



QR Code Based Passport Smart Card Using an Advanced Encryption Standard (AES) Algorithm

Vivek N. Waghmare, Anju R. Unnithan, Deepjyoti B. Korde, Tejswini N. Patil and Siddhi A. Suryawanshi
Department of Computer Engineering, Sandip Foundation's, Sandip Institute of Technology & Research Centre, Mahiravani,
Nashik- 422213

ARTICLE INFO

Article history:

Received: 15 June 2020;

Received in revised form:

17 July 2020;

Accepted: 28 July 2020;

Keywords

QR Code,
QR Scanner,
Authentication,
Security,
Verification.

ABSTRACT

The implementation of QR code based smart card has been becoming an ever increasing popularity in the traceability of products. This QR code smart card contains the Passport details, Pan card details, Aadhar card details and Voters card details. QR code is helpful to store and process the information through black and white dots on the QR scanner which transmit by the reader. The QR reader reads the data present in the passport and sends the data by using QR Scanner through wireless network. As soon as the card shown, using QR reader, the details of the person appear on the computer screen and verify it using the data present in the system and if it matches then the details of the passport holder is displayed. It reduces the burden of documentation which thereby reduces the time consumption. This makes the system centralized by increasing the security.

© 2020 Elixir All rights reserved.

Introduction

Fake passport is a wide spread problem all over the world and every day new issues regarding the same are reported. Passport is issued by one department to an individual and when it is presented to third parties, they cannot easily find out if it is fake or genuine. Also passport issued by one government department are often used to obtain Id from other department.

According to a report from The Hindu back in 2017, a case was reported against a few Immigrants from Bangladesh carrying fake passports. This is not an incident of one of a kind. Every year thousands of fake passport cases are reported. To combat this it is necessary that passports are bound to documents that verify the identity of the individual and validate the citizenship of the passport holder.

This approach aims at developing a system that uses QR code based passport smart card using Advanced Encryption Standard Algorithm. The objective of this system is to provide a secured verification of passport. A third level security can be used for the same. This system also aims at providing a unique identification through QR Code.

Related Work

Piotr Bilski et al. proposed an architecture that consists of computerized portable units carried by border officers and the server cloud infrastructure. It reads from passports and confronted against local and remote data, stored in the central database. The paper presents the general architecture of the proposed border control system. The structure of the application, responsible for connecting the RFID reader with the portable computer and communicating with the Internet database via the Web Services technology is presented [6].

M. Prathilothamai et al. suggested that big data is an emerging technology that is becoming an essential part of national governance. Aadhaar is the unique identification scheme of India, handled by the Unique Identification

Authority of India (UIDAI), which deals with big data. Every person above the age of 5 years has to register their demographic details (Name, Date of Birth, Address and Phone number) and biometric details (10 fingerprints and both iris) and then these details are used to verify the authenticity of the person when any services are required by him. Passport is a legal document that is carried by a person when he travels between countries, but in the case of the older passports with no biometric data, a person may have more than one legal passport with different demographic details [7].

Shivani Kundra et al. analysed the study of various technologies used in E-passport design. A cryptographic security analysis of the e-passport using face fingerprint, palm print and iris biometric that are intended to provide improved security in protecting biometric information of the e-passport bearer. Together, RFID and biometric technologies promise to reduce fraud, ease identity checks, and enhance security. At the same time, these technologies raise new risks. The system explore the privacy and security implications of this worldwide implementing next-generation authentication technology: e-passport. This system describe privacy and security issues that apply to e-passports, and then analyze these issues in the context of the International Civil Aviation Organization (ICAO) standard for e-passports [10].

Shiv Kumar, Shrawan Kumar Sharma et al. analysed citizen can use e-governance tool to apply UID, VOTER ID, PAN CARD etc to maximize the uses of the tool with the help of web application like e-Mitra and Internet. Presently only three types of services are provided [9].

Abdulsalam Dukyil et al. developed a system that uses fuzzy multi objective model for a RFID-enabled passport tracking system under an uncertain input data. A new decision making algorithm was used to select the best solution method [8].

