QR코드를 이용한 통합 교육 자격 입증 시스템

함디 압둘만* · 교수 장종욱*

*동의대학교

Centralized Educational Certificate Authentication System Using QR Cod Tag

Hamdi Abdurhman* · Prof. Jong-Wook Jang*

*Doing-eui University

E-mail : hamdiabdu2@gmail.com jwjang@deu.ac.kr

ABSTRACT

An educational institution issued a degree certificate to those students who have successfully completed all studies included in different levels of the degree program. The degree certificate presented by the University is of major significance in the person's life but the fabrication and circulation of fake certificates is inexpensive because a paper document can easily be forged with the availability of advance printing and copying technologies. So, there is a need to adopt a centralized authentication process that can verify and ensure the authenticity of a document. In order to prevent the spread of fake degree certificates a method is proposed where the integrity of the contents with in the certificate can be verified with the use of and Smart Phone Application. A Quick Response (QR) Code will contain a digital signature over the data such as degree holder's name, major program, Grade Point Average (GPA) obtained etc. Which will be signed by university authorities after the registration in central system and deployed in university. In order to verify the digital signature a person need to use a specific smart phone application which will scan and authenticate the certificate without gaining access to a user's security credentials such as password.

Keyword

Authentication, Degree certificates, Digital signature, QR code, Centralized system

I. Introduction

The advancement of digital printing and scanning technology grown rapidly. The incident of fraud and forgery of an educational certificate also increased, which are easily available at cheaper prices but has very high efficiency and quality document, which threat to the integrity of both the certificate holder and the educational institution that has awarded the certificate. The manual verification of these documents is a tedious task because it involves multiple level of human interaction and it is also a time consuming task which imposes an extra burden to the university or colleges because they have to verify all the students who have passed from their college. Hence, it is necessary that the universities adopt a process that can ensure security of information and authenticity of the issued certificates[1].

Even if the rapid development of technology shaping the world, but most of educational institutions use a manual way of authenticating educational certificates for graduated students. Due to this reason the existing manual process of authenticating document has the following limitation. 1) There is no centralized system to verify each and every certificate issued by any educational institution. 2) Highly forged certificates can easily evade the manual authentication process. 3) The manual authentication system cannot effectively combat corruption among educational institution's employees (those who issue non approved certificates) 4) It takes much effort and time to authenticate graduate certificates issued from different educational institutions.

To solve the above problems, we propose Centralized Educational Certificate Authentication System Using QR Code Tag. The approach we used to print digital signature with degree certificates, basic information of the graduated student such as degree holder name, program, major CGPA and university name will be integrated with one of pairs of keys (private

key) then data and digital signature can be encoded and printed at the bottom of every graduated student degree certificate and any anonymous person or organization can scan that QR code by using specific smart phone application in order to authenticate the certificate. The merit of this proposed method is that the degree certificate will not relay on the manual verification process with is tedious and time consume. This method is also allow to you to have a single specific smart phone application to authenticate all degree certificate that are registered under centralized educational certificate authentication system.

Ⅱ. Background of the Project

This section provides background information related to this paper:

1. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document. A valid digital signature gives a recipient reason to believe that the document was created by known sender (authentication), that the sender can't deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are most commonly used where it is important to detect forgery or tampering [2].

Digital Signature Algorithm (DSA) is pair of large numbers that are computed according to specified algorithm within parameters that enable the authentication of the signatory, and as a consequence, the integrity of the data attached. Digital signature generated through DSA, as well as verified. Signature are generated in conjunction with the use of private key; verification takes place in reference to a corresponding public key. Each signatory has their own paired public (assumed to be known to the general public) and private (known only to the user) keys. Because a signature can only be generated by an authorized person using their private key, the corresponding public key can be used by anyone to verify the signature [3].

