iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4243

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Digital Document Sharing Securely Using Enhance QR Code

Bhavnesh Chaudhari[1], Akshay Waikar[2], Saly Lopes[3]
[1, 2, 3] *Computer Engineering Department, St. John College of Engineering and Technology, Palghar, Maharashtra, India*

Abstract: ***These days, technology has mostly influenced numerous systems that are used. Several organizations are creating efforts in developing a system for saving people's time, efforts and giving comfort. Organizations around the world are interested in delivering numerous services through the web. In the existing system, we submit documents for checking procedure for that we have to submit verified copies of original documents. This procedure involves large numbers of paperwork and makes not any use of technology. The proposed system aim is altering this current approach into a straightforward approach of document verification. AES for encoding the information, DSA to digitally sign the documents and Encoded QR-code for sharing the documents within the system. Therefore the user is going to be able to share the necessary documents to third-party organizations (school, college, hospital, etc.) simply by sharing associated encoded QR code. The third party will be able to verify the trustworthiness of documents with the utilization of digital signatures.***
Keywords: QR code, DSA (Digital Signature Algorithm), AES (Advanced Encryption Standard) Algorithm.

I. INTRODUCTION

The existing system involves huge human efforts and paper work for document verification. Proposed system aim is to reduce human efforts and paperwork. In proposed system documents are verified with the utilization of digital signature and then uploaded on the database. Documents will be shared by encoded QR code with third party organizations. A user just needs to share system made encoded QR code and third-party organization scan that QR code for accessing the user documents. The proposed system eliminates the documents if the user uploads fake documents. Authorized person verify the documents and apply digital signature on genuine documents. Third party organizations also check the genuineness of documents by using the digital signature. If documents are change or renewed then it is necessary to updated documents from time to time. In the existing system, the user needs to submit the same document hard copy with different organizations which include lots of paper loss. In the proposed system user need to submit documents only once and he can share the documents digitally with many organizations securely. The proposed system will offer access to user documents without any difficulty and share documents securely with third-party organizations. The proposed system has a simple interface and it is easy to use.

II. LITERATURE SURVEY

In [1], QR i.e. "Quick Response" code is a 2D matrix code that is designed by keeping two points under consideration, i.e. it must store a large amount of data as compared to 1D barcodes and it must be decoded at high speed using any handheld device like phones. QR code provides high data storage capacity, fast scanning, omnidirectional readability, and many other advantages including, error-correction (so that damaged code can also be read successfully) and different type of versions. Different varieties of QR code symbols like a logo QR code, encrypted QR code, QR Code are also available so that user can choose among them according to their need. Now, these days, a QR code is applied in different application streams related to marketing, security, academics etc. and gain popularity at a really high pace. Day by day more people are getting aware of this technology and use it accordingly. The popularity of QR code grows rapidly with the growth of Smartphone users and thus the QR code is rapidly arriving at high levels of acceptance worldwide.

In [2], initially, the barcodes have been widely used for the unique identification of the products. Quick Response i.e. QR codes are the 2D representation of barcodes that can embed text, audio, video, web URL, phone contacts, credentials and much more. This paper primarily deals with the generation of QR codes for Question Paper. The author has proposed encryption of Question Paper data using AES Encryption algorithm. The working of the QR codes is based on encrypting it to QR code and scanning to decrypt it. Furthermore, the author reduced the memory storage by redirecting to a webpage through the transmission and online acceptance of data.

In [3], the demands of Android smartphones and its use has increased rapidly. As a result, the need for competent message and file sharing techniques for Android phones has increased. Messaging has emerged as one of the most important features and applications

in mobiles. The existing messaging techniques incorporate the use of the internet and SMS service. Various techniques of message passing and file sharing by using Wi-Fi/Internet through QR code for hiding purpose and maintaining its integrity are developed. This paper presents an overview of the existing techniques of secure message passing and file sharing in android phones. The overview is followed by the author suggested approach which incorporates the RSA algorithm which can be used to encrypt and decrypt the message and MD5 algorithm can be used to check its integrity. The suggested approach ratifies the concept to reduce the use of mobile data while sharing of text or other files over the internet.

