IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || March. 2022 || PP 30-34
National Conference on Innovations and Research in Science & Technology (NCIRST-22)

Traffic Police Management and Detection of Stolen Vehicle Using QR Code

Prof. Shegar Sneha Ramdas.[1], Jagtap Pooja Sanjay[2] , Jagtap Raghinee Vilas[3],Khose Akanksha Sakharam[4],Shinde Kaveri Dattatray[5]

[1](Department of Computer Engg. SGOI COE, Belhe, /SPPU, Pune, India)
[2](Department of Computer Engg. SGOI COE, Belhe, /SPPU, Pune, India)
[3](Department of Computer Engg. SGOI COE, Belhe, /SPPU, Pune, India)
[4](Department of Computer Engg. SGOI COE, Belhe, /SPPU, Pune, India

Abstract : *This project aims at implementing a vehicle document check system where databases and documents are Retrieved by the traffic police by their smart phones and the physical documents are not needed to be carried along there by saving time in document verification. Initially we assign them unique identity numbers and scan their RC, Insurance, Emission paper, vehicle name, and number and store it in the database at the back end. Using the above information, we create a QR code and stick it on an irreplaceable part of the vehicle. At the front end we create an application with which traffic police can scan the QR code on his phone and all the details about the owner of the vehicle and all the documents earlier stored will be shown on the phone. We can make the driver's license as unique identification if needed for the application query search in case scanner fails to work. I this project, System mainly focuses on traffic police management for no need to carry the document of vehicles. Here, System Use QR code technique for the documentary purpose. In this system, the main actor is retailer, traffic police, department police. Through this actor our system become very helpful to user and government also.*

Keywords *- QR Code, Android, AES Algorithm, Encryption, Decryption.*

I. INTRODUCTION

1.1 GENERAL:

Traffic police management becomes issue nowadays. It becomes hectic to manage documents manually. So, QR code makes it easy. We make documentary of vehicle and generate one QR code, it will help to police management easily.

1.2 BACKGROUND:

The cases of road accidents have gone up as the number of vehicles increased multifold. Over speeding and traveling without necessary documents is a common sight now and to deal with this, traffic cops have to do vehicle verification every now and then. Yet, the process is not devoid of challenge.

Firstly, stopping a driver and verifying each document manually is a tedious task. It consumes a lot of time and effort. Secondly, it is difficult to determine the authenticity of the documents. The driver may show a fake or duplicate document and get cleared. The whole process to validate the genuineness of traffic documents is a taxing job. Thirdly, with the thefts going up, it's becoming quite difficult to track the stolen vehicles. So, it's time to make the vehicle verification process more quick and efficient. And one of the solutions is to use QR Code technology. In existing system, all manual process is available. Documentary maintenance is very hectic.

1.3 OBJECTIVES OF STUDY:

Vehicle security is an important issue in our society. for improving methods of vehicle security in public and private places. When the license plate number is missing or unknown then how to find the vehicle information is really a big challenge.

1.4 SCOPE OF WORK:

Today, QR Codes are being used worldwide across various industries. These include aviation, chemicals, sports, product packaging, and transportation.

This quick and robust system will propose to detect and describe features of a vehicle image, specifically in an android application using QR code mounted on vehicles. After description of QR code it fires the query on database for searching information in the database. Real time android applications are the real challenges for this system.

1.5 NEED OF STUDY:

Now a day's Vehicle security is an important issue in our society. for improving methods of vehicle security in public and private places. When the license plate number is missing or unknown then how to find the vehicle information is really a big challenge. To overcome this issue, we are proposing Vehicle Identification System which is a QR code based system that will help in identifying the vehicle in public or private places like Traffic signal and Society, buildings, parking respectively.

We are proposing an application that replaces the current manual processes for checking the vehicle documents through police. User side suitable to carry documents. We are designing an Android + web application named Traffic Police Management which will be beneficial for people to help for do not carry documents of vehicle and maintained the document.

II. LITERATURE SURVEY

1.PAPER NAME: E-RTO MANAGEMENT SYSTEM

This paper describes author surveyed problem of RTO, RTO employees having lot of work burden of making registration, license issue, transfer, etc. which requires lots of paper work. As a result people cannot get things done right time. This system helpful for RTO officials to maintain record systematically and reduce lots of paper work and manual efforts.

2.PAPER NAME : VEHICLE TRACKING USING RFID

This paper describes technique has been discussed for challan system. Here, user provides details to RTO database.

By scanning QR code which contain overall information of the vehicle. We get vehicle owner details. This system also detects culprit vehicle.

III. SYSTEM ARCHITECTURE

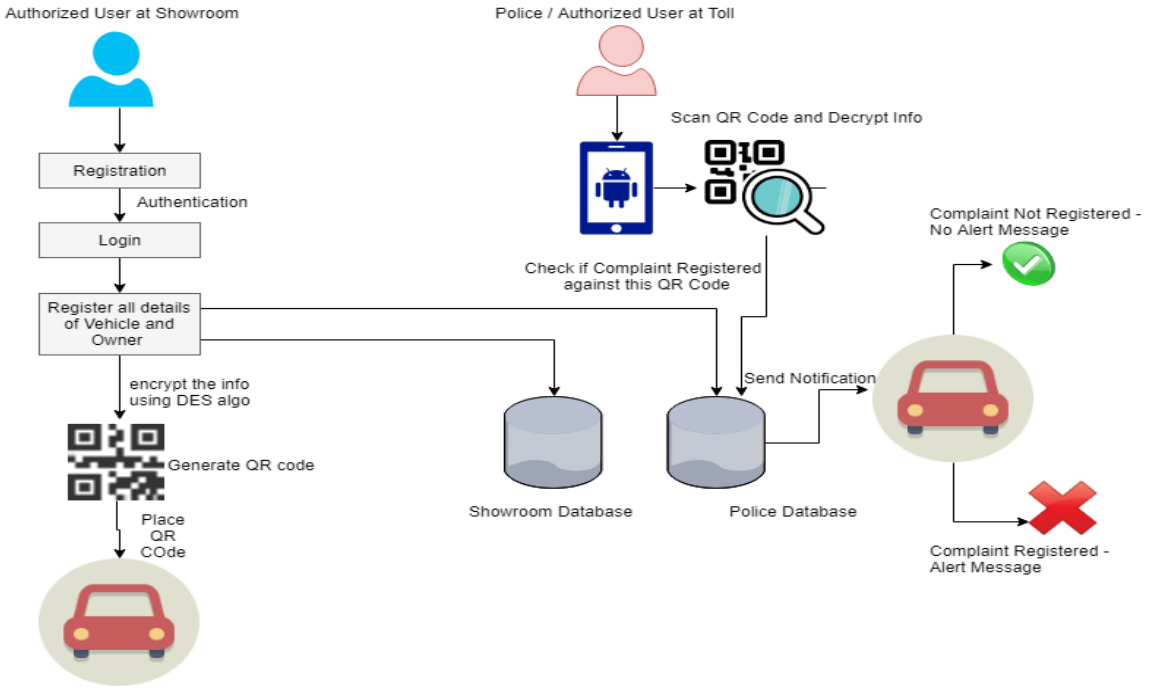

Fig. System Architecture

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented.

When we buy a vehicle then authorized person of showroom take our all details regarding the vehicle and register all the details of vehicle and owner of vehicle. Then taking all the details QR code is generated for that vehicle holding that particular information about that vehicle using encryption algorithm. That QR code is placed on vehicle also the owner of vehicle can also have a soft copy in mobile while travelling at any time. At a time when we have to show the documents to the traffic police then they can simply scan that QR code and can examine all the documents.

