IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, June 2022

Secure Vehicular Ad Hoc Network Communication using BlockChain

R. Arunachalam[1], Rajeswari. A[2], Serafin. J[3], Subathra. R[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India
r.arunachala@gmail.com and rajenthiransubathrasr@gmail.com

Abstract: *The vehicular social networks supports diverse kinds of services such as traffic management, road safety, and sharing data. Among these, secure data transmission has turned to be a spotlight. Ciphertext- policy attribute- based encryption may be adopted for data sharing. In traditional schemes, access policy is stored and granted by the cloud, which lacks credibility. To end this, we present a Blockchain Based Multi-Domain Vehicular Authentication scheme, in a which privacy-preserving authentication method is proposed to guarantee the Security.*

Keywords: Vehicular Ad Hoc Network(VANET); Communication BlockChain; SHA-256 algorithm; Authentication; Road Condition Report

I. INTRODUCTION

The Vehicular Ad Hoc Network (VANET) is a self-organized ad hoc network in which vehicles and roadside units (RSUs) are often connected via wireless communications .Each participating vehicle is equipped with an On-Board Unit (OBU) (a wireless communication device) that allows it to connect with other cars and Road Side Units(RSU)s nearby. RSUs can also link to the backbone network for data sharing, such as over the Internet communication device), which allows vehicles to communicate with the neighboring vehicles and RSUs. The RSUs can also link to the backbone network for data sharing, such as over the Internet. The following components make up a typical VANET network model (see Figure 1): Traffic Control Center (TCC)[1], RoadSide-Unit (RSU)[2], Vehicle[3], Internet[4]. Wired/wireless communication[1], vehicle-to-vehicle communication[2], and vehicle-to-RSU communication[3] are the three basic modalities of communication. The vehicles and/or RSUs are connected to the Internet via wired/wireless communication, with the other two wireless communications managed by the Dedicated Short Range Communication (DSRC) protocol. This protocol is used to make short-range communication easier.

Vehicles can interact with one another or with RSUs to share current road traffic conditions (e.g. weather and congestion situation)[1] or driving status (e.g. location and speed) primarily using OBUs and DSRC. This can effectively avoid traffic accidents by implementing a prompt response (for example, rerouting to avoid traffic congestion). These traffic messages can be obtained from the RSUs via the Internet by TCC.

Supporting smart processing and real-time response in modern intelligent transportation systems is one of the benefits of VANETs. However, there are possible safety risks that should not be overlooked, particularly when using wireless communication, which is more sensitive than cable connection.

While message authentication can help to minimize some of these assaults, we must also examine how to secure the privacy of automobiles (and their owners/drivers). When a vehicle shares its traffic status with another RSU or car, for example, its identity is revealed. An attacker could use this information to track down the vehicle's location. Furthermore, automobiles broadcast messages concerning road traffic conditions and driving status on a regular basis. The traceability of the cars is made easier by the frequency of the broadcasted message. Clearly, there are worries about privacy and security.

Monitoring Communication Authentication (MCA) [4], [5] is one of the proposed techniques to support secure communications on VANETs. The vehicle's privacy should be conditionally safeguarded via an MCA protocol in the context of VANET. For most entities, this means that the vehicle stays anonymous, yet a trusted entity can extract the vehicle's true identify. This allows one to track down a misbehaving car (for example, one that has sent a fictitious traffic

DOI: 10.48175/IJARSCT-4579

status) and impose the appropriate punishment.

PKI-based [4]–[6] and ID-based [7]–[10] are the two primary categories of existing MCA protocols for VANETs. The latter group avoids the problems that PKI-based protocols have with key/certificate preloading and revocation, and some systems, such as [1], [11], [12], even offer batch verification to boost performance. These ID-based methods, on the other hand, introduce new issues, such as the inability to revoke the vehicle's private key. This problem, as well as others like frequent interactions and the need for concept hardware, are still present in the BlockChain-based MCA protocols that have recently been proposed (e.g. [13], [14]). As a result, we are driven to present a PKI-based BCPPA protocol that addresses for the mentioned concerns.

