Secured E-Documents and Sharing using Encrypted QR-Code

Harshal Pandit
B.E. Computer Engineering
Viva Institute of Technology Mumbai

Shailendra Nipane
B.E. Computer Engineering
Viva Institute of Technology Mumbai

Suraj Jadhav
B.E. Computer Engineering
Viva Institute of Technology Mumbai

Sunita Naik
Assistant Professor
Viva Institute of Technology Mumbai

ABSTRACT
Nowadays, technology has largely influenced various systems that are used. Many organizations have been making efforts on developing system for saving people's time, efforts and providing convenience. Organizations around the world are increasingly interested in the potential for delivering various services through internet. The proposed system aims at developing a system for managing user's documents by uploading them on cloud database after verification and making them available to the respective users. Thus the user will be able to share the required documents to third party organizations just by sharing an encrypted QR code. The third party will also be able to verify authenticity of documents with the use of digital signatures. The proposed system will not involve generation of any new documents. This system will save time and provide convenience to the user. The system will provide access to the user through secured login.

Keywords
Digital Signature, QR-Code, AES Encryption (Advanced Encryption Standard), Secure Sharing of Documents.

1. INTRODUCTION
In traditional system submission of documents is needed for a verification procedure. It is needed to submit attested copies of original documents. This procedure involves lots of paper work and makes limited use of technology and also has very less transparency. The proposed system aims at changing this traditional approach into a simple approach of document verification using digital signature and uploading on database and also allows sharing using encrypted QR-code. The proposed system will provide access to various digitally signed documents through the web portal and physical movement of documents to various government offices will be reduced and it will also reduce misplacement of user documents. An individual just need to provide a system generated Encrypted QR code and the authorized third party agency will get access to your documents by scanning the QR code. The proposed system eliminates fake documents as there will be a manual Verification of documents before user registration. The documents will be signed digitally through digital signature by an authorized user. The authorized third parties would be able to verify the authenticity of the documents with the help of digital signature. The digital documents would be required to be updated from time to time in case of changes in documents or renewal of documents. The proposed system will have responsive and user friendly interface. Thus it will provide access to important documents of the user with greater ease and convenience.

2. RELATED WORKS
Many systems are being developed to provide government services over the internet. The paper describes the implementation of a system to provide government issued user documents to the user over the internet and sharing of these documents to third parties in a secure way. Encryption is an important aspect of this system [7].

Encryption is cryptographic technique to convert a message or data into such a form that it becomes unreadable and thus safe. There are many encryption standards available for encryption and decryption of data. One such standard is DES (Data Encryption Standard) which uses 56 bit key for encryption and decryption [7]. In spite of being a powerful encryption standard, DES is not used due to its shorter key which makes it less secure. Today many computers can easily crack DES encryption which was not possible some years back. AES (Advanced Encryption Standard) Algorithm on the other hand which uses permutation techniques for encryption is comparatively more powerful than DES [2][12]. It uses 128,192,256 bit keys for encryption. This algorithm has speedy key setup time and good key agility. It also has low memory requirement, which makes it very much suitable for implementation in memory restricted environments. This makes implementation of AES encryption more suitable for the proposed system.

Another aspect of technology that is integral part of this system is "QR Code". Barcodes have been used since many years for purpose of storing small piece of data that can be easily read by a barcode scanner. The limitation of barcodes is that it can store only numbers. Denso Wave a Japanese corporation soon realized need to develop a new technique to store information that can be easily retrieved and has good storage capacity. This resulted in development of QR (Quick Response) code. In QR Code encoding of information is done in both the vertical and horizontal direction, thus holding several times more data than a traditional bar code [5]. The QR code data is used for sharing links, contact information etc. It is not used for any security based applications.

Digital signatures are one of the most important techniques of modern cryptography, and have many applications in information security systems [6]. The proposed system will use digital signature for verifying if the document shared is authentic or not. There are various digital signatures algorithms developed for generation of digital signatures and to verify the authenticity of documents. Once such algorithm used for generation of digital signatures is DSA (Digital Signature Algorithm). DSA is based completely on difficulty of computing discrete logarithms.

3. PROPOSED SYSTEM

The system will provide access to documents of a user over the internet and also facilitate sharing of documents with registered third parties through sharing of Encrypted QR Code. The system will use HTML, JAVA Servlet Pages (JSP), CSS, JAVA, and JQuery. Following are the key technologies used in this system.

