IJARSCT

ISSN (Online) 2581-9429

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

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, November 2024

A Review on VANET Security using Blockchain Technology

Surbhi Priya[1], Dr. Sudeesh Chouhan[2], Mr. Rishi Kushwah[3]

Research Scholar, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh[1]

Assistant Professor, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh[2,3]

Abstract: *VANET enables communication via V2V or communication specifically developed by vehicles. As a result, many technologies and facilities such as passenger protection, advanced vehicle features, and infotainment systems have been well studied. In this article, we used the security algorithm and rewards will be added to the customer. We also analyzed VANET with blockchain technology and analyzed the Internet of Vehicles via blockchain. The Internet of Cars increases traffic safety. Now is the time to pave the way for a new wave of vehicle control by integrating smart cars into the Internet of Vehicles (IoV) using modern and creative protection technology.*

Keywords: V2V, Blockchain, IoV, VANET

I. INTRODUCTION

Ad hoc networks for vehicles (VANET) have been arising as a branch of the MANET. Intelligent Transport Networks (ITS) VANET is viewed as an extensive approach [1]. It has been one of the most significant wireless communications research fields [2]. Now we are discussing VANET's background through the given below fig.1. These ad hoc networks are parented in WANET. VANET is as like MANET, that, without dependence of any other network, organizes its communication mechanism itself. MANET is indeed the military's most standard usage. This is just like data sharing among different computers that simple and basic type of communication. VANET has cell nodes, roadside units(RSU). That is the sensors throughout the vehicles are wireless nodes, it is also called On-Board Unit (OBU) that is the Datashing into and out of RSUs for signal processing. RSUs have deployed fixed units which are the connection among MN as well as the databases or even the internet. There can be lots of VANET programs, maybe the most relevant of all is the enhancement of traffic safety infrastructure through exchanging information via the Web to avoid traffic incidents. that shows the scenarios described below, VANET provides two kinds of vehicle to vehicle (V2V) as well as Vehicle to Infrastructure(V2I) [2].

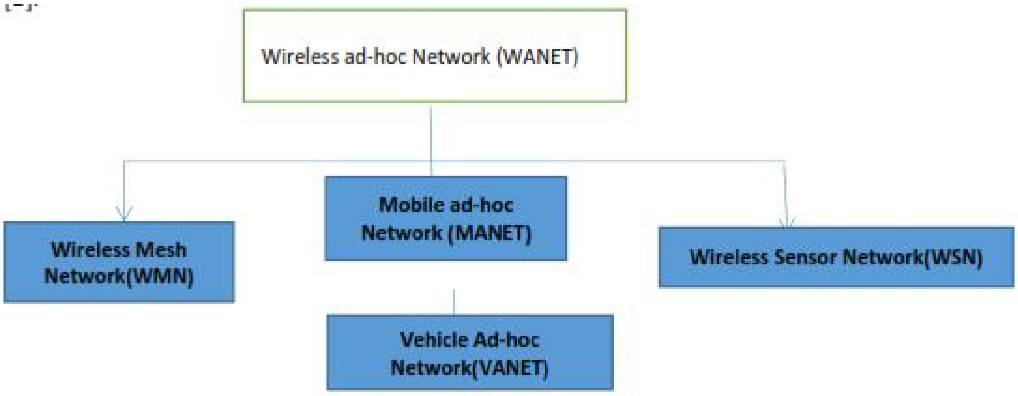
Wireless ad-hoc Network (WANET)
Wireless Mesh Network(WMN)
Mobile ad-hoc Network (MANET)
Wireless Sensor Network(WSN)
Vehicle Ad-hoc Network(VANET)

Fig.1 Types of Ad hoc network

The communication platforms in the vehicle-to-vehicle area (V2V). Almost ten years back from initial research or advanced procedure function [3]. THE latest V2Y1 network surveys last year had more than a thousand quotes on the reference sheet. V2X is nothing but it is the type of VANET such as V2V (Vehicle to vehicle), V2I that's mean Vehicle

