International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure VANET Authentication Using Block Chain

Jinugu Deepika

Student, Rajam, Vizianagaram, 535127, India.

ABSTRACT

Recent advancements in intelligent transportation systems have enhanced the driving experience in vehicle ad-hock network (VANET) systems (ITS). It is essential that the VANET system of today be able to offer low computational cost with great serving capacity. When a user moves from one roadside unit (RSU) to another RSU region, the current roadside unit (RSU) requires re-authentication of the vehicle user, increasing COMPUTATIONAL COMPLEXITY. To solve the aforementioned problem, a block chain-based authentication system is developed. This method's combination of VANET and block chain enables independent car user authentication without the need for a trustworthy authority. The block chain network also safeguards the users' confidentiality and openness of communication. Conditional privacy is also utilized in a number of block chain-based systems.

Keywords: VANET, Block chain, RSU(Road Side Unit), Block chain based authentication protocol, Computational complexity , V2V(Vehicle -to-vehicle), V2I(Vehicle-to-Infrastructure).

1. Introduction

Block chains are used to store data blocks, while cryptography is used to connect them. Once a block has stored all the data it can, it is closed and connected to the block that came before it, creating the data chain known as the block chain. Each block has a fixed amount of storage. A block chain's immutability makes sure that once data has been recorded, it cannot be altered, deleted, or destroyed. HEADER:- The header of the block is the most important part of it. At this moment, the block is connected to the other block. The components of the header portion include 1. Block No. 2.Prev.block 3. Markle root hash, 4. Nonc 5. The creation time stamp. 1.BLOCK NUMBER: The block number uses a number to identify the particular block. 2.PREV.BLOCKHASH: The function's name identifies the block that is connected by a link.

2. Literature Survey

In paper [1], *the following work is suggested: In this paper, a block chain-based system for V2I handover authentication and initial authentication is proposed. Since the required information is kept in the block chain, a vehicle may only perform hash and XOR operations to authenticate to other RSUs after completing initial authentication with one RSU.*

The paper's advantages include rapid and secure handover authentication. Lower computational complexity

[2] In a paper*. The core idea of our EBCPA is a traceable one-time public key creation mechanism, sometimes known as an anonymous public key. This technology can ensure that automobiles communicate with one another in an anonymous manner and that only a reliable individual (like a manager) is capable of discovering a vehicle's actual identity.*

advantages of EBCPA

In paper [3].[3] In a paper. Our approach employs a novel VANET system design with edge computing infrastructure to offer adequate processing and storage capacity, in contrast to the conventional VANET structure. Our certificate-less authentication method makes use of a special session key for every vehicle to prevent interference. Additionally, consortium block chain is used in the production of V2V group keys. Real-time group membership management and efficient group key updates are provided in accordance with this.

This study's strength is the use of a cloud server, which lessens the complexity of storage.

The absence of any revocation mechanisms is a flaw in this article.

Mutual authentication calculations are expensive.

In paper [4].Block chain is getting more and more attention for TM. Alexopoulos et al. used block chain authentication to improve the security of the TM systems. Additionally, a distributed, probabilistic state machine was considered to represent a block chain model that matched TM systems. For the purpose of authentication, they provided an abstract graph-theoretic model of the TM systems. By incorporating trust information into the block chain, this strategy improves the ability of the current authentication method to defend against censorship and stale information assaults. Bendiab et al.

management developed a ground-breaking identity trust architecture based on a block chain. Their recommended design views blockchain as a decentralised trust model that allows cloud service providers to manage their trust connections without relying on a central authority.Block chain is seen in their suggested architecture as a decentralized trust model that enables cloud service providers to control their trust connections without depending on a reliable third party.relying on a trustworthy third party. Furthermore, Goka and Shigeno introduced a distributed, blockchain-based management system for trust and reward in mobile ad hoc networks. This strategy can reduce the harm that recalcitrant nodes do to the network. The decentralised, safe, and data consistency features of block chain are therefore expected to help the TM system in VANETs tackle its existing problems.

In paper [5].The network model for fog computing-based IoV is shown in Fig. 1, which also depicts the communication occurring between various parties. This paradigm includes several communication partners, such as cars, roadside units (RSUs), trusted authorities (TA), fog servers, and cloud servers. There are several channels of communication, such as vehicle to remote sensor unit (V2R), vehicle to cloud server, and vehicle to fog server (F2C). The responsibility of TA is to register each distinct entity before to inclusion in the network. The RSUs are deployed after having the credentials stored in their memory. The essential information is kept up to date by each vehicle's OBU, fog server, and cloud server, allowing it to be utilised for key management and further authentication processes. Every automobile has an OBU that records and processes all ofEvery car has an OBU that processes and saves all of the vehicle's information [4]. Additionally, vehicles come with sensors that pick up on and analyse outside information before sending it to the OBU.

3.Methodology

A. Use in Basic Scenario: About quickly inform nearby vehicles to traffic bottlenecks and accidents, cars may develop and broadcast road-related communications (i.e., make an announcement) over VANETs. Bob, the driver of the automobile, decides to broadcast a message after witnessing a car accident. The messages sent by autos, however, might not be true. To ensure the validity of such an announcement message, Bob will need to collaborate with additional witnesses. Bob begins by asking further witnesses to corroborate his claim. After getting the request and accepting Bob's signature, the witness verifies the communication and offers their assessment. Bob notifies the nearest RSU of an aggregate notice with t confirmations after getting t answers. The RSU then validates the veracity of

Setting B.

1) Establishing roles: T stands for the trusted authority, I for the initiator, and R for the respondent. In the Nomenclature, all symbols and their related Roles are defined in Setting B.1: T is the trusted authority, I denotes the initiator, and R denotes the reply. All symbols and their associated meanings are shown in the Nomenclature.

2) Packets Setting: There are three distinct types of packets produced by the cars in our secure aggregation announcement technique.

1) A set of witnesses receives a "initiation packet" (ITP) from the initiator. To ascertain whether the witnesses concur with the statement and have them sign it, ITP contains mes x0002 sage reports.

2) A response packet is a type of packet sent from the responder to the initiator (RPP). RPP will be given back to the initiator if the witness accepts the signature I've offered. RPP is made up in particular o

Algorithm for Distributed Consensus Algorithm 1. The leader sends block data to all ASUs for verification. the captain All: Request = (Block new||Block hash||Sigleader||timestamp) because Block hash is equivalent to Hash(Block new||timestamp).2. The ASUs will exchange their respective signatures and audit results with one another. Audit = (audit result||ASUj): ADUit result||SigASUl3. If an ASU discovers more than 2f matching audited messages, it will send a confirmation message to all other ASUs. For ASUl and ASUj, confirmation equals (confirmation||SigASUl).4. In case an ASU receives more than 2f + 1 confirmation messages, block data is added to the block chain.

4. Results and Discussion

The letters H, M, and Ex stand for the secure hash functions that are being employed, multiplication, and exponential operation, respectively. The comparative results for computing expenses are shown in Table 4, along with an approximation of the execution time according to [18]. The recommended solution makes advantage of bi linear pairing, which, as was already established, has higher security properties. Remember that all challenging pairing calculations are carried out on the RSU side. As a result, stronger security assurance may be provided for cars with limited resources while incurring lower computational costs, which is crucial for real-world VANET applications. On the RSU and vehicle sides, respectively, computations for key distribution and VANETs verification are described. The letters p and stand for point multiplication and pairing operations, respectively.

5. Conclusion

We developed a V2I changeover authentication for the block chain-based VANET model using the block x0002 chain to reduce the cost of unnecessary calculations during re-authentications and a vehicle revocation without TA support. We discovered via an informal analysis of the proposed protocol that it can fend off several assaults and provide a wide variety of security features. We also showed the correctness and semantic security of the proposed protocol using BAN logic (Burrows-Abadi-Needham logic) and the ROR model (Return on Revenue). With the help of the simulation tool for AVISPA.

Automated Validation of Internet Security Protocols and Applications), we evaluated the proposed protocol's resilience to replay and MITM (man in the middle) attacks. The recommended protocol may also provide more security features and significantly reduce the computational cost of the vehicle as

compared tothe current procedures. Last but not least, we demonstrated the viability of the recommended protocol using NS-3 (network simulator). We will use the recommended strategy in subsequent work and create a more effective technique while taking into consideration the overhead in the RSU imposed by the block consensus.

6.REFERENCES

1. Seunghwan Son , Joonyoung Lee , Yohan Park , Youngho Park , Member, IEEE, and Ashok Kumar Das , Senior Member, IEEE "Design of Block chain-Based Lightweight V2I Handover Authentication Protocol for VANET"IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, VOL. 9, NO. 3, MAY/JUNE 2022..
2. Chao Lin, Xinyi Huang, and Debiao He " EBCPA: Efficient Block chain-based Conditional Privacy- preserving Authentication for VANETs" 0, IEEE Transactions on Dependable and Secure Computing. Citation information: DOI 10.1109/TDSC.2022.3164740,
3. HAOWEN TAN AND ILYONG CHUNG Department of Computer Engineering, Chosun University, (Gwangju 61452, South Korea. "Secure Authentication and Key Management With Block chain in VANETs "Received December 11, 2019, accepted December 21, 2019, date of publication December 27, 2019, date of current version January 6, 2020
4. X. Liu, H. Huang, F. Xiao, and Z. Ma, "A block chain-based trust management with conditional privacy-preserving announcement scheme for VANETs," IEEE Internet Things J., vol. 7, no. 5, pp. 4101– 4112, May 2020.
5. AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment Mohammad Wazid , Member, IEEE, Palak Bagga, Ashok Kumar Das , Senior Member, IEEE, Sachin Shetty , Joel J. P. C. Rodrigues , Senior Member, IEEE, and Youngho Park , Member, IEEE.