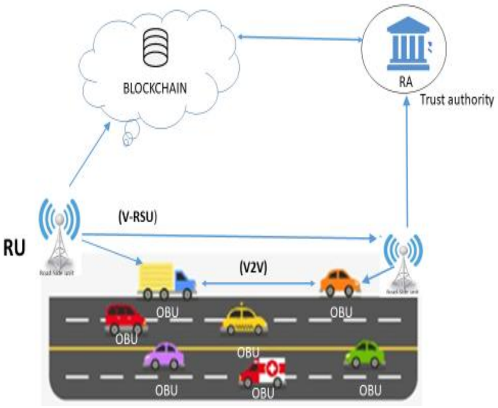


Figure 1: System Architecture

A. Vehicle to Vehicle communication (V2V):

Information is transmitted between various vehicles through V2V communication so that they are aware of warnings and critical information such as traffic alerts, avoiding crashes, and so on. Because VANET is a dynamic topology, the infrastructure is unstable, and it can only transmit information if there are vehicles in the vicinity [3].

B. Vehicle to Road Infrastructure Communication (V2I) :

This type of communication takes place between the vehicles that make up the network and the infrastructure that exists on the roadside. The sensors provide real-time traffic and weather updates, which are mostly carried out through this communication [1].

C. Vehicle to Broadband cloud (V2B) communication:

V2B communication takes place over broadband connections, which are established by e-SIM in the vehicles [1]. Based on the information saved in the cloud, this communication assists the driver with guidance and traffic updates.

II. LITERATURE REVIEW

Fengzhong Qu, Zhihui Wu, Fei-Yue Wang- Vehicular ad hoc networks (VANETs) have stimulated interest in both academic and industry settings because, once deployed, they would bring a new driving experience to drivers. However, communicating in an open-access environment makes security and privacy issues a real challenge, which may affect the large-scale deployment of VANETs. Researchers have proposed many solutions to these issues. We start this paper by providing background information of VANETs and classifying security threats that challenge VANETs. After clarifying the requirements that the proposed solutions to security and privacy problems in VANETs should meet, on the one hand, we present the general secure process and point out authentication methods involved in these processes. Detailed survey of these authentication algorithms followed by discussions comes afterward. On the other hand, privacy preserving methods are reviewed, and the trade-off between security and privacy is discussed. Finally, we provide an outlook on how to detect and revoke malicious nodes more efficiently and challenges that have yet been solved.

Thomas M. Kurihara, Justin McNew, John Moring, William Whyte- This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions. This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions. The safety-critical nature of many Wireless Access in Vehicular Environments (WAVE) applications makes it vital that services be specified that can be used to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay. Additionally, the fact that the wireless technology will be deployed in communication devices in personal vehicles as well as others portable devices, whose owners have an expectation of privacy.

Yining Liu, Wei Guo, Chun-I Fan, Liang Chang, and Chi Cheng- The real-time electricity consumption data can be used in value-added service such as big data analysis, meanwhile the single user’s privacy needs to be protected. How to balance the data utility and the privacy preservation is a vital issue, where the privacy-preserving data aggregation could be a feasible solution. Most of the existing data aggregation schemes rely on a trusted third party (TTP). However, this assumption will have negative impact on reliability, because the system can be easily knocked down by the Denial of Service (DoS) attack. In this paper, a practical privacy-preserving data aggregation scheme is proposed without TTP, in which the users with some extent trust construct a virtual aggregation area to mask the single user’s data, and meanwhile, the aggregation result almost has no effect for the data utility in large scale applications. The computation cost and communication overhead are reduced in order to promote the practicability. Moreover, the security analysis and the performance evaluation show that the proposed scheme is robust and efficient.

III. METHODOLOGY

1. Registration module and Contacts details
2. VANET
3. Accident intimation
4. Weather forecast
5. MongoDB
6. Trace module

Registration and contact module

The details of all the other users can be viewed by the user.

