Preserving Privacy using Distributed Ledger Technology in Intelligent Transportation System

Meghna Manoj Nair

School of Computer Science Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India, manirmeghna@gmail.com

Terrance Fernandez Frederick

Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India, Frederick@pec.edu

Amit Kumar Tyagi

Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamilnadu, 600127, India, amitkrtyagi025@gmail.com

Intelligent Transportation System (ITS) is an enhanced application which mainly aims towards the curation of smart and interconnectivity services to ease the existing transportation systems. It is a field with a plethora of future possibilities so as to provide efficient and advanced techniques by solving and tackling the existing challenges and problems. Especially in cities and countries which aim towards developing smart cities, ITS plays an essential role in advancing the transportation sector with regards to the city. Using a number of AI and ML techniques, a variety of approaches, algorithms and techniques can be put to effective utilization to boost the ITS ecosystem. However, with every boon compliment few banes and plausible bottlenecks. One of the major concerns while using V2V networks is the privacy and security issue. The data being transferred amidst vehicles mainly caters to the status updates on the vehicles adjacent to it, the speed, and driver's information in case of any accidents or wherever required. In such cases, the privacy of the drivers details and personal information are at stake and often poses a major security challenge. Furthermore, there are chances of data breaches and similar attacks by malicious users which can lead to huge data loss and tampering of data. A possible solution to this problem is to approach it through the perspective of Blockchain. Blockchain is a concept of sharing information/ data in a distributed and decentralized manner. The numerous blocks present in a blockchain which are responsible for storing information do so by encrypting and securing the data and hence can be integrated with a V2V system for overcoming the privacy and security challenges.

Keywords • Privacy • Intelligent Transportation System • Security • Blockchain • Encryption

1 INTRODUCTION

ITS has been a field of extensive research and innovation over the years especially with a sharp rise in the urbanization of cities, smart cities, etc. For all those researchers and developers wishing to facilitate and revamp mobility and transportation in a smarter and more intelligent manner, ITS is the best and optimized option [1]. In simple words, ITS is an umbrella term for advanced applications which mainly focus on offering smart and automated solutions and provisions with regards to the transportation methods and traffic systems. The sole aim is to elevate the existing and conventional strategies and approaches that are being used currently so as to boost the elements of safety, efficiency and reliability. In the current world, preserving privacy and personal information of data has become a prime concern especially when considering the bulk and voluminous amounts of data that are being generated everyday by individuals, institutions, etc. Majority of the systems and architectures proposed in the ITS environment also contribute a significant share in the data streams that run around the world today. A few reports and surveys have highlighted the fact that the overall internet traffic has had a drastic growth over the past few years especially from the transportation sector. Models and frameworks which make use of vehicle-to-vehicle networks curetted in an Internet of Vehicles (IoV) environment involves huge volumes of personal data of users involved and indulging in the designed frameworks. In order to execute and implement such systems in a robust and efficient manner, the trust and reliability of the users are of utmost importance. In order to provide trust, the best way is to succumb to a fool proof, safe and secure ITS system with massive privacy goals and regulations.

Though many metropolitan cities including those of urban areas, satellite cities, rural areas etc. can utilize ITS to great benefits, considering the dynamic and pretentious movement of staff, commuters, vehicles, etc., there are all possibilities of tampering or unnecessary modifications of data. This provokes an extreme case of privacy and security concern among all of its users making it hard to rely and trust on the designed ITS framework [3]. On considering the domain of Internet of Vehicles (IoV), it throws up a platform which provisions for the transfer and exchange of data and details among the vehicles involved and the surrounding ecosystem. IoV which consist of three fundamental elements of intra-vehicular network, intra-vehicular network and vehicular mobile network, ensures that these components stay interconnected and interlinked with each other via wireless connections. And such systems indulge in large amounts of traffic flows, hence, the concern of privacy arises yet again [4]. This paper discusses the possibilities of incorporating blockchain techniques to maintain a certain level of privacy and to ensure secure data transfers. One of the emerging technologies which has brought in a revolutionary drive in the privacy and security preservation field is Blockchain. It is a concept which is often referred to as a distributed ledger technology which is extremely useful in tracking and monitoring transactional records, assets, and data by creating different blocks or groups of each.

1.1 Our Motivation

With urbanization taking a spin and leap in majority of the cities and countries across the world, transportation sector definitely requires a smarter and intelligent transformation to catch up on the fast-moving world. However, as enlisted earlier, there are a number of problems related to privacy and security that do enforce an opposite encounter on the reliability of the frameworks and systems developed using ITS. With Blockchain dominating seamlessly in the privacy sector, the integration of blockchain with ITS is clearly one of the techniques to preserve privacy and security of framework models that are being utilized in the smarter transportation sector. This has been the main motivation and essence for the research work done in this paper. The paper has been split into a few sections which are elucidated as follows. The first section following the motivation discusses about the existing models and systems which proposed with regards to ITS along with blockchain. The next section details about the ITS in depth and also enlightens the elements of Internet of Vehicles (IoV) and the Vehicle to Vehicle (V2V) communication techniques. Following this comes the next section which elaborates on the major privacy challenges faced in ITS. Consequently, the next section elaborates on Blockchain and the integration of blockchain in ITS. The next section then illustrates the results and discussions obtained along with the implementation and finally the conclusion which wraps up the entire research work along with future scope.

1.2 Organization of this work

Section 2 discusses about the literature review of the work and illustrates the existing solutions to the problem of security and privacy in ITS. Section 3 gives the details and brief of Intelligent Transportation Systems (ITS) and Section 4 introduces the concept of IoV in this paper. Section 5 gives a detailed description about the major challenges faced in the field of ITS and IoV and Section 6 talks about the proposed solution and the foundation used for the curation of this solution. Section 7 includes the simulation results which have been obtained while Section 8 discusses about the final implementation results of hashing which have been acquired. Section 9 gives insights on the final results obtained and section 10 throws light on the conclusions which can be drawn with regards to the simulations and results obtained.

