International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

IJIEMR Transactions, online available on 18th October 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13 &issue= Issue 10

DOI:10.48047/IJIEMR/V13/ ISSUE10/30

Title: " BLOCK CHAIN BASED EFFICIENT ACCESS CONTROL WITH HANDOVER POLICY IN IOV-ENABLED INTELLIGENT TRANSPORTATION SYSTEM"

Volume 13, ISSUE 10, Pages: 193- 199

Paper Authors
MS.H.BHAGYA LAXMI, SAKSHI, JOSHNA, INDHU

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

BLOCK CHAIN BASED EFFICIENT ACCESS CONTROL WITH HANDOVER POLICY IN IOV-ENABLED INTELLIGENT TRANSPORTATION SYSTEM

MS.H.BHAGYA LAXMI, SAKSHI, JOSHNA, INDHU

[1]Assistant Professor, Department Of Electronics And Communication Engineering, Malla Reddy Engineering College For Women, Hyderabad.

[2,3,4]Ug Scholar, Department Of Electronics And Communication Engineering, Malla Reddy Engineering College For Women, Hyderabad

ABSTRACT

Recent advances in Internet technology and IoT devices have facilitated researchers to foster a wide range of Intelligent Transportation Systems (ITS) that improve the quality of automated transportation by addressing real-time safety and traffic management issues. The participating ITS agents, such as smart cars and roadside equipment, are required to communicate urgently through an open (unsecured) wireless channel in an unattended setting. To address the security issues, several vehicle-tovehicle (V2V) and vehicle-to-infrastructure (V2I) authentication and access control protocols have been proposed in recent times. However, fast-moving vehicles need to set up frequent authentication with different roadside units, which induces high computation and communication overheads. Consequently, it becomes a bottleneck for the resource-limited vehicle onboard unit devices. As the blockchain supports decentralized storage with data integrity and transparency, in this article, we design a secure and lightweight Internet of Vehicles (IoV)-enabled blockchain-based access control protocol with a handover authentication facility (we call it BACHP-IoV, in short). The handover authentication mechanism exploits no computation-costly cryptographic primitives. Once the transactions or messages have been securely gathered by a roadside unit (RSU), RSUj , residing in a group of vehicles V hi, will form a partial block, which is later forwarded to a cloud server node