3.1 QR Code Encryption

Japanese Corporation Denso Wave developed a two dimensional Barcode known as QR (Quick Response) Code [5]. In this encoding of information is done on both horizontal and vertical directions and thus holding several times more data than a traditional bar code. These codes have rapidly gained popularity worldwide and have been adopted by many systems especially in Japan due to its ability to encode Kanji symbols by default which makes it especially suitable. QR codes are used for storing URLs, addresses, signs, business cards, public transport vehicles, etc. QR Codes consist of different areas that are reserved for specific purposes. QR codes are used for its faster readability and greater capacity to store information [3].

Fig. 1 QR Code

The smallest Codes are of size 21x21 modules as shown in figure 1 above. These are called version 1 QR codes. The size of QR Code increases by 4 modules for each next version of QR Code. The largest QR Code is of size 177x177 known as Version 40 QR Code [1].

QR Codes also have some error correction information which helps the QR Code reader to read the information stored on the QR Code even if some part of the QR Code is damaged. There are four distinct levels of error correction: L, M, Q, H. the lowest level is L where a QR Code can be read even if its 7% part is damaged or unreadable. The next level is M with 15%, then level Q with 25% and level H with 30% error correction[5],[11].

The capacity of a QR Code depends on the version and error correction level as well as on the type of data that needs to be encoded. A QR code can encode three data modes which are Numeric, Alphanumeric and Byte [8].

3.1.1 Encrypting QR Codes

Encryption of QR Code makes use of AES Encryption Algorithm. The contents of QR Code are first encrypted using AES Algorithm with a Private Key from the Database and same key used for decryption at third party end.

3.2 Digital Signature

Digital signatures are one of the most important inventions of modern cryptography [4]. A signature and thumb impressions are used in various legal operations to authenticate documents. A signature for an instance on a document shows authenticity and helps to identify the person who has authenticated that particular document. In computers a similar technique is used to check if some document is authentic or not. This electronic technique is known as “Digital Signature” [9].

Some of the reasons for applying digital signatures are:

3.2.1 Authentication

Digital signatures are used to authenticate the user who created or owner of the document. When the owner has a key that was used to create the signature it becomes easy to authenticate the owner.

3.2.2 Non repudiation

Non Repudiation provides an important aspect of digital signatures, it ensures that an entity that has signed a particular information cannot at a later time deny having signed it.

3.2.3 Integrity

The integrity of a message is maintained because if a person tries to change the contents of an original document the digital signature changes and thus document will become invalid as this document will have new signature [6].

3.3 Proposed System Stepwise Procedure

The stepwise procedure of the proposed system is as follows:

1. The data operator will get himself/herself registered by a specified enrollment and verification procedure after this he/she will access the system through a login procedure.
2. User will carry his/her documents to data operator at the data center for his/her enrollment.
3. The user information and documents will be uploaded on the database.
4. The Authorized person will apply digital signature to documents after verifying.
5. After successful verification of uploaded documents User will receive his/her unique user-id and password.
6. The Third party user will get Registered and verified.
7. Third-party requests documents to user.
8. The user logins and selects the documents that are stored on the database.
9. The system will generate encrypted QR code which will be shared to third party to get the requested documents.
10. Third party will get access to the User Documents provided by the user through Encrypted QR code.