Using this system, we can also find the stolen vehicles. Suppose our car is missed from our place, we can register the complaint to any near by police station. Then by taking the details they can activate the complaint i.e. the car is stolen. By then any car that come across with such specification is verified and the car can be found out.

IV. ALGORITHM

1.AES ALGORITHM:

The AES algorithm is a symmetric-key cryptographic algorithm and a block cipher. This algorithm uses the same key to encrypt and decrypt. AES actually supports a variety of block sizes and keys that will be used. But after being standardized by the National Institute of Standards and Technology (NIST), Rijndael uses fixed block and key length sizes of 128, 192, and 256 bits, so commonly referred to as AES-128, AES-192, and AES256 [14]. In general, the encryption process in AES divided into two namely the encryption process itself (Encryption Process) and key generation (Key Expansion / Key Schedule) or round key. In the encryption process the AES-128 algorithm operates as follows (outside the round key generation process) [15]: First step is adding Round-Key. Perform XOR between initial states (plaintext) with the cipher key. Second step is Round as much as Nr-1 times (nine rounds on AES128). The process of each round is:

a. Sub-Bytes: bytes substitution by using the substitution table (S-box).

b. Shift-Rows: shifting state array rows by wrapping.

c. Mix-Columns: scrambles the data in each state array column.

d. Add Round-Key: performs XOR between the current states with round key. 3. Final Round. Process for the last round: a. Sub Bytes b. Shift Rows c. Add Round Key

1.1 Encryption :

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.
Each round comprises of 4 steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The last round doesn't have the Mix Columns round.
The Sub Bytes does the substitution and Shift Rows and Mix Columns performs the permutation in the algorithm.
Sub Bytes :
This step implements the substitution.
In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.
The next two steps implement the permutation.
Shift Rows :
This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.
    - MixColumns :
    - This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.
    - This step is skipped in the last round.
    - Add Round Keys :
    - Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.
1.2 Decryption :
The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns **:**

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

AES instruction set is now integrated into the CPU (offers throughput of several GB/s)to improve the speed and security of applications that use AES for encryption and decryption. Even though its been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.

Data Flow Diagrams:

