Preserving Privacy using Blockchain Technology in Autonomous Vehicles

Meghna Manoj Nair[1], Amit Kumar Tyagi[1,2] [0000-0003-2657-8700]*
[1]School of Computing Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
[2]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India
mnairmeghna@gmail.com, amitkrtyagi025@gmail.com
*Corresponding author: amitkrtyagi025@gmail.com

Abstract. With transportation and automation being some of the major fields of interest in research in the current world, Autonomous Vehicles (AVs) and Intelligent Transportation System (ITS) have been taking the spotlight especially in the current era where mobilization and automation are proliferating. One of the major fields of research and development in the transportation field is the networking of various smart vehicles together for enhanced data acquisition and automated driving. This paper talks about one of the major challenges which is commonly found in developments in the related field which is privacy preservation. Privacy is a term which describes the safety and security of the information retrieved from the users for computation. When developing applications which indulge in automation and networking, privacy is one of the major parameters to be considered because there are high chances of attacks, data breaches and leakages. This paper discusses a possible solution of integrating the Blockchain technology with the systemic framework for encrypting and hashing the data and securing the information from any sort of mishaps and glitches. The paper also throws insights on ITS, AVs and Internet of Vehicles (IoV) and how Blockchain can be integrated to the ITS framework.

Keywords: Privacy, blockchain, autonomous vehicles, intelligent transportation system, encryption, security

1. Introduction

Automation and autonomous systems have been taking over in various fields over the years, especially in the transportation sector where intelligent and smart network systems are taking shape. Autonomous vehicles are those automated vehicular systems which enable the vehicle to perform required and necessary actions and decisions on its own without the interference of any humans. This is made possible by using various sensors and tech gadgets to sense the surrounding environment and take necessary actions. In fact, these driverless systems extract the benefits of a completely automated vehicular technology to ensure that the vehicle is responsive and decisive to all the conditions just like how a human would. Autonomous vehicles itself have classification, let alone the other various categorizations for the types of interconnected transportation networks. There are mainly six different levels of automation as mentioned below [1]:

- Level 0: human drivers are completely in charge of the decisions and controls of the car
- Level 1: the Advanced Driver Assistance System (ADAS) complements the human driver in terms of maneuvering controls or with regards to the speed system of the vehicle

- Level 2: the ADAS is autonomous enough to ensure that it can take care of maneuvering and controlling the speed system in most of the conditions. However, it requires the physical presence and attention of the driver at all times to carry out the remaining tasks when required
- Level 3: the Advanced Driving System (ADS) is capable enough to perform automated driving in most of the conditions however, it needs the human driver to regain control in incidents where the system can't take effective decisions
- Level 4: the ADS has the ability to perform the tasks independently and doesn't require any human intervention is some of the situations and conditions
- Level 5: the ADS is completely automated and is autonomous enough to comply and execute all tasks independently without any human interactions for assistance. In majority of the cases, 5G technology is integrated with the network to establish connections between the vehicles on the road and the other sensory devices in the transportation sector.

Apart from the innovation and advanced technologies being utilized in vehicles, extensive researches are being conducted in developing systemic frameworks that are capable of interconnecting vehicles among themselves, with the ground station, On-Board Units (OBUs), etc. paving for an Intelligent Transportation System (ITS). This would not only incorporate mobility to a great level, but would also establish stable intercommunication techniques like Vehicle to Vehicle (V2V) communication, providing a larger coverage for interconnection [2]. As shown in Fig. 1, ITS is a framework that is a combination of users/drivers, roads and traffic control systems and vehicles which are integrated using enhanced communication technologies and Internet of Things (IoT). Each of the components of such a system work towards achieving the common goals of ensuring safety, improvising traffic efficiency, convenience and mobility, and uplifting the industrial presence. Fig. 2 describes the working scheme and the interaction of the various nodes involved in an ITS. Road Side Units (RSU) are an integral part of any ITS as they indulge in sensing and collecting information pertaining to the vehicles and other nodes and transmits them to the control centers and authorities. GPS systems are used to track the location and position of various vehicles and the vehicles interact with each other either by V2V communication, vehicle to roadside communication and inter-roadside communication.