It is processed by the user module, which obtains all the user's information.

A local host is connected to the web system.

The user fills out personal information in order to register with the web system.

VANET

Vehicle-to-vehicle and vehicle-to-infrastructure communication are both possible in vehicular ad-hoc networks (VANETs).

A innovative smartphone-integrated driving safety application is modelled here, as well as a traffic signal priority control system, in order to clear the way for the emergency vehicles.

Road Traffic Management Using Data Retrieval in a VANET Environment), a server, and roadside units (RSUs and SA)

Accident intimation

An accident management system that uses VANET in conjunction with public transportation systems that uses the cellular technology.

The system ensures real-time communication between vehicles, ambulances, hospitals, roadside units, local governments, and cloud servers.

Weather forecast

Weather forecasting system that uses VANET in conjunction with public transportation systems that use the cellular technology in public transport.

DOI: 10.48175/IJARSCT-4579

This ensures the possibility of real time communication among vehicles, ambulances, hospitals, road side unit, sub authorities and cloud server.

The weather conditions are communicated to the cars.

MongoDB

MongoDB is a document database that combines scalability and flexibility with the querying and indexing capabilities that you want.

It is used to display the speed of cars as well as a performance chart.

Trace module

It's utilised to keep track of a vehicle's exact location.

Vehicler Registration

In the registration phase, every vehicle Vj gets the authorization (e.g., a secret key) from its administrative subauthority SAi. .i picks a random value ri;j 2R Z_p , calculates the secret key vskj = (vskj;1; vskj;2; vskj;3) where vskj;1 = sski;1; vskj;2 = gri;j vskj;3 = sski;2 _ hri;jH2(SAikVjkvskj;1kvskj;2) and gives vskj to Vj securely. Vehicle Vj is able to verify vskj as follows ^e(vskj;3; g) ?=^e_h; vskj;1-yH1(SAikvskj;1) _vskH2(SAikVjkvskj;1kvskj;2) j;2

IV. AUTHENTICATION ALGORITHM

The SHA-256 algorithm is a variant of SHA-2 (Secure Hash Algorithm 2), a successor to SHA-1 developed by the National Security Agency in 2001. The SHA-256 hash function is a patented cryptographic hash function that generates a 256-bit result. The underlying principles of extra security modules have been the various breakthroughs witnessed in network security, encryption, and hashing. One of the most extensively used hash algorithms is the secure hash algorithm with a digest size of 256 bits, also known as the SHA 256 algorithm.

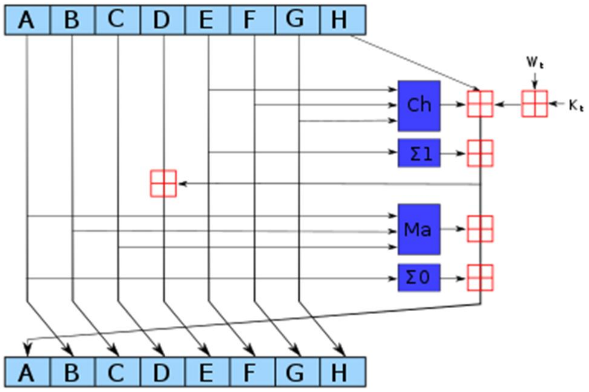


Figure:2 Hash Function

Step 1 - Pre-Processing. ...
Step 2 - Initialize Hash Values (h) ...
Step 3 - Initialize Round Constants (k) ...
Step 4 - Chunk Loop. ...
Step 5 - Create Message Schedule (w) ...
Step 6 - Compression.