I.INTRODUCTION

OVER the last few years, rapid technological development and research have been carried out in the fields of the Internet of Things (IoT), smart grids, smart city-based applications, etc. Communication among various things, such as smart devices, vehicles, and so on, is an inherent part of Information and Communications Technology (ICT)-based infrastructures. These ICT-based infrastructures can play a useful role in e-health care, automatic transportation, and various other fields. Intelligent Transportation System (ITS) is one such application area that is growing in popularity. ITS facilitates the sensing, analyzing, and controlling of a safe and reliable driving experience by protecting responsible entities and messages from various cyber attackers [1], [2], [3]. Vehicular ad hoc networks (VANETs) are a key part of the intelligent transportation systems (ITS) framework. VANETs are created by applying the principles of mobile ad-hoc networks (MANETs) to the domain of vehicular networks. The VANETs system can be represented as a two-layer architecture. The upper layer is made up of trusted authority (T A) and the lower layer is made up of roadside units (RSU) and vehicles. Each vehicle is equipped with an onboard unit (OBU). Typically, an ITS consists of various RSUs. An RSU is in charge of validating the signals sent by the moving vehicles that make up its group or cluster, which is established dynamically. The OBU is sometimes regarded as a transportable unit. An OBU can function whether a car or a person is moving or stationary. VANETs consist of various entities, where the vehicles are connected in an ad-hoc manner for exchanging data with each other. Generally, VANET uses different technologies to ensure a non-identical way of communication like vehicle to vehicle (V2V), vehicle to road-side unit (V2RSU), and road-side unit to the cloud server (RSU2C) [4], [5]. On the other side, the Internet of Vehicles (IoV) spans a larger network that involves various entities, like “humans”, “smart things” and other “heterogeneous networks”. Thus, IoV provides real-time information exchange on the roads in a smart city among the “deployed vehicles and sensors”, “vehicles and vehicles”, “vehicles and roads”, and “vehicles and personal devices” with the help of various wireless communication technologies [6]. Blockchain technology facilitates an immutable, decentralized, secure, and anonymous way of storing data, providing robustness against various types of information security-related attacks[7], [8]. As a result, in recent years, the use of blockchain for smart vehicles that enable ITS communication has become a natural choice [9]. In a real-life scenario, due to the continuously increasing number of vehicles, the traffic load might exceed the capacity of the existing infrastructure. Such a system authorizes the formation of secure data management and sharing techniques for data at rest or in motion. In general, VANET uses various non-identical ways of communication like vehicle to vehicle (V2V), vehicle to a roadside unit (V2RSU), and roadside unit to the cloud server (RSU2C) [4], [5]. The use of blockchain technology has become more common in recent years across a range of applications. Singh and Jindal devised the blockchain-based strategy of the independently edge-envisioned ecosystem[10]. Here, adjacent edge devices are employed to generate the decoupling blocks on the blockchain. This could offer a safe cryptosystem for smart healthcare in a smart city [11]. Zhou et al. [12] introduced a blockchain-based volunteer edge cloud for IoT applications to solve the growing issues of large-scale IoT applications. Their suggested approach increases the adaptability of software development while reducing the complexity of IoT devices. Energy trading calculation, which is done using real-time processing, is one of the key requirements of the tactile Internet. To overcome such challenges, Choo et al. [13] proposed an energy trading scheme for electric vehicles (EVs) using blockchain, which can perform securely. This scheme also ensures resilience against a single point of failure. Inherently, IoV-enabled ITS requires frequent message communications among various entities of the system through insecure wireless channels. This allures potential adversary agents to launch several active and passive security attacks like eavesdropping, revealing, modifying, deleting, or intercepting communicated messages [14], [15]. In a real-time scenario of an ITS, the presence of such security vulnerabilities may lead to several catastrophic results. Thus, the guaranteed enforcement of detection and prevention of such security attacks is an indispensable requirement. Inherently, IoV-enabled ITS requires frequent message communications among various entities of the system through insecure wireless channels. This allures potential adversary agents to launch several active and passive security attacks like eavesdropping, revealing, modifying, deleting, or intercepting communicated messages [14], [15]. In a real-time scenario of an ITS, the presence of such security vulnerabilities may lead to catastrophic results like fatal accidents, etc. Thus, the guaranteed enforcement of detection and prevention of such security attacks is an indispensable requirement. Very recently, the blockchain has been used as a cuttingedge technology to address a set of intriguing issues in several IoV-based applications. Vishwakarma et al. [16] used the "modified practical byzantine fault tolerance (mPBFT) consensus algorithm" to design a blockchain-based security protocol for secure communication and storage in a software-defined network (SDN)-enabled IoV. Their experimental results show that the storage, computation, and communication overheads are noticeably low as compared to those for the other stateof-the-art schemes. Lin et al. [17] proposed a new parkingsharing network using the blockchain to build a decentralized, but trustworthy network. Their proposed scheme exploits the "theory of planned behavior (TPB)" to find an effective way to get timely information about available parking lots. For VANETs, Zhou et al. [18] proposed an efficient certificateless conditional privacy-preserving authentication (CPPA) scheme. They indicated and proved the security loopholes of Ali et al.'s protocol [19]. The authors experimentally demonstrated the efficiency of their scheme over the existing solutions, in terms of verification, signing, and bandwidth requirements.

