ISSN: 2096-3246
Volume 54, Issue 02, April, 2022

Optimization of Secured Data Transmission in Van-Cloud

Sarbjit Kaur[1], Ramesh Kait[2]
Department of Computer Science and Applications, Kurukshetra University,Kurukshetra[1]
Department of Computer Science and Applications, Kurukshetra University,Kurukshetra[2]

Keywords:
VANET, Trust Evaluation, Routing Protocol, Self-Configured Networks

ABSTRACT

Using ad-hoc networks in automobiles, timely data transfer may reduce road accidents. Due to limited transmission capacity, the vehicular ad-hoc network distributes data over many hops. The network's dynamic design generates frequent route disconnection due to mobile vehicles. Despite to these constraints, timely message delivery continues to be an issue. This study discusses the problem of timely message transmission in vehicular communication networks. This research presents a secure and efficient data routing strategy for heterogeneous ad hoc networks. First, node trust is calculated using an entity-centric paradigm. This also assists in determining the network's connection durability and collision likelihood. For timely distribution, an improvement in connection reliability and duration is necessary. Additionally, to decrease data collisions and improve network delivery ratio. Several network parameters were used to assess the enhanced model for data distribution. Experiments demonstrate a decrease in latency and packet loss ratio. In our protocol, the cloud evaluate each person's trustworthiness based on vehicle-uploaded attribute values. Using the cloud's reliability, network vehicles select trustworthy forward nodes and complete the route.

1. INTRODUCTION

The notion of Vehicular Clouds was introduced by Abuelela, M., and Olariu, S. [1]. Similar to a regular cloud, resources (computing power, storage, and internet connection) may be shared and rented out through the internet. The technology of vehicle ad hoc networks (VANETs) has become a popular research issue in recent years. The basic motive is that massive vehicle fleets will be on the road in the near future, with numerous automobiles idling in parking lots and resources going unused. These assets can be used to create money and rented out[2].

VANETs are a special kind of network based on the concept of connecting vehicles together to fulfil a certain function. The nature of this work is random. Each vehicle retains its connection to the network and controls its own communication needs. VANETs bring us a world of new application possibilities, making our journey not only safer but also more entertaining. Furthermore, one of the most essential applications of VANET is in situations when there is no infrastructure and it is critical to transmit information in order to save human lives. The job of vehicular ad-hoc networks is to let moving vehicles talk to each other in a certain situation. Vehicle-to-Vehicle (V2V) communication connects a vehicle directly to another vehicle. Vehicle-to-Infrastructure (V2I) communication connects a vehicle to infrastructure, such as a Road Side Unit (RSU)[1][2].

Because of the popularity of cloud computing and the evolution of its technology, people may use cloud services from anywhere and at any time [3]. Cloud computing, as defined by the National Institute of Standards and Technology (NIST), is a model that allows network access on-demand to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be quickly set up and taken away with little management work or service provider interaction [4]. A vehicular cloud is created by combining cloud-based services with car networks. Vehicle clouds may access services such as computing-as-a-service (CompaaS), storage-as-a-service (STaaS), network-as-a-service (NaaS), entertainment-as-a-service (ENaaS), information-as-a-service (INaaS), and traffic information-as-a-service (TIaaS) [5]. Cars that are permanently parked in the parking lot are referred to as "static infrastructure." A dynamic cloud solution, on the other hand, can consist of a pool of computing/storage/communication capabilities in automobiles that are networked via VANET infrastructure and further linked to the Internet by roadside devices [6] [7].

The security mechanisms work by encryption and decryption of the information, but do not consider the optimized use of the network resources. The Malicious Packets Detection System is a set of technologies and solutions that enforces security policy and bandwidth compliance on all devices seeking to access Cloud network computing resources, in order to limit damage from emerging security threats and to allow network access only to compliant and trusted endpoint devices. The communication bridge between the cloud and users, are repeatedly exhibiting many security flaws that will inevitably lead to massive cyber-attacks. In this research, we present a cloud-based secure data transmission mechanism that integrates several cloud-based security measures.

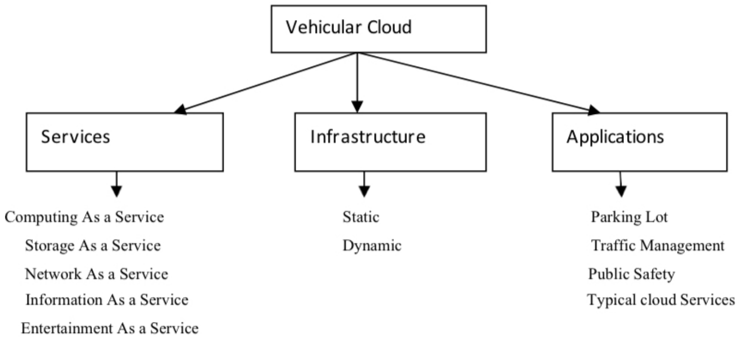


Figure 1: Vehicular Cloud Taxonomy

2. LITERATURE REVIEW

Yan, G et al. [8] proposed the concept of combining the VANET with the cloud. This paper presents Vehicular cloud computing and covers some of its unique traits as well as a number of key research issues. A number of potential application scenarios are given and analyzed in order to illustrate the numerous possibilities of the powerful VC idea. Eltoweissy M et al.[5] determined that the fundamental drive for their notion of vehicular clouds is the assumption that, in the near future, the massive fleets of automobiles on our roads, streets, and parking lots would be recognized as enormous and underused processing and communication resources. These assets may be utilized somewhere that would generate comparable profits. Although researchers introduced the concept of vehicular clouds for the first time, they did not discuss their potential structural structure.