In [4], the author explains valid and generic software environment is introduced which offers the possibility to evaluate and compare different Optical Transmission Patterns (OTPs). This framework generates a huge library of evaluation images applying synthetically all distortions one should expect for a real-world application. The synthetic analysis environment is based on OpenGL, which enables three-dimensional Operations covering for example perspective projections as well as dynamic three-dimensional modifications through vertex programs and tessellation. The author examined most common OTPs, like the QR-Code, MaxiCode, and EAN- 13. To evaluate the expressiveness of the OpenGL environment, the author builds a mechanical device offering practical results, which can be confronted with our theoretical results. The author found out that QR-Code delivers the best decoding results but still suffers from decoding problems within certain angles. Moreover, the author could prove that the results of the OpenGL environment highly correlate with the practical result.

III.PEOPOSED SYSTEM

The system will offer access to documents of a user over the internet and also ease sharing of documents with registered third parties through sharing of Encrypted QR Code. The proposed system focuses on securely sharing the document to the third party. This system consists of an authorized person who apply the DSA (Digital Signature) on genuine document. The DSA signed document ensure the documents are valid and authenticated by an authorized person. The user sends the document copies to the authorized person, the authorized person check document copy is valid or not. The document is forged then authorized person reject that particular document and only valid document after applying DSA will be stored in the database. The user selected the document which has to be share with the third party organizations, system will generate QR code with AES (Advanced Encryption Standard) encryption for user selected documents. The system will be trained in such a way that if the authorized person verified and valid document to be stored on the database. The third-party access that document by the user provided encoded QR code.

A. Architecture Diagram

The architecture diagram in figure 1 shows the web page portal which is divided into two parts that is built in portal and expand web portal. In built in portal the sub portals are user management, authority management and third party management portals. And in expand web portal there are procedure which perform some tasks that are upload document by user, digitally signing document by authorized person and generate QR code of that documents through the system. This two web page portals are link to the database. Database stores valid documents, and information about user, third party.

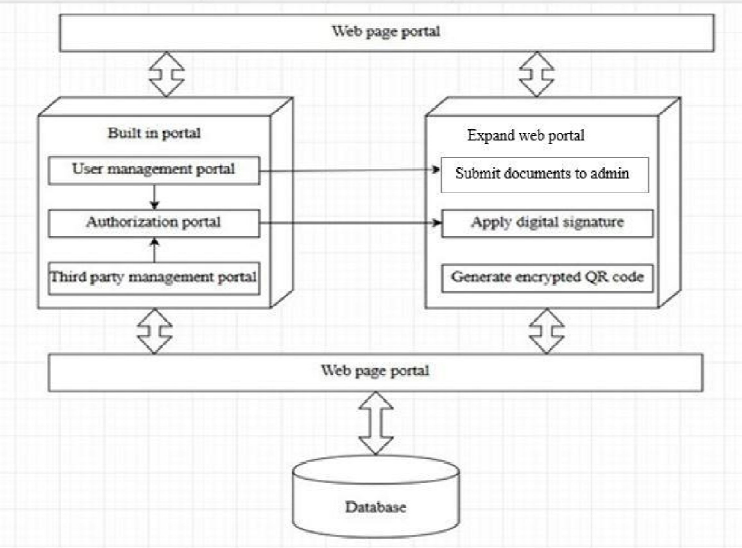


Fig 1 Architecture Diagram of the proposed system

1) *User Management Portal:* It contain the information about user like user profile, user documents. Which are uploaded by the admin. User share the document with third party whenever required. User also able to update his profile.
2) *Authorization Portal:* Administrator provides the username and password to user when user register with the system. Administrator also verify user documents and upload verified documents on database with digital signature.
3) *Third Party Management Portal:* It contain the information about third party organization. Third party receives document share by user. Third party also update their profile.

B. Flowchart

After registration by the user, the user submits or upload the documents to the staff. Then these documents are check by the authorized person if the documents are fake then documents are rejected otherwise documents are digitally signed by the authorized person and he stores these documents on the database. When the user wants to share the documents with third-party organizations, the user selects the documents from the database that third party requires. The system generates the encoded QR code for the user selected documents. The user shares the encoded QR code of documents with the third-party. Third-party scan that QR codes to access the user documents and finally third-party receives user documents successfully.