A DSA digital signature is computed using a set of domain parameters, a private key x, a per-message secret number k, data to be signed, and a hash function. A digital signature is verified using the same domain parameters, a public key y that is mathematically associated with the private key x used to generate the digital signature, data to be verified, and the same hash function that was used during signature generation. These parameters are defined as follows [4]:

p	a prime modulus, where $2^{L-1} < p < 2^{L}$, and L is the bit length of p. Values for L are provided in Table 2
q	a prime divisor of (p − 1), where $2^{N-1} < q < 2^{N}$, and N is the bit length of q. Values for N are provided in Table 2
g	a generator of a subgroup of order q in the multiplicative group of GF(p), such that $1 < g < p$
x	the private key that must remain secret; x is a randomly or pseudo randomly generated integer, such that $0 < x < q$, i.e., x is in the range [1, q−1]
y	y the public key, where $y = g^{x} \bmod p$.
k	a secret number that is unique to each message; k is a randomly or pseudo randomly generated integer, such that $0 < k < q$, i.e., k is in the range [1, q−1].

Table 1: DSA parameters

This standard specifies the following for the pair L and N (the bit lengths of p and q respectively)

L=2024	N=160
L=2048	N=224
L=2048	N=224
L=3072	N=256

Table 2: Selection parameter Size and Hash function for DSA

2. QR code

QR a machine-readable code consist of an array of black and white squares, typically provides the following features. 1) High capacity encoding of data: while conventional bar codes are capable to storing a maximum of approximately 20 digits, QR code is capable of handling several dozen to several hundred times more information. It is capable of handling all types of data, such as numeric and alphabetic characters, Knaji, Kana, Hiragana, symbols, binary, and control codes. Up to 7,089 characters can be encoded in one symbol. The symbol version of QR code ranges from 1 to version 40. Each version has a different module configuration or number of modules. (The module refers to the black and white dots that make up QR code.) "Module configuration" refers to the number of modules contained in a

symbol, commencing with version 1(21 x 21) modules) up to version 40(177x177 modules). Each higher version number comprise 4 additional modules per side. As the amount of data increase, more modules are required to comprise QR code, resulting in large QR cod e symbols. 2) Small printout size: since QR code carries information both horizontally and vertically, QR code is capable of encoding the same amount of data in approximately one-tenth the space of traditional barcode. 3) Kanji and Kana capability: As a symbology developed in Japan, QR code is capable of encoding Japanese Industrial Standards (JIS) Level 1 and Level 2 kanji character set. In case of Japanese, one full-width Kana and Kanji character is efficiently encoded in 13 bits, allowing QR code to hold more than 20% data than other 2D symbologies.

4) Dirt and damage resistant: QR code has error correction capability. Data can be restored even if the symbol is partially dirty or damaged. A maximum 30% of codewords (a unit that constructs the data area. In the case of QR code, one codeword is equal to 8 bits) can be restored (data restoration may not be fully performed depending on the amount of dirt or damage). There are four error correction levels are available for users to choose a cording to operation environment. Raising this levels are available for users to choose according to the operating environment. Raising this level improves error correction capability but also increase the amount of data QR code size.

QR code Error correction capability	
Level L	Approx 7%
Level M	Approx 15%
Level Q	Approx 25%
Level H	Approx 30%

Table 3: Data restoration rate for total codewords

5) Readable from any direction in 360^0: QR code is capable of 360 degree (omi-directional), high speed reading. QR code accomplishes this task through position detection patterns located at the three corners to the symbol. These position detection patterns guarantee stable high-speed reading, circumventing the negative effect of background interference. 6) Structured appending feature: QR code can be divided into multiple data areas. Conversely, information stored in multiple QR code symbols can be reconstructed as a single data symbol. One symbol can be divided up to 16 symbols, allowing printing in a narrow area [5].

This concept has been playing a significant role in reshaping our perceptions of how objects in our physical world can be linked to related information in the digital world. QR Codes serve as one of the most effective and intuitive ways to input our request to our mobile devices. The technology behind QR Codes is available as open source. This makes this technology a favourable and the most viable option compared to other proprietary tools.

III. Proposed System Work Architecture

A. System model and method

The Educational certificate will contain a QR Code Tag which contains a digital signature over the data such as degree holder's name, enrolment number, roll number, total marks obtained etc. This will be signed and embedded with QR code by university authorities. In order to verify the digital signature a person need to use Educational Certificate Authentication System (ECAS) smart phone application which will scan the QR Code and authenticate the certificate.