Rasheed Hussain [9] envisioned the new VANET Cloud architecture by dividing the VANET Cloud into three architectural frameworks named Vehicular Cloud, Vehicles using Cloud and Hybrid Vehicular Cloud and also outlines security and privacy issues. Rajbhoj Supriya [10] addressed the various security and privacy issues related to Vehicular Cloud. Today cloud technology becomes very popular and provides various services that are cost effective, scalable and easy to manage. Some applications may comprises of sensitive data like credit card payment, transactions. As in VANET, high mobility, scalability and difficult of establishing trust relationship among nodes make the security and privacy issues more challenging task. Kamran Zaidi [11], examined aspects of security and privacy and provided solutions. As with vehicular internet, the vehicle is not only a mode of transportation, but it is also outfitted with a vast array of sensors and provides vital data. This article discusses many security mechanisms, including PKI (Public Key Infrastructure), Digital Signature, and trust-based schemes. The author developed a system that uses car and driver's license identifiers to create a new digital identity. Wenshuang Liang [12] provides a summary of the primary aspects of VANETs. First, the fundamental network architecture was explained, followed by an explanation of three research issues: routing, security and privacy, and applications. Although researchers have gained much progress but there are still many challenges in intelligent transportation system that attracts the researchers to continue their efforts in this area. Dutta et al. [13] defined VANET which is self-organizing and self-managing network in a distributed fashion. So the success of network is totally depending on the routing protocols. Communication with minimum delay and minimum overhead is critical issue and also a key challenge. So there is need to design the better paradigm with appropriate forwarding strategy and network model. Navneet Kaur [14], showed how VANET vehicles act as router to propagate the messages to other vehicles or road side units. There are some unique characteristics that differentiate the VANET from other ad-hoc networks like high mobility, continues disconnection and other obstacles like high buildings in urban area and reduced number of road side units on highway. Author discussed the various challenges, applications and provide the routing taxonomy that consists the protocols that are appropriate for highway and urban scenarios.

Mohammed Saad Boba [15], discussed the protocols that follows the greedy forwarding approach for data dissemination. There are number of protocols have been proposed by many researchers using greedy forwarding approach. It this paper author limited the protocols by selecting only those that are appropriately designed for urban scenario. At the end comparison of all these protocols is given. Mishra, R., Singh, A., & Kumar, R. [16], highlights the data accessibility issues in VANET. Accessibility becomes poor if the connection between the vehicles is lost. Accessibility can be increased using replication. Author proposed a algorithm to allocate the replica on vehicles according to the density of vehicles. If the area is dense then replication should be reduced and should be high in sparse. Saied Raeeszadeh [17] , uses Location/Identity Separation Protocol (LISP), which may distinguish between hosts and devices. As a new paradigm for IP addressing, LISP will make internet routing more scalable. Author proposed a algorithm on three bases of traffic, shortest route and road safety that use fuzzy logic at server site. Author [18] used SMRP (Spatial-Temporal Multicast Routing Protocol) for data dissemination in Vehicular cloud network. It build a dynamic mesh overlay to send the packet to the desired node using filtering method. Filtering method is used according to the types of message. Author proposed an architecture with three inbuilt cloud models-V2V, roadside Cloud and cloud internet. Zhipeng Tang [19], explored the security cooperation which is anticipated to be a fundamental research area in VCC. Due to hostile nodes, security cooperation in VCC has become a difficult challenge. Author presented DBTEC (double board rust estimation and correction) approach that combines indirect trust estimation in Public board and direct trust estimation in private board to calculate trust value of automobiles while selecting cooperative partners.

3. TOKEN BASED SECURED DATA DISSEMINATION MODEL IN VAN-CLOUD

To investigate the topic of secure data disseminations, we have chosen for experimental methods in this work. To begin, vehicle registration must be done on the cloud. The cloud server then issued a JWT (JSON Web Token) token to access the system. In the future, vehicles will always need to utilize this token when communicating with the cloud to transfer data or make use of cloud services. The vehicle won't be able to make the use of cloud services until the cloud confirms the token is legitimate. In addition, we have implemented Trust Factor, which provides evidence of a third-party system's reliability.

With the framework shown in figure 2, we have created a multi-tiered architecture for our experimental study. This layered architecture controls the channel for the transmission of secured information. It also enables information sharing without requiring any special infrastructure, like a base station, and allows for performance in very dynamic environments.

