International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 13 • Issue 1 pp. 1-5 Jan - June 2021 www.csjournals.com

A Survey on Secure Fog-Computing Infrastructure for Internet of Vehicles

Kusuma G S
Assistant Professor, Vemana Institute of Technology, Bengaluru, Karnataka, India

Abstract: Vehicular Adhoc Networks_(VANETs) are subgroup of Mobile Adhoc Networks_(MANETs), which consists of Roadside Units(RSUs),On Board Units(OBUs), and Internet of Vehicles which transfer the information to each other through the wireless media.VANETsrequires the secure communication between V2V and V2I when vehicles are moving with high speed. This communication intern generates the large amount of data which has to be used for further computation and storage.To secure this data and satisfy the needs of VANETs, Fog computing is an augmentation of cloud computing is used, which provides services to user based on their request at the network edge. In this paper, surveyed various security challenges, security algorithms used in VANETs Infrastructure.
Keywords: VANETs, Security, Fog Computing.

Introduction: VANETs are constituted as a subtype of Mobile network consists of vehicle nodes which are embedded along with On Board Units(OBUs) performs vehicle to infrastructure and vehicle to vehicle communications. Now a days, Internet of Vehicles(IoVs) plays a important role in the establishment of Intelligent Transportation system(ITS).With the drastic development of the IoVs where vehicles generates huge information during transmission and creates the security complications in IoVs. IoV Systems offers two way of communication vehicle-vehicle and vehicle to infrastructure communication through wireless media using IEEE802.11p which provides safety requirements such as authentication, privacy and data integrity [1].Internet of vehicles ensures traffic safely by processing the huge amount of data. Communication between vehicles and roadside infrastructure accomplished by exchanging the messages and generates huge amount of data which intern leads in demand of storage and further computation.Security is the major problem in transferring information between V2V and V2I.In V2V Communication, individual vehicle sends information such as vehicle location, speed, traffic etc., to other connected vehicles, which in turn make other vehicle to take the decision if necessary. In V2I communication,particular vehicle requests the service with roadside units(RSU's).RSU's acts as a actuator and send the information to an authenticated server. To satisfy the real world demands such as high mobility, reduced latency, etc., in a real time VANETs development and to enhance the performance of a system fog computing is used.

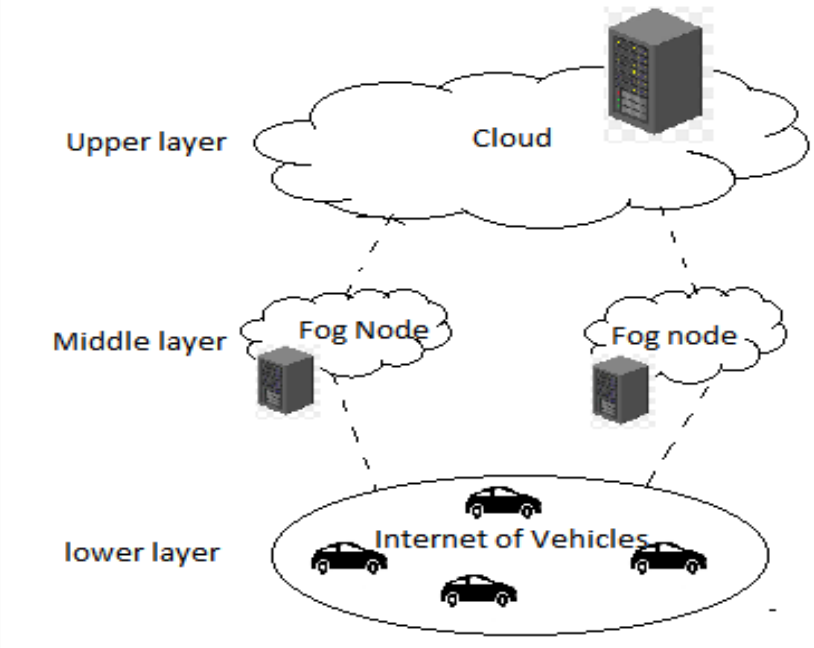

Fig1:Basic fog-oriented VANETs Structure

Fog Computing Overview:

Fog Computing[2] which is an extension of cloud computingconsists of fog-nodes connected directly near the edge devicesperforms computation at the edge of networks and provides services to the internet of vehicles in a VANETs environment. Task with low latency requirement applications executed by fog nodes and task with large latency requirement application executed by the cloud.Vehicles connected to IoV varies from small to larger range, it is complicated to measure the delay caused by each vehicle in a connected vehicular network. This gives the concept of fog-computing comprises of fog nodes with fog head acts as central processing unit which helps in transmitting the valid information such as vehicle access requests, each vehicleinformation etc., between the connected vehicles securely with reduction in the delay[3].