DOI: 10.48175/568

to infrastructure. In the Current era, Strong radio communication management problems because of to its decentralization and its strong quality of service (QoS) specifications for transport safety apps force the production of potential vehicle-on-vehicle (V2V) and vehicle-on -infrastructure wireless communications networks (V2I) systems [4]. Vehicles will communicate their location as well as the speed for surrounding vehicles on even a regular basis utilizing IEEE 802.11p to prevent conflicts with road traffic [4].V2Y is a component of intelligent transportation networks (ITS) is the main reason for this. The ITS scope is larger than V2X because it still involves road, ground, and air transport networks. However, the focused scientific work just started to evolve after the public and private sectors revealed the services. Enhanced network performance ("green"), decreased traffic delays, economic development, passenger content, but most specifically, health is the driving factor for all of ITS. This is more apparent in V2X as traffic crashes in major developing countries already take millions of lives every year. While we are constrained to V2Y only, that zone's width is large. For few years V2V mechanism has already been known after work on the V2V mechanism because it varies from those of other conventional communication systems. The closest approximation may be between cellular as well as I antenna heights each of the transmitter (Ty) and receiver (Ry) are small, and both Ty and Ry are mobile, and V2V can be distinguished from either the V2V channel.

While there is a protocol for V2V communications (5.9 GHz UNII band; particular-range committed communications, DSRC, Traditional). Traditional wireless local area networking (WLAN) for all devices might not be enough [5]. Throughout the Wi-Fi Standard, the lowest two levels of the networking routing protocol are the transmitting scheme[5]. However, when modern V2V technologies grow, such technologies can have to be supported by modern standards. It may be Standard Wireless Metropolitan Area (WMAN). A broad range of implementations of the 802.16 specifications are also assigned to as WiMAX by energy sector established technology.V2V technologies provide higher bandwidth speeds, rapid comment channel structured disappearing, or smarter FEC encoding to boost efficiency. For potential V2V environments, it is also feasible to add certain specifications.

Whatever the transfer method, wireless channels information is important for the optimum development and efficiency of any V2V network. It should be well established that perhaps the effects of the computational channel evaluation offer basic information in the data link-form architecture or study
among all communications systems.

II. LITERATURE REVIEW

Sr.	Reference	Issues	Action / study
1.	[1]	Security	The author suggested to security in communication between two vehicle such as threat. They also provide taxonomy.
2.	[2]	Pros and cons of research work	The author analyze the research work in future and also discuss about the security issues.
3.	[3]	Less dynamic channel.	The author proposed modeling vehicle-to-vehicle (V2V) wireless channels and also give their effect.
4.	[4]	Vehicular safety	The author broadly discuss about the VANET and also they give on overview of modeling of V2V channel and their safety.
5.	[6]	IoV Setting, security and privacy	The author proposed a model which distribute the message to vehicles on real time and their data be store in blockchain. They also contribute the block generation rewarded by some of the bitcoin.
6.	[7]	Cyber attack lie DOS attack	The author show's two extensive first one is when the vehicle densities will high another is fog device friendly that traffic light verify the vehicle efficiently.
7.	[8]	Cyber-attack in online Transaction	The author suggested the algorithm to secure the transaction. That algorithm implement in identity or verification time through Digital signature.
8.	[9]	trust, reliability, and security	The author proposed integrate blockchain technology into ad hoc vehicular networking. Which increase the trust, reliability and their

			secure environment. They also proposed their architecture of that model.
9	[10]	Security in VANET	The author proposed the security architecture of VANET which is based upon the Blockchain security and mobile edge computing.
10.	[12]	Real time connectivity.	The author suggested reducing problem is real time connectivity through fog computation and the also discuss in broad way about the challenges of VANET.
11.	[14]	Smart contract methodology	The author discusses the overview of smart contract in blockchain.
12.	[15]	Affects of decentralization	The author analyze the affect of decentralization in consensus. They also discuss antitrust policy.

