QR CODE BASED DIGITAL ACADEMIC TRANSCRIPTS

Shraddha Nalkar [#1], Monika Talekar[#2], Priyanka Bamne[#3] , Snehal Patil[#4]

[#]*Computer Department, University Of Pune*
AISSMS's IOIT, Kennedy Road, Shivajinagar, Pune-411001, Maharashtra, India.
[1]shraddhanalkar187@gmail.com, [2]monikatalekar@gmail.com
[3]priyabamne92@gmail.com, [4]sneyan1307@gmail.com

Abstract—**In Today's Modern World it is not always possible to keep records of all students (eg: roll-no, name etc.) in paper documents as it is very time consuming and tedious job and maintain these paper documents will harm the plant ecosystem and environment eventually. For this reason digitization of those records is the best option but digitization is too costly as digital data grows in size, there is a need of larger space and hence we need to add new servers and more space to hold those data. To overcome this problem, in our project we are introducing a new method to digitize academic transcripts by embedding the QR Code. This can only be retrieved and decrypted using our own application by providing access to authorized person.**

Keywords— **Marks sheet, QR Code, Encryption, and Decryption.**

I. INTRODUCTION

This is now a common thing that student for higher education, loan and any other purpose get fake certificates and uses it to get their job done. Some have been caught but there are some who have got succeeded even having a fake certificate with them. To protect against this crime we are going to design a project which can help us to identify whether the academic marks sheet are being tampered or fake.

In Today's Modern World it is not always possible to keep records of all students (eg: roll-no, name, address, contact no, photo etc.) in paper documents as it is very time consuming and tedious job and maintain these paper documents will harm the plant ecosystem and environment eventually. For this reason digitization of those records is the best option but digitization is too costly as digital data grows in size, there is a need of larger space and hence we need to add new servers and more space to hold those data.

To overcome this problem, we present a new method to digitize the academic transcripts i.e. mark-sheets, and embed the digital format in the mark-sheet itself in the form of encrypted QR Code, so that the digital data cannot be retrieved by any unauthorized person. The student Mark sheet will be printed along with a QR-Code. The authorized person will be having a application on his android device which will scan the QR-Code on the digital marks sheet. The Android app will decode the QR-Code and accordingly connects to the Website and retrieves the original copy of the marks sheet along with the student photo registered with the certificate. On receiving the copy, the authorized person can easily detect the submitted copy is original or not.

When any student approaching for higher education loan or higher education or getting job then the marks sheet along with QR Code is scanned by the Android Application which in turn connects to server for authentication. If authenticated, then the server sends all the required information on the Mobile phone which can be used for verification purpose otherwise error message will occur.

QR Code is a type of 2 dimensional matrix barcode, which gained popularity because of its large capacity to hold digital data and it can be integrated in any mobile devices. In our mark-sheet system, we save the essential data of each student in the QR Code, like the student's name, roll number, registration number, semester and year of study, marks obtained in different subjects and grades secured. But, all the data saved and embedded in the QR Code, are encrypted, and then the QR Codes are printed in the mark-sheet of the student. The authorized person will be having an application on his android device which will scan the QR-Code on the digital marks sheet and accordingly connects to the website for the verification purpose.

II. ALGORITHM

AES Algorithm

Advanced Encryption Standard (AES) is the current standard for secret key encryption. In our project we are going to use AES algorithm technique for encryption of QR code**.** The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a Mix Column.

The need for coming up with this algorithm is that weakness in DES. The 56 -bit keys of DES were no longer consider saved against attacks based on exhaustive key searches and the 64-bit blocks were also considered as weak.AES is based on 128-bit blocks, with 128-bit keys.

Features of AES

1. *Symmetric and parallel structure*- This gives the implementers of the algorithm a lot of flexibility. It also stands up well against cryptanalysis attacks.
2. *Adapted to modern processors*- The algorithm works well with modern processors (Pentium, RISC, parallel etc).
3. *Suited to smart cards*- The algorithm can work well with smart cards.