1.3 Scope of this work

Considering the evolution in the walk of life with respect to urbanization and transportation being the heart and soul of mobility, ITS and IoV are concepts which have extremely high probability of proliferating in the future as it has already begun. With such huge influx in a particular tech strategy, security and privacy concerns are at steak because of the large volume of data involved in for the interaction, communication and transmission between vehicles and other embedded systems. The fact that there are numerous technologies which can be integrated with these main stream ideas for further enhancement and upskill, expands the scope and study of privacy preservation in ITS along with Blockchain which seems to be conquering the technical industry.

2 LITERATURE REVIEW

ITS has been an area of implementation which has already been experimented with in some of the well- developed countries across the world. The United States of America (USA) has incorporated an Electronic Route Guidance System (ERGS) succeeded by the integrated surface transportation efficiency programs (ISTEA) which were two of the few frameworks that lay the stepping stone for the ITS revolution in the USA [1]. However, these proposals slowly evolved with time so as to improvise the efficiency and response times of the systems along with the main aim of enhancing the privacy and security. With that they introduced the Vehicle Infrastructure Integration (VII) on the metrics of technical and economic viability of the networking community involved. Similarly in Japan, one of the most technically advanced and smart countries in the world, the government has yielded a massive amount of investment with regards to ITS with a cognizant response. They created the very first Vehicle Information Communications System (VICS) so as to cater to the needs of real time traffic data collection and analysis. However, over the next few years, they introduced an extemporized versions – the version 2.0 of the VICS model for the development of the Smart way [3][4].

On the other hand, the European Union (EU) introduced the European Road Transport Telemetric Implementation Coordination Organization (EUREKA). The main objective of introducing this system was to gain control and maintain order in solving traffic related problems [2][3]. Following the EUREKA model, EU also put forth a few other models like Dedicated Road Infrastructure for Vehicle Safety in Europe (DRIVE) and ERTICO in order to establish closer connection between the government and private enterprises. Apart from these, another framework called Program for European Traffic with Highest Efficiency and Unprecedented Safety (PROMETHEUS) was put into execution for an advanced management. One of the other technically forward countries, South Korea, has also established strong pillars in the field of ITS, making it the leader of the pack. This country had curated the efficiency law for the transportation system and had even devised a twenty-year master plan in 2000 for its ITS projects [5][6]. Apart from these few of the other applications in the field of ITS include Advanced Traveler Information System (ATIS) which is to optimize the possible paths of travelling from the desired source to the destination with the least amount of time.

Similarly, the Advanced Traffic Management System (ATMS) is one of the other commonly proposed branches of the ITS which involves Knowledge Based System, GPS in traffic control and AI techniques [6]. Few of the works and researches elucidate the effect and importance of Attribute Based Encryption (ABE) for maintaining the privacy and security of models in ITS. In order to bring about a positive change in privacy while accessing policies, a few authors have also proposed a CP-ABE model which infuse ciphertext technology. In addition to this, a proposal on the Privacy-Aware-S-Health access control system (PASH) was also made for protection of privacy related policies by hiding them [7].

3 INTELLIGENT TRANSPORTATION SYSTEM (ITS)

Over the years, with urbanization and technological advancements taking strong routes around the world. One of the domains which has maximum potential for developments is in the field of transportation as this sector is what supports mobility and affects other urbanization factors. In fact, ITS has been turning out to be an integral part in both economic and social development. One of the main reasons as to why this sector has gained a massive attention is because of few of the daily troubles faced by people using transport in daily life including those of traffic congestions, environmental pollution, consumption of energy, accidents and risks, expensive maintenance requirements, and so on. In order to overcome these hassles, a smart and intelligent solution needs to be implemented with precise and accurate execution this is where ITS comes to the rescue.

ITS is an apprehensive transportation management system catering to various vehicular services with the main objective of portraying innovative and smart solutions to the afore mentioned problems. Indeed, ITS is a field which calls for a multifaceted and interdisciplinary approach for carrying out operations and tasks in the particular domain. However, when proposing a system or framework for ITS, it’s essential to have a clear and organized format framework proposal for the same though it may pose to be a critical issue [8]. Few of the major motives of introducing ITS is to minimize the traffic congestions involved, reduce the risk of accidents by providing a vehicular network for all involved vehicles to communicate and stay up to date with each other, for localized convenience metrics, for extracting real-time information from running vehicles, and so on. Because of the impact, effect and revolutionary styles and solutions brought in by the technology, ITS has expanded to numerous countries, cities and metropolitans across the globe. Data collection, data transmission, data analysis, and traveler information are some of the major components involved in the implementation of ITS. In fact, ITS is a field which has evolved with time and over ages, transforming the transportation sector into a domain which is safer and efficient for extracting the required benefits. Most importantly, ITS is a field that has evolved not just with regards to technology but also pertaining to the fields of public and private communications and interactions.

4 INTERNET OF VEHICLES (IOV) IN ITS

IoV is an expansion of the Internet of Things (IoT) in the transportation field. It broadly covers the traditional ad-hoc networks correlated to vehicles and other advanced technological frameworks. IoV has two major features/attributes of highlight which focus on vehicular networking and vehicular intelligence [5][6]. Vehicular networking is what further exposes VANETs (Vehicle Ad-hoc Networks) and with the increase in technological enhancements and vehicles on the road, a strong lineal bond between IoT and VANETs are indulging to the spurge in IoV [9]. In simpler words, just like how IoT is a vast network connecting various nodes and components together, IoV is a subset of IoT which restricts the nodes or components that are being interconnected to that of vehicles. Currently, internet has an essential value in any of the tech related domains and the world has seen a spike in the number of gadgets and devices that are being curated specifically to be internet friendly [8].

