Traffic Violation Data Security System

Aromal M,[1] Arun Jiju Joseph,[1] Fleming B Vinu,[1] Sharan George Mammen,[1] and Praveen J S[1]

[1]*Mar Baselios College of Engineering and Technology,*
Mar Ivanios Vidyanagar Nalanchira P.O, Thiruvananthapuram, Kerala, India Pin: 695015

Abstract. Since the road resources are limited and the number of vehicles on road are increasing at a tremendous rate, traffic monitoring has become a huge challenge and higher management costs have resulted in implementing a manual traffic monitoring system. Many traffic violations are difficult to capture with human observation. It is incontrovertible that a more intelligent and less cost scheme to solve the traffic management problem is necessary. In this paper, we aim to design a smart traffic management system using image processing, which can identify a vehicle's license plate and add the violations in a blockchain. The computerised traffic monitoring system relies heavily on licence plate detection. The algorithm uses Canny Edge Detection to detect license plate. Tesseract is used as an OCR engine to recognize the characters from the detected license plate. OpenCV module is used with python for image processing and cloud storage is used to store the details of registered license plates. IoT cameras will be placed at every junction and the license plates of traffic violators will be captured. Then the license plate number along with the violation will be added to blockchain and a notification will be sent to violator. If the license plate is not registered, then the anomaly will be reported to Motor Vehicle Department.

Keywords: Blockchain, traffic violation, proof of work, image processing, data security

I. INTRODUCTION

In the present society, fast portability is a current need.As a result, people use different kinds of transportation utilities that include vehicles, subway systems, trains, and bicycles. Also, these kinds of transportation facilities are used or adopted due to their solace and feasibility. Predicting a continuous and steady growth in the population, there will be an increase in the number of vehicles, which is much quicker than the infrastructure of transportation.

In a country like India which is having one of the largest population it will be difficult for manual traffic monitoring so we could be able to say that the currently existing is not transparent. Also the database could be easily tampered so we will be using a blockchain technology for the security. Since India has witnessed a massive increase in the number of vehicles and so traffic monitoring has become a huge challenge. Surveillance used to be limited to the presence of police officers on the roadways who would report any traffic offenses. At present, we have CCTV cameras installed at every junction but tracking a vehicle is yet done manually, by tracing a vehicle from one traffic signal to other. This system has a poor performance and many traffic parameters such as vehicle density over time, average speed of vehicles, etc. Recently, there has been a emerging interest in the use of automated systems capable of providing information about road traffic on highways and city roads and also tracking them.

In a growing computer network of technology,the blockchain is used as a cryptocurrency system.For the past years, designs in blockchain-based systems have undergone a huge change,that is they had been very much successful in different decentralized applications.The ability to identify and get a clarity on a blockchain has various match with ongoing demands in the security of data.In a blockchain-based applications it is largely depend on the tokens which are available digitally for the design of the system.It can limit the blockchain based technology which is executed largely in cryptocurrency related related systems.The Blockchain is not only used for linking vehicles and infrastructures as a whole together in decentralized network but also provides dispensable and unchanged ledger to an automatically document vehicular data with timestamps.Moreover, the distributed ledger gives more dependable data inputs directly for traffic monitoring systems.

The purpose of this project is to implement a system that provides database security while ensuring transparency to the public. Manual traffic monitoring by law enforcement agencies is ineffective and fails to detect many violations. This traditional system is also responsible for many road accidents. The manual violation detection is prone to human error, causing the violator to be unaware of the violation. The system discussed in this paper provides all the solutions to the above-stated problems.

II. SYSTEM FUNDAMENTALS

A. Image Processing

The fundamental step in violation detection is image processing. In this project, we use an IOT camera which has a processing unit for license plate detection and recognition. First, the camera captures the image of vehicle which violated the traffic rules. As a pre-processing step, the image is converted to grayscale for faster pro-

cessing. An edge preserving filter, Bilateral filtering is applied to the image to reduce the noise and smoothen the image. Canny edge detection algorithm is used to identify the edges in the image. Contour is the line that connects all of the points along an object's boundary that have the same intensity. From the detected contours, 4 sided polygons are extracted, the license plate is chosen as the contour with the largest area. Tesseract is used as the Optical Character Recognition (OCR)[4] to recognise the characters from the license plate.