Piotr Bilski et al. proposed a border control system which connects a RFID reader with internet database. M. Prathilothamai et al. analysed the big data used in aadhar card which when used with passport provide unique authenticity. Shivani Kundra et al. analysed the various technologies that used in E-passport design. Shivani Kundra et al. suggested the solution for various privacy and security issues that apply to e-passports. Shiv Kumar, Shrawan Kumar Sharma et al. suggested the use of e-governance. Abdulsalam Dukyil et al. developed RFID enabled passport tracking system.

Goals and Objectives

- Secure verification of Passport.
- Third level security.
- Unique Identification through QR Code.

Proposed System

Proposed smart card simplifies the process by making use of a QR tag which will contain all the details present in the passport such as passport details, pan card details, aadhar card details, nationality and all other required details. When the person shows the card to the QR Scanner, the data is read and then verified using the data present in the system and then if the details matches then it displays the details of the passport holder.

In this system there is an admin officer who can add all the required registration officers. Then this admin assign all the work to the registration officers. Each registration officers adds the data, verifies the data and provides the user with the smart card. These data are stored in the database and are accessible to the admin and the passport officer. At the airport, the passport officer scans the QR code and verifies the identity of the person.

Age wise restriction is provided. Aadhaar card is compulsory for all above 3 years, Pan card is compulsory for all above 15 years and Voters card is compulsory for all above 18 years to generate passport smart card. A unique id is created by merging last 4 digits of Aadhaar card, last 2 digits of Pan card, last 2 digits of Voters card and a unique index of passport. To ensure security this unique id is encrypted into a string using AES Encryption Algorithm. A QR Code is generated using this id. On scanning of QR Code this id is obtained. This id is searched in the database by passport checker. The id is decrypted and the passport validity and other details can be checked. The Fig. 1 depicts the architecture of the system.

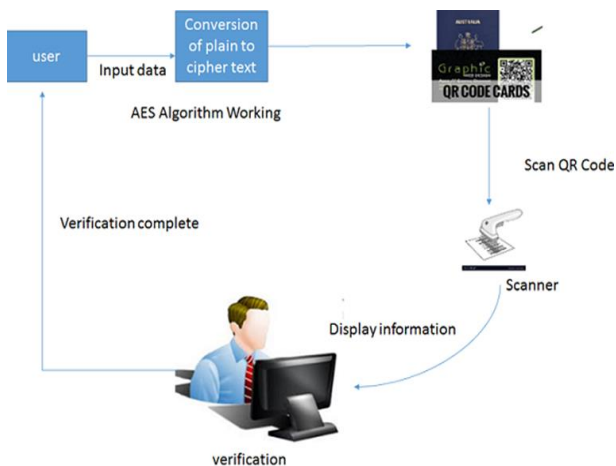


Fig 1. System Architecture

The following Fig. 2 shows the behaviour and flow of control of the system.

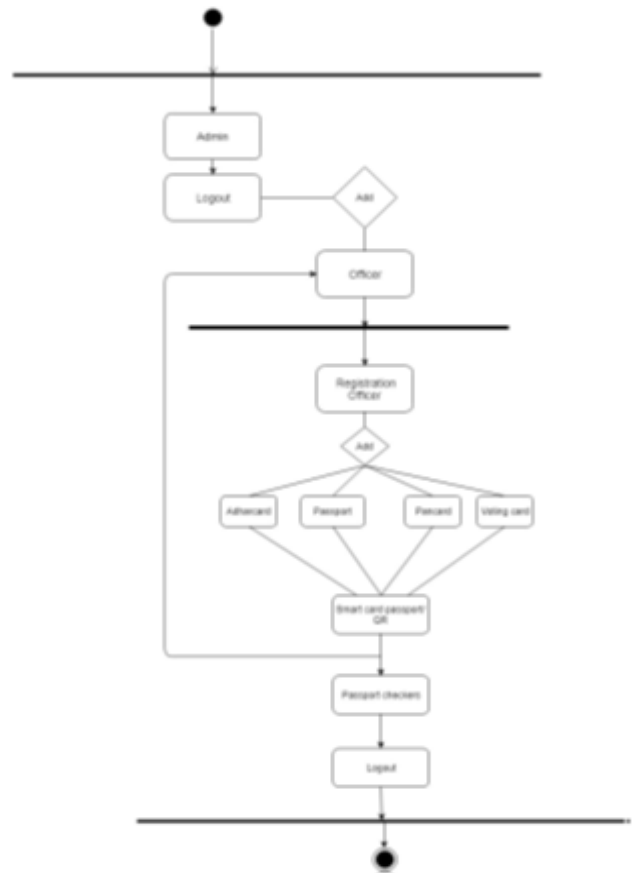


Fig 2. Activity Diagram

Algorithm

As mentioned earlier AES Algorithm is used in this system for encryption and decryption.

