



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

Smart Vehicle Authenticator System

Dr. P. BALASHANMUGAVADIVU, ARUN M, HRITHIK S, LOGESHWARAN P, MOHAMMED FHAYAZ M

Associate Professor, Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal Dt, India

Students, Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal Dt, India

ABSTRACT: In day-to-day life there is lots of increment in population. Considering the positive aspects of the QR Code, the proposed method is brought into actual practice will definitely prove to be a boon. In the proposed project vehicle documents are verified using QR code. By using our system, the driver will go through the verification process through a reliable and efficient manner by a traffic inspector. Through our system user can access vehicle documents using QR code. Now a day most of the people are using their own vehicles. Due to this traffic work has been increased. So, this work deals with the creation of a real-life android application, where all the necessary details of a vehicle (i.e., Registration Certificate, Insurance Policy and vehicle's Pollution Under Control Certificate) are coordinated and stored by the database of RTO admin without much effort and it can be accessed by both the user and vehicle inspector. We can digitalize all documents which are taken care of without so many efforts and hard work.

I.INTRODUCTION

The introduction of different cloud-based applications, as well as other cloud technologies authentication challenges, continue to introduce several threat vectors to many organizations. Furthermore, the answers on dealing with identity management, authentication, and access-control security in the many heterogeneous environments constitute diverse challenges to many industries. Things-enabled communications, such as Internet of Things (IoT) and Internet of Vehicles (IoV), for instance, are particularly affected by this authentication challenge. "Unique QR Code For Vehicle Verification" is for traffic police using QR code to avoid to carry the physical documents it also avoid some security Issues and also reduce.

Improving Transparency in system and lots of time should be saved. It can save the amount of time of user and authority. It deals with the creation of an android application where all details of the vehicle. The admin (RTO Admin) can handle or control the addition, updating and removing of documents on a cloud server and also they give the Unique ID (mobile number) and password login page(fig-1) to the particular user and also notification alert feature if citizen's documents expired.

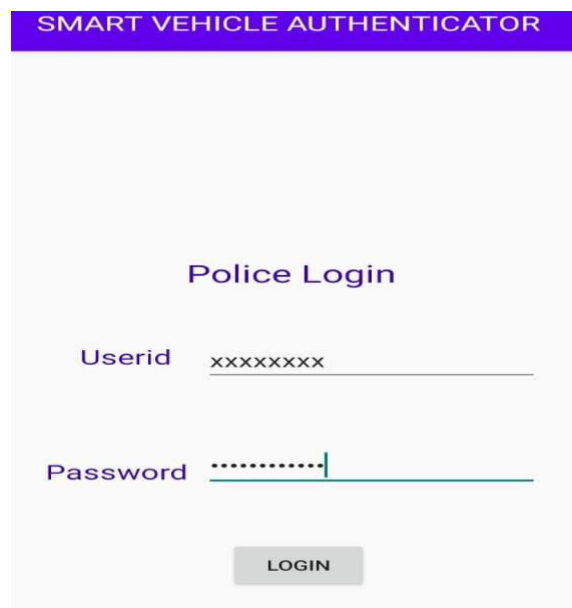


Fig – 1 Login Page

Security and privacy are great importance to a cloud server and message authentication. Without security, it is difficult to store and securely send the data from the cloud server to an authorized person. Here AES algorithm is used to provide strong security to cloud server and mobile authentication.

Now a day's population has become a major factor to be considered as a result the number of vehicle's are growing by increasing problems of vehicle and license registration, insurance and tax validity for RTO administration and documents verification by traffic inspector. RTO employees having lot of work burden of making registration, license issue, transfer etc, which requires lot of paper work.

As a result people can't get the things done in right time, which is the waste of time and energy. Similarly the vehicle owner sometimes forgets to carry the license and other vehicle related documents at the time of inspection. This paper proposed an approach to solve such problems that is by storing all the information related to vehicle and driver at database by RTO administrator and an android application is provided by both the vehicle inspector and user to retrieve vehicle related information and also we can add a provision to track a stolen vehicle.

This project targets to store the information related to vehicle such as insurance, license, PUC details, insurance details, personal details of the applier and registration date. This application would be installed in Android phones of traffic police and user. And it will provide input fields to traffic police to enter the vehicle number as well as to scan the QR code in order to retrieve the information related to vehicle and license from database. This application also generates fine if the user violate traffic rules and location at

II.LITERATURE REVIEW

In literature review, many IoT applications have been proposed some of which have suggested and designed authentication systems and some others have performed evaluation procedures. From these, a number of QRC-based methods have been performing smart services utilizing the QRC itself. But the very important thing to consider is that: are these QRC-based IoT applications authenticated. For example, there exist many systems concern authentication, data privacy, and security such as internet of things (IoT) [1], smart applications [6], cryptography and data encryption. This has contributed to a smart life environment in terms of data privacy, security, and computation time. In general, these proposed systems may fail to achieve a high level of security. One of the biggest issues is when the application becomes susceptible for unusual actions.

