Vehicular cloud computing security issues and solutions

N. Priya, J. Sridhar*, M. Sriram
Department of computer Science engineering, Bharath University
***Corresponding author: E-Mail: sridhar.cse@bharathuniv.ac.in**

ABSTRACT

Vehicular cloud is a new concept which is an extension of conventional cloud. The idea of Vehicular cloud (VC), taken into account in order to improve the usage of the resources that are idle in vehicles when they are not in use, these resources are clubbed to form the cloud. The resources that are included in the vehicle are front camera, rear camera, processing unit, GPS system and sensors these resources collaborate with each other to obtain the information regarding the surroundings. The information generated need security as it is disseminated among all the vehicles, the attacker may create a threat to the information which is stored on to the VC and this create a serious issue. To address some of the issues the mechanism that are used in VANET are adopted in VCC**.** In a VC, vehicular resources involved computing power, storage, and Internet connectivity that can be shared between drivers. They are connecting with customers through internet. VC concept is an important society impact that needs security and privacy issues that should be corrected. The main purpose of this work is to find the security challenges and privacy threats in VCs. Also we discussed about some security plans too.

KEY WORDS: Challenges, cloud computing, privacy, security, vehicular cloud

1. INTRODUCTION

Nowadays the vehicles are joined with heaps of workplaces, for instance, web by which customer can update him with what is happening far and wide, GPS (Global Positioning System) allow the customer to track the zone, the on-board units which are nowadays sent with limit capacity is used to track the status of the vehicle, and furthermore the driver. Preceding the vehicle gathering was the bit of mechanical planning, yet today the considered road wellbeing and negligible exertion of equipment, these vehicles has changed into "PC on wheels or PC framework on wheels" which has been wound up contention for maker to advance a valiant exertion and hold the spot in advancing. The vehicular cloud is a mix of both VANET (vehicular offhand framework) and cloud computing, by which better utilization of advantages is possible.

The VANET (vehicular specially appointed system) utilizes the portability model of MANET (versatile impromptu network). In this system versatile hub are vehicles, which faculties the encompassing and forward the data to other hub on the bounce by jump premise, here the hubs speak with one another with help of DSRC(Dedicated Short Range Communication)link, which go from short range to medium extent (300-1000m)this remote correspondence channel particularly intended for car use. The autos will be having front and raise camera, and in addition the radar that gives data of surroundings, for example, the street conditions or climate condition, the vehicles go about as a test to assemble the data that can be conveyed up and down the street.

Cloud computing is the framework which permit the client to utilize the assets on the premise of pay-per-use [10]. The assets might incorporate programming similar to, application programming, working framework and equipment like capacity, processor and so forth. This model has remembered the client from the issue of having assets that are not reasonable. The administrations gave by the cloud are Storage as an administration (SaaS), Information as an administration (IaaS), and Platform as an administration (PaaS).Without the utilization of costly customer's client can have admittance to these administrations.

Vehicular cloud makes use of the devices such as sensors, storage and computing devices in order to create a cloud. Most of the time these devices are idle i.e., before in VANET the devices are turned off when they are not in use because of this it creates routing problem. This proposal allows the interested user to rent their resources and increase the economy. The VCC uses V2V (vehicle to vehicle) communication and also V2I (vehicle to infrastructure) communication the infrastructure here is, the Roadside Unit (RSU).

As vehicle are the presume that is the producer of the information and consumer of the information the security issues that arises need to be addressed , the cloud participants are the vehicle, which has got high mobility and providing security for each is a tedious task, as here every interested user shares it resources with other user there is no differentiation between the attacker and the legal user because as all are involved in building the cloud, in the traditional cloud security is provided by keeping the attacker at the bay which cannot be adopted in this system. The user is made available with the information at the right place and time, as the content produced and consumed is relevant to local vicinity. The internet cloud provides facility of uploading the content as well using the resources unlimitedly, but it is time consuming as well costly to upload and download every single record to the cloud.

If any accident or traffic happened in roads that information can be recorded by cars and the record is send to all nodes, that information is used to investigate about the incidents like accidents and the user who send the information is act as a an evidence. The vehicles can also helpful for recording the environmental conditions such as cyclone like any environmental disasters.

Vehicular cloud creation: The internet cloud is created by cloud provider where the services are processed and maintained by him, where as in vehicular cloud, the cloud is created on the fly by using the resources of the vehicle, this can be done by making the vehicles to interact with each other. Here the region is divided into specific grids and for each part of a grid the virtual machine is allocated which is responsible for providing access to the information as well as maintaining the information, if there is congestion in particular region and if the request cannot be handled the virtual machine request to other virtual machine for the resources.

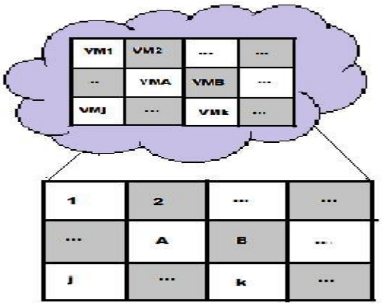

Figure.1.Area divide into cells and each mapped to respective virtual machine

The Fig (1) depicts mapping, here Virtual Machine1 (VM1) is mapped to cell1, Virtual Machine2 (VM2) to cell 2 and so on.

For example video surveillance is an important application that uses storage devices present in the vehicles, but this creates a problem of storage as well as the video is surveyed offline by the transportation agencies. To overcome this problem the vehicles first will create vehicular cloud, here the requested vehicle will become a controller for the cloud and then they communicate with Roadside cloud as shown in Fig(2). Here the vehicles that have gathered information (video) will request for the resources to the virtual machine, after receiving Virtual machine on the roadside will allocate the resource for the vehicle in need, as soon as the vehicle gets the resources it will upload the video to the cloud, when the vehicle migrates from one place to other place, the uploading of video continues on other roadside cloud.

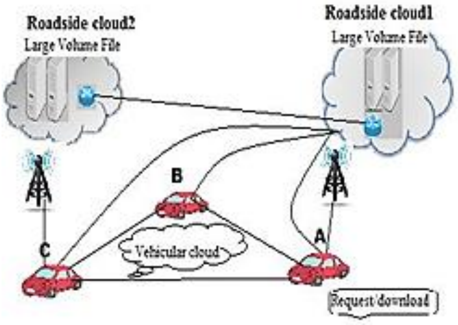

Figure.2. Creation of cloud for downloading video file

While downloading the file requesting node will look for the neighbor node if they are in coverage then the cloud is created as shown in Fig(2). Node A requesting for download of a file, observes the neighboring nodes i.e., B and C. the VM is created on both the nodes B and C, all the three vehicles will download the file from the roadside cloud in this way the vehicle A will have the file before it moves out of the range of roadside infrastructure, as it moves out the remaining each part will be downloaded from the vehicle by using V2V communication.

Security issues: As the information generated here is very sensitive that that need to be handled carefully. The security issues that may arise are listed in. Providing authentication to each and every vehicle is the tedious task due to the high mobility, as vehicles will be sharing same physical infrastructure it's difficult to keep the attacker at the bay. Though the attacker and target are located on different machines but they share same infrastructure in Vehicular cloud. The intruder mainly effects on confidentiality, integrity and availability. The confidential information can be the user identity, virtual machine location on which the target's services are executing and valuable documents that are stored on the vehicular cloud. The integrity is nothing but tampering the information, the attacker may alter the information generated by the legal user. Availability, the attacker may change the privileges that make the resources unavailable to the target user.

Problem of authentication in vehicular cloud is because of the frequent change in the vehicle's location, for example if the vehicle records for accident event and generates the message, verifying such information depending upon the location is difficult as the location of vehicles changes spontaneously, due to the short transmission range the recipient may tend to be out of reach, as well it is difficult to update the security key pair.

Technology behind security: In order to provide security in terms of authentication and confidentiality, geographic location based security mechanism can be used which ensures the physical security, here the messages are encrypted using geographic location key which specifies the decryption region, where actually the node should exist in order to decrypt the message encrypted with geographic location key.

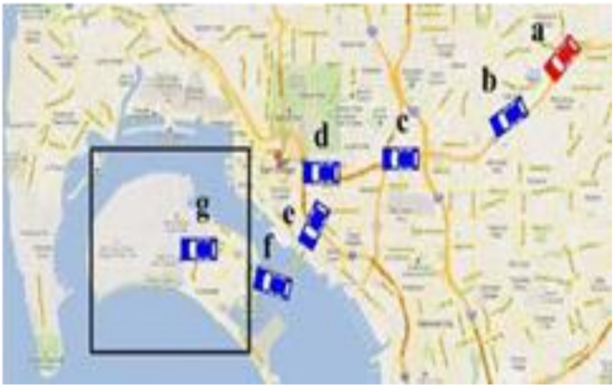

Figure.3. This algorithm is repeated by client during message exchange

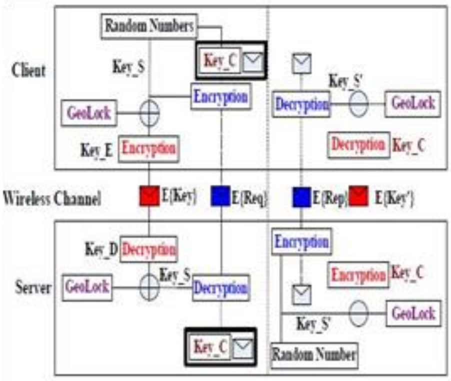

Figure.4. Illustration of Encryption and Decryption process

Geo Lock Function: Parameters for this function are GPS position, time and speed. Here GPS position is considered along with decryption region is fed as input to the function, this GPS location is divided by the length of the decryption region, and later the integral remainder are concatenated and then they are hashed in order to obtain GeoLock. The flow is GeoLock is shown in Figure 4.

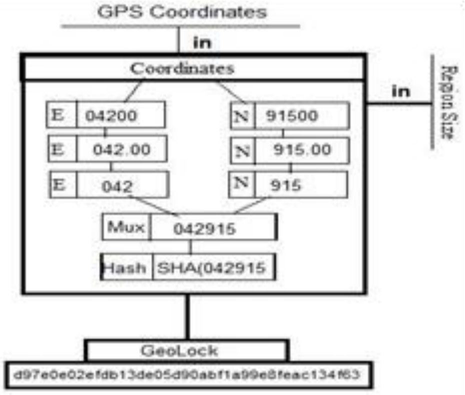

Figure.4.GeoLock Algorithm, here the region is 100m and the GPS coordinates are divided by 100m and then the integral remainder is concatenated to form input to hash algorithm

2. CONCLUSION

This paper describes about novelty in Intelligent Transportation System and also highlights the security issues that are caused due to the high mobility of the vehicles. To overcome security problem, the methodology used in VANET that is GeoLocation based encryption/decryption is adopted, which is a hybrid encryption that generates the session key to encrypt location information as well as symmetric key that is used for the further communication.

REFERENCES

Achudhan M, Prem Jayakumar M, Mathematical modeling and control of an electrically-heated catalyst, International Journal of Applied Engineering Research, 9 (23), 2014, 23013.

Analysis Of Security Challenges And Implementation Of Security Mechanism In Vehicular Cloud Computing, Neetakattimani, Gbhaskar, International Journal Of Current Engineering And Scientific Research (Ijcesr), 2 (7), 2015

Gopalakrishnan K, Sundeep Aanand J, Udayakumar R, Electrical properties of doped azopolyester, Middle - East Journal of Scientific Research, 20 (11), 2014, 1402-1412.

Gopinath S, Sundararaj M, Elangovan S, Rathakrishnan E, Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow, International Journal of Turbo and Jet Engines, 32 (1), 2015, 73-83.

Ilayaraja K, Ambica A, Spatial distribution of groundwater quality between injambakkam-thiruvanmyiur areas, south east coast of India, Nature Environment and Pollution Technology, 14 (4), 2015, 771-776.

Kerana Hanirex D, Kaliyamurthie KP, Kumaravel A, Analysis of improved tdtr algorithm for mining frequent itemsets using dengue virus type 1 dataset: A combined approach, International Journal of Pharma and Bio Sciences, 6 (2), 2015, 288-295.

Lingeswaran K, Prasad Karamcheti SS, Gopikrishnan M, Ramu G, Preparation and characterization of chemical bath deposited cds thin film for solar cell, Middle - East Journal of Scientific Research, 20 (7), 2014, 812-814.

Premkumar S, Ramu G, Gunasekaran S, Baskar D, Solar industrial process heating associated with thermal energy storage for feed water heating, Middle - East Journal of Scientific Research, 20 (11), 2014, 1686-1688.

Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan Vehicular ad hoc networks (VANETS): status, results, and challenges: Telecomm Syst DOI 10.1007/s11235-010-9400-5 Springer Science+Business Media, LLC, 2010.

Sundar Raj M, Saravanan T, Srinivasan V, Design of silicon-carbide based cascaded multilevel inverter, Middle - East Journal of Scientific Research, 20 (12), 2014, 1785-1791.

Thooyamani KP, Khanaa V, Udayakumar R, Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, 20 (12), 2014, 2464-2470.

Thooyamani KP, Khanaa V, Udayakumar R, Partial encryption and partial inference control based disclosure in effective cost cloud, Middle - East Journal of Scientific Research, 20 (12), 2014, 2456-2459.

Thooyamani KP, Khanaa V, Udayakumar R, Using integrated circuits with low power multi bit flip-flops in different approch, Middle - East Journal of Scientific Research, 20 (12), 2014, 2586-2593.

Thooyamani KP, Khanaa V, Udayakumar R, Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, 20 (12), 2014, 2604-2612.

Thooyamani KP, Khanaa V, Udayakumar R, Wide area wireless networks-IETF, Middle - East Journal of Scientific Research, 20 (12), 2014, 2042-2046.

Udayakumar R, Kaliyamurthie KP, Khanaa, Thooyamani KP, Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, 29 (14), 2014, 86-90.