International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 9728-9734

Higher Educational Certificate Authentication System Using QR Code Tag

Hamdi A. Ahmed* and Jong-Wook Jang *

**Department of Computer Engineering, Dong-eui University,*
176 Eomgwangro, Busanjin-Gu, Busan, 614-714, Korea.

Abstract

Digital signature are used to detect unauthorized modification to data and to authenticate the identity of signatory. The Quick Response (QR) code was designed for storage information and high-speed readability. This paper proposed a method that QR code will contain a digital signature with the student data such as degree holder's name, major program, Grade point Average (GPA) obtained and more, which will be signed by Higher Educational Institute (HEI). In order to use this system, all HEI have to registration in central system and deployed in each HEI. All digitally signed certificate generating process are offline. To verify the digital signature signed with QR code, we developed specific smart phone application which will scan and authenticate the certificate without the need to address the certificate issuing institution and gaining access to user's security credentials.

Keywords: Authentication, Degree certificate, Digital Signature, Encryption Key, QR code

INTRODUCTION

The development of technology is increasing day by day, most of the people now depend on technology and we use various technologies to accomplish specific tasks in our lives. As well as the development of Information Technology (IT) allows for us to perform human tasks and share information quickly, safely and correctly without hassle from all over the globe. As the world keeps on developing, technology will be changed, the method we used to solve problem might not work not be efficient tomorrow. So, we need the way an authentication process done in a particular way and use them in our daily life.

Degree certificate is one of the most sensitive document that awarded by Higher Education Institution (HEI) to formalize their achievement with a certificate unique to them and their accomplishment. Now a day the advancement of digital printing and scanning technology growing rapidly. The incident of forgery of important document such as a degree certificate and personal identification card also increased, which are easily available at cheaper prices without much exertion. The manual verification of these certificate is 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 students who passed from their HEI.

Even if the rapid development of technology shaping the world an authentication process is also required to be done in a precise way. According to our survey, most of HEI use a manual way of authenticating 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 HEI. 2) Highly forged certificate can easily evade the manual authentication process. 3) The manual authentication process can't effectively combat corruption among educational institution's employees (those who issue non approved certificates). 4) It take much effort and time to authenticate graduate certificates issued from different HEI.

This paper argues that those kinds of authentication delay and forgeries can be solved by developing authentication system using digitally signed QR code tag and developing smart phone application to authenticate a degree certificate issued from any registered HEI.

This paper organized as follows: We started with an introduction of the availability of advancement of printing and scanning at cheap price. In Section 2, provides related work in document authentication research area and theoretical background of this system follow by Section 3, proposed system model and methods. Lastly in Section 4, result and discussion. Finally, Section 6 represents conclusions of this paper.

PAPER BACKGROUND

This section is split into three sub-section (2.1, 2.2, and 2.3). We start with an overview of related work in Section 2.1. Followed by Description of the standard QR code features in Section 2.2. Lastly the definition, usage, and parameters of Digital Signature in Section 2.3.

Related work

An overview of related literatures with document authentication. Researchers are being developed different types of document authentication method. On this paper [1] they developed a system for managing user's document by

uploading them on cloud database making them available to respective users by sharing an encrypted QR code. Also, Digital Signature, QR Code and Smart phone are used to authenticate degree certificate offline mode [2].

QR Code Feature

According to a joint technical committee of the International Organization for Standard (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 18004:2015 QR Code is a matrix symbology. The symbols consist of an array of nominally square modules arranged in an overall square pattern, including a unique finder pattern located at three corners of the symbol (in Micro QR Code symbols, at a single corner) and intended to assist in easy location of its position, size, and inclination. A wide range of sizes of symbol is provided for, together with four levels of error correction. Module dimensions are user-specified to enable symbol production by a wide variety of techniques [3].

Typical features provided by QR code are: High capacity encoding of data, Small printout size, Kanji and Kana capability, Dirt and damage resistant, QR code has error correction capability the detail about data restoration rate for total codewords are found in Table 1, Structured appending feature, and Readable from any direction in 360^0 [4].

Table 1. Data restoration rate for total codewords

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

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 favorable and the most viable option compared to other proprietary tools.