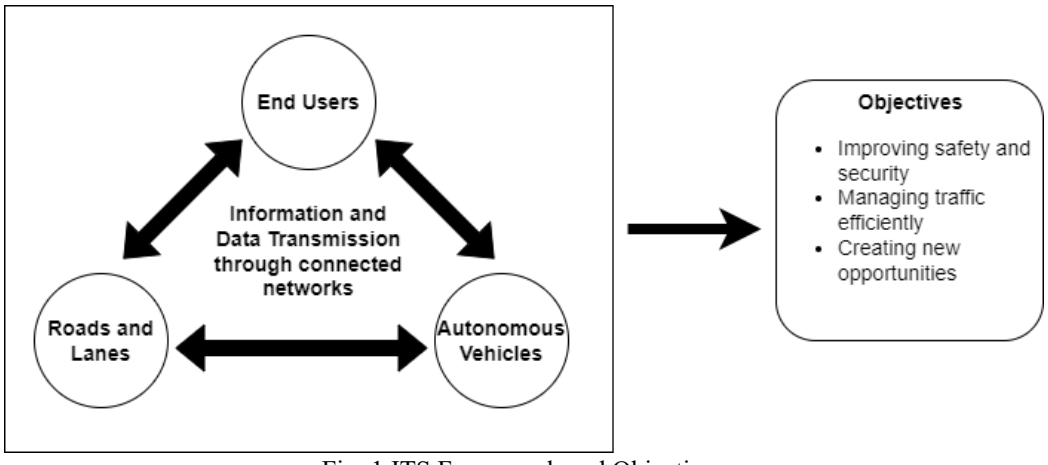

Fig. 1 ITS Framework and Objectives

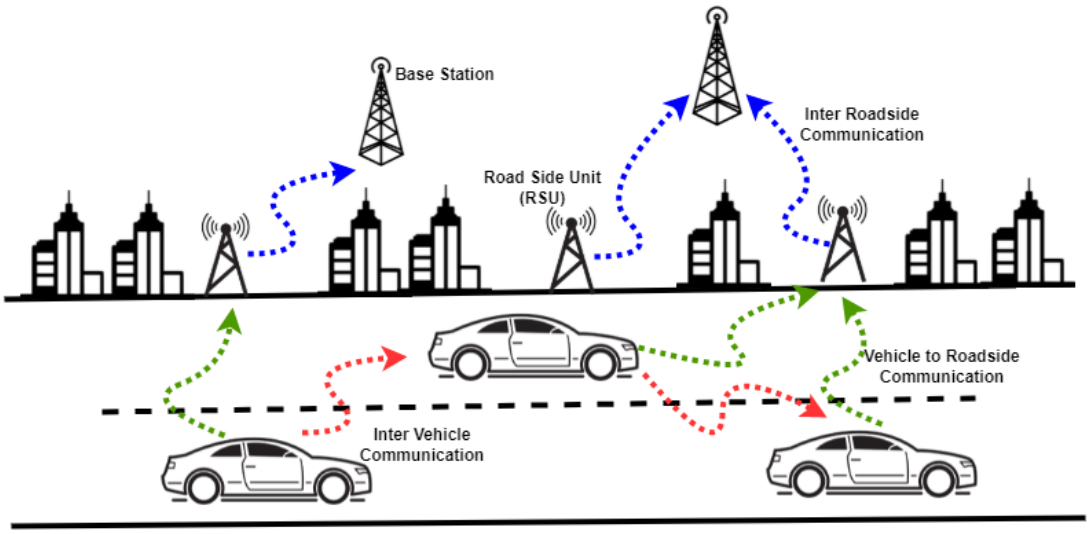

Fig. 2 Working schemes and Nodular interaction of AVs and ITS

1.1 Autonomous Vehicles and Intelligent Transportation System

In a world where automation and technological advancement have been taking over, Autonomous Vehicles (AVs) is a perfect fit. AV, often called as driverless vehicle, is a vehicle which has the necessary technology and mechanisms integrated to operate and execute functions on its own without the presence of any human interference. The vehicle would be curated in a way such that it would be able to sense its surroundings and maneuver the vehicle on its own without much of human assistance and many of them incorporate various feedback mechanisms to ensure that the vehicle learns from the various challenges it's being exposed to while in action. These type of futuristic vehicles and automation system is one of the major fields f research and extensive research is being carried out with regards to the various aspects of the same. One of the major attractions of AVs is the various advantages it showcases. One of the major advantages it showcases is the possibility of providing increased safety during travel and reduced risks of accidents. Thousands of deaths occur each year due to accidents during travel, mainly due to reckless and rash driving by drivers. Using AVs will ensure that road safety rules and guidelines are being followed and that the risk of accidents are reduced to a great-extend. Most importantly, AVs prove to be a complementary aid for all those users who face difficulty in driving due to factors like age, physical disabilities, etc. [13] When a number of AVs connect and interact with each other, it is often considered under the broader perspective of Intelligent Transportation System (ITS). However, just like how every coin has two sides, these massive strategies and frameworks are highly questionable when it comes to safety and security of data and its extremely essential to ensure that the users details and confidential information are safe and aren't breached or leaked. Blockchain is one of those technologies which can surely provide safe data transmission by utilizing a distributed ledger technique.

As an organization of this work, the main motive of this work is to showcase the various aspects and perspectives of the security and privacy sector of AIVs and ITS [3]. Section 2 of this paper elucidates some of the existing works and researches in this field as literature review while Section 3 focuses on the safety approaches and parameters for such automated vehicles and its systems. Section 4 discusses about scope / importance of **Internet of Vehicles (IoVs) in Today's Smart Era from an user's perspective.**

Following this Section 5 talks about the possible issues, risks and challenges (including security values) in VANETs and ITS while Section 6 discusses about proposed work whereas section 7. throws light on simulation results. Section 8 talks about future work/ opportunities for future in intelligent vehicles followed by the conclusion.

