IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Certificates Verification System using Advanced Encryption Standard

[1] Anbudevi R,[2] Subhashini S,[3] Dr.S.Kannan , [4]R.Ramya
[1&2]UG Student,[3] Professor,[4]Assistant Professor,
[1,2,3&4]Computer Science & Engineering,
[1,2&3] E.G.S. Pillay Engineering College, Nagapattinam,Tamilnadu, India.
[4] A.V.C College of Engineering, Mayiladuthurai Tamilnadu, India.

Abstract:In the world today, individuals consistently fake their certificate to get a job or to present where and when required. The best way to single out those fake certificates is through verification. Notwithstanding, the paper verification sets aside a long process to handle certificate verification on the grounds that the certificates need to return to the issuing institutions which is tedious and time wasting. To this end, the certificates end up not getting verified or are delayed due to long process. Hence, in this paper, a certificate verification system utilizing QR code is created for simple check of the certificate authentications. This paper talks about the development of a certificate verification system, design a Quick Response code utilizing Advanced Encryption Standard method that will then be executed into the certificate of the students. The purpose behind the Advanced Encryption Standard Technique is on the terms that it is the most secure type of encryption technique in the world today. It is the most regular security protocol utilized for various wide applications. Overall, the implementation of Advanced Encryption Standard and Quick Response Code gives great execution, production, light, and fast responses in a certificate verification system.

Index Terms – **Quick Response code, certificate, verification, Advanced Encryption Standard**

I. Introduction

A certificate is a statement or a document that is issued to a student or a person after the completion of a specific education either formal or informal (Singhal and Pavithr, 2015). Certificate verification is a system of application that is used by a school administration to make and manage certificates for students in a computerized manner where the certificates can be created, printed and verified. Certificate verification is rather tedious, with some institutions receiving the verification process from a third party. Attempts to use Information Technology have been questioned as universities' would not allow third party organizations access their verification database, as a result of which the verification process remains partially or entirely manual (Boukar, Isa and Salisu, 2017). In addition, fraud or plagiarism in the initial documents becomes a challenge in the academic community. The downside faced by such organizations in the process is that the validity of the documents cannot be completely checked. The tedious nature of the paper work influences the process of authentication of documents by the issuing institutions, contributing to an increase in the number of forged certificates in the world (Boukar, Isa and Salisu, 2017). Consequently, a new, safe and automated method is embedded into the system which is the use of Quick Response (QR) code and a smart-phone QR scanner that is used to read, authenticate and verify the QR code on the certificates. Quick Response code is a two-dimensional barcode that is usually used to encode bits of information represented as black square dots placed on a white square grid (Uzun and Bilgin, 2016). They are designed to decode the data quickly (Pons, 2011). It is the most popular type of verification system used in the world. It has a wide storage space and fast readability and it brings greater reliability and security in the existing process of issuing the degree certificates to the university students (Singhal and Pavithr, 2015).

The online bank verification system (Mohadikar and Devade, 2013) and attendance system (Tresnani and Munir, 2011) are examples of the QR Code application system. Therefore, this research studies the generation of a Quick Response Code and the implementation of the Quick Response code into a certificate for verification. A secure QR code will be designed based on the references to the student's records printed on certificates. Next, a mobile scanner will be developed that will be used on mobile devices with the help of AES algorithm which then decrypts the QR Code to validate the certificates. This system will be designed to enable only the scanner to be able to decrypt and translate the QR-code because of the securely embedded properties generated by the system. The QR code generated which contains the student's detail will be printed on the certificate. If the QR code is scanned using a mobile QR scanner and it doesn't provide any relevant information, then it shows that the certificate is fake (Singhal and Pavithr, 2015)