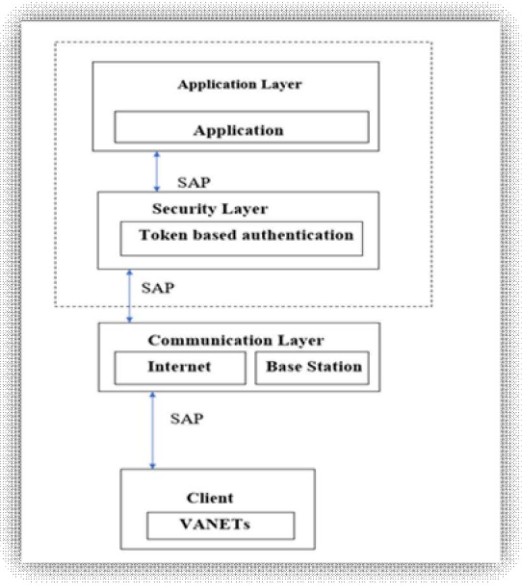


Figure 2: Layered Architecture of VANET

- *Client Layer:* The end users make up the client layer, which is the architectural component of the VANET-Cloud that is at the most basic level. A VANET node that has a need for a VANET-Cloud service is referred to as an end user. Their Vehicle ID, access token and other registration parameters may distinguish end users from other individuals.
- *Communication Layer:* This layer's aim is to establish a connection between the client in the lower tier and the VANET Cloud server (data centre) in the higher layer via SAP (Service Access Point).
- *Application and Security Layers:* The two highest levels in a cloud infrastructure are the application layer and the security layer. It is the responsibility of the application layer to provide cloud services to the end user. SAP offers these features to its end user directly. There is also a security layer in the cloud, which is responsible for generating access tokens and verifying their authenticity upon each user's communication.

Figure 3 and algorithm 1 both give an explanation of the sequence chart and algorithm that are used in the process of authenticating the user and producing a token. Therefore, these two pieces of information provide an explanation of how the system actually works. A JSON Web Token is a method for securely exchanging information between parties that is both self-contained and concise. This method is documented by an open industry standard (RFC 7519). The authenticity of the data is validated by the digital signature. The following architecture, which makes use of JWT tokens, is what we've come up with to ensure the safety of the data.

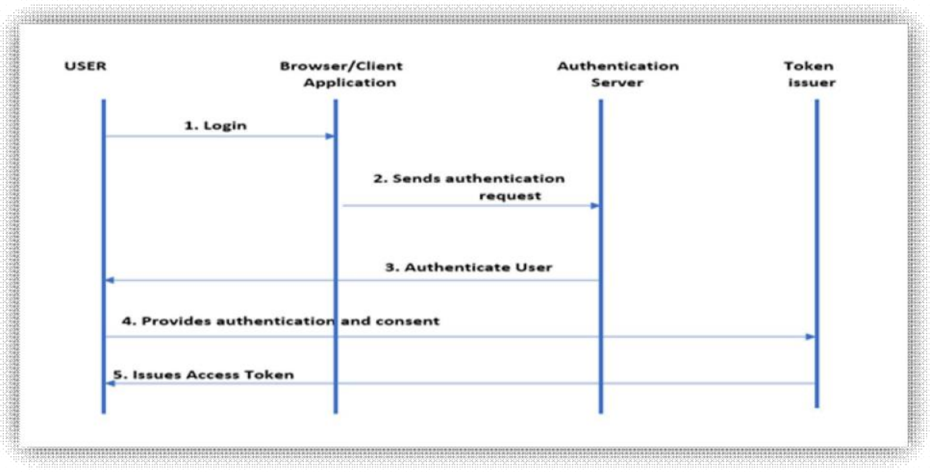

USER
Browser/Client Application
Authentication Server
Token issuer
1. Login
2. Sends authentication request
3. Authenticate User
4. Provides authentication and consent
5. Issues Access Token

Figure 3: Authentication and Token Generation Process

```
Algorithm 1: Authentication Process

  $V_i=\{V_1, V_2, V_3 \ldots\ldots V_n\}$ is the set of Vehicles. $C_{server}$ is cloud server. This Authentication algorithm
  describes how the vehicle registered itself on cloud server.
Step1:  if $V_i$=new Vehicle then
        a)  Vehicle $V_i$ open the URL of $C_{server}$
        b)  Click on create user
        c)  After entering detail as shown in figure 4 , Username with first 4 characters of name, last 4 digits of
            mobile number and last 4 digits of vehicle number will be generated.
        else
        Enter the login credentials
Step 2: After successfully registration
        If user= new user
        then JSON web Token generated (steps given in sequence diagram figure 3)
        else
        user can view the Access token, Trust factor, Message Passing and Dashboard detail (shown in figure 7)
```

4. RESULTS AND FINDINGS

This work has different features and have been programmed in front-end and back-end to extend the features of the data transmission. This is a real-time application that was built using cloud computing. The whole repository of code is now hosted in Linode's private cloud. The front-end development is done using Bootstrap. And the back end is written in Python using Django and Flask. These modules are used to create programs that run on the server. Flask's restful API is utilized for front-end and back-end communication. Python is a high-level programming language that may be put to many uses since it is interpreted, interactive, and object-oriented.