One of the main reasons as to why IoV is used at an expanding rate is because it helps in solving and overcoming some of the issues and bottlenecks in the transportation sector including those of monitoring speed and speed limit, traffic management, reducing accidents and risks, and so on [9][10]. One of the main purposes of IoV is to offer services and solutions which help in the interaction of all connected vehicles in the network, the traffic management systems, respective transport authorities and any other node corresponding to these. By communication and transfer of data and information, it also carries out efficient processing, computation, analyses, sharing, protection of data, etc. IoV is one of the apt components of development in ITS. In fact, ITS applications which are propelling in Europe and Japan have utilized IoV technologies. IoV is often used in ITS to establish a strong and supportive network framework which is capable of interlinked various people with numerous vehicles and different environmental systems [10].

5 CHALLENGES AND ISSUES

Over the years, with urbanization and technological advancements taking strong routes around the world. Though ITS and IoV are fields with great and prolific advancements in the transportation sector across the globe, there are a few realms which often adds up to the vulnerability of the services provided in this domain. Listed below are some of the major challenges and issues faced in the efficient functioning of ITS which is coherent with that of IoV and Vehicle to Vehicle communication:

- Interoperability: The various sources from which data is required may not possess the necessary mandate to permit data transfer and the format and structure of the data being transferred may not necessarily adhere to the standards and desired formalities.
- Data Analysis: Analyzing and processing data received from systems and components that are interconnected can be cumbersome especially when the raw data needs to be edited or standardized.
- Security: There are various classifications under this domain which prove to be a risk for ITS management and operation. Confidentiality, integrity, authentication and identification, and cyber-attacks are few of the areas of high concern all throughout the ITS applications.

Of all the major domains of concerns and issues listed above, the one which pulls up the most amount of concern is that of privacy and security. It is one of the major challenges in the ITS domains which acts as a true obstacle for establishing trust and reliability from the users of the framework [10]. There are various types of security issues which hinder the growth of the ITS applications across the society. The data which is gathered from numerous sensors and interconnected gadgets from the vehicles in the system are often spatially correlated and coherent to each other. It's extremely important that data and information connected in such ways are handled with care and must also preserve the anonymity of the personal details of the driver from which the data has been extracted. Apart from this, one of the other major concerns is that of possible cyber-attacks which can lead to data breaches and leakages, identity theft, and even malfunctioning of the entire system. Some of the commonly visible attacks in ITS include broadcast tampering, denial of services (DoS), routing, sybil attack, jamming, brute force, man in the middle, illusion attack, node impersonation, malware spamming, and position faking. The possible threats are in abundance and hence it is extremely important that a proper systematization and structuring of the ITS framework is developed.

6 PROPOSED SOLUTION

The main objective of this paper is to overcome the privacy challenges faced in the field of ITS. As mentioned earlier, this is because it is one of the best ways to gain trust and ensure reliable services to the users in the domain of smart and intelligent developments in the transportation domain. Blockchain is a distributed ledger technique which allows storage of data in individual blocks which are further chained together to form a chain of blocks of interrelated data. This ledger technique is immutable in nature and provides capability to log all transactions and track assets in the network. Over the years, blockchain has acquired credibility and acknowledgment from numerous domains be it finance, health, commerce, etc. most in correlation to the security and privacy of data. The main advantage of the blockchain system is that each time data is stored into a blockchain, it is encrypted using profound techniques or other relevant cryptographic methodologies. This ensures that the data is highly secure and will provide guaranteed privacy of data and information while maintain the anonymity of the people involved. In the current world, majority of the businesses utilize extensive amounts of data for their analysis, surveys and researches to improve business tactics, marketing strategies, etc. Blockchain is an ideal option for such kinds of information delivery as it promises an immediate, collective and transparent data gathering and transferable technique which provides information with speed and accuracy. Moreover, the fact that blockchains can be simultaneously used for tracking orders, payments, accounts, production and so on [11].

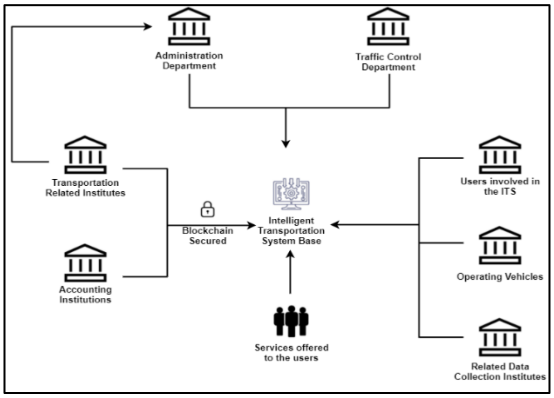

Administration Department
Traffic Control Department
Transportation Related Institutes
Blockchain Secured
Intelligent Transportation System Base
Users involved in the ITS
Operating Vehicles
Accounting Institutions
Services offered to the users
Related Data Collection Institutes

Figure 1: Work flow of Blockchain system

The solution proposed for overcoming the privacy concerns in ITS in this paper revolves around that of blockchain technique. Blockchain has the potential to provide a trusted, safe and secure model for a decentralized and distributed ITS network. Figure 1 can be used to grasp the entire working process of a blockchain system for establishing security in an ITS framework. After the dataset which is to be chained is collected, a genesis block is created. The genesis block is often considered as a pointer to the reference of the very first block in the chain. Following the creation of the genesis block, the next step is to hash the created block and generate the timestamp for the same. After this step, the next data which is to be appended in the new block is captured and hashed along with the timestamp. It then branches out to the sub step of maintain the time stamp for the newly created block and also links the blocks together using the hash keys of the previous blocks. In a similar manner all the blocks are hashed with respect to the nonce which is to be stored in the block, following which the blocks are interlinked and chained with each other which eventually leads to the creation of a blockchain. The data being collected from the sensors and devices undergo the above mentioned Blockchain encryption process before further distribution or processing.