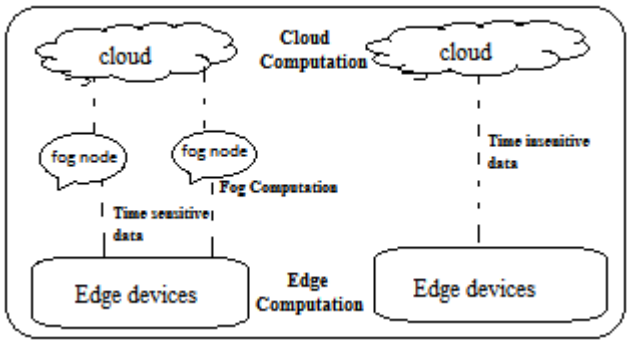

Fig2:Fog Computing model vs cloud computing model.

As there is lots of necessity of cloud computing, due to which there are some unsolved issues because of inherent problems such as un-reliable latency, lack in high-mobility support and location-awareness. Fog-computing well known as edge- computing address the issues of cloud computing by providing more resources and services to the users at the network edge.

There have been several research work carried out in the area of secure fog computing for VANETs applications using various security algorithms. In section I, reviewed some existing security protocols/algorithms to overcome the security issues in VANETs. Section II describes the comparative study of security techniques and evaluation parameters, Finally section III illustrates brief conclusion.

I. Related works:

MhidiBousselham et.al.[4], introduced a new security algorithm on decoy technology and user behaviour profiling (UBP) to avoid the securityand privacy problems in Vehicular cloud servers with fog-computing environment by delivering the decoy files. This technology achieves high efficiency at the time of malicious attack by making intruder not able to differentiate between the original and a decoy file.In Vehicular cloud system,it also decreases the cost of damage at the time of insider attacks.
Mimi Ma,et al[5],proposed key agreement protocol which achieves high level of security in case of high mobility and achieves low latency in VANETs with fog computing. Protocol generates the session key in order to save confidentiality of messages transmitting between connected vehicles and between fog nodes to provide mutual authentication by guaranteed the validity of all users.
JianbinGao,et al[6],used the architecture of SDN based Block chain protocol in 5G Networks. Here the block chain is used to enhance the trust between vehicles as the information shared by the vehicles are important and also improves the efficiency of the system. The protocol introduces two models such as trustand communication models, to examine its efficiency. Fog computing used in this architecture is to diminishes the handover problems among the vehicles.
Xingchen Liu, et.al.,[7] A blockchain basedmanagement trust model is presented here to realize the information synchronization and credibility. And an aggregateanonymous vehicular protocol is proposed to allow vehicles to send data anonymously in the un-trusted environment to ensure the privacy concepts of the vehicle. Based on vehicles reputation value which are stored in road side units calculates the reliability of a messages. Trusted authority used to identify the malicious users.
Jiawen Kang, et.al.,[8] proposed scheme called fog computing based Privacy Preserved Pseudonym Scheme to ensure secure communication between vehicles. Pseudonym management done at the edge network. Pseudonym fogs assignsPseudonym to closeby vehicle for privacy protection.Cloud layer which is the main core of the

system execute complex tasks by storage resources. This scheme improvise location privacy of the vehicles and decreases communication overheads.

Muhammad AwaisJaved, et.al., [9] proposed Fog Assisted Protocol for vanet application where it consists of cluster of vehicles, cluster head. Cluster head which transmits the traffic information between vehicles and fog embedded Road side units using C-V2X and IEEE 802.11p technologies. Cluster head collects the query request from the vehicles and communicates with RSU in a bidirectional manner. RSU based on the request sends the traffic response to requested vehicle. Cluster based method makes the transmission in simple way. By the time the traffic response is ready from the RSU, there is the changes in the location of requested vehicle. Its difficult for Fog RSU to identify the location of vehicles. Using the proposed protocol, fog RSUs communicates with cluster head and gets the updated location of the requested vehicle. Then the transmission takes place with the help of C-V2X multi hop transmission and reduces the traffic load.

Kuljeet Kaur, et.al., [10] to improve the driving safety and vehicular services, fog computing and lightweight authentication mechanism are used in the proposed system for reliable and secure communication between vehicles in case of high mobility to ensure optimal quality of service.

Sultan Basudan, et.al., [11] proposed certificate less security scheme applied for fog based vehicular crowd sensing applications in improving storage and communication overhead at the same time it maintains privacy.
In crowd sensing reports,RSU consists of fog nodes deletes the repeated reduplicated data by securing the original information of crowd sensing reports. In the scheme, Communication overhead between vehicles, RSUs, in terms of the ciphertext length were analysed.