In this research, a VANET Cloud application has been developed where communication take place between Vehicle to cloud via RSU and directly also. In this structure, VANETs first register with the cloud, and then data exchange between the cloud and the VANET starts with the security token JSON Web Token (JWT). The registration of the VANET on the cloud will be as follows:

- Open the application
- Click on login if already have account otherwise register as new user (shown in fig 4).

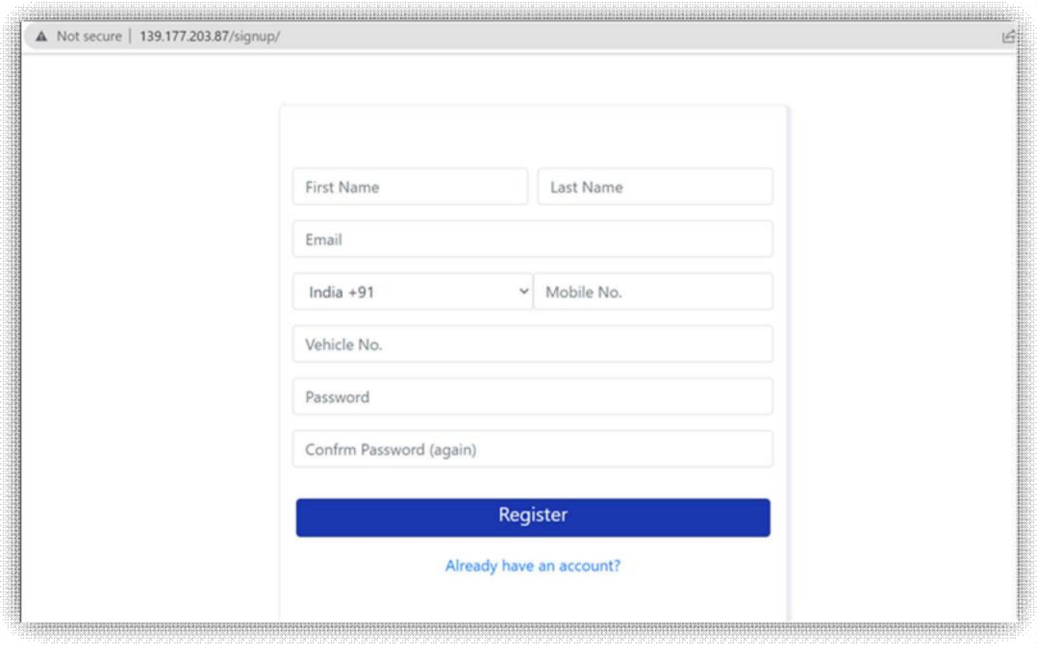
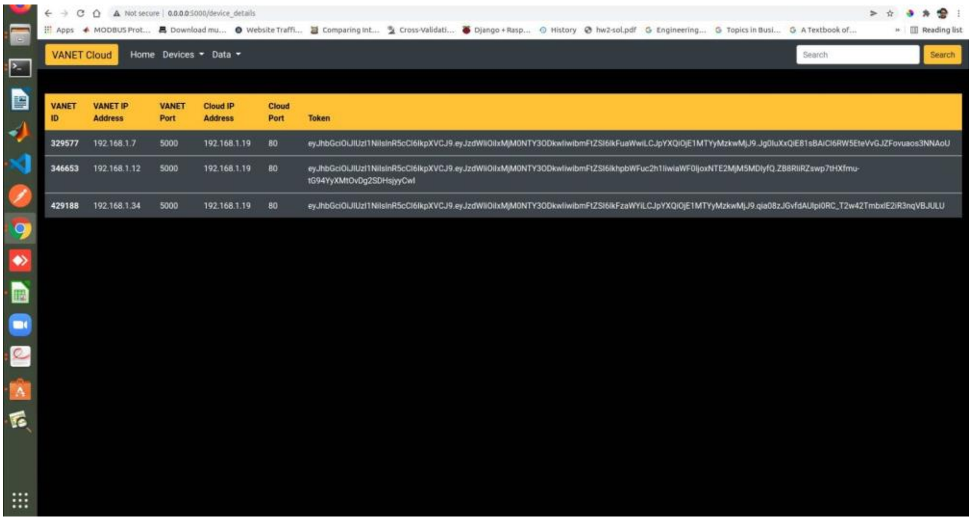