Digital Signature

A Digital Signature (DS) is a mathematical scheme for demonstrating the authenticity of digital message or document. A valid DS 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). DS are most commonly used where it is important to detect forgery or tampering [5].

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 [6].

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 in table 2: DSA parameters and table 3: selection parameter size and hash function for DSA. This standard specifies the following for the pair L and N (the bit lengths of p and q respectively) [7].

Table 2. DSA parameters

p	A prime modulus, where $2L–1 < p < 2L$, and L is the bit length of p. Values for L are provided in Table 3
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 3
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].

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

Table 3. Selection Parameter for Size and Hash Function for DSA

L	N
2024	160
2048	224
2048	256
3072	256

SYSTEM MODEL AND METHODS

This section is split into four sub-section (3.1, 3.2, and 3.3). We start with overall system model Section 3.1 Followed by system business rule in Section 3.2. Lastly, Design of the system in Section 3.3. Finally, System Security in Section 3.4.

Overall System Model

The overall system mode shown in the figure 1. The degree certificate will contain a QR Code Tag which contains a digital signature with graduate student data such as degree holder's name, Grade Point Average (GPA), Cumulative Grade Point Average (CGPA), institution alias etc. This will be digitally signed and generate with QR code by using local Higher Education Certificate Authentication System (HECAS) system (system that deployed in each HEI but first we have to register in HECAS central system then the HECAS central system will generate the system that deployed in each HEI). Then the institution admin send to HECAS central server (system will receive digitally signed and generated certificate data from all HEI). In order to verify the digital signature a person need to use our proposed smart phone application which will scan the digitally signed QR Code and authenticate the certificate.

System Business Rule

Overall description of system business rule shown in figure 2, assume that HEI already registered in central system. Frist the HEI admin feed graduate list data to local HECAS (system deployed in each HEI), then the institution local system generate QR code tagged authenticable certificate and make ready to award to those student going to graduate. The institution admin submits data through secure channel to the central HECAS, the central HECAS administration commits data to the central server. Finally, after the issued Degree certificate provided to graduated student then, the end user can able to scan digitally signed printed version of QR code from certificate provided and authenticate through secure gateway from central server. Overall description of system business rules shown in figure 2.