V. EXISTING SYSTEM

Bloom filters were used to construct a novel privacy-preserving signature technique for inter-vehicle communication in an existing system. In an automatic dependent surveillance-broadcast system, data authentication and integrity protection has been developed. Routing based on topology or ad hoc VANETs are, in general, infrastructure-free networks, and many routing protocols developed for previous ad-hoc networks, such as MANET, based on various network topologies, can be used to VANETs with few adjustments. Proactive, reactive, and hybrid topology-driven protocols are divided into three types. A number of such protocols have been created to meet the requirements of the VANET environment. In a proactive protocol, nodes update their routing tables on a regular basis with information about new routes in the network. By sending periodic HELLO packets, this informant information is distributed to all nodes. However, this method entails a significant amount of control overhead. This limits the utilisation of scarce wireless resources like available bandwidth. Available bandwidth is an example of a resource. Reactive approaches, such as AODV, DSR, and BRP nodes, on the other hand, will only deliver control data when it is required. This cuts down on the costs of setting up the link and speeds up the distribution of the real data. However, this solution still imposes excessive resource overheads, such as route maintenance for used/unused routes. Due to VANET's strict network design, these useless paths are generated and broken. Overheads in reactive protocols are related with determining the best path to convey data. The path-finding procedure is started by sending a message known as a Route Request Message (RREQ).

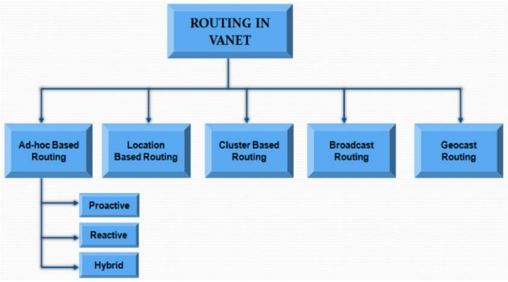


Fig 3 Routing Types in VANET

Routing based on location. Location or Position Based Routing protocols are another type of protocol that has piqued the interest of researchers. To help disperse the information, this system of protocols obtains information about the geographic location of vehicles from many sources such as maps, the Global Positioning System (GPRS), or even remnants of traffic models. Several studies have examined the performance of well-known topology-based protocols like AODV and DSR in conjunction with the Position Based algorithm, and the findings have demonstrated that the Position Based algorithm outperforms the basic topological approach. Position-based protocols, unlike topology-based protocols, do not require route maintenance and can be constructed whenever the need arises. This relieves undue demand on bandwidth, which is already scarce in the VANET environment. Greedy Perimeter Stateless Routing (GPSR) is an example of a location-based protocol that does a search for the closest neighbour. Each node is aware of its own location as well as that of its immediate neighbours. GPSR is well suited for dynamic topological networks because it has this special information for the primary node. In the event where there is no nearby Neighbour, GPSR uses perimeter mode with face routing to maximise the search for the desired destination. In a highway context, a performance comparison of GPSR and DSR has been presented. When GPSR is used, it has been demonstrated that route delay is reduced.

Drawbacks

External sources for destination location
Delay
Increasing the network congestion
Flooding in route discovery initial phase

VI. PROPOSED SYSTEM

In this project, privacy preserving authentication implemented based on SHA-256 algorithm. Different types of feature implemented based on different kind of features as root authority (RA), many sub-authorities (SAs), many roadside units (RSUs), a cloud server, and many vehicles. SHA-256 algorithm trained based on these features. And MCA protocol is used to monitoring the road vehicles.

DOI: 10.48175/IJARSCT-4579

Advantages:

- Public safety
- Traffic management
- Traffic coordination and assistance
- Traveller information support
- Comfort

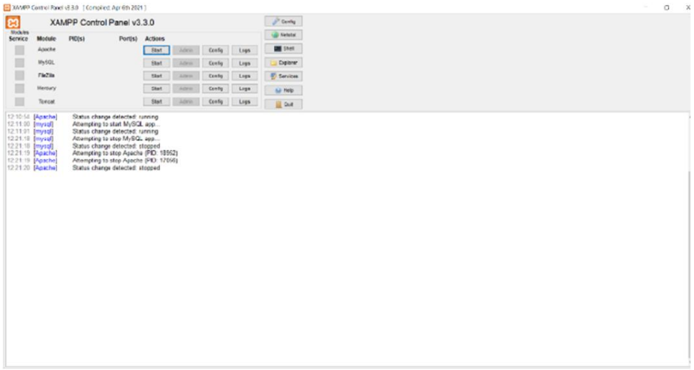
VII. SOFTWARE APPLICATION

XAMPP is an excellent local development environment, but it is not intended for production use. We want to make it as simple as possible to host PHP applications written with XAMPP.

