Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 1, April 2021, pp. 516~521
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i1.pp516-521

Web-based document certification system with advanced encryption standard digital signature

Henny Indriyawati, Titin Winarti, Vensy Vydia
Faculty of Information Technology and Communication, Semarang University, Indonesia

Article Info

Article history:

Received Mar 12, 2020
Revised Dec 5, 2020
Accepted Jan 13, 2021

Keywords:

Advanced encryption standard
Certification
Encryption
QR Code

ABSTRACT

Web-based degree document certification system with a digital signature in Semarang University has a purpose to support academic to do online document certification through a system. The main problem which occurs in academic administration is a long document certification process that causes an ineffective and inefficient certification process. To solve the problem, a system that can encrypt a document for better security is required. This system is built with the advanced encryption standard algorithm with a 128-bit sized key to encrypt confidential information inside the document. During the encryption process, this algorithm operates using 4x4 bit array blocks and passing many encryption processes for at least 10 (ten) times. The application is analyzed with object-oriented analysis and modeled with unified modeling language. The result of this research is a system which can secure document with AES algorithm with a 256-bit sized key. The security element in this algorithm will make easier to identify the owner of the document. The secured document is easily accessible through PHP-based web or available QR code. When decrypting the document, the application will activate the camera function and decrypt the information document.

Corresponding Author:

Henny Indriyawati
Faculty of Information Technology and Communication
Semarang University
Soekarno-Hatta, Tlogosari, Semarang, Central Java, Indonesia
Email: henny@usm.ac.id

1. INTRODUCTION

Document digitalization is a process converting analogue into digital data for preserving purposes. By preserving data into digital version, this action will help the owner whenever he lost the document. The problem losing original document also occur everywhere especially Semarang University. This university has an obligation to release official document for its alumni to help them finding a job. Semarang University must issue degree certification including transcript for every alumnus that graduate every semester. Since Semarang University must issue official document every semester, the effectiveness and efficiency might decrease. Besides that, the document legality also become a problem since many fake degree certificates issued by inresponsible third party.

Fake degree certificate case caused many problems to the alumnus as well as the citated university. The occurance of this case affect university's reputation and my reflect to university's output to industry. In order to prevent the problem to occur soon, a certain safety measurement must be applied to new issued official document. This research has a purpose to design a new safety measurement to protect document against illegal replication especially document spoofing by using encrypted data signature.

In order to provide strong sncryption data, this research used advanced encryption standard as encryption process with key size 128-bit. The process of issueing encrypted data is done by a system used by administration staff. Hence, the issued document received by the alumnus contains not only study information but also legality of document written as encrypted data embedded as QR Code [1, 2].

The embedded QR Code makes the originality verification faster [3, 4]. Hence, the company can verify the originality of the issued degree certificate. QR code has been used for many purposes such as security features or degree certificate verification methods[5]. However, QR code verification has weakness such as manipulable data or misused certificates. To counter measure the weakness of QR code, the written data used in QR code must be encrypted. Hence the required system must capable to verify the originality of degree certificate and certification online with AES digital signature. Thus, improve the efficiency and effectivity of academic staff and shorten the administration process of degree certificate certification. Compared to barcode, QR code can store larger data by making two dimensions marking in the surface. Barcode only store data as stripped one dimension marking in the surface, so only capable to store limited number of data [6, 7].

There were many researches about securing certificate against fake certificate, which help industry determines whether the document is authentic or now. Securing certificate of higher education or lower with QR code can successfully counter fake certificate. Since these certificates contains digital signature of degree's holder name, registration number, certificate registration id, and transcript. The QR code watermarked into the certificate in specific location to enable easy scan for user [8-14]. Besides that, the usage of near field communication (NFC) [15-18] also help academic or university increase the security of the certificate. NFC chip inserted inside the certificate recorded with owner's authentic information, so the industry just need to swipe their smartphone near the certificate [19].

However, most of the researches store the data directly inside the QR Code and NFC chip. Hence, the authenticity of the data is not guaranteed. Besides that, research which used NFC chip as extra security become a problem when the owner makes a copy of his certificate. The copy of certificate does not have NFC chip on it, so the verification will be pointless. Adding extra chip in the certificate copy also increase the cost of the service. The most problematic thing in NFC is the fact that NFC reader is required in order to read the data. Not all smartphones have NFC reading/writing capability, so having NFC in certificate without NFC reader is like adding paperclip in a paper [20, 21].