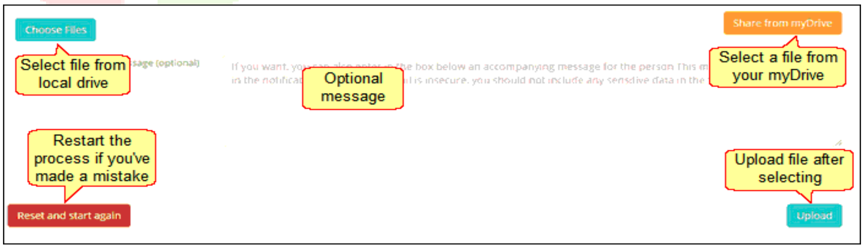
2. RELATED WORK

Certificate verification has become an important task today. It is the process of ensuring that the certificate issued after the completion of an education phase presented by an individual is genuine and that the holder is the rightful owner (Singhal and Pavithr, 2015). Moreover, a certificate has to be verified to ensure that its content is true and also to ensure that the issued certificate comes from an accredited source. Certificates are written and printed using special paper and has become a very important document for job application and for pursuing to higher degrees. Counterfeit degrees have become very common with the development of forgery technology, however, and that is why verification is very necessary (Ghazali and Saleh, 2016). Several researchers has worked on this area to evade the idea of Certificate counterfeit, QR code and Smart phone were proposed assolution to attendance system for both employees and student, (Cho and Bae, 2014; Kumar and Kareemulla, 2017; Masalha and Hirzallah, 2014).

The attendance system proposed by these researchers was online system that requires lecturer to generate QR code that would be scanned by the students and sent via wired/wireless network for necessary automaticattendance checking, (Cho and Bae, 2014; Masalha and Hirzallah, 2014). The major extension offered by the work of (Kumar and Kareemulla, 2017) was the introduction of fingerprint and voice verification for authentication in order to avoid proxy of attendance. Also, in 2016, a new enhancing security inidentifying documents using QRCode was developed (Revathi, Annapandi and Ramya, 2013). This system consists of QR reader and Biometrics finger print readers which are used to verify the certificate originality in order to eradicate fraudulent certificate. In this system, it focuses on using image of the certificate to generate into QR code and finger print of the person during the run time. Dey, Nath and Agarwal (2013) developed a new Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. In this system, the essential data of each student are saved 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. So, in future if the student or any other person wants to see the marks digitally or wants to send the academic information to any University or Organization in digital format, then the QR Code can be scanned and the embedded information can be decrypted and sent. This research proposed a new method, where the marks obtained by a candidate will also be encoded in QR Code in encrypted form, so that if an intruder tries to change the marks in the mark sheet then it will be impossible in the QR Code, because the encryption key is unknown. Al-Khalifa (2008) also made it known that cell phones are becoming an important aspect of our lives. The comfort and convenience they provide certainly made our lives much easier than ever before. Two brilliant features found in modern cell phones are: the integration of digital cameras and the ability to access the Internet anytime and anywhere, thus, enabling us to seek information when we need it.

The benefit of such a feature in modern mobile phones can be further extended to include blind and Visually Impaired (VI) people. Also, with the introduction of speech technologies in cell phones such as the use of Nuance TA, which converts the displayed text on the mobile handset into speech, the blind and Visually Impaired (VI) person can easily interact with the mobile handset as a sighted person do. The idea of utilizing the capabilities of modern mobile phones with 2D barcodes to assist Visually Impaired (VI) and blind people identify objects in the environment is very promising. Thus, our proposed system uses mobile phones, which are inexpensive, portable and nearly a ubiquitous mainstream consumer product widely used by blind people, not like some expensive assistive technologies, to verbally identify objects tagged with 2D barcodes. Schultz (2013) brought to the notice that libraries and museums are increasingly looking to mobile technologies, including quick response codes, to better serve their visitors and achieve their overall institutional goals; however, there is a lack of information regarding patrons' perceptions of quick response codes-information. This case study explored staff members' and patrons' perceptions of quick response quick response codes at Ryerson University Library and the museums.

3. METHODOLOGY


Choose Files
Select file from local drive
sage (optional)
If you want, yo... the box below an accompanying message for the person This m
in the notificat... l is insecure, you should not include any sensitive data in the
Optional message
Share from myDrive
Select a file from your myDrive
Restart the process if you've made a mistake
Reset and start again
Upload file after selecting
Upload

3.1 Upload methodology

This module is done after completing the user authentication. If the user authentication is success, then only this module is appeared. The uploading module is a new intent for login module. When user is login successfully, and redirected to uploading module. Once you synchronize your files with your computer or mobile device, you can access your content via your local file system instead of a Web browser. You can also access your files when you are offline. Offline edits will automatically sync with one Drive for Business the next time you connect.

3.2 Code implementation

For this module, an xml file is created for to display the user interface. In the xml file we are included some components like button. On the required button we label it as UPLOAD. When user click the UPLOAD button all the selected documents/files will be uploaded to server.

- Intent i = **new** Intent(Intent.***ACTION_OPEN_DOCUMENT***);

- The above statement states that creation of an intent. For the above intent an action is established, that document opening.