Figure 1. Over all system workflow

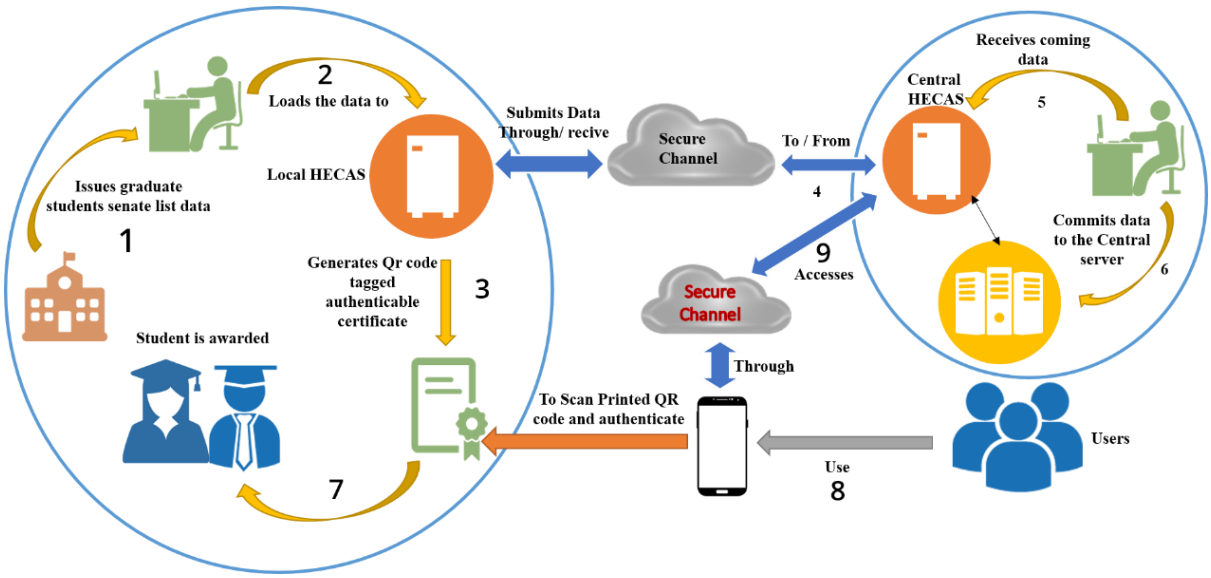

Figure 2. System business rule

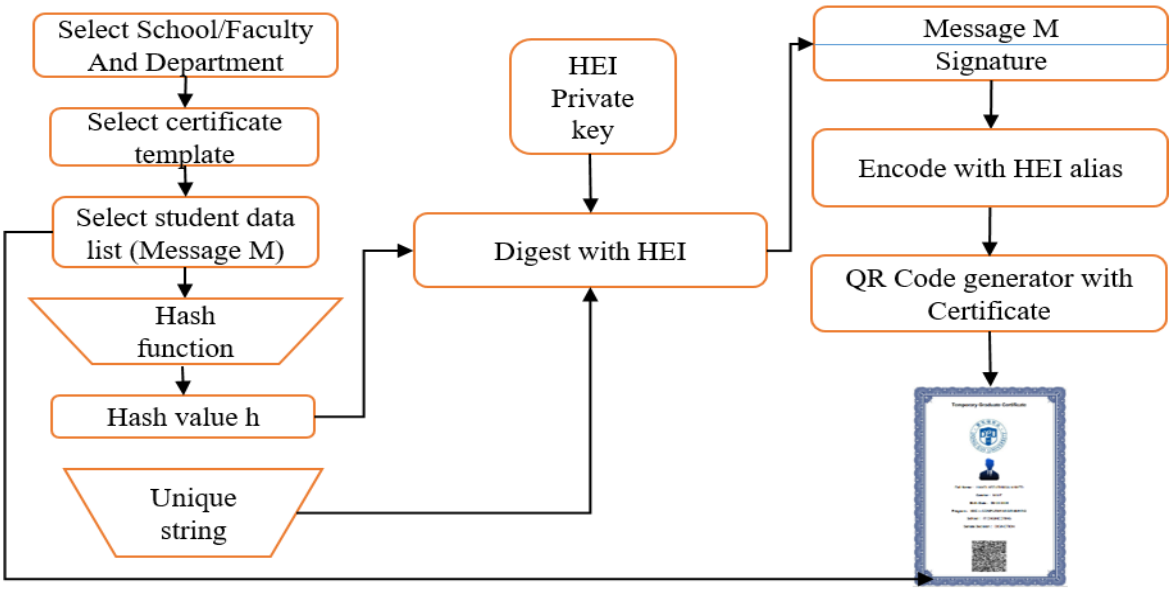

Figure 3. Diagram show that how to Generate authenticable certificate

Design of the system

The overall software architecture of HECAS was developed base on Model View Controller (MVC) pattern in Hypertext Preprocessor (PHP) Codeigniter framework.

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 (JavaScript Object Notation) [8] as the main data request and response format.

QR code encryption and decryption method are as follows: the information in the QR Code consists of encrypted full certificate information (full name, department, GPA …) with dual encryption key (HEI private and public key) and the verification process is done by decrypting the former encrypted message by using the HEI public key.

Step to Generate of Authenticable certificate

We followed the following steps to generate authenticable HEI certificate. Diagrammatical representation of the steps are found in figure 3.

i. First we have to select the school or faculty and then department.

ii. Followed by selection of certificate template which are predesigned with the HECAS and unique to each HEI.

iii. Selection of student data list (for this experiment we used and implemented using Microsoft excel and access) file type, which contain all information like student name, birth date, CGPA, GPA… etc.

iv. Before starting generation of encrypted QR Code, we have to generate unique hash string to identify the current data feed later on to recognize whether the certificate is generated from HECAS or not

v. To obtain digest message we applied Hash function and resulted in hash value

vi. To sing obtained hash value we used HEI private key which are resulted to gain digital signature on the initial input data.

vii. Lastly, to easily identify HEI from central HECAS we used HEI alias and encoded on top of digital signature and fed into QR Code generator.

viii. Finally, the QR code generator, result in output with pre-selected template certificate.