In order to solve problem in previous researches, this research will use advanced encryption standard [22] as extra security for encoded QR code. Instead of owner's data, decryption link with encrypted code is written inside the QR code. This link will lead to decryption system to decrypt encrypted certificate code to check the owner's data. Hence, there is no owner's data inside the QR code. In order to understand the problem better, this research will limit the problem only to official degree certification, advanced encryption standard algorithm; and QR Code. The main contribution of this research is the usage of modern algorithm Advanced Encryption Standard to encrypt the confidential data and embedded as QR Code in the document.

2. RESEARCH METHOD

The research method applied in this study is observing the process of document certification done by the administration staff in the university. The manual process of document certification was shown in Figure 1. According to the Figure 1, administration staff issued two documents such as degree certificate and transcript for every alumnus of the university. In order to add authenthicity, all the documents signed and stamped by the dean before the alumnus receive it. After that, all alumni will get the documents to help them looking for a job. All job vancacies require copy of certified documents to check the background of job seeker. Hence, alumnus will make a copy of each documents and request re-certification to the administration staff.

This process repeated many times according to alumni's number for each semester, and the process re-certification add extra weight to the administartion staff and dean. By adding extra safety measurement, this feature will remove some burden of re-certification. Since this safety measurement already added at the beginning of printing, document authenticity won't be a problem anymore. Figure 2 explain how the safety measurement through AES encryption and QR code added to the document before Administration staff print the documents.

Before administration staff print the needed documents, the documents must be watermarked with AES encrypted authentic data via QR Code. The encrypted data obtained by creating certificate code based on document number combined with uniqueness, and code of dean combined with current time. This base code will be encrypted with AES-128bit and linked with link checker. QR Code generator created QR Code based on the combination of link checker and encrypted data. The generated QR Code watermarked into the document as an extra safety measurement of the documents. The process of code encryption explained in Figure 3.