II.LITERATURE SURVEY

L. F. Herrera-Quintero, J. C. Vega-Alfonso, K. B. A. Banse, and E. Carrillo Zambrano, "Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture," IEEE Intell. Transp. Syst. Mag., vol. 10, no. 2, pp. 17–27, Summer 2018

Traffic congestion has been an actual problem in large cities, causing personal inconvenience and environmental pollution. To solve this problem, new applications for Intelligent Transportation System (ITS) have been created, to monitor actual traffic conditions. Therefore, fast, reliable and safe systems are desirable for creating a real intelligent transportation environment. Deep learning algorithms have been proposed for a better understanding of traffic behavior from a security-related perspective. Thus, we aim to maximize the safety problems using a deep learning algorithm, where a novel policy gradient model is presented for detecting vehicular misuse. The proposed model uses a triple network replay algorithm, maximizing the network convergence speed. Three networks are selected to optimize the policy network variables. Finally, the replay algorithm is partitioned with the aim of obtaining a faster model. Simulations on a real urban map are performed in a scenario with the integration of 5G or 6G networks. An architectural model for the integration of a Vehicular Ad-hoc Network (VANET) and cellular networks is determined in software-defined networking (SDN). The results show that the accuracy prediction of the proposed system presents better performance compared to related studies, where the proposed model increases its convergence speed and cumulative reward. Thus, the ITS improvement by the proposed deep learning algorithm increases the prediction accuracy, and reduces the transmission delay, treating the traffic path according to the congestion. About 8 million traffic accidents occur every year, causing an injury to 7 million people [1]. Additionally, there are many problems that originate in traffic, including car crashes and traffic congestion, decreasing the population's productivity by 2% [2]. Thus, 90 billion hours are lost due to traffic problems around the world [2]. Additionally, 220 million metric tons of carbon are generated by vehicular transportation [3]. As a result, these problems decrease the people's quality of life [4], [5], [6].

Many related studies for intelligent transportation system (ITS) have been developed [7], [8], [9]. ITS is commonly based on different technologies, such as repositories of big data, machine and deep learning algorithms, and communication technologies [10]. Thus, ITSs are responsible for collecting actual traffic, vehicle, and road data, providing a real-time monitoring traffic service [11].

In the last decade, ITS solutions have been investigated, and AI algorithms have been developed in several research areas [12], [13], [14], [15], [16], [17]. Some improvements have been obtained in AI algorithms, mainly in relation to reinforcement learning [18], [19]. Some studies have explored AI algorithms in discrete action space. However, the action space is continuous or very large, the algorithms based on discrete action spaces do not present good results. Hence, algorithms based on reinforcement learning to be used in continuous action have been studied [20], [21], [22].

Methods that study the actions in real-time space scenarios for analyzing the policies in a direct model [23], [24] have been developed. Hence, some policies are determined through a loss variable, and the connection of agents and reservoir surroundings occur given a compensation for each interaction. A deep deterministic policy gradient (DDPG) is presented in [25], and the proposal described using a deep Q-learning approach with a continuous action domain to simulate physics tasks, that were applied to an ITS system. Another proposal improved the DDPG algorithm using two layers of neural networks [26]. The method introduces a fuzzy algorithm and the Broyden–Fletcher–Goldfarb–Shanno (BFGS) [27] algorithm using the Armijo–Goldstein model [28], improving the efficiency of learning and the convergence of the two layer neural networks without exploring an ITS scenario. Another study was proposed in [29], where the segmented experience was studied with the aim of improving the training efficiency; the study demonstrated high training stability and it was tested in a simulator containing 3D vehicle scenarios. However, it only addressed the training stability. In [30], the learning curve theory is used in the introduced model to obtain a more efficient result on the replay action. In [31], an improved algorithm is proposed, in where the algorithm uses data entropy based on weights. The study showed that the proposal algorithm caused a speed increment to obtain the final model, improving its performance in terms of speed training and efficiency. Another algorithm is proposed in [32], which uses the DDPG and an improvement of the experience replay, which is based on prioritization steps. Thus, the proposal obtained a time reduction for training in relation to similar works, considering an autonomous driving scenario.