B. Blockchain

Blockchain can be described as an immutable distributed ledger and was developed by Satoshi Nakamoto who created Bitcoin[2], a peer-to-peer electronic transaction system. In a blockchain technology, there is no centralised system to coordinate the system. Only nodes are present, each of which has copy of the ledger and validates the transactions. Blockchain is useful in any scenario which requires authenticity, integrity, transparency and security.Blockchain involves a distributed database that will be shared among nodes in a computer network.In a databse, a information or data will be stored by blockchain in a electronically digital format.Since Blockchains are very much known for a major role in cryptocurrency systems, that are bitcoins, for sustaining a protective and decentralized transaction record.The creation of blockchain ensures accuracy and security of data record and produce a trust without the help of third party systems.

A major variance between a database and blockchain is regarding the structure of data or how the data is structured.Blockchain stores information jointly in the form of groups , called as blocks, which contain the lay of information. The blocks contain storage capabilities and when completed, are closed and linked with previously contained block, known as data chain which is called as Blockchain. The latest data or information which follows a newly included block that is compiled to a newly formed block that will be included to the chain once stored.

The proposed system uses blockchain to ensure data security, data transparency, and data availability. The blockchain provides equal rights to all members of the blockchain network. Blockchain also helps to reduce the cost of setting up and maintaining the system.

C. Network

A computer network is a collection of computers that share resources shared by network nodes. To communicate with each other, the computers use standard communication protocols across digital linkages. These linkages are comprised of telecommunication network technologies based on physically wired, optical, and wireless radio-frequency methods that can be configured in a number of network topologies. The proposed system uses a peer-to-peer network. A peer-to-peer (P2P) network is a distributed application architecture in which jobs or workloads are dispersed among peers. Peers are equally privileged and equally capable participants in the application. The P2P network is able to share storage, network bandwidth, and processing power among peers without the need for a central server. In contrast to the typical client–server architecture, where resource consumption and supply are split, peers are both resource suppliers and consumers[3]. Multiple IoT cameras are used in the proposed system. Wireless or wired connections are used to link these IoT cameras to the network. Multiple IoT cameras, miners, and public users make up this system network. The system must ensure that all network nodes have access to all of the network's data.

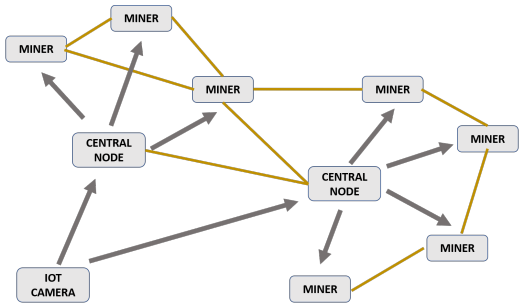

FIG. 1. blockchain network

D. Database

The prime database technologies incorporated in this project include Google Firebase as the MVD database, cloud file storage to store captures of violations and SQLite3 as the blockchain database to store the mined blocks.

Google Firebase is a NoSQL database with real-time functionality and a secure authentication system. Firebase was used to store the details of all registered license plates by the Motor Vehicle Department. The details stored include details of owner such as name, contact address, etc. and vehicle details like engine number, chassis number, vehicle make, model and colour, etc. The details of vehicle can be obtained from the license plate of the violator's vehicle.

Cloud file storage is used to store the captured image of the violation. The image stored in the cloud can be accessed by a url.

SQLite3 is a text-file based SQL database and is used in this project as the blockchain database. Each node in the blockchain network possesses a separate copy of the whole blockchain data. The data in each node is updated frequently. With its high throughput, low latency, powerful query functionality, SQLite3 is an excellent database for a decentralised network.

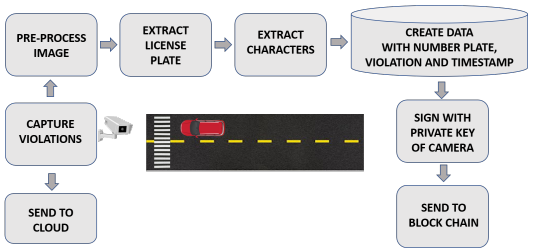

FIG. 2. functions of IoT camera

III. SYSTEM DESIGN MODEL

The proposed system is a traffic violation monitoring system that is highly secure, transparent, and 24/7 available. The system is primarily comprised of IOT cameras, miners, and public users.