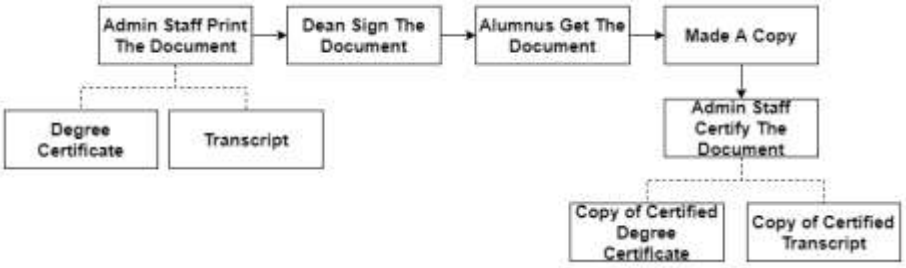

Figure 1. Flow of issuing official document

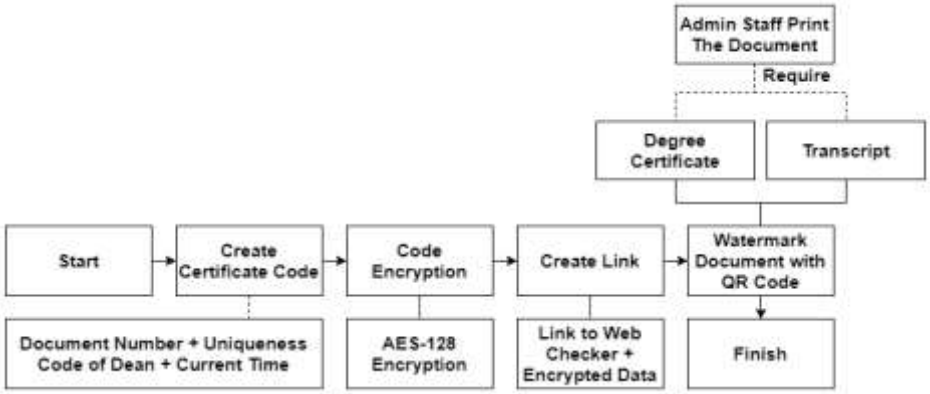

Figure 2. Flow of adding encrypted data via QR code watermarking

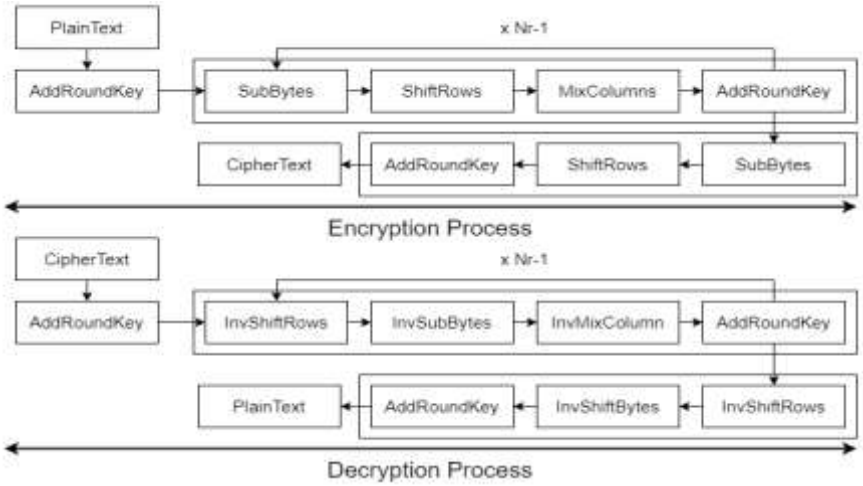

Figure 3. AES encryption and decryption process

In the AES algorithm, the number of input blocks, output blocks, and the key are 128 bits. With a data size of 128 bits, it means that the block size or Nb = 4, which shows the length of data 22 per line is 4 bytes. With an input block or data block of 128 bits, the key used in the AES algorithm does not have to be the same size as the input block. The cipher key in the AES algorithm can use keys with 128-bit, 192-bit or 256-bit long. The difference in key length will affect the number of rounds that will be implemented in this AES algorithm. The encryption and decryption process are explained in [23-26]:

a) Encryption

The input copied into the state will be subjected to an AddRoundKey byte transformation at the beginning of the encryption process. After that, the state transforms SubBytes, ShiftRows, MixColumns, and

AddRoundKey repeatedly. This process is called the round function in the AES algorithm. The last round is somewhat different from the previous rounds, where the state did not experience the transformation of the MixColumns in the last round.

b) Decryption

To build an easy-to-understand inverse cipher for the AES algorithm, the cipher transform can be reversed and applied in the opposite direction. InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey are the byte transforms used in the inversion cipher.

The implementation of AES is used in encryption and data documents. The system that already has a hash will be used to encrypt the data (diploma/transcript) that the user uploads. The results of the document will be stored in a database. The data input that was copied to the state at the beginning of the encryption process. After that, the state will repeatedly transform as many rounds (Nr) as SubBytes, ShiftRows, MixColumns, and AddRoundKey. This process is called the round function in the AES algorithm. The state is not given the transformation of MixColumns in the last round.

3. RESULTS AND ANALYSIS

The result of this research according to the previous explanation is an encoded QR Code which contains encrypted data. In order to read decode as well as decrypt the content inside the QR code, a special system is required to read the content. The system is built with laravel framework and MySQL database to decrypt the content inside QR Code. Database was used to store data about certificate number, unique id, code of dean, and time of code generation as well as the owner's information. The encryption process of from certificate code until QR code generation is explained below with example:

The Figure 4 explained how the encryption process of certificate code start. The certificate code was made from document number, uniquely generated id, code of dean, and time of generation to increase uniquness of the code. This information combined into a string before entering the encryption process with AES. The encryption process required plaintext (certificate code) and 128-bit sized secret key. Since AES is a symmetrical algorithm, the used key for encryption and decryption is same. From the encryption process will resulting a hexadecimal value instead base64 value. Since base64 used special characters, then it is not usable for web link. The ciphertext from encryption process is combined with decryption links and then encoded as QR Code.