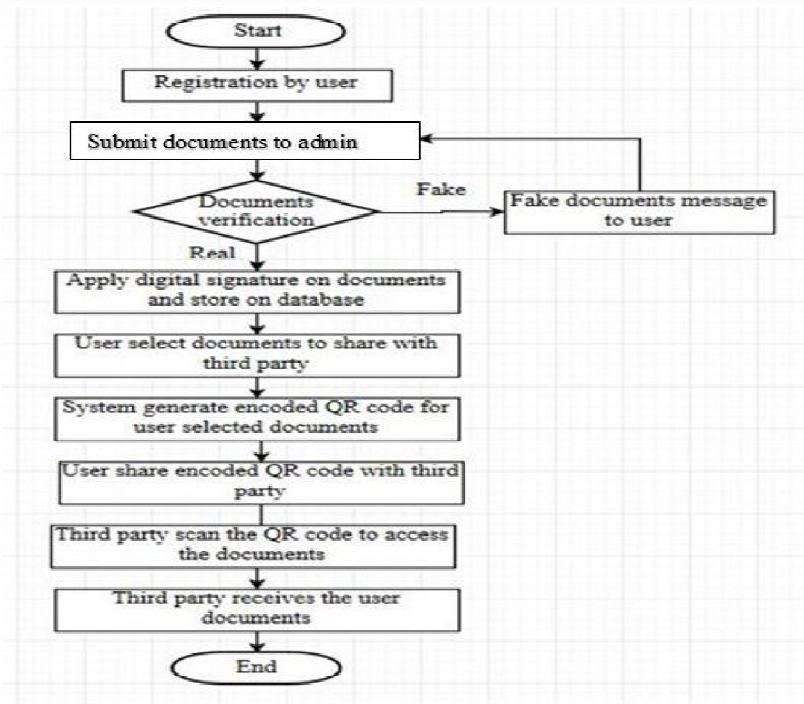


Fig 2 Flowchart of the proposed system

C. Advanced Encryption Standard (AES)

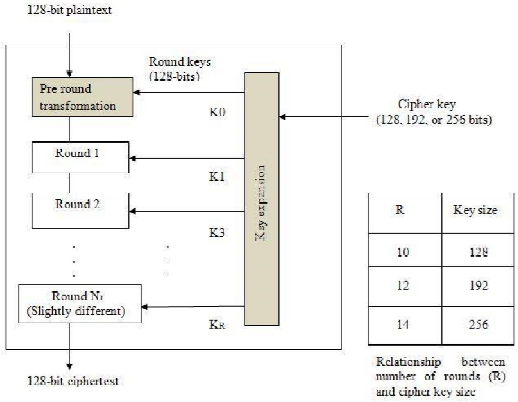


Fig 3 AES structure

AES is based on 'substitution–permutation network'. It is an iterative rather than Feistel cipher. It comprises of a series of linked operations and some of which involve replacing inputs by specific outputs (substitutions). Others involve bits shuffling around (permutations) the series. AES performs all operations on bytes instead of bits. Therefore, AES handle the 128 bits of a plaintext block as 16 bytes. These 16 bytes are organized in four columns and four rows to form as a matrix – 16. The number of rounds in AES is not fixed, depends on the length of the key. AES has 10 rounds used for 128-bit keys, 12 rounds used for 192-bit keys and 14 rounds used for 256-bit keys. All these rounds of AES uses a different 128-bit round key, which is calculated from the original AES key. The representation of AES structure is given in the above figure.

1) Encryption process: Here, we restrict to description of a typical round of an AES encryption. Each round contain of four sub processes. The first round process is represented below figure.