The emergence of new network technologies, such as the 5th generation (5G) and 6th generation (6G) have demanded new services through vehicular networks; therefore, solutions that consider the integration of these new generation technologies with vehicular networks are necessary [33], [34], [35]. In [36], possible incidents in vehicular traffic with 6G

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

networks are studied. Thus, studies that deal with ITS scenarios supported by 5G and 6G networks are relevant.

The vehicular ad-hoc network (VANET) [37] is represented by wireless technology to be used in ad-hoc networks in mobile vehicles, such as vehicle-to-vehicle (V2V) [38], [39], vehicle-to-pedestrian (V2P) [40], and vehicle-to-network (V2N) [41] or vehicle-to-infrastructure(V2I) [42] to enhance road safety. It can also provide short message service (SMS), Internet service, image and video based services, and other data using new network infrastructures [43], as depicted in Fig. 1, in which heterogeneous networks (HetNet) are considered [44]. However, a framework for security problems that considers 5G [45] networks and future 6G network models [46] is missing. The scenario used in this work involves information retrieval via 5G or 6G models, using a VANET for information dissemination, and the software-defined network (SDN) provides interoperability between vehicular communication (V2X) [47], [48], [49] and device-to-device (D2D) communication [50]. Considering the ITS scenario presented in Fig. 1, our proposed solution demonstrates our intent to improve the ITS security aspects by considering a high accuracy and a fast response, reducing the transmission delay, and treating the traffic route according to the congestion. For analyzing the performance, the accuracy, data transmission, and the traffic changes are studied with the aim of analyzing a complete real-time scenario.

III.EXISTING SYSTEM

VANET is an autonomous & completely self-organizing wireless communication network. In this network the cars are called dynamic nodes and Infrastructure is called Static node which involve themselves as servers and/or clients for exchanging & sharing information. Various researchers are working on VANET to find the solution for current traffic congestion problem. Many methods are used to reduce the traffic congestions detection and management using VANET**.**