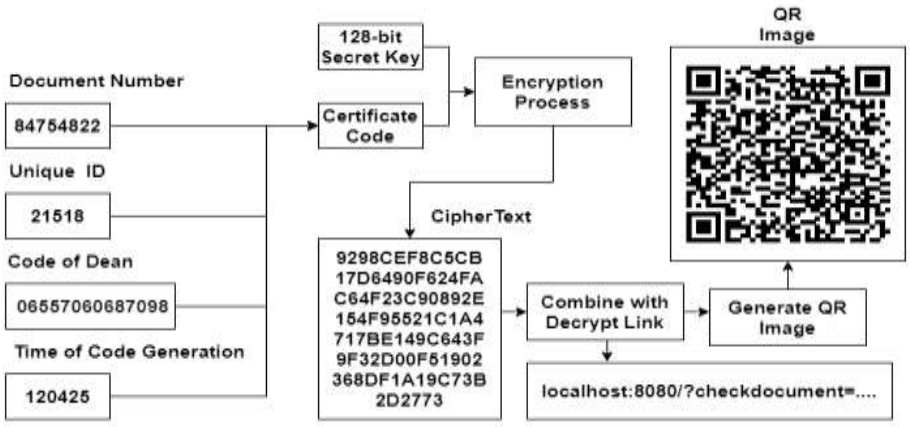

Figure 4. Encryption process for secure QR code

The Figure 5 explains how QR Code app decode the QR code and data decryption through website. The decryption process starts from decoding QR Image to get Decryption Link. This decryption link contains url to the system and encrypted certificate code. When the user opens the link, he will see a browser open the system. The system will receive the encrypted certificate code through GET method and start decrypting the certificate code. The decryption process requires similar 128-bit sized secret key, in order to decrypt the certificate code. The secret key is already hardcoded to the system, so the user does not need to know what the secret key is. Once the decryption process done, the system will extract the data from the plaintext. This data consists of two things: document number and code of dean used for search query in the database. Search query will decide whether the data is authentic or not according to the result. If the result is zero row, then the

possibility of fake certificate is high. If the result return one row, then the certificate is authentic. In order to read the encrypted data inside QR Code, the user who wished to verify the data must use QR Code app. The decryption process using web system is exaplined in Figure 5.

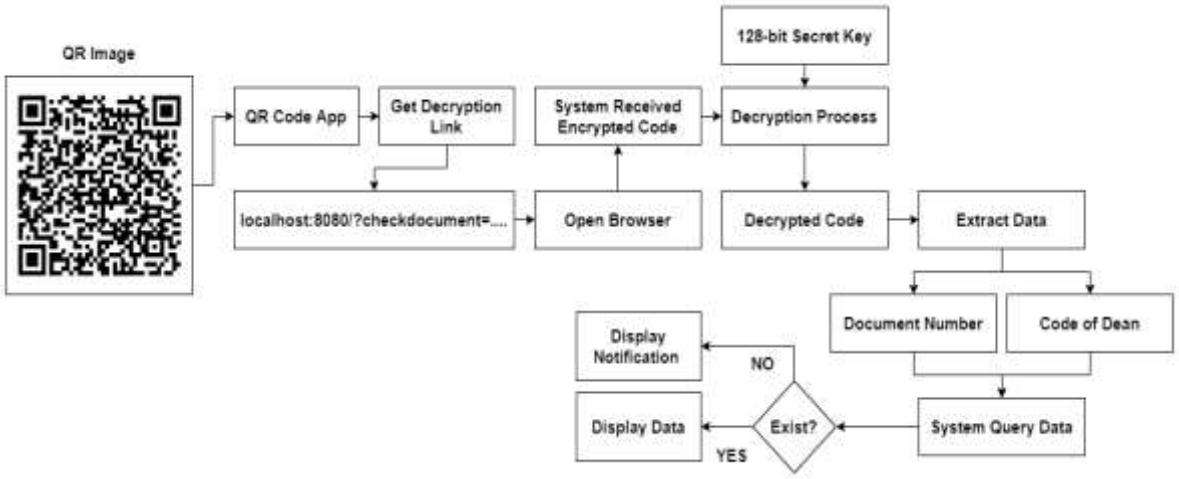

Figure 5. Decryption process by system

4. CONCLUSION

According to our findings, the results of the research can be concluded that the process of adding extra security layer to diploma certification help to prevent identity theft by third party. This extra security layer helps company employer to verify the validity of holder's information. The security paramter used in this security layer consists of many unique data such as document number which only generated once by the government, system generated unique id, Code of Dean which belongs to faculty's dean, and generation time. At least there are three unique data which were used as security parameter in the certificate. Besides that, the encryption and decryption algorithm used in this research is advanced encryption standard which has strong security mechanism supported with 128-bit sized key. Hence, the process to crack down this algorithm without proper key may take a lot of time. The ciphertext of algorithm used with web decryption link and masked as QR code instead using URL text. The usage of QR code ease employers to verify with smartphone instead typing it to web browser. The process of data decryption was done by the system instead in smartphone. This web has a role to decrypt the data and display the matched data into web browser. However, this research has several weaknesses and need some proper improvement such as. This research used 128-bit sized key instead 192-bit or 256-bit which provide better security. The security paramater added to the algorithm is too few and only one data which related to the owner. Adding owner-related data as security parameter will increase the security better than before, and android-based notification apps which help owner when to get their certificate also important.