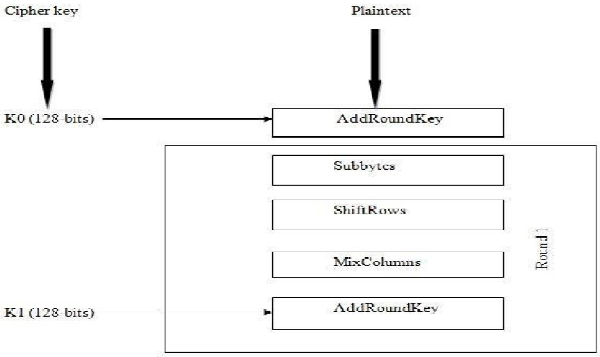


Fig 4 Encryption process of AES

2) *Byte Substitution (Sub Bytes*): The 16 input bytes are substituted by observing up a fixed table (S-box) given in design. The outcome is in a matrix of four rows and four columns.

3) *Shift Rows:* Respectively the four rows of the matrix is shifted to the left. Whichever entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as (i) First row is not shifted, (ii) Second row is shifted one (byte) position to the left, (iii) Third row is shifted two positions to the left, (iv) Fourth row is shifted three positions to the left, and (v) the result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

4) *Mix Columns:* Every column of four bytes is transformed by special mathematical function. This function takes the four bytes of input of one column and outputs four totally new bytes, which interchange the original column. The result is another new matrix be made up of 16 new bytes. It must be noted that this stage is not implemented in the last round.

5) *Add Round Key:* In Add Round Key method16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is last round then output is the ciphertext. Or else, the resultant 128 bits are taken as 16 bytes and we initiate another similar round.

6) *Decryption Process:* The process of decryption of an AES ciphertext is same as the encryption process in the reverse order. Each round has of the four processes shown in the reverse order as Add round key, Mix columns, Shift rows, Byte substitution. Since sub-processes in every round are in reverse fashion, totally different for a Feistel Cipher, the encryption and decryption algorithm needs to be independently executed, whereas they are very closely linked.

D. Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) can be used by the receiver of a message to validate that the message has not been changed during transit as well as certain the originator's identity. A digital signature is an electronic signature which proves identity of sender to the receiver when receiver receives the sender's message. For storing data and programs digital signatures are generated so that integrity of data and programs may be checked at any time.

The DSA is used by a signatory to generate a digitally sign on the data and by a verifier to check the authenticity of the signature. Each signature has a public and private key. The public key is used in the signature verification process and the private key is used in the signature generation process. For both signature verification and generation, the data (which is referred to as a message) is reduced by means of the Secure Hash Algorithm (SHA). An attacker, who does not know the private key of the signatory, cannot generate the correct signature of the signatory. In simple words, signatures cannot be fake. However, by signatory's public key, anyone can verify a properly signed message.