2. Literature Review

Autonomous Vehicles being one of the highly researched fields, numerous authors and researchers have portrayed their work on the same through surveys, virtual experiments and analyses. In [3], the authors have proposed a scheme for privacy preservation for AV's and ITS in an urban area wherein the transmission of data and information from one node to the other within the network is secured using Emergent Intelligence (EI) technique. EI is a robust technology which provides automation, versatility, flexibility, etc. The Crypto++ package has been used to implement the same. The authors of [3][4] have put forth a different perspective on preserving the security and privacy of AVs in ITS using the concept of grouping. In the proposed model, they have put forth a hierarchical layout of the ITS framework with the following layers: Sensor/actuator, Vehicle, AVs Group, and Cloud respectively. The mechanism used for preserving privacy is to group the AVs in the vehicular layer with a certain leader who will be the only node communicating with the RSUs from the group. One of the important metrics considered for performance analysis and other approaches is the size of the group and the major restriction is that the chosen leader must not be restrictive in terms of power, storage, energy etc. A permutation scheme is used to encrypt the data bind transmitted from the group leader to other nodes, RSUs etc [5]. The authors of [6][7] have put forth an autonomous privacy preservation mechanism which involves the AVs to connect with the central node/authority only once after which, the connections will be renewed within frequent intervals without necessitating a permanent contact with the central node. It incorporates a pseudonym like authentication framework wherein the central node would send credentials to the subordinate AVs and this central authority node can revoke the users/driver's anonymity without the need to establish direct contact with the vehicular node. On the other hand, in [8], the researchers have suggested a framework which integrates the Paillier Crytosystem in accordance with the Chinese Remainder Theorem to gather and collect the data from various sections of the road transport system in order to save bandwidth and additional authentication requirements [9]. This system is majorly autonomous as it allows its users/drivers to generate the private/public key pair for their communication needs. One of the other proposals for privacy preservation is in the field of Cooperative – ITS (C-ITS). C-ITS is a transportation framework which involves numerous stations and points which can detect their surrounding environment and interact with each other. In order to preserve privacy, four main parameters are taken into consideration: anonymity, unlinkability, pseudonymity, and unobservability [10][11]. These strategies ensure that the stations are up to date with the pseudonyms being generated by the central node from a given pool and secures the interaction and transmission of data from nodes to local stations respectively [12].