REFERENCES

[1] N. Kucirkova, J. Audain, and L. Chamberlain, "QR codes," in *Jumpstart! Apps*, 2018.
[2] S. Tiwari, "An introduction to QR code technology," in *Proceedings-2016 15th International Conference on Information Technology, ICIT 2016*, 2017, doi:10.1109/ICIT.2016.021.
[3] A. S. Narayanan, "QR Codes and Security Solutions," *Int. J. Comput. Sci. Telecommun.*, 2012.
[4] L. F. F. Belussi and N. S. T. Hirata, "Fast QR code detection in arbitrarily acquired images," in *Proceedings-24th SIBGRAPI Conference on Graphics, Patterns and Images*, 2011, doi:10.1109/SIBGRAPI.2011.1.
[5] Wei X., Manori A., Devnath N., Pai N., Kumar V., "QR Code Based Smart Attendance System," *Int. J. Smart Bus. Technol.*, Vol. 5, No. 1, pp, 1-10, 2017, doi: 10.21742/ijsbt.2017.5.1.0.
[6] L. Várallyai, "From Barcode to QR Code Applications," *J. Agric. Informatics*, Volume 3, issue 2, 2013, doi:10.17700/jai.2012.3.2.92.
[7] T. Lotlikar, R. Kankapurkar, A. Parekar, and A. Mohite, "Comparative study of Barcode, QR-code and RFID System," *Int. J. Comput. Technol. Appl.*, 2013.
[8] A. Singhal and R. S. Pavithr, "Degree Certificate Authentication using QR Code and Smartphone," *Int. J. Comput. Appl.*, vol. 120, No.16, 2015, doi:10.5120/21315-4303.

[9] Z. Yahya *et al.*, "A new academic certificate authentication using leading edge technology," *in proceedings of the 2017 International Conference on E-commerce, E-business and E-Government*, *pp. 82-85*, 2017.
[10] T. Guhan and S. Sebastian, "Certificate Authentication Using QR Code and Smart Phone," *Int. J. Emerg. Technol. Eng. Res.*, 2017.
[11] B. R. Suteja, R. Imbar, and M. Johan, "Implementation of QR Code on E-Certificate for Events at Maranatha Christian University," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 5, 2019.
[12] H. A. Ahmed and J. W. Jang, "Document certificate authentication system using digitally signed QR code tag," in *ACM International Conference Proceeding Series*, 2018.
[13] H. A. Ahmed and J. W. Jang, "Higher educational certificate authentication system using QR code tag," *Int. J. Appl. Eng. Res.*, 2017.
[14] M. Chen, "Certificate Anti-counterfeiting System Based on QR Code and Digital Watermarking," vol. 9, no. 10, pp. 109-116, 2016.
[15] G. Madlmayr, C. Kantner, and T. Grechenig, "Near field communication," in *Secure Smart Embedded Devices, Platforms and Applications*, 2014.
[16] R. Want, "Near field communication," *IEEE Pervasive Comput.*, vol. 10, issue 3, pp. 4-7, 2011, doi:10.1109/MPRV.2011.5.
[17] M. J. Harnisch and I. Uitz, "Near Field Communication (NFC)," *Informatik-Spektrum*, vol. 36, Issue 1, pp.99-103, 2013, doi:10.1007/s00287-012-0672-x.
[18] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC) Strengths and Weaknesses," *Semiconductors*, 2006.
[19] Y. Hunegnaw and P. Bagane, "NFC based Anti-Counterfeiting Scheme for Certificates Identification and Verification using a Smartphone," *Int. J. Pure Appl. Math.*, vol. 118, no. 7, pp. 447-454, 2018.
[20] Y. Zhao, B. Mahoney, and J. R. Smith, "Analysis of a Near Field Communication wireless power system," in *2016 IEEE Wireless Power Transfer Conference, WPTC 2016*, 2016.
[21] M. Mustafa AbdAllah, "Strengths and Weaknesses of Near Field Communication (NFC) Technology," *Glob. J. Comput. Sci. Technol.*, 2011.
[22] A. U. Rahman, S. U. Miah, and S. Azad, "Advanced encryption standard," in *Practical Cryptography: Algorithms and Implementations Using C++*, 2014.
[23] M. A. Ako, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," *Cryptogr. Netw. Secur.*, 2017.
[24] FIPS, "Specification for the advanced encryption standard (AES)," *Federal Information Processing Standards Publication*. 2001.
[25] Daemen J., Rijmen V., "The Advanced Encryption Standard Process. In: The Design of Rijndael. Springer, Berlin, Heidelberg, 2002, doi:10.1007/978-3-662-04722-4_1.
[26] P. Townsend, "AES Encryption," *Technology*, 2013.