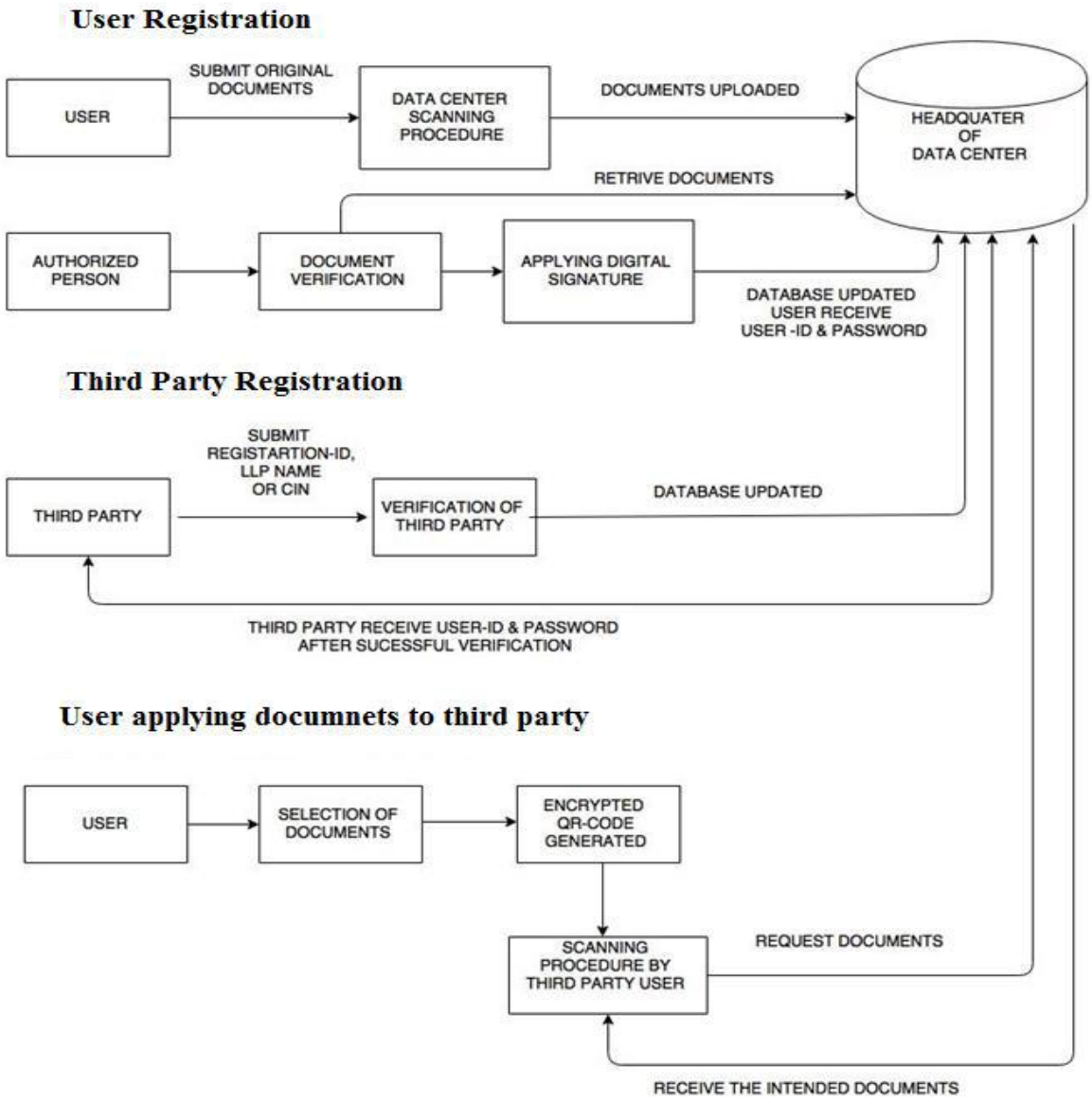

Fig. 2 Proposed System

Figure. 2 above shows the proposed system flow. In this flowchart the first part shows user registration procedure. The second part depicts registration of a third party organization. The last part of the flow chart shows how a user will use the system.

4. RESULTS

The proposed system when compared to manual system shows following results and advantages as stated in table 1. Below.

Table 1: Comparison of Traditional v/s Proposed System

Traditional System	**Proposed System**
Repeated manual verification	One time manual verification
Involves use of paper i.e. Attested copies of Document	Limited or no use of paper
The operational efficiency and consistency is low as compared to web-based	The operational efficiency has been increased due to web-based method
Involves physical movement of documents	No physical movement of document
Risk of Loss of original Documents	Original Documents remain Safe with user
Verification of authenticity of documents time consuming and complex	Easy to verify authenticity of documents and less time required

The proposed system proves to be a better approach in many aspects. It uses technologies that will enable users to save time and at the same time provide security.

Following images are the partial implementation of the proposed system.