III. INTERNET OF VEHICLES

Vehicles become fitted with internet connectivity systems into an Internet of Vehicles(IoV) trying to set and different sensors which enable vehicles to capture and send information, like position, speed including road conditions for many other vehicles or roadside units(RSU) throughout the surrounding area[6]. These telecommunications are often classified as vehicle either vehicle-to-road side interactions, respectively [6]. A real-time alert signal would be transmitted to surrounding vehicles where it is sensed that an emergency brake is in effect in vehicle Y such that necessary steps can be taken by several other vehicles, especially vehicles behind and to the, beyond, or next to vehicle Y. The driver can choose an alternate route when getting certain alerts in real-time, for instance, warning notifications about road conditions (e.g., ices roads or floods). This rather warning can typically be delivered to cars in a larger area and does not want to be sent in real-time. A smart light will turn the signals process to that of an appropriate traffic algorithm (like fluent reasoning, adaptive algorithm, and improving education) to reduce the period of awaiting such that free-standing users can depend on the location, pace, and path of drivers. After that the huge number of challenges which is security. Let's take an example to understand the security challenges, Suppose an Attacker whose name is John and their group so, they are attacked through the fake alert information to mislead another vehicle. However, they ensure their authentication non-repudiation and their identity of notification [6]. Even if an incorrect or fraudulent notification is identified will different organizations expose a real message generator profile.

IV. EASE OF USING

4.1 Blockchain

Blockchain has become a system that is distributed. The encryption of the hash function is being used to store information in a link as well as the data becomes malicious and identifiable[10]. Which maintain data integrity, the system uses a consensus protocol. Hence, blockchain technologies may be used to resolve that protection issue throughout the VANET ecosystem and reduce reliance on trustworthy centralized authorities. To enables members to freely and comparatively efficiently track as well as inspect transaction processing. A blockchain database is managed autonomously using a node to node network and a distributed time-stamping server [11]. Due to the rapid growth of digital media implementations and new inventions in the field of social-machine technology, broadband is strongly engaged worldwide [9][24].

4.2 Vehicle ad hoc Network (VANET)

In the current era, the prevalence of ad hoc vehicles (VANETs) networks has increased. This year's growing number of vehicles already introduced significant global problems with traffic collisions, road traffic pollution, fuel use, and atmospheric pollution [12]. Traffic collisions across both established and emerging countries become recurrent challenges. This tends to lead to major damage to property and existence. Intelligent Transportation Systems (ITS) has initiated VANETs to create a better road infrastructure to resolve these issues to make their trip safer, more efficient, trouble-free, and entertaining. The theory of MANETs, its random advancement of such a wireless mobile network-for vehicle framework is established through the implementation of both the MANETs [13].In the "Vehicle-to-car-to-car-ad-choc" mobile connectivity and networking frameworks, VANETs had first been described. Which communications may be constructed and data can always be exchanged between vehicles. Throughout the United States, in Europe, and also in Japan, there is significant standardization of VANET system stacks, which leads to its domination of the automotive sector. VANET research began in 2000, with scholars employed in mobile ad hoc systems, at universities and testing laboratories[23].