Certificate Authentication Process

The authentication schema of degree certificate are shown in the figure 4. To scan QR Code from the HEI certificate, we development android application for this experiment. The following steps are applicable to get response on the validity scanned certificate.

i. First, the proposed smart phone application scan the QR Code from the certificate the app response will give error message, if the QR code was not generated by HECAS.

ii. If the condition is yes, the app send encrypted data to HECAS central system. Using JSON.

iii. After the data received by the central system, then the data will be decoded to check the HEI alias and looking in the database the public key.

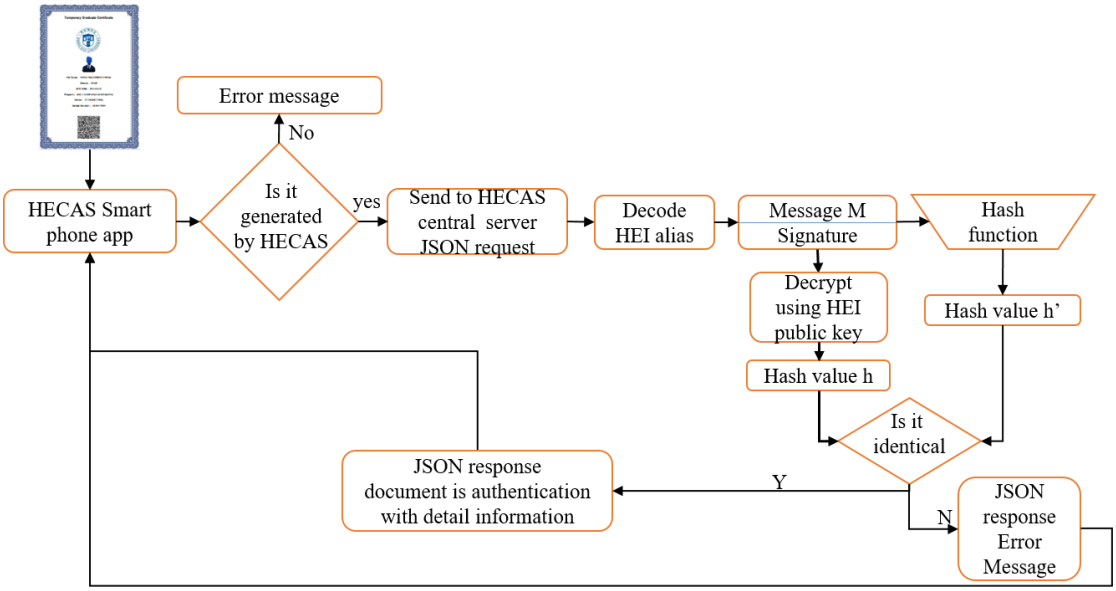

Figure 4. Schematic representation of proposed authentication method

iv. On the Message M hash function will be applied to get Hash value h'

v. We use university public key to decrypt and generate Hash value h.

vi. Then, if the Hash value are identical the system add detail information base on the certificate id from database and response to the HECAS smart phone application.

vii. If the Hash value is distinct, invalid certificate will be send to HECAS smart phone application.

Based on the response, the users of our proposed smart phone application can simply destination forgery from the original and also avoid modification of message which are not encrypted as first place but necessary for detail information about the certificate holder without any further scan.

Design of the system

Security requirement are important factors in this system and mainly store data in central database. To login to central HECAS, each HEI admin authenticated through a method called google 2FA (Two Factor Authentication) in addition to user name and password. All HEI admin have to manage their database with limited database privileges in central system and there will be strict admin activity monitory logging system in order to make the workflow accountable and transparent.

As shown in the figure 2 step 4, when HEI send certificate data to central system, the central system authenticate the incoming data with HEI admin credential. This credential was gave to the HEI at the first registration time and cross check with it. If this credential is correct the central system send an encrypted ftp detail to HEI. Then, the HEI send data to specified location to the HECAS central system. We designed the way to validate and commit data before submitted to central server.