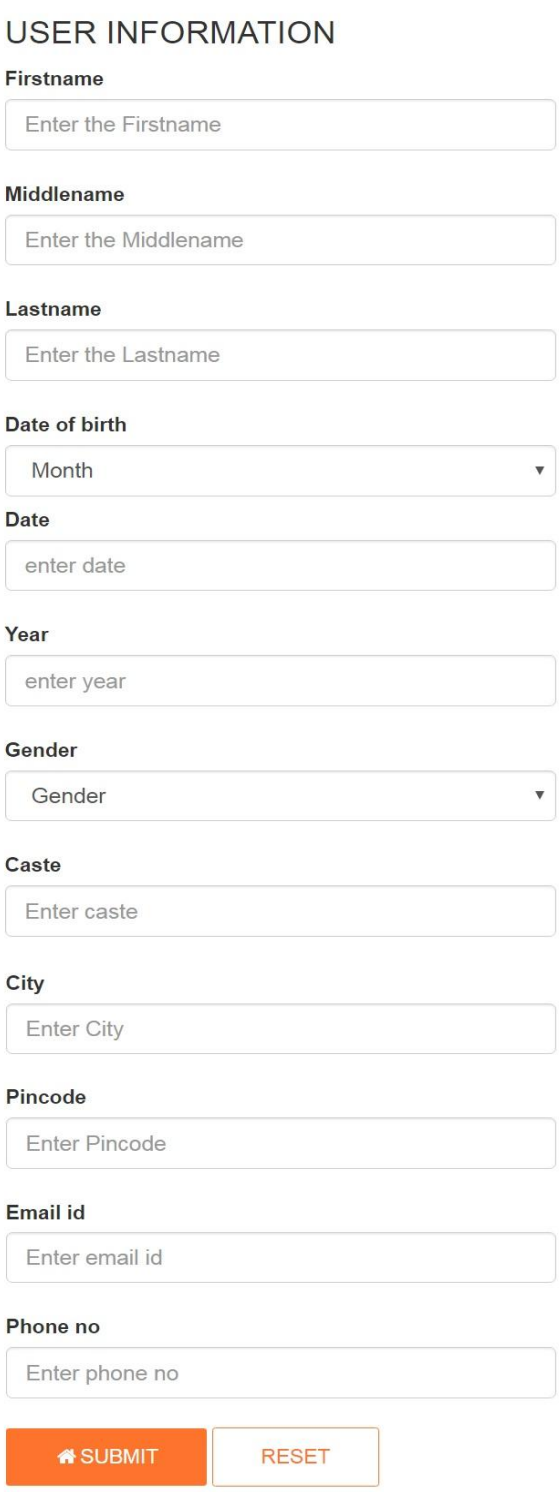

Fig. 3 User Registration

Figure 3 above shows the user information registration. In this basic information of the user like name, address, contact no etc. will be obtained through a form.

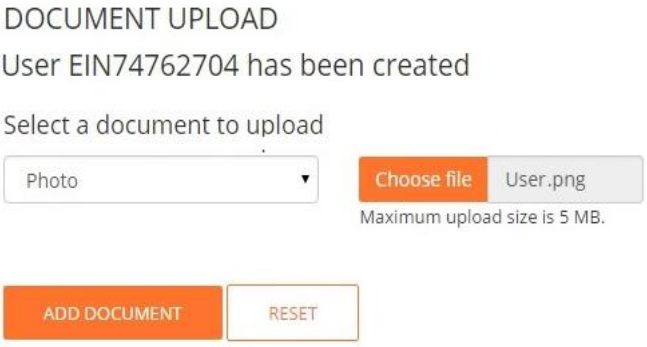

Fig. 4 Uploading User Document

Figure 4 above shows user document uploading procedure wherein user documents will be uploaded.

Fig. 5 Selection of User Documents

Figure 5 above shows selection of user documents by user for generation of a QR Code for document sharing purpose.

Fig. 6 Generated QR Code

Figure 6 above shows generated QR Code after selection of user Documents. The generated QR Code will be shared with Third party with whom the user intends to share his/her Documents

5. CONCLUSION

The implementation of the proposed system will avoid carrying of original documents, attestation of documents and provide a simple and better approach. As the documents will be stored on database the user will have access of his documents from anywhere and at any time. The proposed system provides a good level of security as it uses an encryption algorithm for encrypting the data stored on QR code. DSA Algorithm is used for digitally signing the documents. Encrypted QR-code will be used for sharing the documents in the system. The proposed system will avoid the tedious and cumbersome task of repeated verification of documents. The proposed system can be used by a large number of organizations where the requirement of document verification is more.

REFERENCES

[1] Ankit Singhal and R S Pavithr "Degree Certificate Authentication using QR Code and Smartphone" IJCA, June 2015.

[2] Abha Sachdev and Mohit Bhansali "Enhancing Cloud Computing Security using AES Algorithm." IJCA April 2013.

[3] K.M. Revathi, P. Annapandi, P.K.Ramya "Enhancing Security in Identity Documents Using QR Code" in International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013

[4] Digital Signatures, http://technet.microsoft.com/en-us/library/cc962021.aspx, last accessed on 22/01/2016.

[5] QRCodes,http://www.qrcode.es/en/2013/12/%C2%BFcual-es-el-tamano-minimo-de-un-qr-code, last accessed on 22/01/2016.

[6] Digital Signature Algorithm Analysis and Hash Signature. http://www.upsdn.net/html, last accessed on 22/01/2016.

[7] N. Smart, "Cryptography: An Introduction", 3rd Edition, pp. 131-134

[8] QR Code Tutorial, http://www.thonky.com/qr-codetutorial

[9] Digital Signatures, http://technet.microsoft.com/en-us/library/cc962021.aspx, last accessed on 22/01/2016.

[10] International Organization for Standardization ISO/IEC 18004 Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code,http://raidenii.net/files/datasheets/misc/qr_code.pdf , last accessed on 22/01/2016.

[11] QR Code Tutorial, http://www.thonky.com/qr-code-tutorial, last accessed on 22/01/2016.

[12] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.