ISSN No:-2456-2165

Review on Block Chain based Privacy-Preserving Authentication Scheme for VANETS

Kajal Ganvir
Department of Electronics & Telecommunication Engineering
J D College of Engineering & Management
Nagpur, India

Neetu Gyanchandani
Department of Electronics & Telecommunication Engineering
J D College of Engineering & Management Nagpur, India

Shyam Bawankar
Department of Electronics & Telecommunication Engineering
J D College of Engineering & Management Nagpur, India

Abstract:- Recent advances in machine learning and the desire to expand the "smart city", various technology companies and car manufacturers have begun to pour billions of dollars into research and development of private cars. While many companies are working hard to build their own cars, it is important to start planning how these vehicles will interact with other infrastructure. Because passenger and pedestrian safety is highly dependent on this communication, careful design and use of these networks is essential. Blockchain is one of the important key parameters in terms of security. It has garnered a lot of attention in recent years. There are three categories of BC Public, private and consortium which is discussed in the paper.

Keywords:- *Block Chain, Security.*

I. INTRODUCTION

The fitting of wireless gadgets is reduced due to reduction in production cost. The requirement of easiness and comfortability in day to day life there are increase in the IoT devices also it gains network connected to internet. Protection to the vehicle can be possible and increase the road safety to the transportation enhances due to the increase due to the IoT. Intelligent Transport system having network with motors and extra members infrastructure is called the Vehicular Ad-hoc Network (VANET).The benefits of peer to peer(p2p) network is that it reduces the delay , flow rate, increases efficiency, easily detect losses if any nodes fail. These are some factors which alter VANET with traditional network. The talk to node can be happed through central node. while nodes talk personally, in P2P networks. in contrast to moving through the central medium first. Blockchain is a technology that attracts distributed ledgers to provide deal between peers on the network, in the absence permission of an exterior organization. It is due of the type of writing methods used, the integrity of this transaction is guaranteed. BC was invented by an anonymous person or group with name Satoshi in a white paper called Bitcoin. A Peer-to-Peer Electronic Cash System. The use of Bitcoin blockchain has been the first of many digital currencies, which are digital currencies that can be made secure transactions without a central bank or government sponsor. Although previous use of blockchain is the best in the case of cryptocurrencies, this hi tech used by various company due higher potential. BC technology is expected to utilize power-sharing in communities to make advantages to organization and floats where the height of faith is required. Due to the features of VANET and the advantages that BC offers,types of BC and BC tech to VANET infrastructure and any potential disruptions in operation.

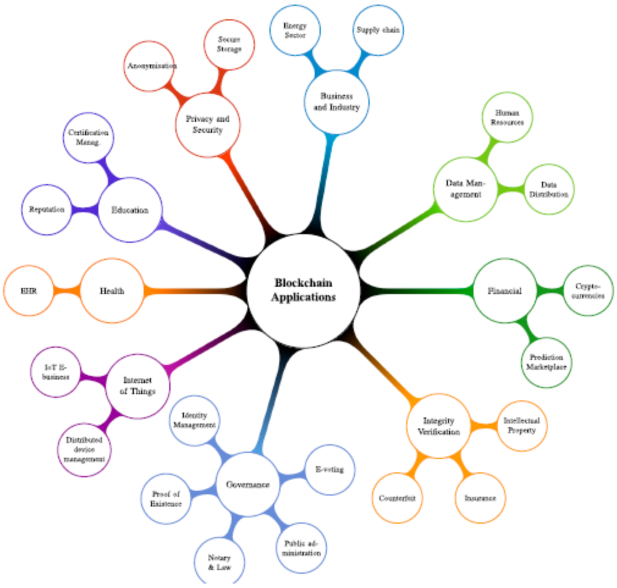

Fig. 1 Different Blockchain application in a different location

II. MOTIVATION

The NHTSA, which is a division of the US Department of Transport, classifies the state of private vehicles into five categories. It goes from zero, where there is no automation, so one has complete control of the car, up to five, where the at any circumferences it can perform well without human input.