Sarah Iqbal,et,al.,[12]To maintain the better Quality of Service, the proposed scheme with vehicular network where vehicles acts as fog_nodes. Tasks assigned to the connected vehicle based on thework load.RSUs helps vehicle to perform the task efficiently.Blockchain security method is used to provide better security and maintains privacy using centralised database. Block chain based data model is difficult to forge and tamper.

Yunseong Lee, et. al.,[13] the systemis described to overcome the message integrity and service stability problems in Vehicular network.In the proposed scheme, Road side unit acts as fog server and vehicles acts as fog devices.Road side units provides the vehicle related services to the each connected vehicle. In order to secure services provided by the RSUs,Block Chain based hyper ledger fabric framework implemented between different RSUs for verifying each transaction.

LiangjunSong,et.al.,[14],proposed framework for analysing trusted authority, fog head and vehicle. Trusted authority acts as server generates the secrete_key, system public_key and control parameters which are loaded to each connected vehicle. Based on the vehicle information trusted authority track the vehicle and also identify the fog head. Fog head helps in communicating between the vehicles and it is responsible for monitoring the security issues. Vehicles embedded with position monitoring system which helps fog head to identify the location of vehicle. If fog head cancelled due to connectivity issues, then the vehicles reselects the fog head. proposed deep learning based two way vehicle authentication scheme for better privacy protection.

Seyed Ahmad Soleymani,et.al[15], Based on the fuzzy logic proposed trust-model which access the accuracy and integrity of the message sent by the sender. Authentication module used here protect against Sybil attack by providing unique identity to each vehicle. In this scheme, Authentication ID is used to detect whether the data sent by the sender is authorised or not and also it verifies the vehicle belongs to valid network or not.The lifetimeof the messages which is the duration between start time and expiry time of transmitted messages exists due to the dynamic characteristics and high mobile vehicles. The scheme helps in calculating the lifetime of the Expired messages treated and transmits the fresh message in high mobility scenario of vehicles.

II. COMPARATIVE STUDY

Table I summarizes the various Security concepts used in VANETs Applications. Data Security is the major problem faced during the transmission of messages between the vehicles and Road side units embedded with fog nodes. The VANETs system is effective when the system is designed with highly secure with fog computing technology.

Table I: Comparative table for Security techniques used in Fog Computing based Vehicular Adhoc Networks.

Paper	Key feature	Evaluation Parameters
MhidiBousselham et.al.[4]	-The technology used to detect the unauthorised access to original information by generating the decoy files	System Accuracy
Mimi Ma, et.al.,[5]	-Provides high security by generating session key using a agreement key protocol	Total Computation Cost
Jianbin Gao, et.al.,[6]	-Enhance the trust between vehicles as the information shared by the vehicles are important	Packet delivery ratio, Transmission delay

	and also improves the efficiency of the system	
Xingchen Liu, et.al.,[7]	-Aggregate Anonymous vehicular protocol, where aggregation of messages in VANETs is done to provide authentication and decreases the network overhead. The reliability of messages is improvised by the threshold number vehicles.	Average computation time, reputation value, average latency
Jiawen Kang, et.al.,[8]	-Vehicle privacy protection was accomplished by using privacy preserved Pseudonym scheme.	Decrease in communication overhead
Muhammad AwaisJaved, et.al., [9]	-Secure traffic information transmission between vehicle and fog RSU with less traffic load using cluster based technology.	Data reception value and delay of traffic messages.
Kuljeet Kaur, et.al., [10]	-Key exchange and light_weight authentication mechanism for vehicular fog infrastructure is used to reduce to communication overhead. -Provides authentication, user privacy and confidentiality.	Reduction in communicational and computational overheads with improvised security features.
Sultan Basudan, et.al., [11]	-It uses homomorphic technique to measure the performance of secure computation from the RSUs.	Reduction in Communication overhead between fog nodes.
Sarah Iqbal,et,al.,[12]	-It handles different workloads using fog vehicles. -It uses Block chain based security scheme for providing security between vehicles and RSUs.	Queuing delay,work completion rate and latency
Yunseong Lee, et. al.,[13]	-It uses service allocation with a vickrey Clarke groves (VCG) auction scheme for securing the service transaction.	Average Communication& propagation Latency
LiangjunSong,et.al.,[14]	- The fog oriented authentication scheme comprises of two layers-authentication layer for vehicles out of the fog and monitoring layer for the remaining vehicles for providing better security.	Better authentication accuracy and adaptabilityto a high speedwireless network
Seyed Ahmad Soleymani,et.al[15]	-Fuzzy logic used for secure transmission. -Calculates the life time of messages, and generates the fresh messages during high mobility of vehicles.	Accuracy and data integrity.