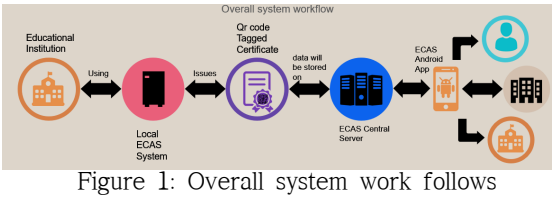


Figure 1: Overall system work follows

B. System business rules

Frist the institution feed graduate list data to local system of institution, the institution local system generate QR code tagged authentication certificate and awarded to the student.

The institution submits data through secure channel to the central system, the central administration commits data to the central server, finally the end user scans the printed QR code and authenticates though secure gateway.

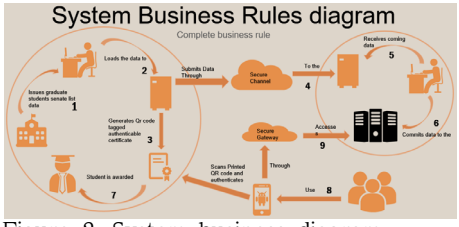


Figure 2: System business diagram

C. Design of system

Android client/server interaction

We have optimized our system for the most

efficient response time by utilizing a lightweight request transmission technology available which is known as JSON, as the main data request and response format [6]

The QR code decryption and encryption method the Information in the QR Code consists of encrypted full certificate information (full name, department, GPA ...) with [2]dual encryption keys (educational institution's private key & public key) and the verification process is done by decrypting the former encrypted certificate message by using the educational institution's public key.

D. Security

Security requirements are important factors in this system as classified education certificates and personal data will be stored in the database. Strict user validation will be done during login to the central system in order to authenticate the system Administrators.

Also there will be strict admin activity monitory logging system in order to make the workflow transparent, verifiable, and accountable.

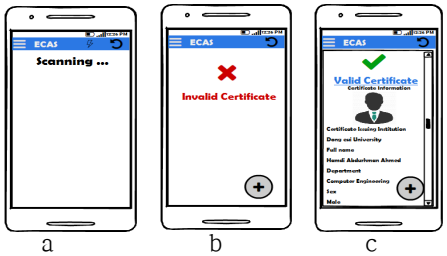
The generation and authentication of certificate validation codes (QR codes) will be done using a high level encryption methods to make document copying and forgery very hard and even impossible.

E. Result of implementation of educational certificate autehntication system

We deployed the project on remote server for testing purposes.

Figure 3: sample generated certificate

The figure below shows the result of the certificate



a b c

Figure 4: ECAS Android application QR code a) scanning interface b) invalid and c) valid certificate respectively

Ⅳ. Conclusion

The proposed design and development of centralized education certificate authentication system using QR code, facilitate the centralized system where each educational institution can issue an authenticable digitally signed educational degree certificate and provide a handy android smart phone application to authenticate educational certificate issued from any registered educational organization.

The proposed system will reduce the certificate forgeries occurring and will automate authentication process of educational certificates by providing a means where each educational institute can prepare and publish certificates that can be easily authenticated by other organization through a facilitated process without the need to address the certificate issuing institution.

The proposed method is cheap, cost effective, don't take much effort and save time to authenticate graduate certificate from different institution.

Acknowledgement

This research was supported by the 2015 Human Resource Development Project for Local Innovation and Creativeness (NRF-2015H1C1A1035898) and the 2016 Human Resource Development Project for New Local Industry (No.2016H1D5A1910985) of the National Research Foundation of Korea.

References

[1] Ankit Singhal, R. P. (2015). Degree Certificate Authentication using QR code and Smartphone. International Journal of Computer Application (0974-887) Volume 120 - No.16, June 2015, 38.

[2]. (2017, 4 26). Retrieved from WIKIPEDIA: https://en.wikipedia.org/wiki/Digital_signature

[3] Rouse, M. (2016, 05 11). SearchSecurity. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/Digital-Signature-Standard

[4]. (2016, 05 11). National Institute of Standards and Technology. Retrieved from U.S Department of commerce: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[5] INCORPORATED, D. W. (2017, 04 26). QR code.com. Retrieved from http://www.qrcode.com/en/about/

[6]. (2016, January 10). Retrieved from JSON: http://www.Json.org