3. Safety Approaches for Autonomous Vehicles and Intelligent Transportation System

Guarantying safety to the users of a fully autonomous vehicles or an ITS framework is one of the major challenges posing a hinderance to the conventional standards followed for similar software. One possible way is to propose a standard completely based on assigning particular scopes for the safety nodes in the system. It is always important to have a feedback system to ensure that the system keeps learning from the new experiences and challenges it's being exposed which in turn improvises the decisive skills of the system. Some of the conventional standards which can be adopted include:

- ISO 26262: This is one of those standards that are capable of ensuring the safety of integrity levels in the autonomous vehicle by adopting a V based process model and by addressing the software and hardware requirements at varying integrity levels. In simpler terms, it mainly helps the system to be free from any type of faulty designs and helps in developing mitigation plans in case of a fault.
- ISO 21448: This is an extension of the previous standard which is used for ensuring the safety of the intended functionalities of the modules within the system. It covers handling situations of predicting misuses and issues which may arise during user interaction and focuses on elaborating over the operational necessities.

Apart from the above-mentioned safety standards, there are various other safety standard approaches like IEC 61508, SAE ARP 4745A, SAE ARP 4761, etc. IEC standard mainly covers the aspects of chemical process supervision and control. While SAE standards cover the those in terms of aviation [14].

4. Role of Internet of Vehicles (IoVs) in Today's Smart Era

With Internet of Things (IoT) taking over the new era in nearly every field, it has had a massive impact in the transportation sector too resulting in the enhancement of traditional Vehicular Ad-Hoc Networks (VANETs) through IoV. IoV is one such aspect which guarantees promising results and innovative solutions to various problems and ideas in the same [15]. In fact, IoV is one of the best ways to interconnect various vehicles together in a holistic environment [16]. In simple words, IoV is a type of distributed network which complements the usage of data generated by AVs, ITS and VANETs with the main aim of allowing the interconnected vehicles to communicate and exchange data with each other and with the users, drivers, ground station, etc. [17]. Dwelling deeper into the field of IoV, there are five main categories of network communication [18]:

- Intra-vehicle: These systems are responsible for supervising and monitoring the working and performance of the internal components. This is achieved through On-Board Units (OBUs).
- Vehicle to Vehicle (V2V): These systems are useful in complementing the wireless data transfer strategies with information regarding the velocity and location of surrounding vehicles.
- Vehicle to Infrastructure (V2I): These systems are responsible for data transmission through wireless means for exchanging data among vehicles and respective Road Side Units (RSU).
- Vehicle to Cloud (V2C): They ensure that the systems permit the vehicles to gain access to extra data required through the internet via supportable Application Programming Interfaces (APIs).

IoV has a plethora of benefits to it apart from just a mediator platform used for exchanging data and information from one node to another within the transportation network. However, when IoV is integrated with AVs and ITS, it potentially supports various functions like those of intelligent traffic management, dynamic information services. Intelligent vehicle control, etc. Further, the most daunting fact, that millions of people are injured and face death due to traffic accidents and spend hours in traffic jams because of the lack of proper management systems. However, with IoV, there are many new applications and opportunities that provide great services to the drivers, users and the entire network to have a smooth and efficient flow. Furthermore, IoV can be accounted as one of the base foundational components for opening up various service providers like parking spot identifier services, real-time traffic information services, location-based services, etc. [19]. Fig. 3 shown below portrays the architecture of IoV which has around 7 cumulative layers. The first layer contains the various possible options which support the interaction with the users via User Interaction surfaces. The next layer is the Data Acquisition layer which is responsible for collecting data from numerous components and sources including those of sensors, navigational systems, traffic control systems, etc. Following which is the Data Filtering and Preprocessing layer which

helps to analyze and filter out any noisy data from the collected set which is then passed onto the communication layer that handles the passage of data by choosing the appropriate network choice. Control and management layer handles the different service providers of the network and takes care of the various policies to be included. The processing layer analyzes the huge volume of information being passed down by utilizing the various types of cloud computational structures. And finally, the security layer is responsible for authenticating and validating the data transmission and communications occurring and has direct access to all the layers.