Figure 4: Application Frontend

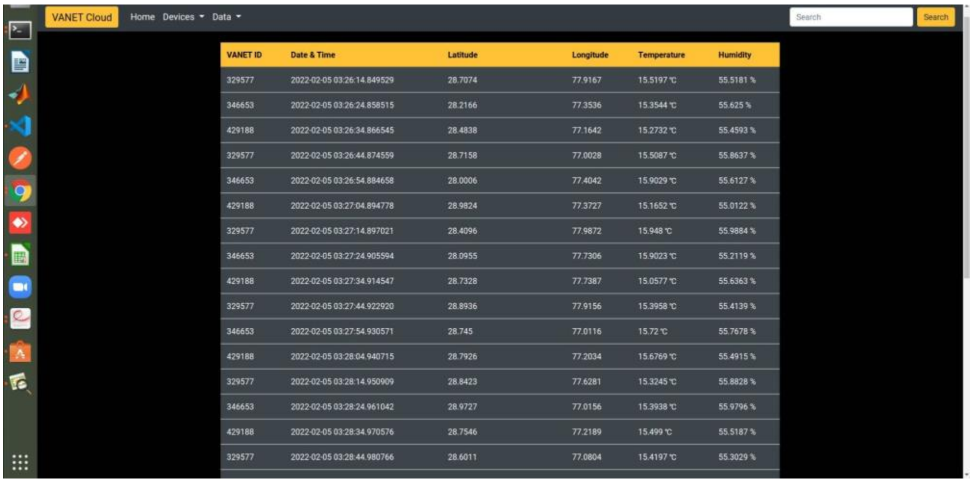
After registration, a token will be generated for the VANET, so that VANET can securely communicate with the cloud. No VANET can send packets to the cloud without a valid token. The use of encrypted tokens greatly improves the security of the communication.



VANET ID	VANET IP Address	VANET Port	Cloud IP Address	Cloud Port	Token
329577	192.168.1.7	5000	192.168.1.19	80	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkFuaWwiLCJpYXQiOjE1MTYyMzkwMjJ9.Jg0luXxQiE81sBAiCl6RW5EteVvGJZFovuaos3NNAoU
346653	192.168.1.12	5000	192.168.1.19	80	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkhpbWFuc2h1IiwiaWF0IjoxNTE2MjM5MDIyfQ.ZB8RIIRZswp7tHXfmu-tG94YyXMtOvDg2SDHsjyyCwI
429188	192.168.1.34	5000	192.168.1.19	80	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkFzaWYiLCJpYXQiOjE1MTYyMzkwMjJ9.qia08zJGvfdAUlpi0RC_T2w42TmbxlE2iR3nqVBJULU

Figure 5: Client Authentication through JWT

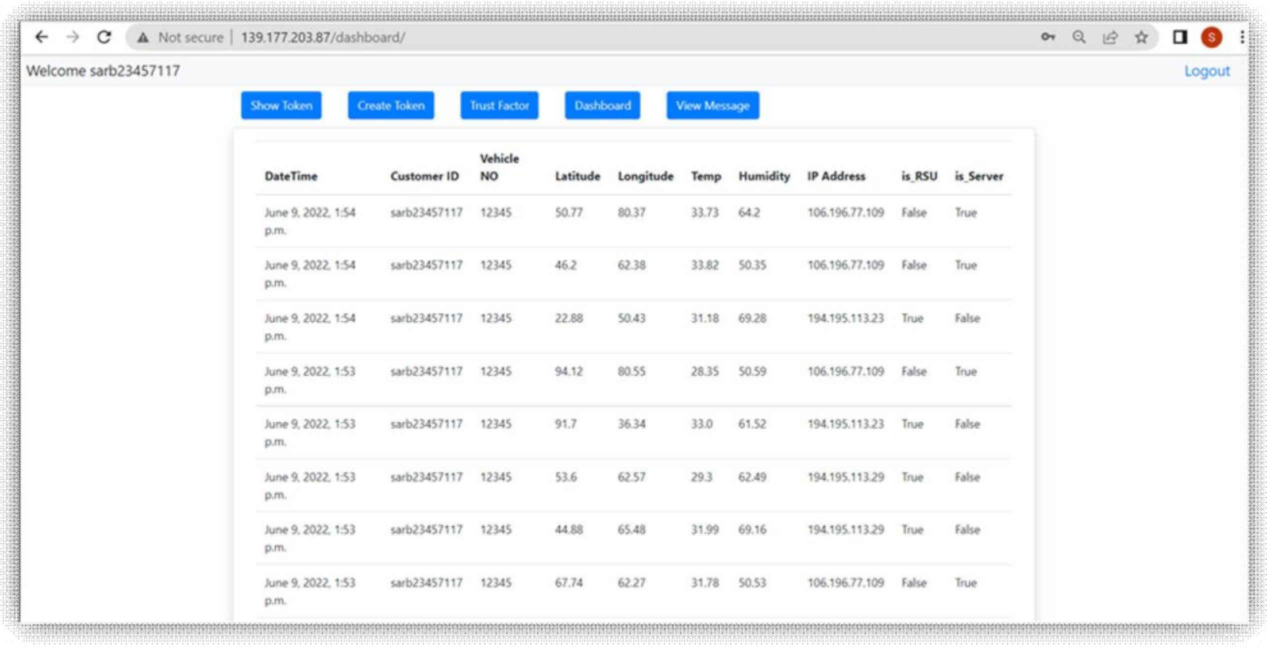
The tokens shown in the above figure 5 are JSON Web Token, which is used to authenticate the clients. With the help of tokens, a VANET can easily send data directly to the cloud. In this proposed model three VANETs running at different IP addresses and sending data to the cloud has been used. The communicated data (presumed random data) with the cloud is shown in the figure 6.