  - i.addCategory(Intent.***CATEGORY_OPENABLE***);

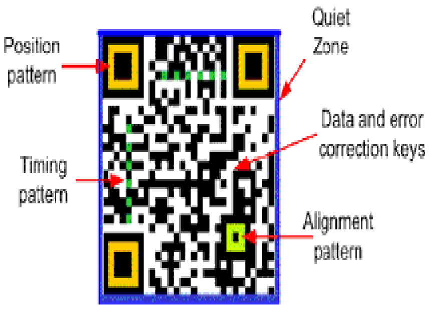
- The above statement states that, which category has to be open. Based upon this statement the required files are open.

  - i.setType(**"image/*"**);

- The above statement states that, which type of files would be upload to server.
- It must be any type when we declare as *(all).

  - startActivityForResult(i, ***READ_REQUEST_CODE***);

- READ_REQUEST_CODE is got from the user. If the user starts the operation of upload the activity will be invoked.



3.3 MD5 algorithm:

- The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512.
- Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. At least one bit and at most 512 bits are appended.
- A 64-bit representation of the length of the message is appended to the result
- of step1. If the length of the message is greater than 2^64, only the low-order 64 bits will be used.
- The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words.
- A four-word buffer (A, B, C, D) is used to compute the message digest.
- Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first:

word A: 01 23 45 67

word B: 89 abcdef

word C: fe dc ba 98

word D: 76 54 32 10

Four functions will be defined such that each function takes an input of

three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z

G (X, Y, Z) = XZ or Y not (Z)

H (X, Y, Z) = X xor Y xor Z

I (X, Y, Z) = Y xor (X or not (Z))

Uses md5 algorithm to store password details*:* The MD5 hashing algorithm is one-way cryptographic function that accepts a message of ant length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

The MD5 message digest hashing algorithm processes data in 512-bit block, broken down into 16 words composed of 32 bits each. The output from MD5 is a 128-bit message digest value. The goal of message digest function is to produce digests that appear to be random. MD5 algorithm is impossible for an attacker to generate a message matching a specific hash value.MD5 algorithm is impossible for an attacker to create two messages that produce the same hash value.

3.4 Methodology for after processing

After processing the data, the resultant data is stored in the database. Eliminates the need to store all documents thus saving physical space. The student does not need to carry all documents physically. MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact. For example, file servers often provide a pre-computed MD5 (known as md5sum) checksum for the files, so that a user can compare the checksum of the downloaded file to it. Most Unix-based operating systems include MD5 sum utilities in their distribution packages; Windows users may use the included PowerShell function "Get-File Hash", install a Microsoft utility, or use third-party applications. Android ROMs also use this type of checksum.

4. Adding QR Code to System:

ID card is using the regular bar code for some extra information of anyone. But there is a problem here as it does not contain all the information in details. But if the bar code can be replaced by QR code than one can easily insert or make a link to more information. For example: the QR code can be linked to the web address or some other web link so that anyone can get more information easily. Point to be noted that QR code is totally free. Lots of popular business companies are already started the using of QR code. So, adding the QR code to the ID card will make a new era to have more information of the student.

Comparing QR code and other codes

Subject	Traditional Id card	Normal Id card	QR Id card
Type of Id cards	Handwritten	Bar code ID card	QR code ID card
Scan speed of barcode from smart phone	Do not have any facility	2.5 seconds	3seconds
Picture taking options	No	Yes	Yes
Price of each code	No code	0.5 pence	0 pence

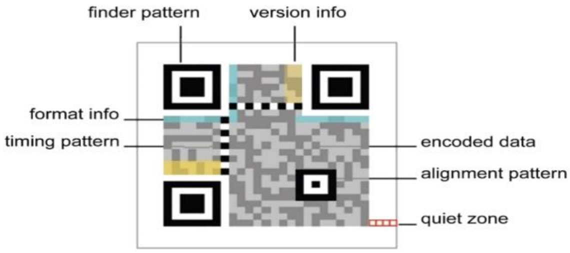
The Quick Response (QR) Code was designed as an improvement in comparison to its predecessor, the 1D barcode because it can contain more information. It was first designed for the automotive industry in Japan but later it become so popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC code.

QR Code The smallest QR Codes is of size 21x21 modules which is called version 1 QR Code and with each successive version the size of the QR Code gets increased by 4 modules so the largest QR Code is of size 177x177 modules which is version 40.

QR Codes also include some error correction information which is some redundant data that will help a QR reader accurately read the code even if part of it is unreadable. There are four levels of error correction: L, M, Q, H. The lowest is level L which allows the code to be read even if 7% of it is unreadable. Another level is M which provides 15%, then level Q which provides 25% and then level H which provides 30% error correction.