4.3 Smart contract methodology:-

Smart contracts may be designed and applied on various blockchain networks (e.g. Ethereum) [14]. A various number of platforms which provide a range of smart contract they create tools. This permits the performance beyond external parties in online transactions. Computer scientist, advocate, & cryptographer Nick Szabo, who invented the word, first suggested smart contracts in just the late 1990s [15]. This smart contract does not become specifically similar to either the classic contract model, it may be a computer system of some type. This may be used as a protected encrypted process as it operates as well as the formalized results such as from a value swap between both the parties become purely applied and only managed till a contract is placed in a database or public ledger with precise contract information [15]. when we are talking about their implementation of it the application which is Byzantine algorithms that accommodate faults enables cybersecurity to shape smart contracts via decentralization. Due to the strong customization that they bring to purchases, smart contracts have become one of the much-desired innovations[16]. A broad range of smart contract which uses through the financial sector or we can say that the banking sector, it may be wellness or living science to renewable supplies among the voting system. Smart contracts are just not simply digital (most of which depend on trustworthy authorities to achieve agreement and implementation) or machine learning (somewhat robotic) contracts[17]. Proof of Work(PoW) and Proof of Stake (PoS) become several frequently debated principles for establishing the democratic agreement.POW rewards database defenders solving complex crystallographic challenges to verify transfers and develop new blocks.

4.4 Fair Blind signature scheme:-

The blind signature method is a procedure to receive a Signature from either a signature so that the user does not relate his interpretation of the procedure to the corresponding set of texts. For decentralized wireless payment services, blind signature schemes can be used [18]. In private mobile payment networks, blind signature mechanisms can be used. A blind signature is a digital version of a signature to cryptography proposed by David Chaum that masks (blinds) the substance of a statement while signing [19]. It can be provided for used in UN-alkalinity. Which prohibits the signer from connecting to a future blind edition the blinded document it signatures to validate. A collection of popular public-key sign systems, such as RSA and DSA, can also be used to enforce blind signature systems. A blind signature scheme is a protocol for receiving a signature with an issuer so that the issuer's interpretation of the protocol can not be connected to the corresponding message/signature pair [22].In the privacy protocols where even the issuer and the message writer are separate parties blind signatures are used systems of e-cash., blind signature systems provide optimal connectivity And thus deceptive users could misuse. A blind-signature scheme is a primitive cryptography that enables a user to receive digital signatures from the issuer of the message of the user's choosing in a manner that can not link the vision of the issuer of the protocol to the resulting pair of messages/signatures [22].

4.5 Multi-signature or Threshold mechanism:-

Across the past couple of years, public cryptocurrencies with impervious and irreversible sensor histories have provided unprecedented openness and audibility. This scheme, which enables m user to sign a signature message[6]. Rather than always m separate signatures, its multi-signature efficiency is a single signature for whom the duration is considerably shorter than those of m separate signatures.it refers to more than one key that is required for a transaction to be signed and that is generally used to share responsibilities [20].

Multi-signatures function in Cryptocurrency by generating a multi-signature account, then when we develop it, we determine which keys and most are required to register the transactions. After that build
a payment after such a bit, citizens with signed keys, and nothing else.

In the case becomes different for both the standard signatures, as we have just one digital signature, some secret key, and another signature[20]. Such a signature party, Each signer has a similar public key

DOI: 10.48175/568

that is identical to all of us which share secret key forms.

4.6 Secret distribution of threshold

The secret minimum sharing(t,m) method will transmit the secret S to m associates S1, S2,..., Sm [6]. The secret S may be restored with either the number of contracts in t(threshold). Its security of both the secret exchange network ensures because no less than t amount of shares is retrieved.

V. RELATED WORK

The suggested VANET Protection Architecture is extensively explored in this section as regards the implementations of the Bitcoin blockchain. We added the complexity in security when the message receiver receives the message at the time verified that Digital signature which is very important in Cryptography and blockchain. Few essential criteria for verifying the individuals participating in the deal, such as digital signatures.

It uses the idea of public and private keys which produces signatures at the start of the process, so each frame has to be verified before performing transactions [8].

The issue with EI-Gamal is that T requires to be high to ensure the integrated log issue. The T of at least
1024 bits is the guideline. To minimize the signature size schnorr introduced the new EI-Gamal-based method, this signature may be as big as 2048 bits, but also with a limited scale.

Whether Nikhil requires Sahil to share the public and private keys before another conversation starts, as specified below.