However, there exist several attempts to propose secure applications e.g., in which their aims are to protect data and attain authentication. These examples have designed a QRC based authentication mechanism for users in order to prevent threats and to increase security of users' private contents. The QRC is a very effective technology for many IoT applications in terms of safety and authenticity e.g., these reviewed in a QRC technology has been used in order to perform an authentication procedure for users engaged with an cloud computing environment. QRC has a good feature that is it can store a huge portion of information in a very small area. A lot of IoT applications can exploit such a feature and re-use it based on needs. Many examples are in detailed reviewed in. Therefore, these contents of QRC can be verified in terms of authentication and privacy. Usually, the verification process concerns contents of QRC. If contents of QRC have not been changed in an unauthorized manner, the privacy of QRC can be considered as attained and QRC is private. Therefore, related data needs to be private and secure. Additionally, the related applications should be confidential with the help of QRC technique. In order to do so, a strong security scheme needs to be and the verification process of QRC contents has to be precise. Hence, in this paper, the verification procedure with several security layers are considered. So, the verification procedure consists of a number of steps in order to increase the security of contents of QRC. The proposed QRAM is applied on QRC to verify security objectives. In addition, it verifies the authenticity of QRC. Simply, the QRAM has performed three authentication procedures each of which is applied to a single part of QRC content to produce its distinguished output. Once this procedure has been applied, the computation time is expected to be reduced. For security purposes, the verification procedures will stop immediately and will not go for the next layer's verification if the following possibility has occurred which is: the case that one layer has produced a wrongly compared result. Thus, QRAM instantly halts the verification procedure. There are however many difficulties and challenges still. Thus, there have been research studies attempting to overcome those challenges. An example of those challenges might be a compensation of a technique to be fast-responsive to real-time IoT applications and robust enough against threats. Thus, in order to meet real-time applications, further enhancement is needed. Therefore, QRAM aims to enhance authentication procedures applied to IoT applications that depend on QRC in terms of computation time.

III.METHODOLOGY

Automotive systems are becoming increasingly sophisticated and interconnected to various gadgets. Vehicle safety and security are one the major issues that pose challenges in the automotive field [1].It appears that the security of the automotive systems have to be looked at more closely than what it is now, as ignoring security could lead to disastrous consequences. A sophisticated mechanism that ensures security and safety of automobiles is a requirement of the day. Smart phones have replaced most of the electronic gadgets these days and are user-friendly. They even provide enough privacy to its users. In case of theft or mishandling, smart phones can be easily locked and made unusable, thus preventing unauthorized access. In this work, an embedded system is developed to unlock car using an authorized smart phone.

A QR Code (abbreviated from Quick Response Code) as shown in Fig-2 is a two-dimensional barcode consisting of a black and white pixel pattern which allows encoding up to a few hundred characters [2]. QR code is the trademark for a type of matrix barcode first designed for the automotive industry in Japan. QR codes can be used with many mobile device operating systems like Android Operating System and iOS (iphone Operating System) [3]. These devices support URL redirection, which allows QR codes to send metadata to existing applications on the device. Many paid or free apps are available with the ability to scan the codes and hard-link to external applications.



Fig 1: Bar Code

This work aims at realizing an embedded system that is designed to be implemented in the car to provide key less unlock mechanism for the car doors using the car's unique QR code [4] and smart phone (app). The electronic system realized in this work has the following objectives:

ATmega328P based Arduino Uno microcontroller board is used to realize the system. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, USB connection, a power jack and is as shown in fig- 2 . The HC-05 Bluetooth Module can be used in Master or Slave configuration, making it a great solution for wireless communication. Servo motor (Micro Servo DXW90), that can rotate approximately 180 degrees (90 in each direction) is used for locking and unlocking mechanisms.

A unique QR code is generated for every car and is placed in a secure and accessible location in the car. A smart phone having a customized QR code scanner is used to scan the QR code [5] of car. The QR code scanner designed in this work provides a secure and intended access to the car. The scanner app is designed to work in a unique way for every car, hence is referred to as customized scanner. The user who knows the unique password of the app can scan the code. This scanned data is encrypted and sent to the vehicle's locking system via Bluetooth module.