RESULT AND DISCUSSION

This section illustrate experimental result with discussion.

The proposed digitally signed certificate designed be scan by any smart phone device (android for this experiment) which fulfill the following criteria.

i. Smart phone camera: for best and fast scan it is recommend to use >=8 Megapixel with camera flash and

ii. Minimum operating system, Android 4.3 (Jelly Bean)

The scanning distance between smart phone and minimum QR Code size is approximately 10:1 (1 inch = 2.54 centimeter) [9].

The QR code model 2 version 14 module (73x73) and error correction level H are used to generate digitally signed certificate. This data helps us to determine maximum data capacity in this version.

$$Module = 21 + 4(n - 1) \qquad 4.1$$

Where n is version number and maximum version number are 40 and minimum is 1.

Scan process time using android smart phone device in daylight with good bright environment take less than 2 seconds. We used JSON for serializing transmitting structure data over network connection.

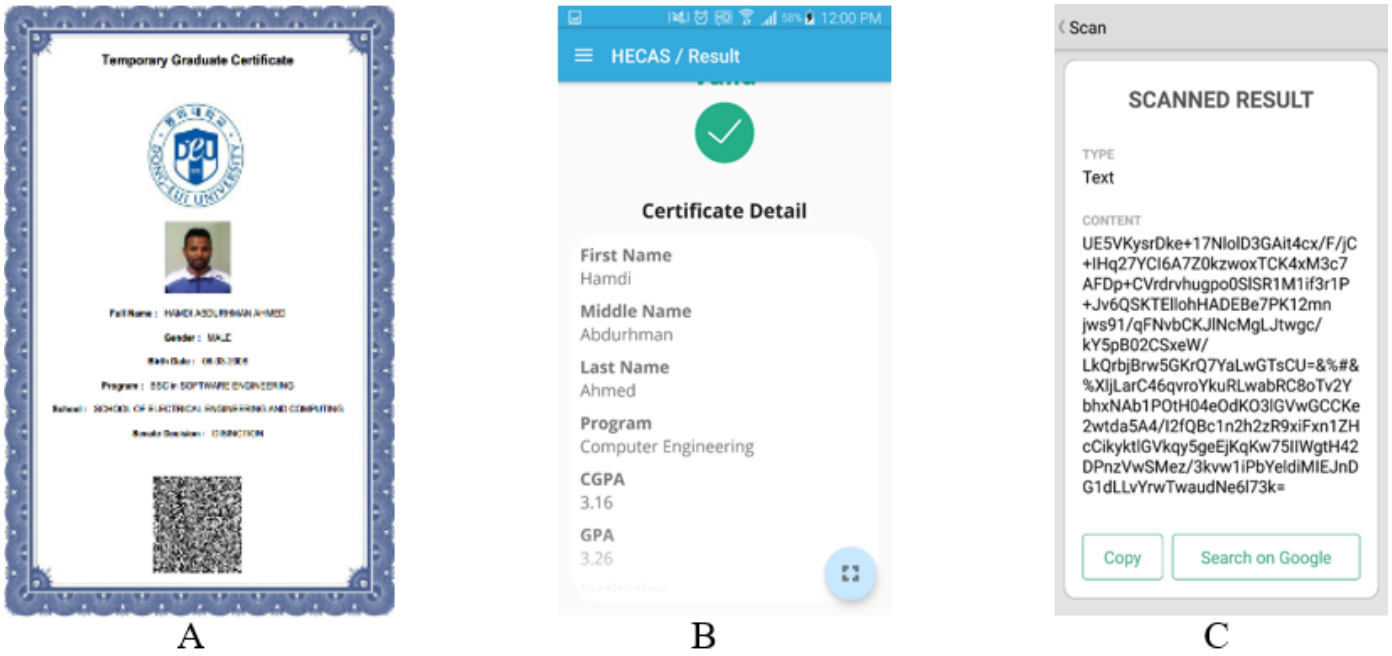

Figure 5. A, Finale output of sample authenticable degree certificate; B, Scanned result using proposed smartphone app; C, Scanned result using other QR code reader

To generate digitally signed certificate we deployed on Windows 10 (64 bit) computer with Intel Core i7 6700 Central Process Unit (CPU) clock frequency 3.40 Gigahertz (GHz) and Random Access memory (RAM) 8.00 Gigabyte (GB). We used our laboratory server as central system.