III. CONCLUSION

VANETs are the application of MANETs and which are the major part of intelligent transport systems. To ensure safety of connected vehicles and avoid unpleasant scenarios, security measures are required to maintain during the transmission of valid data between the connected vehicles and road side infrastructure. For efficient computation and storage,fog- computation is used along with cloud computation.The features of fog to roadside infrastructure are added to the vehicular network for efficient and secure data transmission between vehicles. Survey gives the information about various security techniques applied to secure the vehicles which are connected in vehicular adhoc networks and also different parametric are evaluated in the existing papers were analysed.

REFERENCES

[1] Hsin-Te Wu and Gwo-JiunHorng, “Establishing an Intelligent Transportation System with a Network Security mechanism in an Internet of Vehicle Environment,” IEEE Access,vol no-5,pp 19239 – 19247,2017,DOI:10.1109/ACCESS.2017.2752420

[2] Shanhe Yi, Cheng Li, Qun Li, “A Survey of Fog Computing: Concepts, Applications and Issues,”Mobidata '15: proceedings of the 2015 Workshop on Mobile Big Data,pp 37–42,2015,DOI:10.1145/2757384.2757397

[3] KaneezFizza, Nitin Auluck, Akramul Azim, Md. Al. Maruf, and Anil Singh, “Faster OTA Updates in Smart Vehicles using Fog Computing,” UCC '19 Companion: Proceedings of the 12th IEEE/ACM International Conference on Utility

and Cloud Computing Companion, pp 59–64,2019, DOI:10.1145/3368235.3368842

[4] MhidiBousselham, Nabil Benamar, AdnaneAddaim, " A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System," 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 2019,DOI:10.1109/WITS.2019.8723723

[5] Mimi Ma, Debiao He, Huaqun Wang, Neeraj Kumar, Kim-Kwang Raymond Choo," An Efficient and Provably-Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks," IEEE Internet of Things Journal Vol.6,Issue-5,2019,DOI:10.1109/JIOT.2019.2902840

[6] JianbinGao,KwameOpuni-BoachieObourAgyekum;EmmanuelBoatengSifah,KingsleyNketiaAcheampong,QiXia;XiaojiangDu,MohsenGuizani;Hu Xia, "A Blockchain-SDN enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," Vol.7, Issue-5,pp 4278 – 4291,2020, DOI:10.1109/JIOT.2019.2956241

[7] Xingchen Liu, Haiping Huang, Fu Xiao, Ziyang Ma, "A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs," IEEE Internet of Things Journal, Vol 7,Issue-5,2020,DOI: 10.1109/JIOT.2019.2957421

[8] Jiawen Kang , Rong Yu, Xumin Huang, and Yan Zhang, " Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles," IEEE Transactions on Intelligent Transportation Systems, Vol.9, Issue-8, pp 2627 – 2637,2018, DOI:10.1109/TITS.2017.2764095

[9] Muhammad AwaisJaved,Nazmus Shaker Nafi,ShakilaBasheer,MariyamAyshaBivi,AliKashif Bashir "Fog-Assisted Cooperative Protocol for Traffic Message Transmission in Vehicular Networks," IEEE Access ,Vol.7, pp 166148 – 166156,2019, DOI:10.1109/ACCESS.2019.2953529

[10] Kuljeet Kaur, Sahil Garg, Georges Kaddoum, Francois Gagnon, Syed Hassan Ahmed, "Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, DOI:10.1109/ICCW.2019.8757184

[11] Sultan Basudan;AbdulrahmanAlamer;XiaodongLin;KarthikSankaranarayanan," Sultan Basudan;AbdulrahmanAlamer;XiaodongLin;KarthikSankaranarayanan," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018,DOI:10.1109/Cybermatics_2018.2018.00102

[12] Sarah Iqbal;AsadWaqarMalik;Anis Ur Rahman;RafidahMd Noor, "Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network," IEEE Access,Vol.8,pp 52968 – 52980,2020,DOI: 10.1109/ACCESS.2020.2979248

[13] YunseongLee;SeohyeonJeong;AroojMasood;LaihyukPark;Nhu-NgocDao;Sungrae Cho, "Trustful Resource Management for Service Allocation in Fog-nabled Intelligent Transportation Systems," IEEE Access,pp 147313 – 147322,2020,DOI: 10.1109/ACCESS.2020.3015550

[14] Liangjun Song, Gang Sun, Hongfang Yu, Xiaojiang Du, Mohsen Guizani, "FBIA: A Fog-based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles," IEEE Transactions on Vehicular Technology, Vol.69,issue-5,pp 5403 – 5415,2020, DOI:10.1109/TVT.2020.2977829

[15] Seyed Ahmad Soleymani;AbdulHananAbdullah;MahdiZareei;Mohammad Hossein Anisi;CesarVargas-Rosales;MuhammadKhurramKhan;ShidrokhGoudarzi, "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing," Vol.5,pp 15619 – 15629, DOI: 10.1109/ACCESS.2017.2733225