. N. Mahalle, Dr. K. N. Honwadkar and under the guidance of Prof. S.S.Barde. This work was jointly supported by Borehole Geophysics Research Laboratory, karad (Maharashtra),India.

7 References

[1] Khaleel Mershad, and Hassan Artail, "Finding a STAR in a Vehicular Network", *IEEE Intelligent transportation systems magazine*, pp. 55-68, 2013.

[2] S.Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int. J. Pervasive Comput. Commun.*, vol. 7, no. 1, pp. 7-21, 2011.

[3] Fleming B. Smarter and Safer Vehicles. Vehicular Technology Magazine, *IEEE* 2012;7:4-9.

[4] Gabauer DJ, Gabler HC.Comparison of roadside crash injury metrics using event data recorders. Accident Analysis & Prevention. 2008, 548-58.

[5] Mousannif H, Khalil I, Al Moatassime H. Cooperation as a

Service in VANETs. *Journal of Universal Computer Science* 2011;17:1202-18.

[6] Olariu S, Hristov T, Yan G. The next paradigm shift: From vehicular networks to vehicular clouds. In: S. SINTRONES. 2009.

[7] Olariu S, Khalil I, Abuelela M. Taking VANET to the clouds, *International Journal of Pervasive Computing and Communications*. 2011 ; 7:7-21.

[8] Aijaz A, Bochow B, Dotzer F, Festag A, Gerlach M, Kroh R, et al. Attacks on inter vehicle communication systems-an analysis. 2006.

[9] Lochert C, Scheuermann B, Caliskan M, Mauve M, The feasibility of information dissemination in vehicular adhoc networks. IEEE; 2007. p. 92-9.

[10] Liu Y, Bi J, Yang J. Research on vehicular ad hoc networks. Control and Decision Conference, 2009 CCDC'09 Chinese: IEEE; 2009. p. 4430-5.