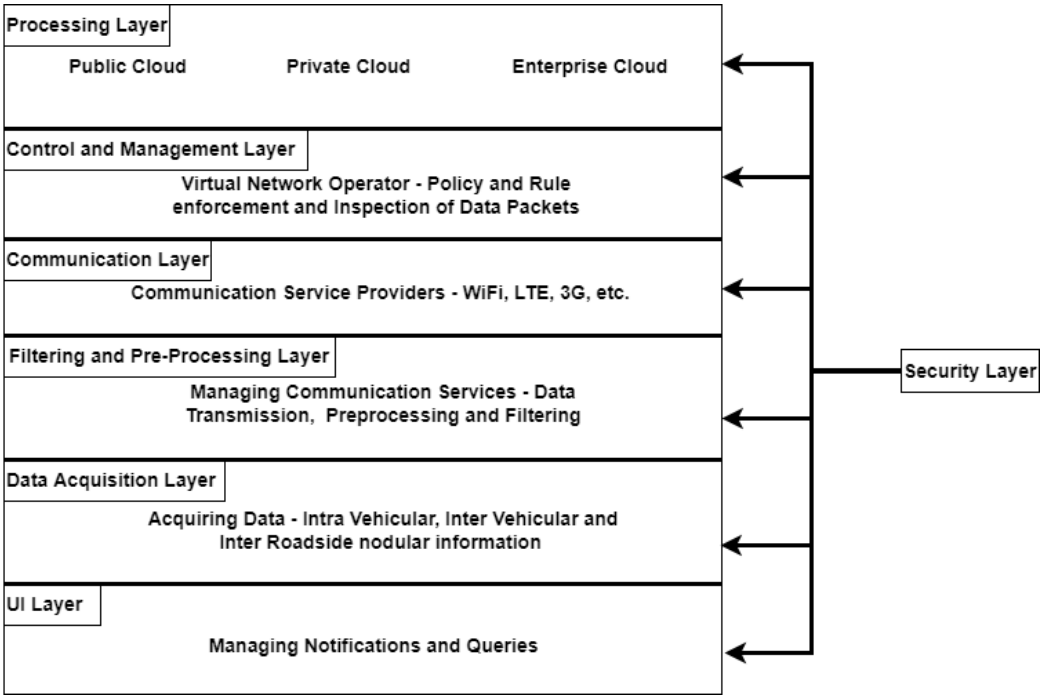

Fig. 3 Seven Layer Architecture of IoVs

5. Critical Challenges and Open Issues towards Autonomous Vehicles and Intelligent Transportation System

AVs and ITSs which seemed to be a dream for many over the years, is now paving its way to reality. However, this too has a number of challenges and issues which needs to be overcome when considering its implementation on a large scale. Considering the various domains that AVs can possibly impact, it has challenges and bottlenecks which range from social to that of the technical field. One of the major challenges that stands out from the rest is the possibility of system crashes or failures due to any tiny bugs or errors in the respective software component of the system [19]. These systemic errors can ultimately lead to dangerous accidents and injuries. Further, the fact there is extensive interaction between the logical decision-making system of the autonomous system itself indicates that there need to be clear definition of boundaries with respect to the private and public information of the users which are extracted [20]. Moving over to the technical challenges faced by the implementation of these autonomous systems. Hardware components pose significant challenges when it comes to the case of wireless interactions and connectivity because in case of any fault in any of the devices, there are chances that it affects the entire system adversely. One of

the other thoughts to ponder upon is in terms of the energy requirement and managements. Lack of suitable and viable energy management can be a potential bottleneck for the growth of AVs [21].

6. Proposed Solution

The main objective of the paper is to device a system that would preserve the privacy and information of the users utilizing the services of AVs and ITS framework. Especially in the beginning stages, it's very essential that the users support and rely on the services and the device and the best way to do it is by providing them reliable and safe service assurance. One of the topics which has taken the spotlight when it comes to securing data is Blockchain. Blockchain is very similar to a database which works on distributed grounds being shared commonly by the various nodes and components of the given network. The data is stored in a digital format. One of the major applications of Blockchain has been in the field of cryptocurrency and bitcoins because it is one of the safest ways to conceal the transactions taking place by making it resilient to attacks and data leakages. In fact, the major advantage of the Blockchain concept is that it promises the security and privacy preservation of any record maintained within it without the requirement or interference of any external parties. Even though Blockchain is compared to that of a database, they're quite different from each other, especially in terms of how the data/record is being stored. The information/record is stored in the form of group like structures called blocks which have a certain capacity. Each time a record is being entered, it is stored in a block in the Blockchain and the block will continue storing information until it's full. Once it reaches its capacity, it will be closed and will be linked to the next block in line, ultimately leading to a chain of various blocks [22, 23, and 24]. As shown in Fig. 4, the blocks not only store information being entered but also consists of details like index, previous hash, hash, timestamp, data. Hash and previous hash are basically values which are produced as a result of the hash function which encrypts the data being stored in the block. In fact, these values are the encrypted products of the hashing algorithm used for the curation of the respective Blockchain. The main advantage of the hash is that it always generates a distinct value. Timestamp stores the time at which the block was created and data stored the records being entered. Previous hash stores the hash value of the previous block to get the blocks linked in an orderly fashion.