With privacy preservation portraying one of the major issues in majority of the domains including that of ITS, integrating Blockchain with ITS is a feasible and viable solution to overcome the privacy hassle. All the devices which interact with gadgets and sensors in the vehicular domain will be installed and integrated with a particular application which represents the client side, while a main application runs on the server side. All the devices and gadgets involved in the ITS framework must be curated in such a way that they are fool proof and resilient to any form of internal or external attacks (be it active or passive). The required information and details are gathered and collected from these systems and are stored in a blockchain relevant environment for ensuring a safe and secure data transfer. After which they can be accessed easily from the server--side application to carry on further processing and computation. The blockchain will be decentralized and maintained by a trusted entity which ensures that the data is accessible to the valid parties on both client and server side for storing and extracting the details to/from the blockchain respectively.

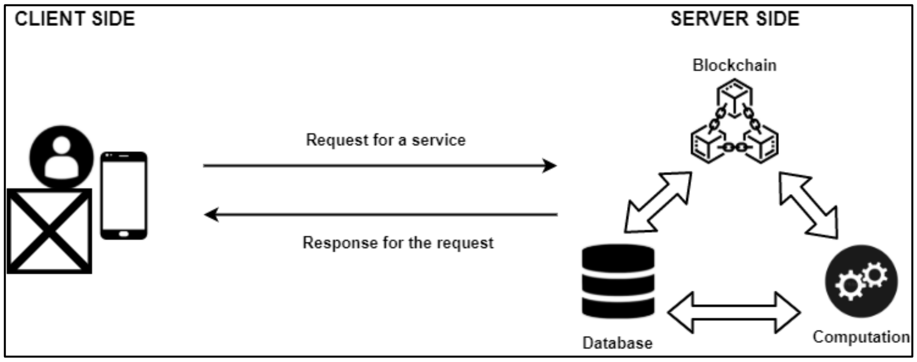
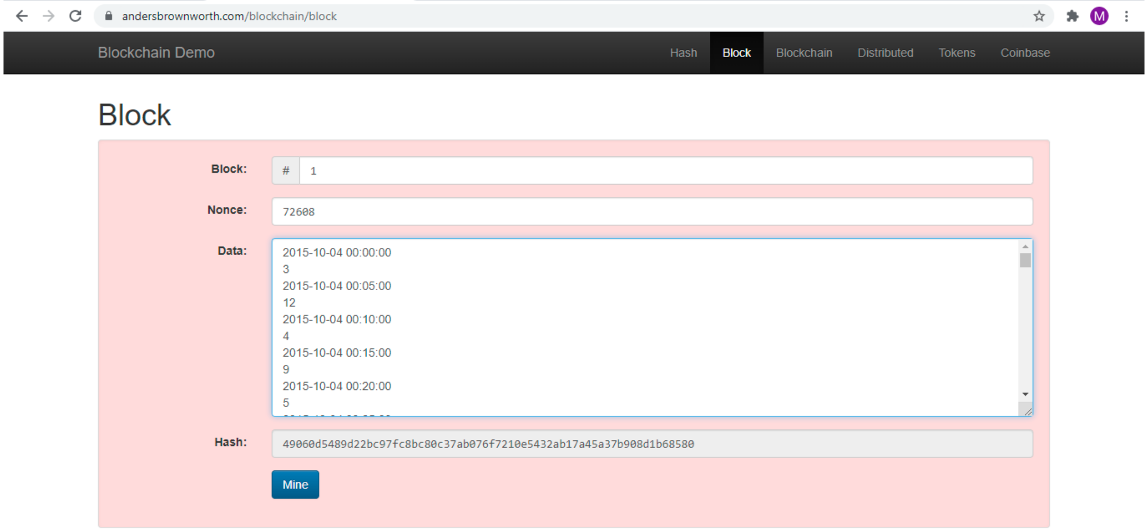


Figure 2: Integrating Blockchain with client and server side in ITS

One of the next major topics which needs to be addressed with regards to the integration of Blockchain in ITS is the communication and flow of data in the entire framework. The end users or drivers of the vehicles involved in the ITS framework will be in touch with the server to transmit and extract details to/from the nodes or components involved. The blockchain is bound to accept request and data stores from both the ends respectively. Further the data stored is completely encrypted and hashed using a generated shared encryption key which is then forwarded to the blockchain to carry out further transactions. The strength and security of this encryption technique is such that even if an external attacker wishes to surpass and leak data from the proposed ITS system, the attacker will not be able to get insights on nearly fifty one percent of the system and would be compelled to compromise on the same, making it nearly intolerable to attack the proposed ITS framework which is safely guarded with blockchain. The client server perspective of the solution can be observed in Figure 2.

7 SIMULATED RESULTS

Over the years, with urbanization and technological advancements taking strong routes around the world In order to visualize and comprehend the working of blockchain model to its completion, a simulator has been used. Anders Brownworth, a researcher and developer in the field of blockchain has created a blockchain simulator which helps in providing a visual representation of the working of the blockchain. The dataset used for the purpose of explaining the concept of blockchain is in relation to an automated traffic control system which has been obtained from Kaggle. The first simulation that has been carried out is with regards to the Block simulator for apprehending the mining of a particular block in the chain. As shown in Figure 3, the field Block represents the indexing or position of the particular block in the chain. The next field Nonce (which stands for number used only once) is a number which is hashed and used to meet the restrictions and guidelines followed by those of Blockchain. The next field is that of Data which is to be embedded with the data that needs to be stored in the particular block. As mentioned earlier, for the purpose of explanation, the dataset used involves the date and time and the number of vehicles which were spotted at a particular junction at the given instance. The next field is Hash which is auto-generated and contains the encrypted key for the particular block that has been created. The red background color on the block shows that it hasn't been mined and needs to be validated.