A. IoT Camera

An IoT camera is a machine vision system that, in addition to image capturing circuitry, can extract application-specific information from acquired images, as well as generate event descriptions or make judgments for use in an intelligent and automated system[7]. IoT cameras capture the violation of the vehicle when a signal is generated for capture. This signal could be caused by speeding, failing to stop at a red light, or riding without a helmet. In each of the above cases, different techniques are used in finding the violation. LIDAR technology is an efficient tool for detecting over speeding. When the LIDAR hardware detects over speeding, it sends a signal to the IoT camera, which then captures the vehicle. Similarly, other offences can be caught by the cameras.

The fundamental reason for installing an IoT camera is to process the images captured. The steps involved in image processing are image preprocessing, extracting the number plate from the image, and extracting the characters from the number plate. The violation image is preprocessed to highlight important information. The general image processing module utilised in this project is OpenCV[5]. To detect number plates, the system employs Canny edge detection. Tesseract is a module that recognises characters from number plates. The output of the image processing section contains the characters from the licence plate as well as the violation code, which symbolises the traffic law that was broken.

Each IoT camera has a unique private key and public key. The private key is generated when the camera is first initialized. A public key generated from the private key helps in identifying individual cameras. A private key is used to generate the signature on the data created by the IoT camera. This signature can be verified by the public key. IoT cameras are utilised instead of traditional CCTV cameras since they eliminate the necessity for a centralised server. The usage of a centralised server may result in manipulation with violation data. IoT cameras allow data to be processed within the camera. The IoT cameras can process images to extract the necessary information and send it to the blockchain network.

B. Miner

Miners are the individuals that participate in the blockchain mining process. Blockchain mining is the process of validating each transaction that occurs on the blockchain network. Miners obtain the mining application from a trustworthy source and use the hardware to run it. Miners perform the mining process in exchange for cryptocurrency. A miner is the entity in the blockchain that ensures its decentalization. The blockchain blocks may or may not have been stored by miners. Miners use several algorithms to validate blockchain blocks. Proof of Work (PoW), Proof of Stake (PoS), and other well-known algorithms are examples. These algorithms work by making the miner's hardware perform computations to solve a mathematical problem. Peer-to-peer networks are the primary means of inter-node communication.

The miner network in the proposed project consists of several miners. Among the miners, there are central nodes that perform the extra task of broadcasting blocks to all other miners. These special miners are normally chosen from the miners that are not behind NAT and have a fixed IP address. The IoT camera broadcasts the message to these central nodes, which is then given to all miners. When a new miner joins the blockchain network, it has the addresses of some central nodes. Then the new miner registers itself with the central node. The central node, on receiving a block, will forward it to this new miner also. When a new message block is received by the miner, it checks if the public key in the block is actually the public key of the IoT camera. This is done to ensure that no other party other than the IoT camera can add a violation to the blockchain. The next step involves the verification of the signature. If the signature is valid, the proof of work algorithm is initiated. Otherwise, the block is dropped. Once the message block is mined using the proof of work algorithm, the newly created blockchain block is added to the blockchain database. The miner also forwards the blockchain block to other miners in the network. Those miners add the new blockchain block to the blockchain database on satisfying the check for authenticity.

C. Public User

Public users are members of the broader public who utilise the service. At all times, the system must ensure that all users have access to the violation data. The proposed system also alerts users when they infringe traffic laws. A public blockchain infrastructure is used in the proposed blockchain. As a result, anyone can join and

observe the blockchain's activity. Users can download mining software and begin mining whenever they want. This contributes to the blockchain's self-governing nature.

IV. SYSTEM IMPLEMENTATION

The proposed system is an advancement in the traditional traffic violation monitoring system that places emphasis on transparency, security, and availability.

The IoT cameras identify traffic offences, which are then turned into blocks. The number plate characters must be extracted from violation images collected by the IoT camera. The image processing unit of the IoT camera does this. For speedier processing, the image is transformed to grayscale as a preprocessing step. To reduce noise and smooth the picture, an edge-preserving filter known as bilateral filtering is performed. The edges in the image are detected using the Canny edge detection technique. A contour is a line that links all points with the same intensity along an object's boundaries. 4-sided polygons are extracted from the observed contours. The contour with the biggest area is chosen as the licence plate. The Tesseract is utilised to recognise the characters on the licence plate using Optical Character Recognition (OCR). This stage's output is the number plate characters that will be used in the next step. This block contains the violation information (vehicle number, violation code, timestamp, and URL to image captured), the public key of the IoT camera, and the signature generated with the private key of the IoT camera.