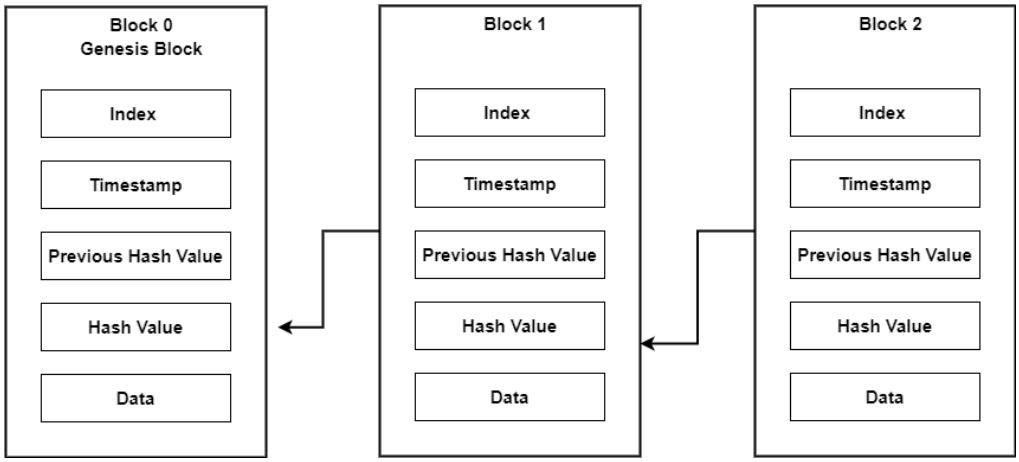

Fig. 4 Connected blocks and their attributes forming a Blockchain

The aim of the proposed solution is to integrate Blockchain with the frameworks of AVs and ITS, which is definitely a feasible, viable and secure option. All the devices and components which are connected to the various sensory nodes need to integrated with a client-side application while the components in the ITS or the corresponding network framework AVs are connected to, need to be curated in a resilient and secure way such that they are safe from some of the major attacks. The network framework mainly contains the components which would be integrated with the server-side application. Each time some information is gathered from the sensors by the functional modules on the client side, they are hashed and stored in a block. This continues until a Blockchain is developed by chaining the blocks together based on their hash values and will ensure that the data is stored in a safe and preserved environment, especially during data transfer. The server-side components then easily access these details and information for necessary computations. Apart from the server and client-side applications, the Blockchain will be majorly decentralized and will be maintained and regulated by one of the trusted nodes to allow easy access to information by the client and server-side nodes. Having said this, integration of Blockchain is what needs to be looked into. The users of the AVs and ITS will be in connection with the server consistently and necessary information passing will take place. The Blockchain will be open to information extraction and information addition from both the client and server sides of the systemic model. The data being stored in the Blockchain will be fully hashed and encrypted with the help of suitable encryption keys. The point to be noted here is that the encryption technique used is an extremely powerful and resilient one making sure that it seals the data from any breaches or attacks.