Block

Block: # 1

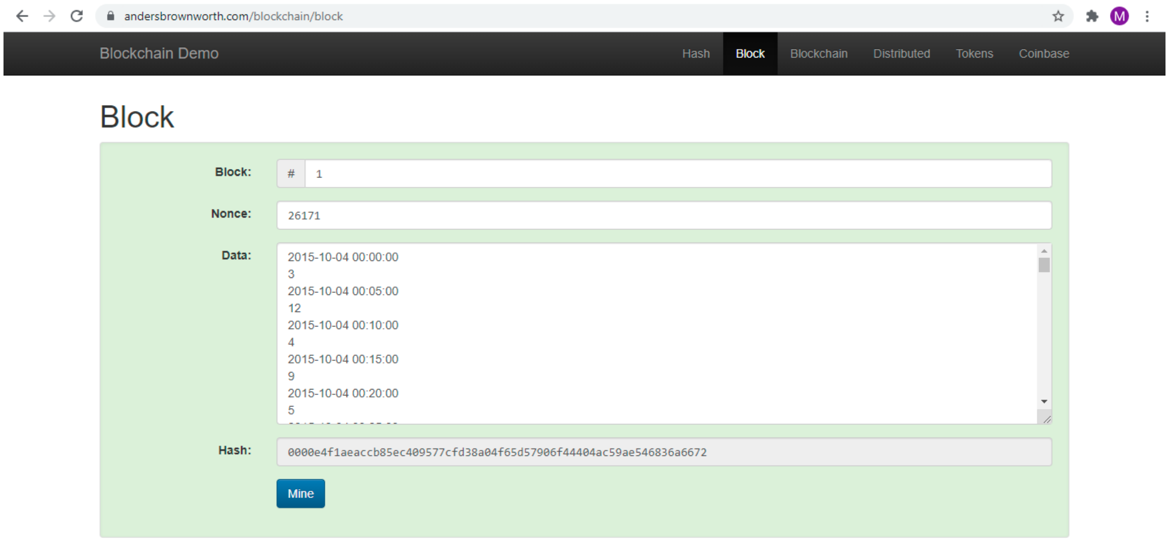
Nonce: 72608

Data:
2015-10-04 00:00:00
3
2015-10-04 00:05:00
12
2015-10-04 00:10:00
4
2015-10-04 00:15:00
9
2015-10-04 00:20:00
5

Hash: 49060d5489d22bc97fc8bc80c37ab076f7210e5432ab17a45a37b908d1b68580

Figure 3: Simulation of a Block before mining

Figure 4 shows the very same block after it has been mined because of which the background color has turned to green and the value of Nonce has been adjusted as per the data that has been entered. Also notice that the hash value has been respectively modified on mining to start with four zeroes which is one of the standardized techniques to maintain the hash value.



Block

Block: # 1

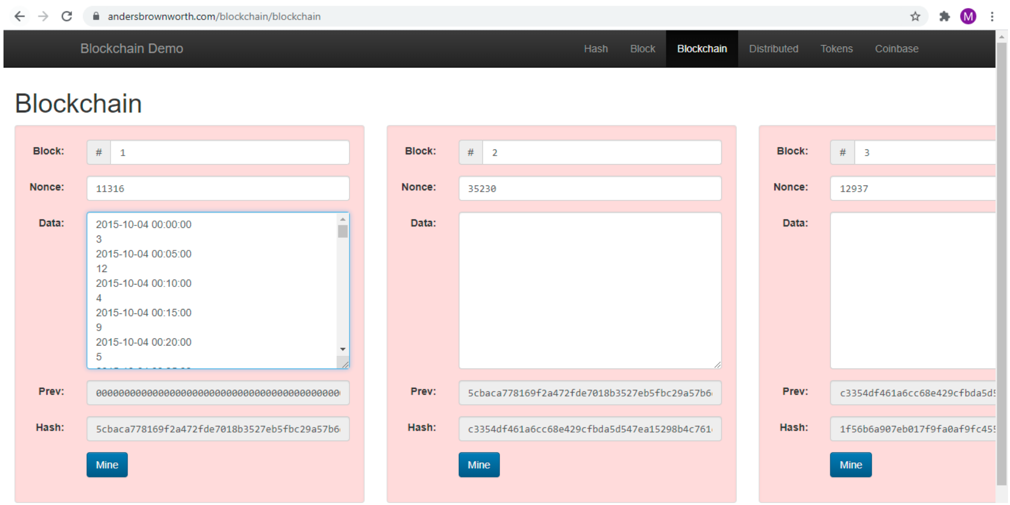
Nonce: 26171

Data:
2015-10-04 00:00:00
3
2015-10-04 00:05:00
12
2015-10-04 00:10:00
4
2015-10-04 00:15:00
9
2015-10-04 00:20:00
5

Hash: 0000e4f1aeaccb85ec409577cfd38a04f65d57906f44404ac59ae546836a6672

Figure 4: Simulation of a Block after mining

After the simulation of a block, the next cohort to be simulated belonged to that of the Blockchain. Figure 5 shows the snap of a blockchain wherein the first block has been entered with data from the dataset acquired from Kaggle with regards to the traffic control system. As observed, since the block hasn't been mined, the background score is set to red. On mining the first block, the Nonce and Hash value is changed accordingly based on the data stored in it and the hash value contains the encrypted key in the standardized format with four zeroes at the beginning. On mining the blocks as seen in Figure 6, it is noticeable that the value maintained in the Previous field is the hash value or the encrypted key of the previous block and in case of the first block, the Previous field is set to all zeroes.