IV.RESULTS

A quick response code-based authentication method (QRAM) is proposed. QRAM is applicable for lots of internet of things (IoT) applications. QRAM aims to verify requests of such an access to IoT applications. Requests are made

using a quick response code (QRC). To authenticate contents of QRC, users will scan QRC to access IoT applications. To authenticate contents of QRC, three procedures are applied. QRAM contributes to IoT automatic access systems or smart applications in terms of authentication and safety of access. QRAM is evaluated in term of security factors (e.g., authentication). Computation time of authentication procedures for several IoT applications has become a considerable issue. QRAM aims to reduce computation time consumed to authenticate each QRC. Some authentication techniques still face difficulties when an IoT application requires fast response to users; therefore, QRAM aims to enhance so to meet real-time applications. Thus, QRAM is compared to several competitive methods used to verify QRC in term of computation time. Results confirmed that QRAM is faster than other competitive techniques. Besides, results have shown a high level of complexity in term of decryption time needed to deduce private contents of QRC. QRAM also is robust against unauthorized requests of access.

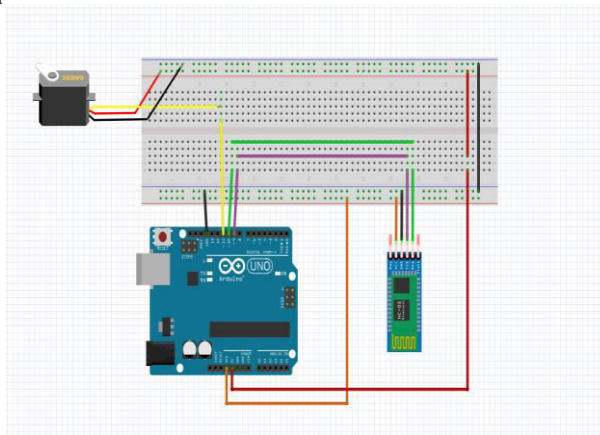


Fig 2: Locking and Unlocking Mechanism

By extension, therefore, this proposed approach can be leveraged in any IoV-based platform for a secure seamless automation process. In terms of security, this proposed approach provides a relatively similar security strength to previous studies. However, the flexibility and ease-of-use of security have been overlooked. Usable security is fundamentally a component of security that has proven to aid technology adoption and enhanced security. In this section, the performance of the proposed QRAM will be analysed. The obtained results after the QRAM has been applied will be discussed and evaluated. The QRAM will be evaluated in term of authentication and computation time.

V.CONCLUSION

In addition, results have shown a high level of complexity in terms of decryption time needed to deduce the QRC's secret key. Obtained results confirmed that the QRAM is robust against unusual threats and potential actions. The QRAM is important to work with applications which require online verification processes. Future works are dedicated to enhance computation time to work in a faster environment under complex scenarios e.g., when there are more than two parties requiring a response in a same time.

REFERENCES

- [1] S.Ponlatha, P.Umashankar, P.BalashanmugaVadivu, D.Chitra, " AN IoT based efficient energy management in smart grid using SMACA technique", Wiley- International Transaction on Electrical Energy System, Vol.31,No.125, pp.1-22, Dec 2021.
- [2] Ms. Ankita V. Gocke, Prof. Rahul V. Dagade "Vehicle Verification system using Advanced Digi-Locker system", International Journal of Computer Applications. 8th Aug 2018.
- [3] David Lorenzia, Jaideep Vaidya, Soon Chun, Basit Shafiq, Vijayalakshmi Atluri "Enhancing the government service experience through QR codes on mobile platforms", Elsevier (Journal). 6th Jun 2014.
- [4] Mr. Komal chorhgade, Mr. Piyush Dahiwele, Prof. Prajakta pise, "RTO automation using QR code", IRJET. 4th Apr 2018.
- [5] Mr. Nilesh R. Patil, Prof. Rajesh Dharmik, "Secured Cloud Architecture for Cloud Service Provider", WCFTR. 2016.
- [6] Mr. Paritosh Patil, Mr. Shrinivas Shah, Ms. Pooja Shivale, Prof. Murali Parameswaran "Park IT- QR based vehicle security", IRJET. 8th Aug 2020.



- [7] Krassie Petrova, Adriana Romanello, B. Dawn Medlin, and Sandra A. Vannoy, “QR Codes Advantages and Dangers”, ICETE. 2016.
- [8] Mr. Manjunath S Patil, Mr. Basavaraj K Madagouda, Mr. Vinod C Desai, “E-RTO Management System”, IJERT. 2013.
- [9] Mr. Sarbjit Kaur, “An Automatic Number Plate Recognition System under Image Processing”, MECS. 2016.
- [10] Mr. Maysaa Abd Ulkareem Naser, Mr. Eman Talib Jasim, Mr. Haider M. Al- Mashhadi “QR code based two-factor authentication to verify paper-based documents”, TELKOMNIKA. 2018.
- [11] Mr. K. Venkateswarlu, Ms. K. Ramya Thanuja,” Vehicle theft detection using QR code”, UGC Care Group I Journal. 14th Jan 2021.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details