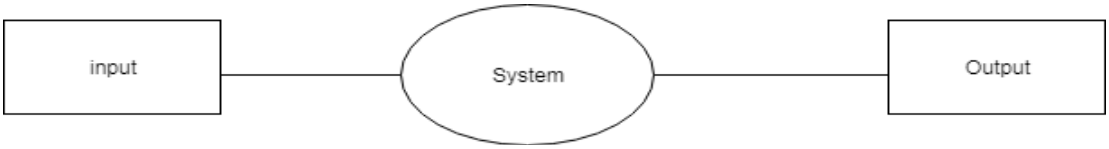

Fig : Level 0 Data Flow Diagram

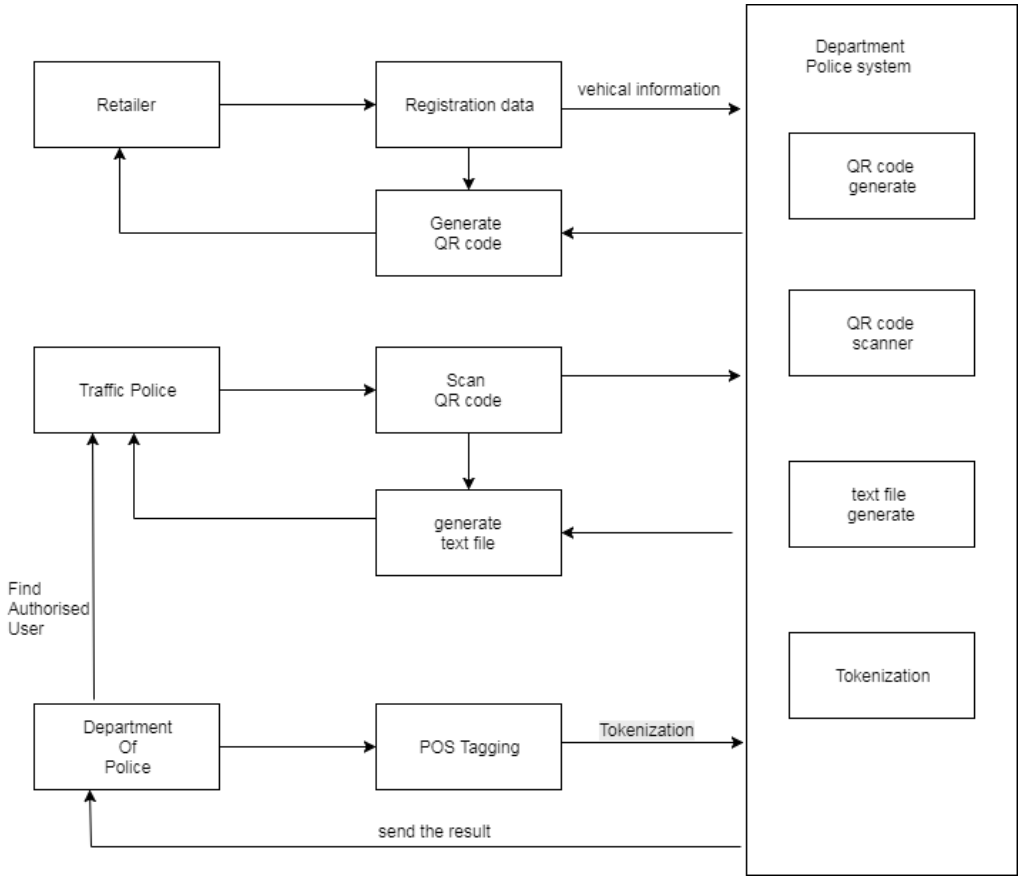

Fig : Level 1 Data Flow Diagram

MATHEMATICAL MODELLING:

- Let S be the Whole system which consists:
- Let S be the Whole system S= {IP, Pro, OP}
- Where,
- A. IP is the input of the system.
- B. Pro is the procedure applied to the system to process the given input.
- C. OP is the output of the system.
- Where,
- A. Input:
- IP= {u, p, r}.
- Where,
- 1. u be the user or retailer.
- 2. p be finding authorized user i.e. traffic police.
- 3.r be send result to traffic police.

ADVANTAGES:

1. QR code technology makes easy the task for User and Police department also.
2. Efficiency is very high.
3. Time complexity is very low.
4. It can be used for document verification in any organization.
5. It is not necessary to carry the documents every time.
6. System is user friendly

V. CONCLUSION

By using this application it is not necessary to carry all the documents and license every time. Only you have to carry QR code in your Smartphone. By using our system the user goes through the verification process through a reliable and efficient manner. User can get QR code by simply registering with the system. Also we can find the stolen vehicle.

REFERENCES

[1]. B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, Global Positioning System: Theory and Practice, Springer-Verlag, 4th edition.

[2]. N. Priyantha, A. Chakraborthy, and H. Balakrishnan, "The cricket location-support system," in Proc. of International Conference on Mobile Computing and Networking, Boston,MA, Aug. 2000, pp. 32– 43.

[3]. P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in Proc. of Infocom'2000, Tel Aviv, Israel, Mar. 2000, vol. 2, pp. 775–584.

[4]. A. Nasipuri and K. Li, "A directionality based location discovery scheme for wireless sensor networks," in First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA,

[5]. C. Savarese, J. M. Rabaey, and J. Beutel, "Locationing in distributed ad-hoc wireless sensor networks," in Proc. of ICASSP'01, 2001, vol. 4, pp. 2037–2040.

[6]. S. Capkun, Maher Hamdi, and J. P. Hubaux, "GPS-free positioning in mobile ad-hoc networks," Cluster Computing, vol. 5, no. 2