VANET ID	Date & Time	Latitude	Longitude	Temperature	Humidity
329577	2022-02-05 03:26:14.849529	28.7074	77.9167	15.5197 ℃	55.5181 %
346653	2022-02-05 03:26:24.858515	28.2166	77.3536	15.3544 ℃	55.625 %
429188	2022-02-05 03:26:34.866545	28.4838	77.1642	15.2732 ℃	55.4593 %
329577	2022-02-05 03:26:44.874559	28.7158	77.0028	15.5087 ℃	55.8637 %
346653	2022-02-05 03:26:54.884658	28.0006	77.4042	15.9029 ℃	55.6127 %
429188	2022-02-05 03:27:04.894778	28.9824	77.3727	15.1652 ℃	55.0122 %
329577	2022-02-05 03:27:14.897021	28.4096	77.9872	15.948 ℃	55.9884 %
346653	2022-02-05 03:27:24.905594	28.0955	77.7306	15.9023 ℃	55.2119 %
429188	2022-02-05 03:27:34.914547	28.7328	77.7387	15.0577 ℃	55.6363 %
329577	2022-02-05 03:27:44.922920	28.8936	77.9156	15.3958 ℃	55.4139 %
346653	2022-02-05 03:27:54.930571	28.745	77.0116	15.72 ℃	55.7678 %
429188	2022-02-05 03:28:04.940715	28.7926	77.2034	15.6769 ℃	55.4915 %
329577	2022-02-05 03:28:14.950909	28.8423	77.6281	15.3245 ℃	55.8828 %
346653	2022-02-05 03:28:24.961042	28.9727	77.0156	15.3938 ℃	55.9796 %
429188	2022-02-05 03:28:34.970576	28.7546	77.2189	15.499 ℃	55.5187 %
329577	2022-02-05 03:28:44.980766	28.6011	77.0804	15.4197 ℃	55.3029 %

Figure 6: Different Running IP Address

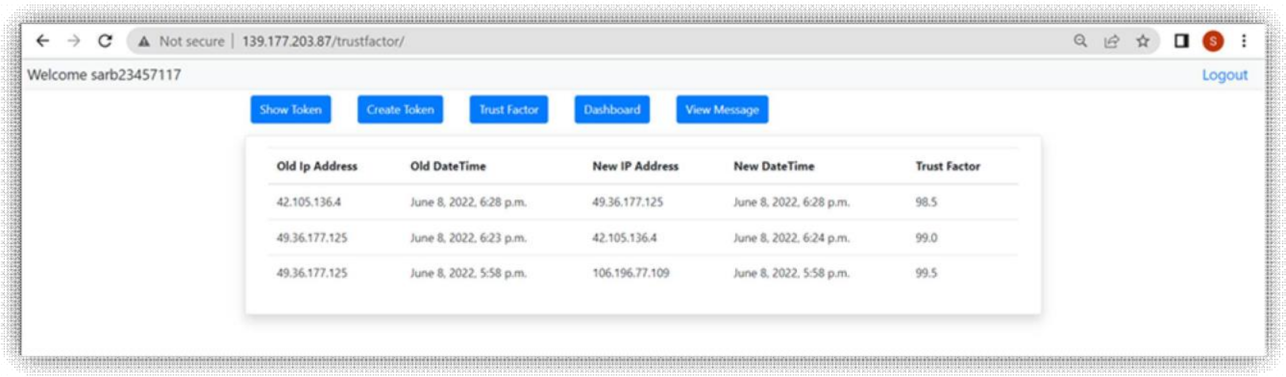
With the experiments, we have observed the frontend system shows the login information from token creation to successful login. The IP addresses in the figure given above shows which vehicle logged in through which IP address. After successfully login, vehicle get the following information:



DateTime	Customer ID	Vehicle NO	Latitude	Longitude	Temp	Humidity	IP Address	is_RSU	is_Server
June 9, 2022, 1:54 p.m.	sarb23457117	12345	50.77	80.37	33.73	64.2	106.196.77.109	False	True
June 9, 2022, 1:54 p.m.	sarb23457117	12345	46.2	62.38	33.82	50.35	106.196.77.109	False	True
June 9, 2022, 1:54 p.m.	sarb23457117	12345	22.88	50.43	31.18	69.28	194.195.113.23	True	False
June 9, 2022, 1:53 p.m.	sarb23457117	12345	94.12	80.55	28.35	50.59	106.196.77.109	False	True
June 9, 2022, 1:53 p.m.	sarb23457117	12345	91.7	36.34	33.0	61.52	194.195.113.23	True	False
June 9, 2022, 1:53 p.m.	sarb23457117	12345	53.6	62.57	29.3	62.49	194.195.113.29	True	False
June 9, 2022, 1:53 p.m.	sarb23457117	12345	44.88	65.48	31.99	69.16	194.195.113.29	True	False
June 9, 2022, 1:53 p.m.	sarb23457117	12345	67.74	62.27	31.78	50.53	106.196.77.109	False	True