Let's suppose N be Mr. Nikhil, S be Dr. Sahil Verma
: signatures
W: Nikhil private key
H: random secret k: message
(e1,e2,f,g): Nikhil public key

Two functions generate two identities during the signing process, and the performance of the first function during the authentication stage is contrasted with the first authentication signature.
Here are two modules: p and q using function 1 and 3 each.
Key generation:
Nikhil will create keys and communicate to the public keys while signing a letter.

Nikhil chooses a prime 'f,' normally 1024 bits long.
Nikhil chooses the second prime of a certain size as both the hashing algorithm digest (actually 160 b), but it can alter in the future. The first g has to be broken ***(f-1), i.e. (f-1)= 0 mod g***

c. Nikhil select e1
The alice picked a primitive variable e0 and computed e1=e (f−1)/g0modf to become the fifth root of module fd.
Nikhil selects an integer for her private key. e. Nikhil have to calculate e2=ed1modf
f. Nikhil's have the public key is (e1,e2,f,g) and their private key is W. Where,
K: message, H: Random secret, u: concatenation
N = Mr. Nikhil, S= Dr. Sahil: Signature, W: Nikhil Private key, n(…) hashing algorithm.
V: verification (e1,e2,f, g): Nikhil's public key. Signing:

The random number H is selected by Nikhil. Please notice that both public and private keys may be used to sign several communications, Nikhil will alter and make a separate message each time. Also notice that it must be between 1 and g. Nikhil has to calculate their first signature from N=h(k/eH1modf) after that the message is pre posted their values eH1modf. The Hash function is then used for digest formation. Net, which is not added explicitly to the post, is linked to k and eH1modf concatenation [21].

The second signature will be calculated by Nikhil S = h+WXN mod g. Now Nikhil has to send the k, N, S Verifying Message

Sahil recipient, suppose k, N, and S are obtained.

After the receiving the keys now, Dr. Sahil calculate V= h(k|eSSNe−SNSmodf)

A message is approved when it is consistent with V modulo f.

This algorithm helps during reward generation to their identity.

VI. DISCUSSION

Securing VANET is an important aspect which depend on several other parameters as well [25-26] including the location, vehicle movement on roadside, data collections, etc. Blockchain can be used in several ways [27-28] to manage the security and privacy concerns significantly. The VANET formed by the UAVs [29-30] has the same security and privacy concerns. In addition to that smart phones and gadgets plays an important role for managing the VANET. However, the smart phones/gadgets [31] have their own challenges of resource constraint, energy efficiency, security, and privacy challenges at the same time.

VII. FUTURE WORK

After this paper author consider the Future work in VANET is Toll tax will be withdrawn automatically if the driver Breaks the rule of traffic so that punishment will withdraw from their V coin account. If we want to add all identity in blockchain so, we have to create a block and add all block or we can say that all vehicular will be add to blockchain with their id such as Car Model, Company Of the car, Owner name , Driver name, Insurance number of the car, Bank account Detail of owner, Address, phone number, etc. These details are store in the block and these detail also available in all RSU (Road Side Unit).

VIII. CONCLUSION

Nowadays, so many challenges in a VANET .this is the main issues and so many research work going on through blockchain technology to secure the VANET. VANET is future technology that will implement everywhere in the world, so that help's to give all the updated information on a real-time basis. Their so many algorithms to secure the application or system. The main attack possible is a middle- man attack to announce the fake message to all surrounding vehicles.

REFERENCES

[1] Gillani, S.; Shahzad, F.; Qayyum, A.; Mehmood, R. A survey on security in vehicular ad hoc networks.In Communication Technologies forVehicles.Nets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science;Berbineau, M., Jonsson, M., Bonnin, J., Cherkaoui, S., Aguado, M., Rico-Garcia, C., Ghannoum, H.,Mehmood, R., Vinel, A., Eds.; Springer: Heidelberg/Berlin, Germany, 2013; pp. 59–74.