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. There are three data modes that a QR Code can encode: Numeric, Alphanumeric and Byte. If a QR Code is created that contain only numerical data then it can encode up to 7089 characters, with alphanumeric mode it can encode up to 4296 characters and with Byte mode it can encode up to 2953 characters.

A QR Code consists of black modules arranged in a square grid on a white background, which can be read by an imaging device then the data can be extracted from patterns which are present in both horizontal and vertical components of the image. QR Codes are 2-dimensional, which results in them having a square filled with data. Besides data, there are certain identifiers helping the code being read correctly. The most common QR Code type is model 2, which is broken down in the following information identifiers.



QR identifiers

There are certain factors which determine the readability of QR Code. The format string is always 15 bits long. To create the string, you first create a five-bit string that encodes the error correction level and the mask pattern in use in this QR code. Then you use those five bits to generate ten error correction bits. The resulting fifteen bits are XORed with the mask pattern 101010000010010.

Fig. 1. PERFORMANCE ANALYSIS AND RESULT

The student's details from the certificate are encrypted into a QR code. The QR code is then added to the student certificate. The already built mobile QR Barcode scanner is used to scan the QR code. When it scans, it shows the link to the URL where the QR code is saved. When the link shows up and it clicked, it redirects to show the details embedded in the QR code and the document can then be downloaded. The document that is downloaded is the Verification statusof the student certificate. The research was tested based on its speed and the results were analyzed and discussed.

Performance Evaluation of the system

In the implementation of the application to the system, there are some impacts that accompany it. To determine the impact that may occur as a result of the implementation of this system, it would require a prototype for the System. The performance of the system is evaluated using response time.

Response Time

It is the time takes for the mobile scanner to scan and decrypt the embedded message in the QR code. Comparing the response time for different data types embedded in a QR Code for the developed system and an already existing system.

CONCLUSION

This research is an attempt to eliminate fraudulent certificates from learning institutions. Verification of academic certificates is one of the significant research areas today, as discussed in the introduction chapter of this research. This work aims to address academic fraud issues. The proposed method enhances certificates verification process. It has resulted in a working prototype using the Advanced Encryption Standard, QR Code andSmartphone to authenticate a university degree certificate. This project allows the QR code embedded in a university certificate to be scanned in order to check the certificate's validity.

Not only does this boost the validity of the certificate faster than manual verification, but it also prevents fake certificates from being created.

REFERENCE

[1] Boukar, MoussaMuslu, Isa Yusuf and Salisu, "A Web Service Based Database access for Nigerian Universities' Certificate Verification System", International Journal of Computer Techniques., 1-7, 2017.

[2] Chernev b., 2019, Tech Jury [online] available athttps://techjury.net/blog/what-is-aes/ [Acessed 06 April 2020].

[3] Cho, D., &Bae, M. (2014). A Study on Development of OTIP System using QR Code based on Smartphone.International Journal of Multimedia and Ubiquitous Engineering, 9(10), 261–270.

[4] .D. L. Tresnani and R. Munir, "Implementation of EmployAttendanceSystem Using QR Code on Android-Based Smartphones," Informatics Techniques, Bandung Institute of Technology, Bandung, 2011. Erasmus University Rotterdam, 2015. [Online] Available: https://www.eur.nl/sites/corporate/files/201711/webbrochure2015_Cheating-plagiarism_EN.pdf, [Accessed 2020].

[5] 5.LAUTECH Journal of Computing and Informatics (LAUJCI) – ISSN: 2714-4194 Volume 2 Issue 1, May 2021 – www.laujci.lautech.edu.ng Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, et al. (2000) Report on the development of the Advanced Encryption Standard (AES). Computer security division information technology laboratory national institute of standards and technology administration.

[6] Kumar, B. D., & Kareemulla, S. (2017). Smart Mobile Attendance System for Employees Using QR Scanner. Asian Journal of Applied Science and Technology (AJAST), 1(5), 35–39. Masalha, F., & Hirzallah, N. (2014). A Students Attendance System Using QR Code. International Journal of Advanced Computer Science and Applications (IJACSA), 5(3), 75–79.

[7] Michelle Schultz (2013). A case study on the appropriateness of using quick response (QR) codes in libraries and museums. Library and Information Science Research. Vol 35, Num 3, pp 207-215. N. Mohadikar and C. Devade, "Online Banking Authentication System Using QR-Code and Mobile OTP," International Journal of Engineering Research and Applications (IJERA), pp. 1810-1815, 2013.