The created block is subsequently sent out to the network's miners. When a miner receives a block, it is verified for authenticity. The public key and signature provided in the block are used to do this. Miners must also ensure that the block's public key matches the set of public keys provided by the authorities. This list of public keys also associates camera public keys with the locations where they are mounted. Miners run the proof-of-work algorithm once all requirements are met. The miner who discovers the required hash is the first to broadcast the mined block to the rest of the network's miners.

The violation data blockchain allows multiple applications to run on top of it. Vehicle tracking and violation notification are two such examples. The former takes a vehicle number as an input, and the algorithm compares it to the vehicle number on the blockchain, providing information about the car's path. The Violation notification application detects a traffic violation added to the blockchain and reports the offence to the vehicle owner. This can be done by traffic monitoring authorities or by a third party by email or SMS. The openness of the blockchain allows third-party developers to develop applications using the blockchain data.

Algorithm 1 Block Authentication

Require: $keylist$ ←set of public keys of IoT camera
1: Read violation details and create block with data, timestamp and previous hash
2: $message \leftarrow data['message']$, $sign \leftarrow data['signature']$, $key \leftarrow message['key']$
3: Compute hash of data, $hash \leftarrow hash(message)$
4: **if** key is present in $keylist$ **then**
5: Verify signature using hash and signature
6: **if** Signature is valid **then**
7: Mine the block
8: **else**
9: Drop message block ▷ message not authentic
10: **end if**
11: **else**
12: Drop message block
13: **end if**

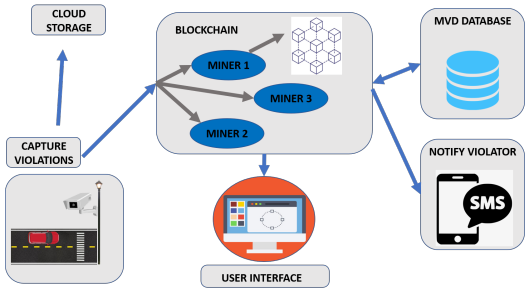

FIG. 3. architecture diagram

V. APPLICATIONS OF SYSTEM

An intelligent traffic management system provides an advantage by offering safe public transportation, strict punishments on violating traffic rules, ticketing system automation, etc. And advanced solutions for solving traffic congestion in major cities around the world.

The first application is that it makes manual traffic monitoring much more compatible and easier for the law violation detectors. Also, it is very efficient to catch those who violate the law or create unnecessary accidents.It provides congestion-free traffic.Helps in improvising traditional ticketing with automated E-bill payment system.Speed sensors to warn commuters over speed violation.Offer safe and punctual public transportation and eradicates any kind of pollution.

The second application is that system that is planned in the project is much more transparent than the existing system, so that there could not be any kind of alterations or modifications by the violators that can lead to corruptions and mismanagement by the motor vehicle department.So any kind of changes done in the system can be easily viewed or detected by anyone who is intended to look into it.

Third application is regarding the databases fed in the file systems, that could be easily tampered and changed according to some influence. So the project proposes an approach that prevents any kind of changes without any

proper reason.The database in the system includes information about vehicle owned by the person with all details regarding him so while violating any kind of law will eventually detect who the person is and all information are taken from databases.The purpose of Block chain system added creates more security for any kind of data manipulations that has been existing for a long time and it keeps more secure the data that are needed to be protected.

Fourth application is about how the vehicles are tracked or being detected by attaining the information from various databases that have been provided and matching with the existing records.Also there will be more actions that will be taken if the number plate of vehicle that has been violated is fake one and further action is taken from the police department if it is related to any other crimes.There wont be any kind of special privileges to politicians, ministers or any top official except VVIP, there will be consideration for hospital uses and some emergency cases that are allowed.The notification of violators are send to those who break the law and are caught on the block chain network.

'Fifth applications is it refers to how the system operates 24x7, without interruption or issues. It also refers to how the system is extremely efficient and well-maintained so that any type of violation may be discovered without difficulty.The cost of maintenance is quite low as compared to the existing system, which requires extensive repairs if it is broken, thus for the violation, a lot more convenient and well-defined system is required.