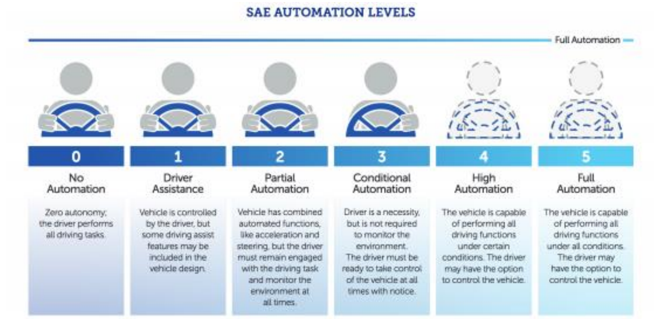
SAE AUTOMATION LEVELS
Full Automation
0
No Automation
Zero autonomy; the driver performs all driving tasks.
1
Driver Assistance
Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.
2
Partial Automation
Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.
3
Conditional Automation
Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.
4
High Automation
The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.
5
Full Automation
The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Figure 2. Automatic levels as defined by the Automotive Engineers Association

Although, for safety and legal reasons, the delivery of private vehicles may range from zero to five at the final speed, this analysis finds a high degree of automation, close to 4 or 5. We will not worry about how human communication affects communication or the logic of the data entry level logic, but instead we will only be looking at the communication method.

A. Communication carriers

There are various car-sharing sites where I can participate. Other examples are a car (V2V), a car to infrastructure (V2I), a pedestrian (V2P), a car to the cloud (V2C), and a car to everything (V2X). Given the nature of the blockchain used to communicate with people, in particular we will be looking at how we can affect V2V and V2I connections. Because of this, we can assume that our CAR and Roadside Units (RSUs) are two categories of peers. RSU standing devices sit on sidewalks or intersections and connect with incoming vehicles, making it easier to communicate, or communicate with other RSUs.

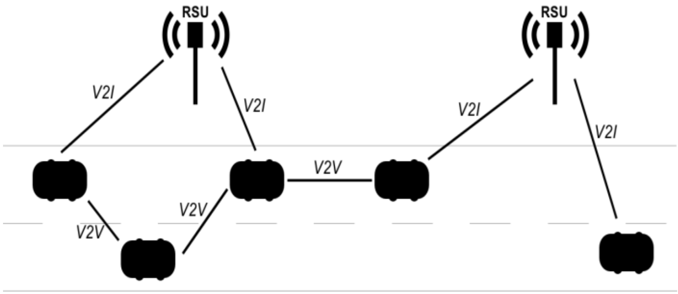

Figure 3. P2P network between V2V and V2I

III. PROBLEM STATEMENT

B. Overview

BC is allocated common details of all completed digital events and shared between participating sites. It consists a clear and unambiguous data of all the events that have taken place. Each event in the blockchain database is verified by multiple network compliance. There are two main types of BC, one is public BC and the private BC. The public BC is an open BC, it can be connected by anyone and connect BC without the need to obtain permission from the central authorities. On the other hand, a private BC is based on an access control process. Allows administrators to control network participants and things like who can connect , read and write to the BC . In a private blockchain, the administrator can create an agreement group. As a result, the private blockchain can switch to a single location, making it vulnerable to a single point of failure.

However, a public BC, there is not any single possibility of failure can have happened. and is able to withstand any attacks.

In traditional computer networks, birth and authenticity are often more important than integrity and availability. For example, transferring personally identifiable information or credit card details to a network without encryption could have serious consequences. However, for VANETs, rebirth is less important. This is because most of the information transmitted is recognizable, such as the speed and direction of the vehicle, so it is no longer a disaster when promised com. Integrity and availability, however, are very important to VANET because motors will need to make decisions based on information obtained from other vehicles or RSUs, and if the data they receive is inaccurate or they lose the ability to send or receive any data at all, the consequences could be disastrous.

B. Secret writing

Encryption, which remains in the Network layer, will be used to ensure that our data is in case the message is captured by an unintentional group. Special consideration for choosing the encryption method for VANET speed communication. The topic of encryption and decryption should be down because our communication is very sensitive to time. In general, faster encryption methods are less secure than their slower counterparts, so it is important to use an encryption method with an acceptable level of security.

C. Authorization

Another advantage of traditional block chain use is that often it is all down to peers to join the network without the need for their verification by a trusted group. While anonymity may help with some implementation, the network of vehicles and roadside infrastructure may be at risk if malicious actors join the network and provide illegal information or facilitate the denial of service information. Accordingly, digital certificates will be distributed by a regulatory authority such as USDOT and supplemented by manufacturers. While deviating from pure blockchain use, this process is required to prevent unauthorized Hardware from joining VANET.