E. Stepwise Procedure Of Proposed System

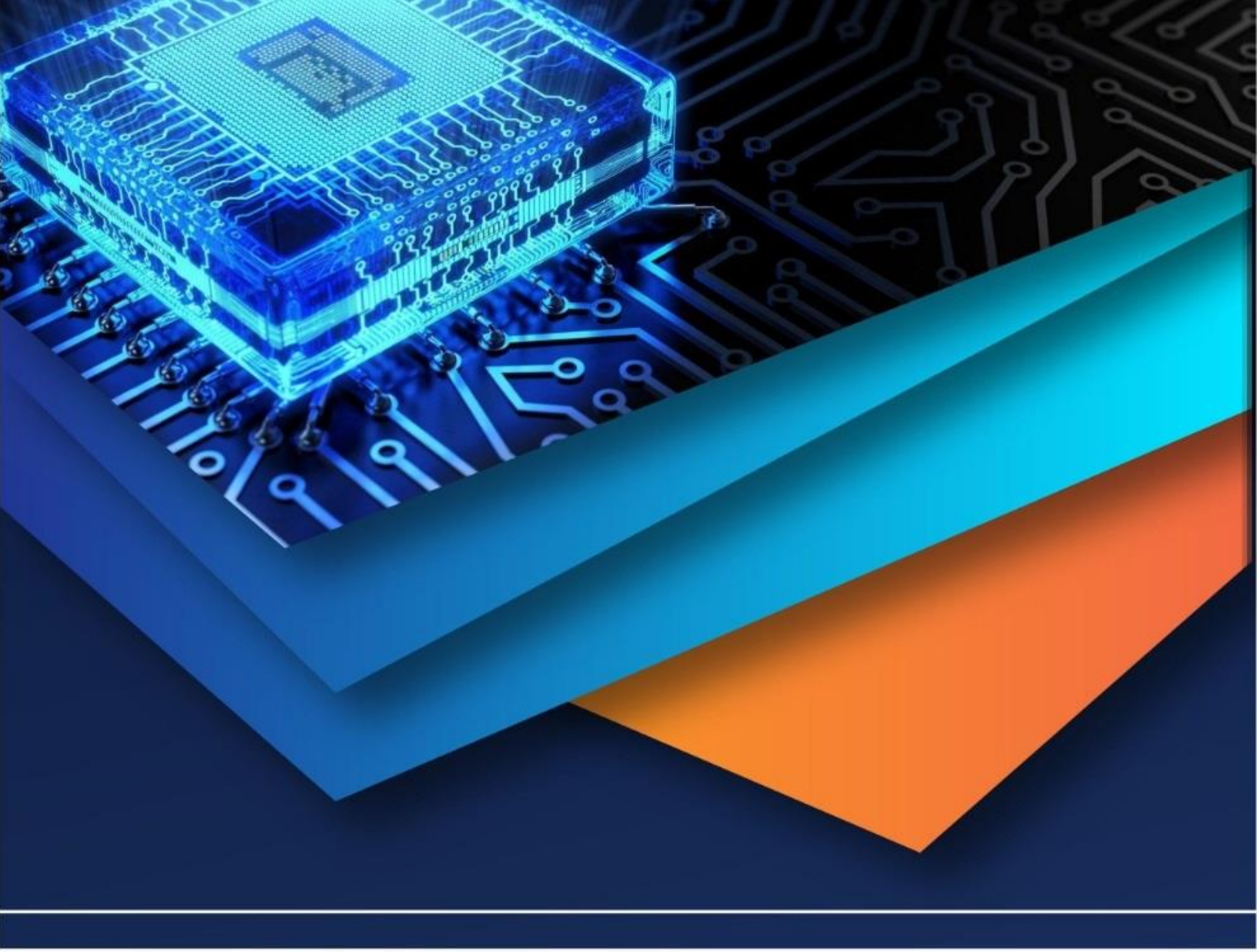
1) The user goes to the staff to register himself or herself with the system.
2) The user also carry his or her documents and submit them to the staff.
3) Staff fills up the user information form to save user information on database and staff send the user documents to an authorized person.
4) After the verification of documents by authorized person user gets his or her user-id and password.
5) The third party also get registered by staff and verified by an authorized person.
6) When the third party needs user documents that third-party requests document to the user.
7) User logins and selects the document from the system that the third party requested.
8) The system will generate encoded QR code for user-selected documents.
9) User shares the encoded QR code to the third party.
10) The third party receives the QR code which is shared by the user and after scanning the QR code third party access the user documents.

IV. CONCLUSION

The implementation of the proposed system can avoid carrying of original documents, attestation of documents and offer a simple approach along with a good level of security using various algorithm like AES for encrypting the data, DSA for digitally signing the documents and Encrypted QR-code for sharing the documents in the system with third party. The System allows user to submit any kind of government documents (adhar card, pan card, etc.), medical reports as well as property documents online. User need to submit documents only once and then he share the documents with different third parties therefore it avoids resubmission of documents. System eliminates the fake documents so there will be no chance of fraud.

REFERENCES

[1] Tiwari, Sumit. "An introductiosn to qr code technology." Information Technology (ICIT), 2016 International Conference on. IEEE, 2016.R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)
[2] Mittra, Partiksha, and Nitin Rakesh. "A desktop application of QR code for data security and authentication." Inventive Computation Technologies (ICICT), International Conference on. Vol. 2. IEEE, 2016.
[3] Shah, Altaf T., and Vikramsingh R. Parihar. "Overview and an approach for QR-code based messaging and file sharing on android platform in view of security." Computing Methodologies and Communication (ICCMC), 2017 International Conference on. IEEE, 2017.
[4] Scheuermann C, Werner M, Kessel M, Linnhoff-Popien C, Verclas SA. Evaluation of barcode decoding performance using zxing library. InProceedings of the Second Workshop on Smart Mobile Applications, SmartApps 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY