ANALYSIS OF SECURITY CHALLENGES AND IMPLEMENTATION OF SECURITY MECHANISM IN VEHICULAR CLOUD COMPUTING

[1]Neeta Kattimani, [2]G Bhaskar
[1]M.Tech, CNE, [2]Assistant Professor
Dept. Computer Science and Engineering, Siddaganga Institute of Technology
Tumakuru, Karnataka
E-mail: [1]kattimani.n.neeta@gmail.com, [2]bhaskar_gopal@sit.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.

Index Terms— VANET, Cloud Computing, Vehicular cloud, Security challenges

I. INTRODUCTION

Nowadays the vehicles are integrated with lots of facilities such as, internet by which user can update him with what is happening around the world, GPS (Global Positioning System) allow the user to track the location, the on-board units which are nowadays deployed with storage capability is used to track the status of the vehicle, as well as the motorist. Before the vehicle manufacturing was the part of mechanical engineering, but today the consideration of road safety and low cost of electronics, these vehicles has turned into "computer on wheels or computer network on wheels" which has been become competition for manufacturer to give their best and hold the place in marketing. The vehicular cloud is a combination of both VANET (vehicular ad-hoc network) and cloud computing, by which better utilization of resources is possible.

The VANET (vehicular ad-hoc network) uses the mobility model of MANET (mobile ad-hoc network)[1]. In this network mobile node are vehicles, which senses the surrounding and forward the information to other node on the hop by hop basis, here the nodes communicate with each other with help of DSRC(Dedicated Short Range Communication)link, which range from short range to medium range (300-1000m)this wireless communication channel specifically designed for automotive use. The cars will be having front and rear camera, as well as the radar that provides information of surroundings such as the road conditions or weather condition , the vehicles act as a probe in order to gather the information that can be distributed all along the road.

Cloud computing is the system which allow the user to use the resources on the basis of pay-per-use [2]. The resources may include software's like, application software, operating system and hardware like storage, processor etc. This model has relived the user from the problem of having resources that are not affordable. The services provided by the cloud are Storage as a service (SaaS), Information as a service (IaaS), and Platform as a service (PaaS).Without the use of expensive client's user can have access to these services.

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 prosumer 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.

The information collected by cars is of most important for example if there is a congestion or there's an accident on road, these vehicles can be used to record the event and disseminate the information to all other nodes, sometimes the information can be used to investigate the accident, the user who are present at the incident can act as an evidence. The vehicles can also helpful for recording the environmental conditions such as cyclone, tornado, or any environmental disasters.

II. Related Work

In [3] this paper the author Olariu has described how both technologies can be clubbed and provide road safety, as well as they have described the issues that arises.

The paper [4] Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs, used to hide the identity which can be done by using pseudonyms instead of using the original identity, this method also provide revocation depending upon the behavior of the vehicle.

III. 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 [3].

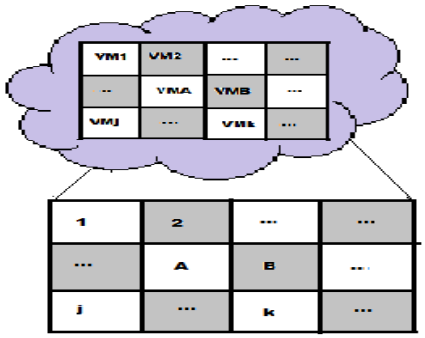

Fig 1. Area divide into cells and each mapped to respective virtual machine.

The Fig (1) depicts mapping, here Virtual Machine1 (VM1) is mapped to cell1, Virtual Machine2 (VM2) to cell2 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 [5] 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.

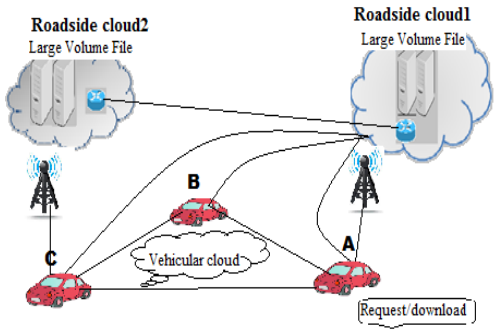

Fig 2. Creation of cloud for downloading video file.

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.

IV. SECURITY CHALLENGES

As the information generated here is very sensitive that that need to be handled carefully. The security issues that may arise are listed in [6]. 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 attacker can attack 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.

V. SECURITY MECHANISM

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 as shown in Fig(3).

Fig 3.Geographical location based encryption, the only node (***g***) in the shaded region can only decrypt and access cipher text sent by vehicle (***a***).

In this technique there are two stages one is security key handshake and message exchange.

Key Exchange Algorithm [on the client side]

Step1: Generation of random numbers *Key_S* and
Key_C (*Key_S* used for encrypting the Aggregated location message (Msg) and *Key_C*).

Step2: E{Req} = Enc{*Key_S*(*Key_C*, *Msg*)}

Step3: Generation of GeoLock using server location.
E{*Key*} = Enc{*Key_E*(GeoLock $\oplus$ *Key_S*)}
Where *Key_E* – Public Key of Server.

Step 4: Transmit E {Key}, E {Req} on wireless
transmission channel.

Algorithm on server side:

Step1: Decrypt=*Key_D*{E{Key}}, where *Key_D*
is private key of server.

Step2: Generates GeoLock using its own GPS Location to obtain Key_S

Step 3: *Key_S* is used to decrypt E{Req} which contains aggregated location information and secret key *Key_C* .

Message Exchange Algorithm [on sever side]

Step1: Generation of random number Key *Key_S'*.

Step2: Encrypt message using *Key_S'* to generate cipher-text E{Rep}.

Step3: The aggregated location message contains the client's GPS position, the server generate a GeoLock of the client vehicle's decryption region.

Step4: The generated GeoLock is XOR-ed with *Key_S'* and then encrypted with *Key_C* to generate cipher-text E{*Key'*}

E{*Key'*}=Enc{*Key_C{*GeoLock⊕*Key_S'}}*

Step5: Both E{Rep} and E{*Key'*} are transmitted to the client over a wireless channel.

Algorithm on client side:

Step1: E{Key} is decrypted using *Key_C* to recover the XOR of the client's GeoLock region and *Key_S'*.

Step2: The client generates its GeoLock based on its current location to recover the *Key_S'*.

Step3: E{Rep} is decrypted using *Key_S'* and reply message is recovered.

This algorithm is repeated by client during message exchange.

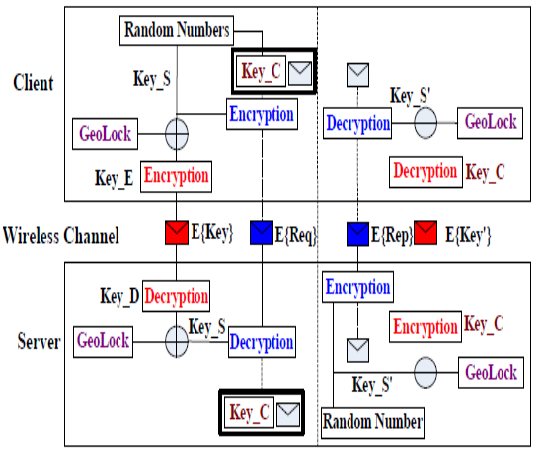

Fig 4. Illustration of Encryption and Decryption process

A .GeoLock 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 Fig4.

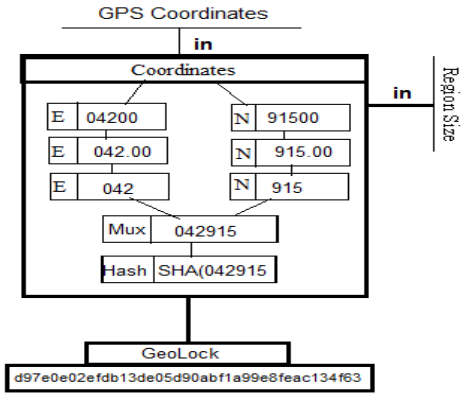

Fig 4: GeoLock Algorithm, here the region is 100m and the GPS coordinates are divided by 100m and then the integral remainder is concatenated to form input to hash algorithm.

VI. 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

[1] 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

[2] Alexa Huth and James Cebula: The Basics of Cloud Computing: The NIST Definition of Cloud Computing at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud definition.pdf

[3] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle: Security Challenges in Vehicular Cloud Computing, IEEE Transactions on Intelligent Transportation Systems, Vol. 14, No. 1, March 2013

[4] Dijiang Huang, Satyajayant Misra, Mayank Verma, and Guoliang Xue*:* PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs, IEEE Transactions on Intelligent Transportation Systems, Vol. 12, No. 3, September 2011

[5] Rong Yu, Yan Zhang, Stein Gjessing, Senior Member, Wenlong Xia, Kun Yang, Senior :Toward Cloud-based Vehicular Networks with Efficient Resource Management

[6] Microsoft, The stride threat model. [Online]. Available: http://msdn.microsoft.com