Simulations were conducted to visualize and get deeper insights into the working of a blockchain using Anders Brownworth's simulator. The dataset used has been pulled from Kaggle and contains the details of the date, time and the number of vehicles spotted by an automated traffic control system. Firstly, a block simulation was carried out. The dataset was loaded into the block. Before loading the dataset, the block remains red in color indicating that it is not encrypted and is hence vulnerable to attacks. The "Block" attribute in the block contains the index number of the block, the "Nonce" attribute stores a hashed number and the "Data" attribute is where the data is loaded into. On clicking the "Mine" option, the block turns green in color and the encrypted data is stored in the "Hash" field. This indicates that the block is safely encrypted and is resilient to any sort of attack. An important point to note is that the hash values maintained in the block are programmed to starts with four zeroes followed by an 'x' and then the encrypted data. The next simulation was to experiment the working of a Blockchain. Starting off with three blocks, each block has the attributes of "Block" (index number), "Nonce", "Data", "Prev", and "Hash". Except for Prev, all other attributes are the same as observed in the first simulation. In the Blockchain implementation, Prev is the field which holds the hash value or encrypted key of the previous block to ensure that chaining of the blocks take place efficiently. Initially the blocks are red, and on uploading the necessary data from the dataset into the three blocks and mining it, it is observed that the Blockchain changes to green color depicting that the data has been encrypted and the blocks have been chained together. The Prev value of the first block in the chain will always be zero as it isn't being linked to by any other block. Another point to be noticed is that each time a new block is appended to the chain, the previously present blocks turn to red depicting that the chain needs to be mined again for establishing proper linkages between the blocks. Only on mining again, will the blocks be linked together and will be completely encrypted.

Moving on to the implementation of the suitable hashing algorithm for necessary encryption. For the Blockchain, the information being stored in the block possess a unique hash value and this hash value is what links the various blocks together into one chain. There are various cryptographic techniques like Symmetric-Key cryptography, SHA-256, Asymmetric-Key cryptography, etc. The hash algorithm used for the implementation of the proposed solution has been executed in a Java environment on NetBeans editor. A class Block contains the functions of getPreviousHash(), getTransaction(), and getBlockHash() along with a constructor used for initializing data members

too store the hash value and the hash value of the previous block. Using this class, a genesis or nascent block is generated following which similar block are generated and linked together. The cryptographic technique of SHA-256 is used for generating the hash value for each of the blocks.

7. Simulation Results

As per the execution of the hashing algorithm in Java environment and the simulations from Anders Brownworth gives a holistic and complete approach to the reliability on Blockchain for integrating it as safety and security mechanism in AVs and ITS. All simulated results can be clearly observed in the implemented algorithm indicating that the Blockchains being created are adhering to all the features and attributes it must possess. The concept of avalanche effect which depicts that the change of data or information in any one block breaks the chain with all remaining block until they're mined again can also be observed in the implemented algorithm. Furthermore, a tiny change in the data held in a block ensures the generation of a new hash value. All these features make Blockchain reliable and suitable for ensuring safety and privacy preservation especially in fields like ITS. To conclude, this paper elaborates on the main safety and privacy challenges in relation to AVs and ITS. Further, the cryptographic techniques and hashing algorithm used in the curation of the proposed algorithm provide one of the best results.

8. Conclusion and Future Opportunities

AVs and ITS being one of the highly researched and massive domains, there are numerous options for future research, improvisation and development. One of the areas which can be dwelled deeper into is the restoration of privacy and security using other mechanisms other than Blockchain. Furthermore, the topic of integration of cloud platforms and cutting-edge techniques for enhancing the implemented systems has great potential for expanding futuristic opportunities. Last but not the least, VANETs, which is an associated field in transportation and automation of vehicles, is one of those topics which covers the networking and interconnection of the systemic devices in the transportation sector and has plenty of areas for extensive research and ideation.

References

[1] Sravanthi, K. & Burugari, Vijay Kumar & Tyagi, Amit. (2020). Preserving Privacy Techniques for Autonomous Vehicles. 8. 5180-5190. 10.30534/ijeter/2020/48892020.

[2] Sodhro, A.H., Obaidat, M.S., Abbasi, Q.H., Pace, P., Pirbhulal, S., Fortino, G., Imran, M.A. and Qaraqe, M., 2019. Quality of service optimization in an IoT-driven intelligent transportation system. IEEE Wireless Communications, 26(6), pp.10-17.

[3] Chavhan, S., Gupta, D., Garg, S., Khanna, A., Choi, B.J. and Hossain, M.S., 2020. Privacy and security management in intelligent transportation system. IEEE Access, 8, pp.148677-148688.