Figure 7: Detail Shown to Vehicle

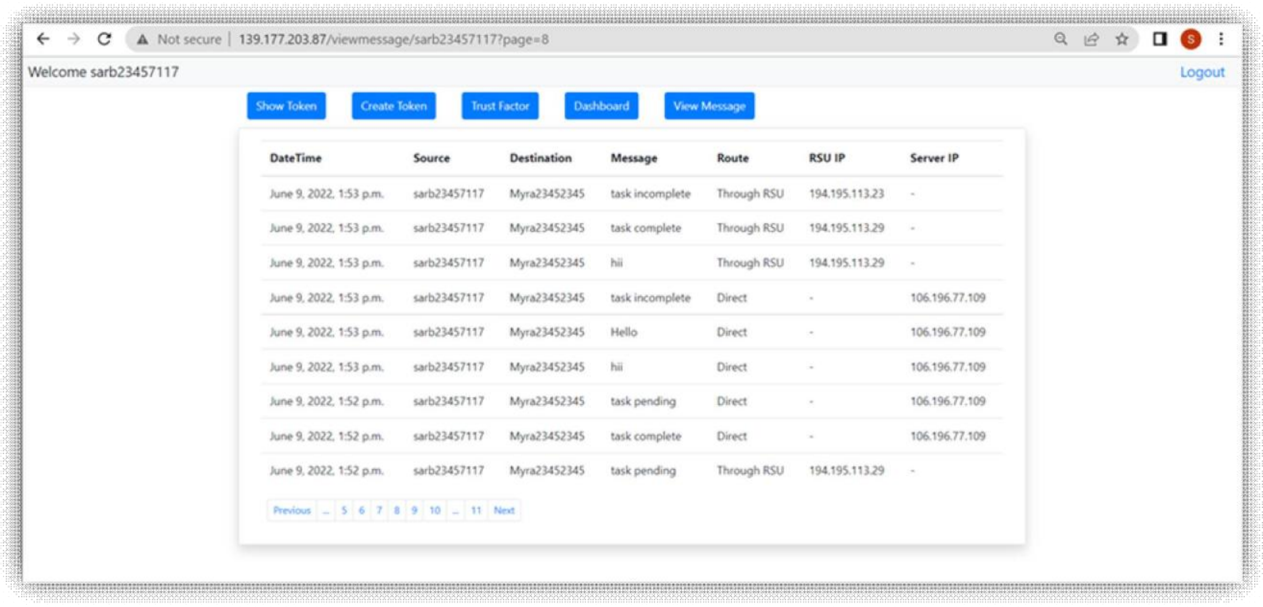
From this output, it has been observed that detail of vehicle has been displayed along with IP address and the availability of RSU and cloud server. If the vehicle has an active data connection, the server value will be shown as true; otherwise, the RSU value will be displayed as 'True'. By selecting the "Show Token" option, a vehicle may see its token, while selecting "Create Token" allows it to generate a new token in the event that the user discovers an inconsistency with the current token. It has been discovered, based on the number of servers that the change in internet availability reflects the change of IP address after disconnecting, which means that it presents a separate IP address for every different internet connectivity for same user. The trust value is reduced by 0.5 for each new connection, and if an IP address changes too often, the server will prevent that specific vehicle from sending messages when a certain threshold has been reached since it will consider it to be a malicious vehicle. The trust factor can be viewed by selecting the 'Trust Factor' option and the detail will be displayed as shown in figure 8.



Old Ip Address	Old DateTime	New IP Address	New DateTime	Trust Factor
42.105.136.4	June 8, 2022, 6:28 p.m.	49.36.177.125	June 8, 2022, 6:28 p.m.	98.5
49.36.177.125	June 8, 2022, 6:23 p.m.	42.105.136.4	June 8, 2022, 6:24 p.m.	99.0
49.36.177.125	June 8, 2022, 5:58 p.m.	106.196.77.109	June 8, 2022, 5:58 p.m.	99.5

Figure 8: Trust information of Vehicle

Trust factor of the IP address found 99.5 that is most trustful network for the VANET. When the user transfers the data to the other vehicle through RSU or cloud server directly then it reflects successful secured data transfer by clicking on 'view message' button as shown in figure 9.



DateTime	Source	Destination	Message	Route	RSU IP	Server IP
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	task incomplete	Through RSU	194.195.113.23	-
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	task complete	Through RSU	194.195.113.29	-
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	hii	Through RSU	194.195.113.29	-
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	task incomplete	Direct	-	106.196.77.109
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	Hello	Direct	-	106.196.77.109
June 9, 2022, 1:53 p.m.	sarb23457117	Myra23452345	hii	Direct	-	106.196.77.109
June 9, 2022, 1:52 p.m.	sarb23457117	Myra23452345	task pending	Direct	-	106.196.77.109
June 9, 2022, 1:52 p.m.	sarb23457117	Myra23452345	task complete	Direct	-	106.196.77.109
June 9, 2022, 1:52 p.m.	sarb23457117	Myra23452345	task pending	Through RSU	194.195.113.29	-