Algorithm: AES Algorithm

Start

A. SubBytes

Substitute bytes from S-Box

B. ShiftRows

Shift elements of each row accordingly Step

C. MixColumns

Performing multiplication with pre defined matrix

D. AddRoundKey

Performing XOR with key matrix

End

The following figure, Fig. 3 shows the working of AES Algorithm.

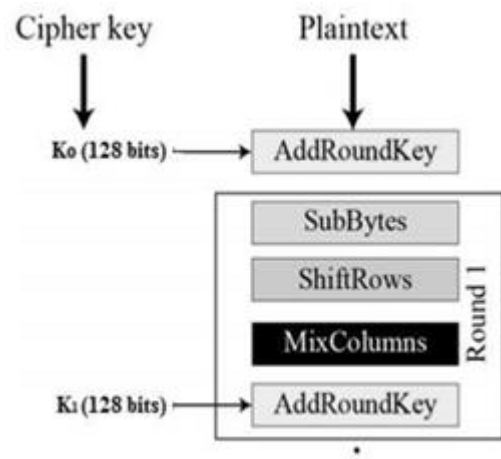


Fig 3. AES Algorithm

Outcome

It is a system that uses a high security algorithm for encryption and decryption. Database contains all information used to generate passport smart card. This includes passport details, pan card details, aadhar card details, nationality and all other required details. It enhances the authenticity by using various other informations like Aadhar card, PAN card, Voters ID. The information on the card is encrypted using AES algorithm into a QR Code. This improves the security of the entire system. The QR code printed on the smart card. It is used to verify the identity of the passport holder. The final product is a passport smart card with a QR Code. The passport checker scans the QR code on the card to verify the identity of passport holder and checks the validity of the passport. On scanning of this card by the passport checker a unique id is obtained which is searched by passport checker to obtain passport card holders details and validity of passport. An existing passport smart card holder can also renew the card on the expiry of their passport.

Conclusion and Future scope

Passport verification system uses QR Tag technology which gives a clear vision about the benefits of using QR Code on QR Tag technology as this system avoids forgery and thus increases the security. This decreases the burden of documentation and thereby reduces the time consumption. The use of QR code tag on QR Tag makes the system centralized and thus improves the security. The security of the system can be further be enhanced by adding Detail information such as Passport details, Pan card Details, Adhar card details, Nationality and all other required details etc and other active validation in the passport system. This system can be improved by using a RFID based card instead of QR Code. It would improve the security of the system.

References

- [1] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers Security*, Vol. 21, No. 4, pp. 372–375, 2002.
- [2] T. Falas, H. Kashani, "Two-Dimensional Bar-code Decoding with Camera-Equipped Mobile Phones," *Proceedings of the Fifth Annual IEEE International Conference on Pervasive*

Computing and Communications Workshops, 19-23, March, 2007, pp. 597-600.

[3] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[4] ISO/IEC 18004:2000. Information technology-Automatic identification and data capture techniques-Bar code Symbology-QR Code, 2000

[5] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards Interfaces*, Volume 31, Issue 4, pp. 723-728, June 2009.

[6] Piotr Bilski, Józef Modelski, "Application of the RFID Technology in the European Union Border Control System."

[7] M. Prathilothamai, "De-Duplication of Passports Using Aadhaar" 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA

[8] Abdulsalam Dukyil, "A Cost-Effective Decision Making Algorithm for an RFID Enabled Passport Tracking System: A Fuzzy Multi-Objective Approach" *Computing Conference 2017* 18-20 July 2017 — London, UK.

[9] Shiv Kumar, Shrawan Kumar Sharma, "Advance E-Governance System" *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS2017)*.

[10] Shivani Kundra, "The study of recent technologies used in e-passport system", September 2014.