NetBeans IDE is a free and open source integrated development environment (IDE) for developing applications for Windows, Mac OS X, Linux, and Solaris. The IDE streamlines the development of Java and HTML5-based web, corporate, desktop, and mobile applications.

CONNECT XAMPP AND NETBEANS-You'll need to download MySQL Connector/J to connect to the Xampp server using the Java programming language and the Netbeans IDE (integrated development environment). Then unzip the connector file and import the jar file into the project libraries. Make sure Apache and MySQL are running in the Xampp.

VIII. CASES



```
12:10:54  [Apache]   Status change detected: running
12:11:00  [mysql]    Attempting to start MySQL app...
12:11:01  [mysql]    Status change detected: running
12:21:18  [mysql]    Attempting to stop MySQL app...
12:21:18  [mysql]    Status change detected: stopped
12:21:19  [Apache]   Attempting to stop Apache (PID: 18952)
12:21:19  [Apache]   Attempting to stop Apache (PID: 17066)
12:21:20  [Apache]   Status change detected: stopped
```

Figure 4: Install the Xampp application and run the administrator

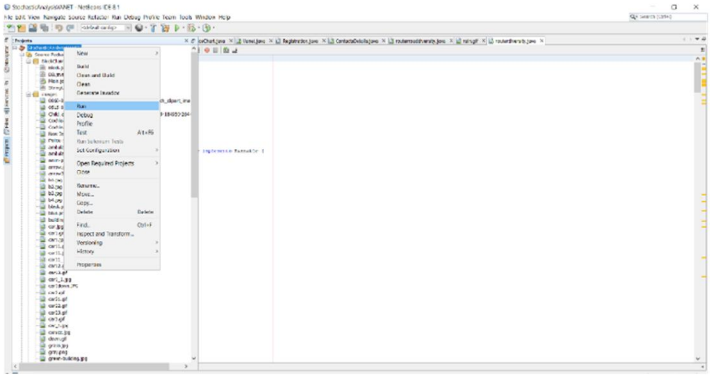


Figure 5: Start the project

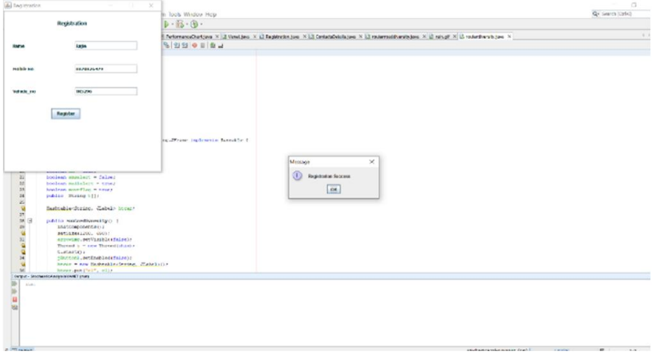


Figure 6: The above figure representing Vehicle Registration process

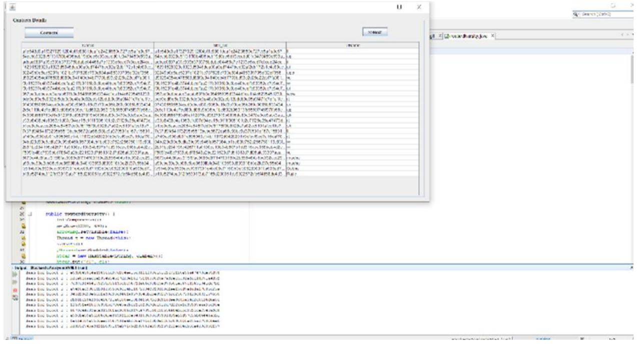


Figure 7: Above figure representing the contact details and to authenticate the vehicle number and phone number.