Figure 9: Communication Detail of Vehicle

5. CONCLUSION

Cloud computing delivers on-demand, scalable, and regularly updated advanced computing resources, without the need to purchase and operate infrastructure on-site. With the cloud computing approaches, and patterns described in this research, data transfer from VANET to cloud is made more efficient and secure, and calculation time is shortened without the enormous work required to manage a conventional on-premise infrastructure. Third parties might have greater faith in the data that was sent through RSU. If compared to the previous system, our method increases the security of the VANET cloud. We accounted for both cases in which an in-vehicle connection to the internet was available and when none was available. We now live in the age of 4G and 5G technologies, which make high-speed internet more accessible than ever. That is why vehicles can talk to each other without going via relay nodes. Hence, by making use of technologies, we may drastically reduce the time it takes to send messages and greatly improve the efficiency with which we move data.

REFERENCES

[1] M. Abuelela and S. Olariu, "Taking VANET to the Clouds," in *In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10)*, 2010, pp. 8–10, doi: 10.1145/1971519.1971522.

[2] F. Ahmad, M. Kazim, and A. Adnane, "Vehicular Cloud Networks : Architecture and Security," in *IEEE/ACM 8th International Conference on Utility and Cloud Computing Vehicular*, 2015, no. January, pp. 571–576, doi: 10.1109/UCC.2015.101.

[3] W. A. Pauley, "Cloud Provider Transparency: An Empirical Evaluation," *IEEE Secur. Priv.*, vol. 8, no. 6, pp. 32–39, 2010.

[4] A. Raza, S. Hashim, R. Bukhari, and F. Aadil, "An UAV-assisted VANET architecture for intelligent transportation system in smart cities," *Int. J. Distrib. Sens. Networks*, vol. 17, no. 7, pp. 1–17, 2021, doi: 10.1177/15501477211031750.

[5] M. Eltoweissy, S. Olariu, and M. Younis, "Towards Autonomous Vehicular Clouds A Position Paper (Invited Paper)," pp. 1–16, 2010.

[6] K. Braekers, K. Ramaekers, and I. Van Nieuwenhuyse, "The vehicle routing problem: State of the art classification and review," *Comput. Ind. Eng.*, vol. 99, no. September 2018, pp. 300–313, 2016, doi: 10.1016/j.cie.2015.12.007.

[7] K. Salimifard and R. Raeesi, "A green routing problem: Optimising CO2 emissions and costs from a bi-fuel vehicle fleet," *Int. J. Adv. Oper. Manag.*, vol. 6, no. 1, pp. 27–57, 2015, doi: 10.1504/IJAOM.2014.059623.

[8] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing," *IEEE Trans Intell Transp Syst*, vol. 14, no. 1, pp. 284–294, 2013.

[9] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking Vehicular Communications : Merging VANET with Cloud Computing," in *IEEE 4th International Conference on Cloud Computing Technology and Science Rethinking*, 2012, pp. 606–609.

[10] M. R. K, "Security Challenges Addressed in Vehicular cloud computing," vol. 4, no. 6, pp. 1961–

1964, 2015.

[11] K. Zaidi and M. Rajarajan, “Vehicular internet: Security & privacy challenges and opportunities,” *Futur. Internet*, vol. 7, no. 3, pp. 257–275, 2015, doi: 10.3390/fi7030257.

[12] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, “Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends,” *Int. J. Distrib. Sens. Networks*, vol. 2015, pp. 1–11, 2015, doi: 10.1155/2015/745303.

[13] R. Dutta and R. Thalore, “A Review of Various Routing Protocols in VANET,” *Int. J. Adv. Eng. Res. Sci.*, vol. 4, no. 4, pp. 221–224, 2017, doi: 10.22161/ijaers.4.4.34.

[14] N. Kaur, “A Survey on Data Dissemination Protocols used in VANETs,” vol. 120, no. 23, pp. 43–50, 2015.

[15] M. S. Boba, S. M. Nor, and S. A. Nagar, “A SURVEY OF UNICAST ROUTING PROTOCOLS BASED- GREEDY FORWARDING STRATEGIES FOR VEHICULAR AD – HOC NETWORKS IN URBAN SCENARIO,” *J. Theor. Appl. Inf. Technol.*, vol. 62, no. 1, pp. 174–183, 2014.

[16] R. Mishra, “VANET Security : Issues , Challenges and Solutions,” in *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1050–1055, doi: 10.1109/ICEEOT.2016.7754846.

[17] S. Raeeszadeh and R. Sabbaghi-nadooshan, “A Novel Method for VANET Improvement using Cloud Computing,” vol. 2, no. 1, pp. 39–44, 2013.

[18] E. Mousavinejad, F. Yang, Q. L. Han, X. Ge, and L. Vlacic, “Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, 2020, doi: 10.1109/TITS.2019.2934481.

[19] Z. Tang, A. Liu, Z. Li, Y. J. Choi, H. Sekiya, and J. Li, “A Trust-Based Model for Security Cooperating in Vehicular Cloud Computing,” *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/9083608.