[2] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam and M. Montaser, "Vehicular ad-hoc network (VANET): Review," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, 2018, pp. 1-6.

[3] Matolak D.W. (2013) V2V Communication Channels: State of Knowledge, New Results, and What's Next. In: Berbineau M. et al. (eds) Communication Technologies for Vehicles.

[4] Nets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science, vol 7865. Springer, Berlin, Heidelberg

[5] IEEE Vehicular Technology Magazine, Special Issue on V2V Communications 2(4) (December 2007)

[6] D. W. Matolak, "Channel Modeling for Vehicle-To-Vehicle Communications," in IEEE Communications Magazine, vol. 46, no. 5, pp. 76-83, May 2008

[7] Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, Shengwei Tian,Blockchain based secure data sharing system for Internet of vehicles: A position paper, Vehicular Communications,Volume16,2019,Pages85-93,ISSN2214- 2096,https://doi.org/10.1016/j.vehcom.2019.03.003 .(http://www.sciencedirect.com/science/article/pii/S2214209618303000)

DOI: 10.48175/568

[8] Jian Liu, Jiangtao Li, Lei Zhang, Feifei Dai, Yuanfei Zhang, Xinyu Meng, Jian Shen,Secure intelligent traffic light control using fog computing,Future Generation Computer Systems,Volume 78, Part 2,2018,Pages 817-824, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.02.017. (http://www.sciencedirect.com/science/article/pii/S0167739X17302157)

[9] Ravi, N., Prashar, D., & Nagpal, A. (2019). A Framework For Securing Online Transaction Through Block Chain. Think India Journal, 22(16), 2383-2392.Retrieved from https://journals.eduindex.org/index.php/think-india/article/view/17138

[10] S. Sharma, K. K. Ghanshala and S. Mohan, "Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture," 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, 2019, pp. 452-457.

[11] X. Zhang, R. Li and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 258-259.

[12] Wikipedia contributors. "Blockchain." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 24 Mar. 2020. Web. 27 Mar. 2020.

[13] Shrestha, Rakesh,et al. “Challenges of Future VANET and Cloud-Based approaches.” Wireless Communications and Mobile Computing, vol. 2018, 2018, pp. 1–15., doi:10.1155/2018/5603518.

[14] Wikipedia contributors. "Vehicular ad-hoc network." Wikipedia, The Free Encyclopedia.Wikipedia, The Free Encyclopedia, 1 Mar. 2020. Web. 27 Mar. 2020.

[15] Alharby, Maher & Aldweesh, Amjad & van Moorsel, Aad. (2019). Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018).

[16] Wikipedia contributors. "Smart contract." Wikipedia, The Free Encyclopedia.Wikipedia, The Free Encyclopedia, 26 Mar. 2020. Web. 27 Mar. 2020.

[17] Macrinici, Daniel, et al. “Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study.” Telematics and Informatics, vol. 35, no. 8, 2018, pp. 2337–2354., doi:10.1016/j.tele.2018.10.004.

[18] Cong, Lin William, and Zhiguo He. “Blockchain Disruption and Smart Contracts.” 2018, doi:10.3386/w24399.

[19] Isha Batra, Sahil Verma, Kavita, Uttam Ghosh, Joel J. P. C. Rodrigues, Gia Nhu Nguyen, A.S.M. Sanwar Hosen and Vinayagam Mariappan, “Hybrid Logical Security Framework for Privacy Preservation in the Green Internet of Things” in MDPI-Sustainability, DOI: 10.3390/su12145542

[20] Stadler M., Piveteau JM., Camenisch J. (1995) Fair Blind Signatures. In: Guillou L.C., Quisquater JJ. (eds) Advances in Cryptology — EUROCRYPT ’95. EUROCRYPT 1995. Lecture Notes in Computer Science, vol 921. Springer, Berlin, Heidelberg

[21] Wikipedia contributors. "Blind signature" Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 4 Jan. 2020. Web. 27 Mar. 2020.