Rijndael supports key length and plain text block sizes from 120 bits to 256 bits, in the steps of 32 bits. The key length and the length of the plain text blocks need to be selected independently. AES mandates that the plain text block size must be 182 bits and key size should be 128, 192 or 256 bits. There are two versions of AES: 128-bit plain text block combined with 128-bit key block and 128-bit plain text block with 256-bit key block.

Operation

Rijndael uses the basic techniques of substitution and transposition. The key size and the plain text block size decide how many rounds need to be executed. The minimum number of rounds is 10 (when key size and plain text block size are each 128 bits) and the maximum number of rounds is 14.

Following are the steps:

1. Do the following one-time initialization processes:

a) Expand the 16-byte key to get the actual key block to be used.

b) Do one time initialization of the 16-byte plain text block (called as State).

c) XOR the state with the key block.

2. For each round, do the following:

a) Apply S-box to each of the plain text bytes.

b) Rotate row k of the plain text block (i.e. State) by k bytes.

c) Perform a mix columns operation.

d) XOR the state with the key block.

III. PROPOSED MODEL

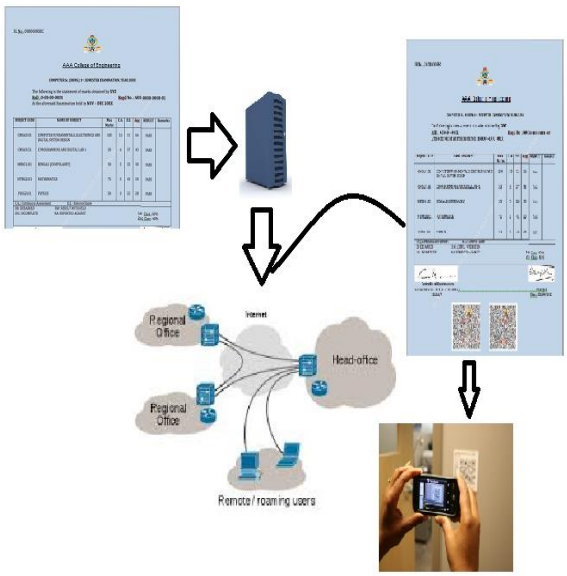

Fig.1 Proposed model

The College administrator updates the information on the server. This information carries the details of Students, their marks and academic marks sheet. Authorized person and students on demand can download these digital marks sheet. The server prints the QRCODE on the digital marks sheet. This QRCODE contains the digital ID of the marks sheet and the data is encrypted and encoded in the QRCODE. The authorized person who is a registered user of the system can scan the digital marks sheet for getting the right information of the marks sheet. The mobile contains an application which can scan the QRCODE on the certificate. The user needs to enter the authentication PIN which is given to him during the registration. This PIN is send to the Server along with the IMEI (International Mobile Equipment Identification) which the server authenticates the User and check whether the application is running on the same registered Mobile. On validating and if found a valid user the server provides an acknowledgement to the Mobile application which further activates the camera for scanning the QR Code. The user now shoots the QRCODE which is printed on the certificate. The mobile application then decodes the contents of the QRCODE and finds the Document Digital ID. This digital ID is further encrypted using the user PIN and is send to the server. The server then decodes the contents and send the all the required information to the user on him mobile application. The Mobile apps show the information that should be there on the certificate. The user can visually validate the contents and can determine the fake information on the certificate. This information help the user to find out the produced certificate is fake or not.

IV. CONCLUSION

The mark-sheet system, presented in this paper, is very effective to save a lot of digital space and the academic records, which are saved in the mark-sheets which cannot be tampered because they are encrypted uniquely using AES algorithm with uniquely generated key which is very secure indeed.

REFERENCES

[1] Advanced Encryption standard
Douglas Selent* Student, M.S. Program in Computer Science, Rivier College.

[2] New Generation of Digital Academic-Transcripts using encrypted QR Code ™ Use of encrypted QR Code ™ in Mark-sheets (Academic Transcripts) 978-1-4673-5090-7/13/$31.00 ©2013 IEEE

[3]QRCode,Wikipedia",http://en.wikipedia.org/wiki/QR_code

[4] SD-EQR: A New Technique to Use QR Codes ™ in Cryptography use of QR Codes ™ In Data Hiding and Securing.