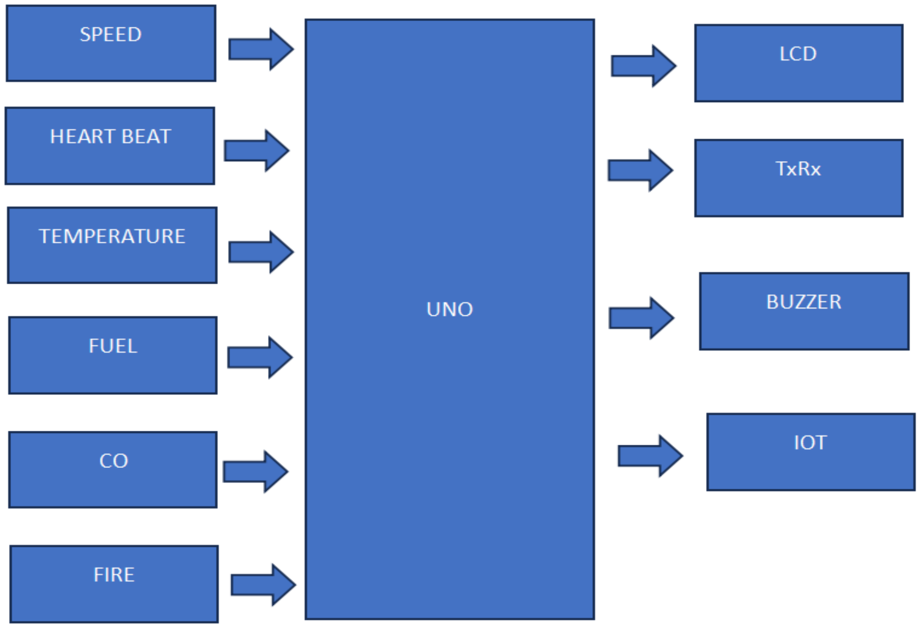
IV.PROPOSED SYSTEM

The expeditious increase within the vehicle popular round the globe, particularly in India has prompted inquire about within the specialty of Intelligent Transportation System (ITS). V2V communication is more practical than current automotive original equipment manufacturer embedded system for lane departure, adaptive controller, blind spot detection, rear parking sonar and backup camera because V2V technology enables ubiquitous 360-degree awareness of surrounding threats. The most objective of the project is to alert the during force when he closes to the front vehicle. The thought is that, if collision avoidance systems can work between vehicles, then every car on the road are safer by avoiding accidents before they will ever happen. The importance of autonomous or semi-autonomous vehicles for intelligent installation is increasing. V2V technologies are simple to implement primarily thanks to their reliance on wireless communication. Having low power and knowledge rate, zigbee happens to be utilized broadly in V2V communication. During this paper, propositions are initiated towards enhancing road safety and handling traffic holdup

.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Block diagram



V.CONCLUSION

In this article, we design a new blockchain-based access control scheme with a handover policy for an IoV-enabled ITS that is not only efficient in communication and computation, but also provides superior security and more functionality attributes as compared to other competing schemes. The proposed scheme allows for both dynamic vehicle addition and vehicle revocation phases. The stored records in the blockchain help in the inter-RSU vehicle authentication handover process. The practical demonstration of the proposed scheme using the NS-3 simulation shows the impact on various network performance parameters. In addition, through the blockchain simulation, we have also shown the computational time needed for the proposed scheme by varying the number of transactions in blocks and the number of blocks mined in the blockchain network. Future research work includes developing a real testbed experiment for implementing the proposed scheme.

VI.REFERENCES

[1] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, “Big data analytics in intelligent transportation systems: A survey,” IEEE Trans. Intell. Transp. Syst., vol. 20, no. 1, pp. 383–398, Jan. 2019.

[2] O. Pribyl, P. Pribyl, M. Lom, and M. Svitek, “Modeling of smart cities based on ITS architecture,” IEEE Intell. Transp. Syst. Mag., vol. 11, no. 4, pp. 28–36, winter 2019.

[3] L. F. Herrera-Quintero, J. C. Vega-Alfonso, K. B. A. Banse, and E. Carrillo Zambrano, “Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture,” IEEE Intell. Transp. Syst. Mag., vol. 10, no. 2, pp. 17–27, Summer 2018.

[4] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proc. IEEE, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[5] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computingbased internet of vehicles deployment," IEEE Internet Things J., vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[6] R. Gasmi and M. Aliouat, "Vehicular ad hoc NETworks versus internet of vehicles - A comparative view," in Proc. Int. Conf. Netw. Adv. Syst., 2019, pp. 1–6.

[7] A. Vangala, S. Roy, and A. K. Das, "Blockchain-based lightweight authentication protocol for iot-enabled smart agriculture," in Proc. IEEE Int. Conf. Cyber- Phys. Social Intell., 2022, pp. 110–115.

[8] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-Based authentication protocol for supply chains in 5G mobile edge computing environment," IEEE Trans. Ind. Informat., vol. 16, no. 11, pp. 7081–7093, Nov. 2020.

[9] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, "Blockchain-based energy trading in electric-vehicle-enabled microgrids," IEEE Consum. Electron. Mag., vol. 9, no. 6, pp. 66–71, Nov. 2020.

[10] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edgeenvisioned IoT-Based healthcare monitoring," IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 491–499, Feb. 2021.

[11] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," IEEE Commun. Mag., vol. 56, no. 4, pp. 24–32, Apr. 2018.

[12] M.-T. Zhou, F.-G. Shen, T.-F. Ren, and X.-Y. Feng, "Blockchain-based volunteer edge cloud for IoT applications," in Proc. IEEE 93rd Veh. Technol. Conf., 2021, pp. 1–6.

[13] K.-K. R. Choo, R. Chaudhary, A. Jindal, G. Aujla, S. Aggarwal, and N. Kumar, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," Comput. Secur., vol. 85, pp. 288–299, 2019.

[14] S. Chatterjee and S. Roy, "An efficient dynamic access control scheme for distributed wireless sensor networks," Int. J. Ad Hoc Ubiquitous Comput., vol. 27, no. 1, pp. 1–18, 2018.