Scan result of proposed system certificate are shown in the figure 5. Figure5 A, show that authenticable certificate, this certificate generate in offline and 4 x 10^2 milliseconds required to generate single certificate. Figure 5 B, show that scanned response result from HECAS central system using our proposed HECAS smart phone application.

Figure 5 C, show that scanned result using other QR Code reader which gives cipher text to user.

The proposed smart phone application allowing us to make things simple in hierarchy level. This app give the decision on the first scan QR Code that allow us to Easley identify QR code generated by HECAS. Also allow the user to get all required information on the first scan. The scan history will be saved automatically and used in case if the user want to recheck the detail of information again.

CONCLUSION

In this paper a system called HECAS and android smart phone application is proposed. This system provide centralized system with distributed HEI. Each HEI can issue to their own graduate student an authenticable digitally signed degree certificate. In addition to that, the system is designed to generate batch digitally signed degree certificate.

The proposed system minimize the circulation of forged certificate, unauthorized modification to data, and authenticate the original identity of certificate.

The proposed method is cheap, coast effective, don't take much effort and save time: to generate and automate authentication process from different part of the world.

Provide all in one: authenticate all degree certificate that are issued from registered HEI and receive detail information about the degree certificate holder with a single scan. The proposed app had capability to keep scan history for later reference and save time by Easley distinguish QR Code generate from proposed system and other QR Code before sending to central system.

In our future work, we will develop this system to framework level and we will add a feature to our smartphone application with more security and usability to authenticate

ACKNOWLEDGEMENT

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Grand Information Technology Research Centre support program (IITP 2017-2016-0-00318) supervised by the IITP (Institute for Information and Communication Technology Promotion) and Human Resource Training Program for Regional Innovation and Creativity through the Ministry of Education and National Research Foundation of Korea (NRF-2015H1C1A1035898).

REFERENCES

[1] Harshal Pandit Shailendra Nipane, Suraj Jadhav, Sunita Naik Secured E-Document and Sharing using Encrypted QR-Code [Journal] // International Journal of Computer Applications (0975 -8887). - July 2016. - pp. 15-19.

[2] Ankit Singhal R.S Pavithr Degree Certificate Authentication using QR Code and Smartphone [Journal]. - [s.l.] : International Journal of Computer Application (0975-8887), June 2015. - Vols. 120-No. 16.

[3] SO/IEC 18004:2015 [Online] // International Organization for Standardization ISO. - 04 25, 2017. - https://www.iso.org/obp/ui/#iso:std:iso-iec:18004:ed-3:v1:en.

[4] INCORPORATED DENSO WAVE QR code.com [Online] // DENSO WAVE. - 04 26, 2017. - http://www.qrcode.com/en/about/.

[5] Digital signature [Online] // WIKIPEDIA the Free Encyclopedia. - 4 26, 2017. - https://en.wikipedia.org/wiki/Digital_signature.

[6] Rouse Margaret Digital Signature Standard [Online] // TechTarget Search Security. - 05 11, 2016. - http://searchsecurity.techtarget.com/definition/Digital-Signature-Standard.

[7] Digital Signature Standard (DSS) [Online] // National Institute of Standards and Technology U.S Department of Commerce. - 05 11, 2016. - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[8] JSON [Online] // JSON. - 01 10, 2016. - http://www.Json.org.

[9] What Size Should A Printed QR Code Be? [Online] // QRSuff.com. - 06 3, 2017. - https://blog.qrstuff.com/2011/01/18/what-size-should-a-qr-code-be.

* *Corresponding author: Jong-Wook Jang, Ph.D.*
Department of Computer Engineering,
College of ICT Engineering, Dong-Eui University,
176 Eomgwangro, Busanjin-Gu, Busan, 614-714, Korea
E-mail: jwjang@deu.ac.kr