[4] S. Chavhan, D. Gupta, B. N. Chandana, A. Khanna, and J. J. P. C. Rodrigues, ''IoT-based context aware intelligent public transport system in a metropolitan area,'' IEEE Internet Things J., vol. 7, no. 7, pp. 6023–6034, Jul. 2020

[5] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, ''Secure enforcement in cognitive Internet of vehicles,'' IEEE Internet Things J., vol. 5, no. 2, pp. 1242–1250, Apr. 2018.

[6] Jolfaei, A. and Kant, K., 2019, June. Privacy and security of connected vehicles in intelligent transportation system. In 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks–Supplemental Volume (DSN-S) (pp. 9-10). IEEE.

[7] Sucasas, V., Mantas, G., Saghezchi, F.B., Radwan, A. and Rodriguez, J., 2016. An autonomous privacy-preserving authentication scheme for intelligent transportation systems. computers & security, 60, pp.193-205.

[8] Ogundoyin, S.O., 2018. An anonymous and privacy-preserving scheme for efficient traffic movement analysis in intelligent transportation system. Security and Privacy, 1(6), p.e50.
[9] Shaheen SA, Finson R. Intelligent transportation systems. Reference Module in Earth Systems and Environmental Sciences. Netherlands: Elsevier; 2013;1–12.
[10] Zear A, Singh PK, Singh Y. Intelligent transportation system: A progressive review. Indian J Sci Technol. 2016;9(32):1-8. https://doi.org/10.17485/ijst/2016/v9i32/100713
[11] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. Paper presented at: Proceedings of International Conference on Theory and Application of Cryptographic Techniques and Advanced Cryptology (EUROCRYPT), Prague, Czech Republic; May 1999:223-238 doi.org/10.1016/B978-0-12-409548-9.01108-8.
[12] D. A. Kountché, J. Bonnin and H. Labiod, "The problem of privacy in cooperative intelligent transportation systems (C-ITS)," 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2017, pp. 482-486, doi: 10.1109/INFCOMW.2017.8116424.
[13] A.Mohan Krishna, Amit Kumar Tyagi, S.V.A.V.Prasad "Preserving Privacy in Future Vehicles of Tomorrow", JCR. 2020; 7(19): 6675-6684. doi: 10.31838/jcr.07.19.768
[14] Koopman, P., Ferrell, U., Fratrik, F. and Wagner, M., 2019, September. A safety standard approach for fully autonomous vehicles. In International Conference on Computer Safety, Reliability, and Security (pp. 326-332). Springer, Cham.
[15] Z. Qingwen, Z. Yanmin, C. Chao, Z. Hongzi, and L. Bo, "When 3G Meets VANET: 3G-Assisted Data Delivery in VANETs," Sensors Journal, IEEE, 10, vol. 13, pp. 3575-3584, 2013.
[16] C. Campolo, H. A. Cozzetti, A. Molinaro, and R. Scopigno, "Augmenting Vehicle-to-Roadside connectivity in multi-channel vehicular Ad Hoc Networks," Journal of Network and Computer Applications, 5, vol. 36, pp. 1275-1286, 9// 2013
[17] Yang, F., Wang, S., Li, J., Liu, Z. and Sun, Q., 2014. An overview of internet of vehicles. China communications, 11(10), pp.1-15.
[18] Amit Kumar Tyagi, S U Aswathy, Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks, Volume 2, 2021, Pages 83-102, ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.
[19] J. Joy, V. Rabsatt, and M. Gerla, "Internet of vehicles: Enabling safe, secure, and private vehicular crowdsourcing," Internet Technology Letters, vol. 1, no. 1, p. e16, 2018.
[20] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading," IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 36–44, 2017.
[21] Jameel, F., Chang, Z., Huang, J. and Ristaniemi, T., 2019. Internet of autonomous vehicles: architecture, features, and socio-technological challenges. IEEE Wireless Communications, 26(4), pp.21-29.
[22] W R, Varsha et al. 'Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. International Journal of Hybrid Intelligent System, Vol 16, Issue 4: 223 – 236, 1 Jan. 2020.
[23] M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.332.
[24] Amit Kumar Tyagi and Sreenath Niladhuri. 2016. Providing Trust Enabled Services in Vehicular Cloud Computing. In Proceedings of the International Conference on Informatics and Analytics (ICIA-16). Association for Computing Machinery, New York, NY, USA, Article 3, 1–10. DOI:https://doi.org/10.1145/2980258.2980263