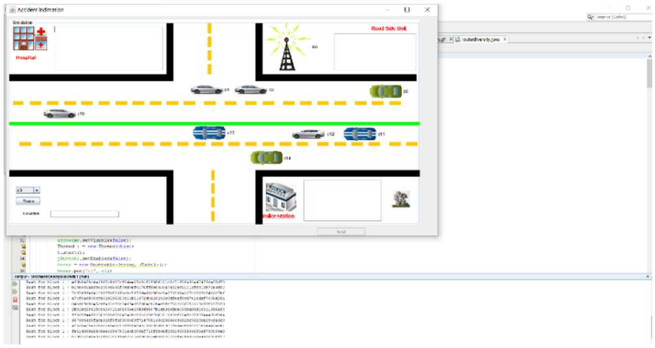


Figure 8: VANET Demonstration

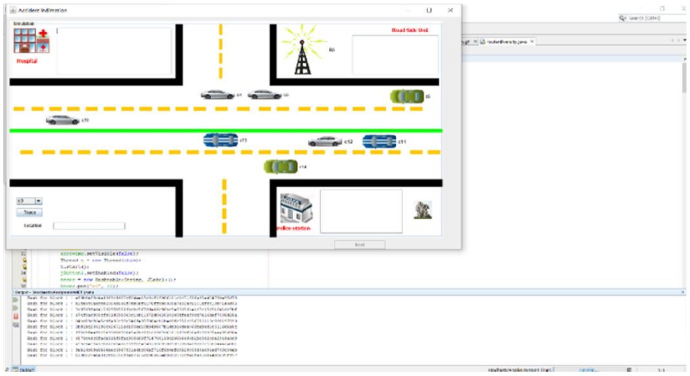


Figure 9 : Accident Intimation

DOI: 10.48175/IJARSCT-4579

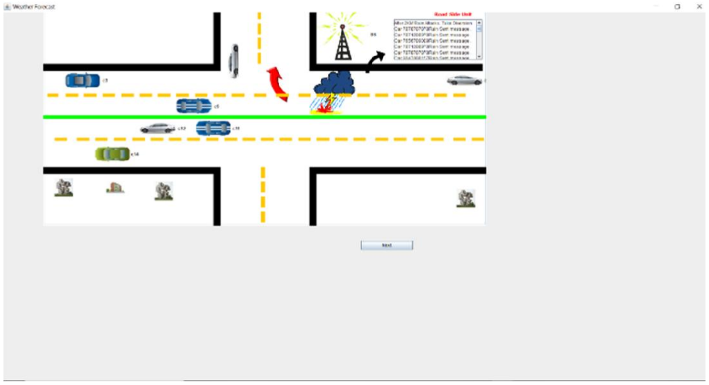


Figure 10 : Weather Forecasting

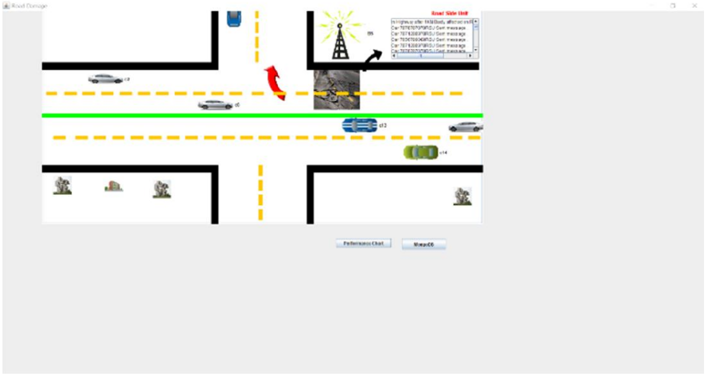


Figure 11: Road condition

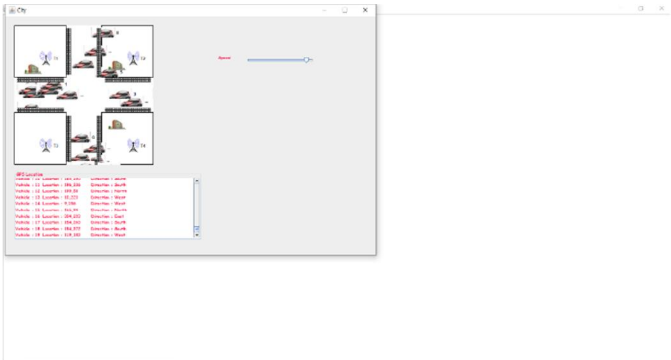


Figure 12: To check the speed of the vehicle

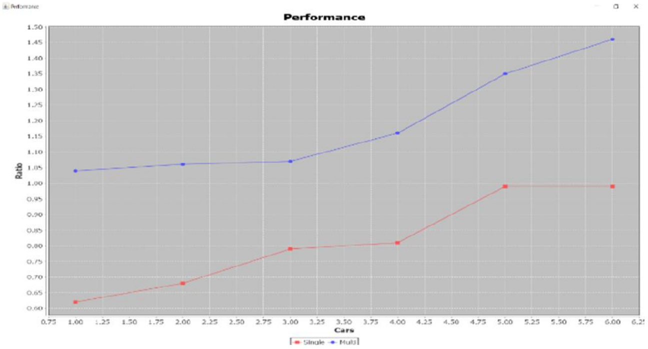


Figure 13: Check the performance of the Vehicle

DOI: 10.48175/IJARSCT-4579

IX. CONCLUSION

In this project, we have proposed a Secure and Verifiable data sharing scheme, which is based on both Cipher text-policy attribute- based Encyption and Blockchain. In our scheme, we have developed a Cipher text -policy attribute- based encryption to realize one-to-many data sharing. Meanwhile, We have also developed a Blockchain to record the access policy of the data. We have designed a policy hiding scheme to hide the sensitive information included in the access policy.

REFERENCES

[1]. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[2]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 2,pp. 559–573, Feb 2010.

[3]. F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, Dec 2015.

[4]. "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages,"IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240,March 2016.

[5]. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, March 2017.

[6]. L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, March 2011.

[7]. Y. Liu, J. Ling, Q. Wu, and B. Qin, "Scalable privacy-enhanced traffic monitoring in vehicular ad hoc networks," Soft Computing, vol. 20, no. 8, pp. 3335–3346, Aug 2016.

[8]. R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud based vehicular networks with efficient resource management,"IEEE Network, vol. 27, no. 5, pp. 48–55, September 2013.