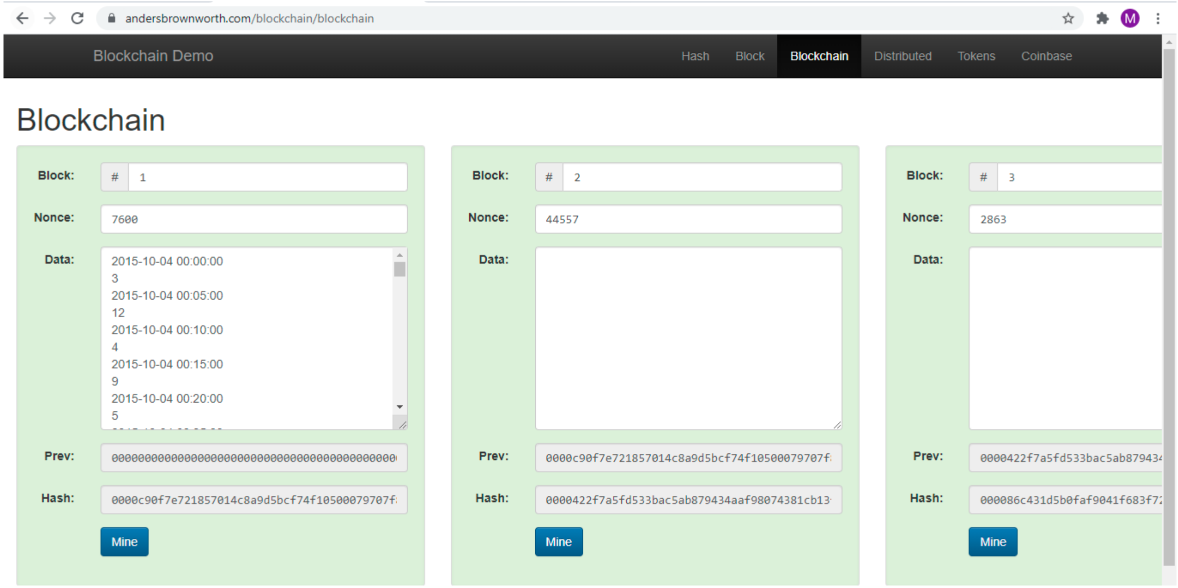
Blockchain

Block: # 1
Nonce: 11316
Data:
2015-10-04 00:00:00
3
2015-10-04 00:05:00
12
2015-10-04 00:10:00
4
2015-10-04 00:15:00
9
2015-10-04 00:20:00
5
Prev: 0000000000000000000000000000000000000000000
Hash: 5cbaca778169f2a472fde7018b3527eb5fbc29a57b6

Block: # 2
Nonce: 35230
Data:
Prev: 5cbaca778169f2a472fde7018b3527eb5fbc29a57b6
Hash: c3354df461a6cc68e429cfbda5d547ea15298b4c761

Block: # 3
Nonce: 12937
Data:
Prev: c3354df461a6cc68e429cfbda5d5
Hash: 1f56b6a907eb017f9fa0af9fc45

Figure 5: Simulation of Blockchain for the first Block



Blockchain

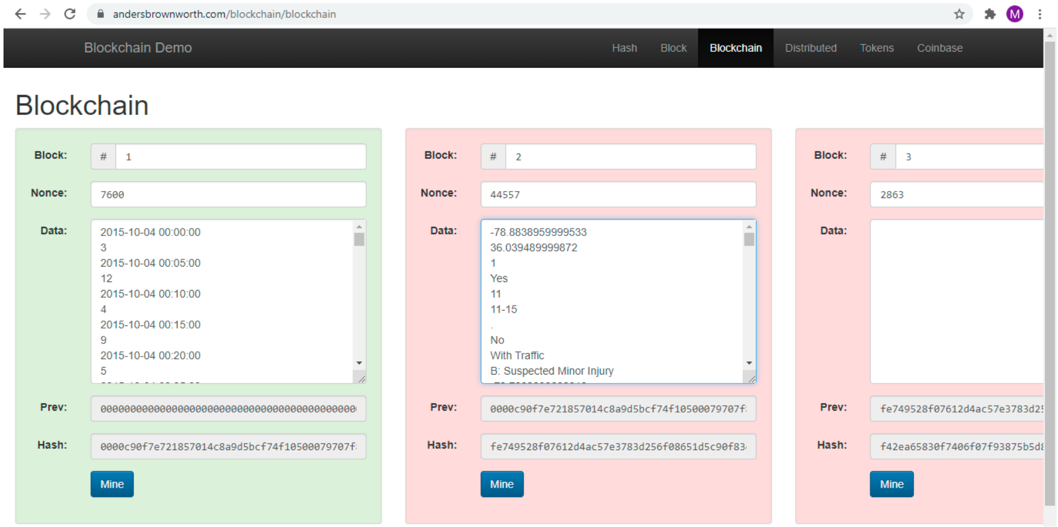
Block: # 1
Nonce: 7600
Data:
2015-10-04 00:00:00
3
2015-10-04 00:05:00
12
2015-10-04 00:10:00
4
2015-10-04 00:15:00
9
2015-10-04 00:20:00
5
Prev: 0000000000000000000000000000000000000000000
Hash: 0000c90f7e721857014c8a9d5bcf74f10500079707f

Block: # 2
Nonce: 44557
Data:
Prev: 0000c90f7e721857014c8a9d5bcf74f10500079707f
Hash: 0000422f7a5fd533bac5ab879434aaf98074381cb13

Block: # 3
Nonce: 2863
Data:
Prev: 0000422f7a5fd533bac5ab87943
Hash: 000086c431d5b0faf9041f683f7

Figure 6: Simulation of Blockchain after mining all the blocks

When a new block is to be appended to the blockchain and when the necessary data is stored in the new block, it is observed that the rest of the previously mined blocks have been broken and the background score is set to red indicating that the chain has been broken and needs to be validated and relinked with the earlier blocks. This simulation is shown in Figure 7. On mining the newly created blocks, the background score changes to green indicating that the blocks have been linked back together in the form of a blockchain with the values stored in Previous and Hash field being modified accordingly.