VI. SYSTEM PERFORMANCE ANALYSIS

The proposed system has been proven to be extremely efficient. A machine with an i3 CPU, 4GB RAM, and 1GB GPU is used for performance analysis. The rationale for selecting this computer is that its characteristics are excellent for most IoT cameras. The complete system was broken into three pieces for in-depth analysis: the IoT camera, Miner, and database retrieval.

The image processing component of the IoT camera was subjected to the following performance tests: The processing time for the violation image was roughly 2 seconds after accurate calculations. This time span includes both number plate detection and identification of number plate characters. The next step in the IoT camera's processing is public key cryptography. The system generated a private key in 0.27 seconds (ECC-curve=P-256). The signature(DSS-fips-186-3) of the message was created in 0.28 seconds using a private key. According to the test results, the entire operation of the IoT camera for a single violation data can be completed in less than 3 seconds.

The performance of the miner part can be divided into two. First, the miner verifies the signature(DSS-fips-186-3) of the message using the public key. According to our test results, the verification was completed in about 0.21 seconds. Second, the miner runs the proof of work algorithm (SHA-256). The accurate time required for pow cannot be predicted since it can be different every time it is executed. but it showed an average of about 0.44 seconds. Thus, the complete execution of single violation data takes about 0.7 seconds.

The database retrieval phase entails getting information from the blockchain database. This step takes roughly 0.29 seconds on average. The time required for retrieval increases gradually as the size of the data in the blockchain grows.

According to the results of the performance analysis, the IOT camera can finish the procedure in the required amount of time, even if the system does not have high specifications. The miners are given very efficient algorithms, which makes it easier for them to complete the mining operation with low-spec hardware. The system can also run block chain applications at a high pace on its own. Thus, the proposed system demonstrates that it is the best way to construct a traffic violation data security system.

VII. CONCLUSION AND FUTURE WORK

In conclusion, we can say that the methods we proposed in the project were more likely to be successful and could potentially make existing traffic monitoring more efficient and convenient. Early mentioned applications, we can say that they help to make the monitoring of traffic much more transparent without any influence or modifications in the system with the help of Blockchain technology, which is more secure. It is also working 24x7 without any disruptions, indicating that the system is well maintained and easy to control.

The proposed system to be implemented in real life needs some additional modifications. Some vehicle data should not be added to the blockchain even if it breaches traffic rules. Ambulances, police cars, and other such vehicles fall into this category. As a result, such vehicles must be distinguished from ordinary vehicles. Color-coding the car number plates is one way to accomplish this. Vehicle with special privileges must be given a different colour than normal vehicles number plate. Using the image processing in IoT cameras, privileged vehicles can now be distinguished. Another issue faced is fake number plates. This can be solved by introducing a new type of numberplate which has an authentication mark along with the number. Then the IoT camera can check for the authenticity of the number plate before adding data to the blockchain.As an improvement to this project, we also propose a system in which miners get tokens by mining the blocks in the blockchain. These tokens can be used to pay the violation fine[6], thus helping the miners and self-sustaining the blockchain system. As technology advances, better violation detection and vehicle identification aid in improving the overall performance of project.

[1] Pradana, Aditya Goh, Ong Sing Jaya Kumar, Yogan Mohammed, Ali. (2018). Blockchain Traffic Offence Demerit Points Smart Contracts: Proof of Work. International Journal of Advanced Computer Science and Applications. 9. 10.14569/IJACSA.2018.091153.

[2] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[3] Rüdiger Schollmeier, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).

[4] T. Chattopadhyay, P. Sinha and P. Biswas, "Performance of Document Image OCR Systems for Recognizing Video Texts on Embedded Platform," 2011 International Conference on Computational Intelligence and Communication Networks, 2011, pp. 606-610, doi: 10.1109/CICN.2011.131.

[5] Shariff, A Bhatia, Raghav Kuma, Raghwendra Jha, Sarthak. (2021). Vehicle Number Plate Detection Using Python and Open CV. 525-529. 10.1109/ICACITE51222.2021.9404556.

[6] D. Tapscott and A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, 2016

[7] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger," in2018 IEEE International Congress on Internet of Things (ICIOT), 2018, pp. 33-40.