[9]. J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, December 2015.

[10]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp.50–58, Apr. 2010.

[11]. C. Gentry, "Fully homomorphic encryption using ideal lattices,"in Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, ser. STOC'09. New York, NY, USA: ACM, 2009, pp. 169–178.

[12]. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and ` J. A. Manjon, "Contributory broadcast encryption with efficient ´encryption and short ciphertexts," IEEE Transactions on Computers, vol. 65, no. 2, pp. 466–479, Feb 2016.

[13]. L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 601–610, April 2017.

[14]. V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," Computers & Security, vol. 60, pp. 193–205, 2016.

[15]. A. Malhi and S. Batra, "Privacy-preserving authentication framework using bloom filter for secure vehicular communications,"International Journal of Information Security, vol. 15, no. 4, pp. 433–453, Aug 2016.

[16]. Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," IEEE Transactions on Industrial Informatics, pp. 1–1, 2018.

[17]. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," IEEE Computer, vol. 45, no. 1, pp. 39–45, Jan 2012.

[18]. B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in

DOI: 10.48175/IJARSCT-4579

the cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, Dec 2014.

[19]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores,"in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007,pp. 598–609.

[20]. A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.

[21]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology–ASIACRYPT 2009, M. Matsui, Ed. Springer Berlin Heidelberg, 2009, pp. 319–33

DOI: 10.48175/IJARSCT-4579