Blockchain

Block: # 1
Nonce: 7600
Data:
2015-10-04 00:00:00
3
2015-10-04 00:05:00
12
2015-10-04 00:10:00
4
2015-10-04 00:15:00
9
2015-10-04 00:20:00
5
Prev: 00000000000000000000000000000000000000000
Hash: 0000c90f7e721857014c8a9d5bcf74f10500079707f

Block: # 2
Nonce: 44557
Data:
-78.8838959999533
36.039489999872
1
Yes
11
11-15
.
No
With Traffic
B: Suspected Minor Injury
Prev: 0000c90f7e721857014c8a9d5bcf74f10500079707f
Hash: fe749528f07612d4ac57e3783d256f08651d5c90f83

Block: # 3
Nonce: 2863
Data:
Prev: fe749528f07612d4ac57e3783d2
Hash: f42ea65830f7406f07f93875b5d

Figure 7: Simulation of Blockchain when a new block is appended

8 IMPLEMENTATION OF HASHING

Over the years, with urbanization and technological advancements taking strong routes around the world Blockchain being identified as one of technologies which support peer-to-peer network, the data being stored in the block possesses a hash value which helps in interconnecting the blocks together, as described in the simulation in the previous section. These hash values are unique to every block and also changes its value each time the data stored in the particular block is modified. The hash values are generated by cryptographic techniques which generate encryption key which are strong enough to resist attacks and breaches. Encryption is the process of transforming plain text into ciphered text which is a random sequence of bits. Decryption is the reverse of encryption and involves the conversion of ciphered text to plain text. For analyzing encryption in Blockchain, a comparative study on the different types of cryptographic algorithms needs to be carried out [12,13].

Symmetric-Key Cryptography: In this particular cryptographic algorithm, a single key is used for encryption purpose. The same key is used for both encryption and decryption throughout the process. However, making use of a single key for both cryptographic techniques can cause a security concern especially in cases when the key is being transferred from/to the sender and receiver respectively [14].

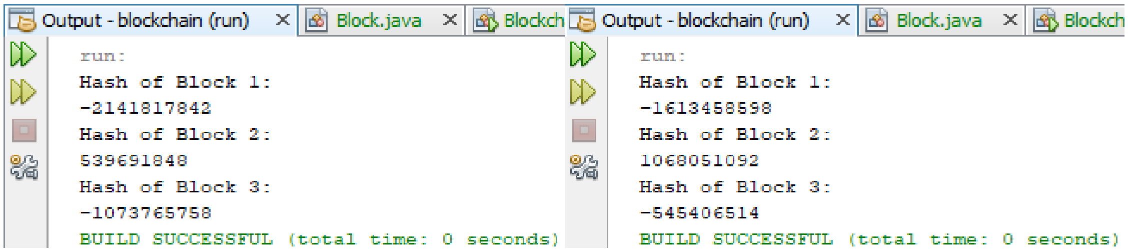
SHA-256: This encryption is one of the highly used techniques in hash functions because of its convenience and ease of usage along with which its security parameters are also high [15].

Asymmetric-Key Cryptography: This particular technique is often known as public-key cryptography and makes use of both encryption and decryption mechanisms. The algorithm in this strategy generates a key-pair and the public key is the one which is openly accessible when compared to that of the private key. These two key types take up the role of encryption and decryption respectively. This technique when utilized in blockchain tends to focus more on the transactional safety.

Based on the above-mentioned cryptography techniques, an encryption technique has been implemented using Java tech-stack in Net-Beans IDE. The algorithmic concept used to build the code revolves around the creation of a blockchain and then using the appropriate encryption technique [16]. The constructor function of class Block initializes the value of the hash value of the previous block to the data member previous Hash and the data pertaining too transaction in data member transaction. The functions getPreviousHash(), getTransaction() and getBlockHash() are used for accessing the private attributes of the Block object. This java package is then imported in the file where the code/algorithms is developed. A genesis block is created at the beginning by invoking the Block constructor following which the hash value for the data stored in it is produced. Similarly, subsequent blocks are created and linked to the previous block and the results are printed.

9 FINAL RESULTS

Over the years, with urbanization and technological advancements taking strong routes around the world Brownworth simulator shows the visualization and gives an idea of how Blockchain can be implemented for storing data in a safe form. The cryptographic technique used is SHA256 and is precise and accurate enough to give secure hash values for linking the Blockchain in a safe and protected way. The encryption technique used in the code above is often stated as a secure and trustworthy technique with hardly any collisions. Further, the avalanche effect of this cryptography algorithm, which makes sure that any change or modification of the data stored will lead to the change of hash values throughout the blocks makes it even more powerful and secure. Figure 10 is a depiction of the results obtained on executing the code mentioned in the previous section [17]. Further, Figure 11 shows how the avalanche effect can be observed when the data in any of the blocks is changed even to a minor extend. It can also be observed that each time the data stored in any of the block is modified, the hash values of each and every block needs to be regenerated and linked together. This shows that Blockchain is one of the reliable ways to ensure safety and security of data in Intelligent Transportation System as it is highly essential that the data obtained from the ITS devices are safe and un-tampered.



```
run:
Hash of Block 1:
-2141817842
Hash of Block 2:
539691848
Hash of Block 3:
-1073765758
BUILD SUCCESSFUL (total time: 0 seconds)
```

Hash Values for original data

```
run:
Hash of Block 1:
-1613458598
Hash of Block 2:
1068051092
Hash of Block 3:
-545406514
BUILD SUCCESSFUL (total time: 0 seconds)
```

Hash Values for modified data

Figure 10: Outputs obtained on executing the code for Blockchain

10 FUTURE OPPORTUNITIES

ITS is a massive field which has high possibilities of expansion and further extensive researches for enhancement, optimization and development. The very fact that ITS has high potential and capabilities is the main motivation for fueling up the research work for the future [18][19]. One major point of concern is to address the security concerns from other perspectives without the utilization of Blockchain so as to draw a comparison and conclude on which ultimately proves to be the most efficient technique [20]. Another domain for further research is with regards to the execution and foundation of the ITS framework on cloud-based platform and by incorporating cutting edge technologies for further enhancement [21]. Another domain which has a high scope for research belongs to that of compatibility and connectivity of the different sensors and gadgets that are involved in the ITS [22]. In the last, several privacy preserving techniques for VANET (including future vehicles) has been included in [23-30] in detail. The researchers are recommended to refer these articles for enhancing their knowledge towards preserving of privacy of users in this smart era with emerging technologies/ modern tools.