IV. LITRATURE SURVEY

VANET blockchain-based privacy preservation authentication (BPPA) program. At BPPA, all certificates and transactions are permanently recorded and unchanged on the blockchain to make the functions of the semi-TAs transparent and validated. However, it is always a challenge as to how to effectively use the blockchain authentication in real-time driving situations (e.g., high speed or large number of messages during traffic). With a novel data structure named the Merkle Patricia tree (MPT), we expand the standard blockchain structure to provide a validation system that is distributed without a demolition list [1].

In this paper, we welcome the PoW consensus process. The integration of all mining vehicles in the blockchain network can be established to produce a new block that can be used as a global reality with the next block. Experiments and analysis show that our proposed local blockchain system can be used effectively on VANET without additional storage [2].

A framework developed by BC to protect user privacy and increase the safety of the automotive system. Remote wireless software upgrades and other emerging services such as powerful car insurance funds are used to demonstrate the effectiveness of the proposed security construction. We argue for quality in structural strength against common security attacks [3].

Complete segregation of BC- based application with a variety of field like logistics, business, health care, IoT, privacy and managing data for analysis, and creating key themes, styles and innovative research areas. We also point out the flaws found in the relevant literature, especially restriction introduced by BC technology and how these restrictions apply to various field and industries. Building on these findings, we identify various research spaces and future exploratory indicators that are expected to have significant value for educators and practitioners [4].

Survey's work first outlined how the research was discussed and followed by the development and implementation of the Blockchain policy. The following are the twelve applications where Blockchain technology looks promising to solve the existing medium system in a low-key way and many security issues are fixed. Some of the most sought after areas are Internet of Things (IoT), Healthcare etc. The findings of the study revealed that there is some work being done on privacy and security issues but there is still much to be done. Blockchain technology has many advantages such as power allocation, publicly available transactions, openness, security. However, there is still more research to be done such as the network, distribution and mining process of the Blockchain system [5].

Challenges to the use of Blockchian use and issues related to security and privacy have been discussed. This is the first time this type of research has been done where Blockchain has a request and a problem regarding their security and privacy has been reviewed [6].

V. CONCLUSION

BC is very important technology today as well as in future. The various aspect in terms of safety and security are provides by the BC. The time delay due to blockchain can be reduces significantly due to middle party is not present. It is very useful in VANET.

REFERENCES

[1]. Zhaojun Lu , Qian Wang , Gang Qu , *Senior Member, IEEE*, Haichun Zhang, and Zhenglin Liu ,"A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, 1063-8210 © 2019 IEEE.

[2]. Rakesh Shrestha a, Rojeena Bajracharya b, Anish P. Shrestha c, Seung Yeob Namb, "A new type of blockchain for secure message exchange in VANET", Digital Communications and Networks 6 (2020) 177–186https://doi.org/10.1016/j.dcan.2019.04.003

[3]. Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine • December 2017

[4]. Fran Casino, Thomas K.Dasaklis, ConstantinosPatsakis,[b]ConstantinosPatsakis[a],"A systematic literature review of blockchain-based applications: Current status, classification and open issues", Telematics and Informatics Volume 36, March 2019, Pages 55-81

[5]. Bhabendu K. Mohanta1 , Debasish Jena2 , Soumyashree S. Panda3 , Srichandan Sobhanayak4 ,"Blockchain technology: A survey on applications and security privacy Challenges"Elsevier, Internet of Things,Volume 8, December 2019, 100107

[6]. Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 2, pp. 760–776, Feb. 2019.

[7]. M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," IET Intell. Transp. Syst., vol. 10, no. 6, pp. 379–388, 2016.

[8]. R. Canetti, D. Shahaf, and M. Vald, "Universally composable authentication and key-exchange with global PKI," in Public-Key Cryptography–PKC. Berlin, Germany: Springer, 2016, pp. 265–296.

[9]. A. Yang, X. Tan, J. Baek, and D. S.Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," IEEE Trans. Services Comput., vol. 10, no. 2, pp. 165–175, Mar./Apr. 2017.

[10]. A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," IEEE Trans. Ind. Informat.,vol. 14,no.8,pp.3701–3711,Aug.2018