11 CONCLUSION

This paper elucidates the safety and security challenges faced in ITS framework. Especially with a huge rise in the number of technologies being adapted to automate and improvise the transportation sector, it is essential that a reliable and trustworthy application is put forth for the customers. This can be acquired by eradicating the chances for attacks, data leakages, etc. Blockchain is one of the best options for solving this issue to a great extent. The implementation of Blockchain can be observed from the explanation given through the simulator used in this paper. Further analysis of the concept can be obtained through the Java code used for building the Blockchain. The cryptographic techniques used in the Blockchain implementation are highly efficient and strong to ensure the complete safety and protection of data to avoid tampering. This paper puts forward the proposal of integrating Blockchain with ITS and explains in depth about the encryption techniques which provide the best results for the cryptographic part along with the simulation of how Blockchain work with respect to their hash values and nonce.

ACKNOWLEDGMENTS

The authors want to thank Centre for Advanced Data Science and School of Computer Science and Engineering, Vellore Institute of Technology, Chennai for providing their kind support to complete this research work on time.

REFERENCES

[1] Yuhong Li 1, Kun Ouyang, Nanxuan Li, Rahim Rahmani, Haojun Yang, Yiwei Pei, 2020, A Blockchain-Assisted Intelligent Transportation, System Promoting Data Services with Privacy Protection, MDPI.

[2] L. Hîrtan and C. Dobre, 2018, Blockchain Privacy-Preservation in Intelligent Transportation Systems, IEEE International Conference on Computational Science and Engineering (CSE).

[3] S. Chavhan, D. Gupta, S. Garg, A. Khanna, B. J. Choi and M. S. Hossain, 2020, Privacy and Security Management in Intelligent Transportation System, in IEEE Access, vol. 8.

[4] J. Contreras-Castillo, S. Zeadally and J. A. Guerrero-Ibañez, 2018, Internet of Vehicles: Architecture, Protocols, and Security, in IEEE Internet of Things Journal, vol. 5.

[5] S. An, B. Lee and D. Shin, 2011, A Survey of Intelligent Transportation Systems, Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 332-337, doi: 10.1109/CICSyN.2011.76.

[6] Bhupendra Singh, Ankit Gupta, Recent trends in intelligent transportation systems: a review, Journal of Transport Literature, April, 2015, https://doi.org/10.1590/2238-1031.jtl.v9n2a6

[7] H. Tian, X. Li, H. Quan, C. -C. Chang and T. Baker, 2020, A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection, in IEEE Sensors Journal, doi: 10.1109/JSEN.2020.3030688.

[8] Y. Lin, P. Wang and M. Ma, 2017, Intelligent Transportation System (ITS): Concept, Challenge and Opportunity,3rd International conference on big data security on cloud (big data security), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids), 2017, pp. 167-172, doi: 10.1109/BigDataSecurity.2017.50

[9] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, 2014, An overview of Internet of Vehicles, in China Communications, vol. 11, no. 10, pp. 1-15, Oct, doi: 10.1109/CC.2014.6969789.

[10] Hahn, Dalton A., Arslan Munir, and Vahid Behzadan, 2021, Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intell. Transp. Syst. Mag. 13.1: 181-196.

[11] https://www.ibm.com/in-en/topics/what-is-blockchain

[12] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), pp.352-375.

[13] Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[14] Yuan, Y. and Wang, F.Y., 2016, November. Towards blockchain-based intelligent transportation systems. In 2016 IEEE 19th international conference on intelligent transportation systems (ITSC) (pp. 2663-2668). IEEE.

[15] Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C., 2016, May. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

[16] Çaldağ, M.T. and Gökalp, E., 2020. Exploring Critical success factors for blockchain-based intelligent transportation systems. Emerg. Sci. J, 4, pp.27-44.

[17] Ajwani-Ramchandani, R., Figueira, S., de Oliveira, R.T. and Jha, S., 2021. Enhancing the circular and modified linear economy: The importance of blockchain for developing economies. Resources, Conservation and Recycling, 168, p.105468.

[18] Alam, M., Ferreira, J. and Fonseca, J., 2016. Introduction to intelligent transportation systems. In Intelligent transportation systems (pp. 1-17). Springer, Cham.

[19] Henry, R., Herzberg, A. and Kate, A., 2018. Blockchain access privacy: Challenges and directions. IEEE Security & Privacy, 16(4), pp.38-45.

[20] Bao, S., Cao, Y., Lei, A., Asuquo, P., Cruickshank, H., Sun, Z. and Huth, M., 2019. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. IEEE Access, 7, pp.80390-80403.

[21] Wen, Y., Lu, Y., Yan, J., Zhou, Z., von Deneen, K.M. and Shi, P., 2011. An algorithm for license plate recognition applied tointelligent transportation system. IEEE Transactions on intelligent transportation systems, 12(3), pp.830-845.

[22] 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.

[23] Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56

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

[25] A. K. Tyagi, T. F. Fernandez and S. U. Aswathy, 2021, Blockchain and Aadhaar based Electronic Voting System, 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, pp. 498-504, doi: 10.1109/ICECA49313.2020.9297655.

[26] Shasvi Mishra, Amit Kumar Tyagi, 2021, The Role of Machine Learning Techniques in Internet of Things Based Cloud Applications, AI-IoT book, Springer.

[27] A. Mohan Krishna, Amit Kumar Tyagi, S.V.A.V. Prasad, 2020, Preserving Privacy in Future Vehicles of Tomorrow, JCR.; 7(19): 6675-6684. doi: 10.31838/jcr.07.19.768

[28] Amit Kumar Tyagi, N. Sreenath, 2015, A Comparative Study on Privacy Preserving Techniques for Location Based Services, British Journal of Mathematics and Computer Science (ISSN: 2231-0851), Volume 10, No.4, pp. 1-25, July.

[29] Amit Kumar Tyagi and Sreenath Niladhuri, 2017, ISPAS: An Intelligent, Smart Parking Allotment System for Travelling Vehicles in Urban Areas, International Journal of Security and Its Applications, Vol. 11, No. 12 (2017), pp.45-66, ISSN: 1738-9976 IJSIA, SERSC Australia.

[30] R, Varsha et al. 2020, Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles. 1 Jan. 2020: 223 – 236.