Implementation of Advanced Encryption Standard (AES) and QR Code Algorithm on Digital Legalization System

Okfalisa[1], Novi Yanti[1], Wahyu Aidil Dita Surya[1], Amany Akhyar[1], Frica A Ambarwati[1]

[1]Department of Informatics Engineering, Faculty of Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru - Indonesia

Abstract. A certificate is an important document that its validity must be ascertained. Fraud over the originality of this document demands a high level of security to ensure that this document is genuine. The Digital Certificate Legalization system (DCL) can regulate and guarantee the mechanism of document validity procedure. By implementing AES and QR Code algorithm, the information contained in the photo-scan of the certificate can be authenticated. The results of the scan are encrypted by using the legalized code in AES Algorithm. The code will be translated using the QR Code and matched to the data contained in the server system. The system will confirm whether the certificate is original or not. In order to test the system, black box testing is applied for functionality check; capacity testing in terms of execution time and memory load of benchmark testing are also examined for system performance measurement. Finally, user response testing is conducted to identify the user acceptance towards the system. As the result, the implementation of AES and QR Code algorithm provides good performance, efficient, light, and fast execution responses (less than one second and less than one megabyte) in a legalized certification checking system.

Keywords: **Advanced Encryption Standard, Certificate Legalization, Digital Certificate Legalization, Legalization Code, Quick Response Code**

1. Introduction

One of the requirements for the job application is a legalized copy of the certificate. The problem may arise due to the limited number of the copied certificates, the numbers of applicants, and the limited time and place. Moreover, fraud or plagiarism on the original documents became an issue in the academic world [1]. Thus, the need for a system that can prove the originality of a certificate is necessary. Besides being able to verify the authenticity of documents, prevention of possible falsification of certificates/diplomas can also be minimized [2]. Document security becomes more protected through official access and privacy provided [3]. Some previous studies such as Rochman et.al., (2017) applied QR Code and Digital Signature to determine the validity of KRS (Kartu Rencana Studi / Study Plan Card) and KHS (Kartu Hasil Studi / Study Result Card) Documents in Higher Education Institution [4]. While Ahmed et.al., (2017) applied QR Code Tag in the process of authenticating documents through digital signatures signed by the Higher Education Institute. Herein, QR Code Tag consists of students data such as students' name, major program, and Grade Point Average (GPA) [5] for such purpose. Another example of QR Code application was on online bank authentication system [6] and attendance system [7]. The implementation of the QR Code is simple, low cost, open source, and the ease of use make this technique interesting to be developed [8 and 9]. QR Code also secure and has a quite large capacity for data storage [10].

Therefore, this research studies the development of the system which encrypts the code (ciphertext) in diploma or certificate to ensure its legalization. The system which will issue and ensure the authentication of certificate copies would require the secrecy of the code placed on the copy of the certificate. It takes cryptography to encrypt and protect the legalized code. Next, the encrypted code (ciphertext) will be translated into a Quick Response Code (QR Code) image so that the encrypted code is more practical in memory usage, execution time, and capacity of data encryption size [3]. QR Code is used to allow the legalization process to be faster by simply scanning it. For the encryption process, the Advanced Encryption Standard Algorithm (AES) was applied in this study. This algorithm has advantages in memory usage, execution time, and capacity of data encryption compared to other algorithms (Such as Rivest, Shamir, and Adleman-RSA, Data Encryption Standard -DES, and BLOWFISH) on implementation in cloud computing [11]. AES also has a security advantage in the formation of key combinations (2^{128}-2^{256}) and the

* Corresponding author: okfalisa@gmail.com

flexibility of key application in both hardware and software, if compared to DES and 3DES [12].

This study applies the AES algorithm to encrypt the legalized copy of the certificate, then the ciphertext will be translated into QR Code which will be attached to the copy of the certificate to replace the conventional stamp. Thus, to produce a digital legalization system called LID that can make copies of the certificate from educational institutions and prove the truth of the information in it. Some applications of AES Algorithm include hybrid encryption algorithm based on AES and RSA on improving data security transmission in Bluetooth communication [13]; The simulation of AES Algorithm process for encryption/decryption [12] which can improve AES used in a variety of application, such as digital video/audio recorders, FRID tags, Smart Cards, ATM, TV set up box, military applications, secure communication system, and etc.

2. Theoretical framework

2.1. Legalization

Legalization is an activity of endorsement of something. Meanwhile, certificate legalization is administrative services to authorize photocopies of certificates or other documents in accordance with their original documents, then certified copies of certificates with the same award as their original certificates. Regarding legalization or certification of certificate, it has been regulated in the ministerial regulation in article one, paragraph three, which reads: Validation is a process of signature and/or seal of photocopy of certificate/STTB/certificate of replacement of certificate/STTB by authorized official after verification in accordance with facts and data or original documents [5].

2.2 AES

The AES algorithm is a symmetric-key cryptographic algorithm and a block cipher. This algorithm uses the same key to encrypt and decrypt. AES actually supports a variety of block sizes and keys that will be used. But after being standardized by the National Institute of Standards and Technology (NIST), Rijndael uses fixed block and key length sizes of 128, 192, and 256 bits, so commonly referred to as AES-128, AES-192, and AES-256 [14]. In general, the encryption process in AES divided into two namely the encryption process itself (Encryption Process) and key generation (Key Expansion / Key Schedule) or round key. In the encryption process the AES-128 algorithm operates as follows (outside the round key generation process) [15]:

1. AddRoundKey. Perform XOR between initial state (plaintext) with the cipher key.
2. Round as much as Nr-1 times (nine rounds on AES-128). The process of each round is:
   a. SubBytes: bytes substitution by using the substitution table (S-box).
   b. ShiftRows: shifting state array rows by wrapping.
   c. MixColumns: scrambles the data in each state array column.
   d. AddRoundKey: performs XOR between the current state with round key.
3. Final Round. Process for the last round:
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

2.3 QR code

QR Code is a two-dimensional barcode [16] which is the development of the barcode bar code previously. If the old barcode data is stored horizontally, but the QR Code data is stored horizontally and vertically. With the ability to store in two dimensions of QR Code certainly can store more data and varied rather than the barcode. The type of data that can be stored in QR Code is [4] including Numerical mode, Alphanumeric mode, 8-bit mode byte, and Kanji Mode.

Some structures of the QR Code are described below [17]:

1. *Finder Pattern.* Three boxes located in each corner of the QR Code corner except the bottom right corner. This pattern serves to detect the position of the QR Code.
2. *Alignment Pattern.* The pattern for correcting distortion from QR Code.
3. *Timing Pattern.* Patterns for identifying the central coordinates of each cell in QR Code with a black and white pattern arranged alternately.
4. *Quiet Zone.* Space needed to read the QR Code. This space makes it easy for detected symbols from an image by using a CCD sensor.
5. Data Area. Data from QR Code is stored or encoded here. Black cells represent binary 1 and white cells represent binary numbers 0.

3. Research methodology

By applying the Rapid Application Development (RAD) software development model, the steps taken from the planning stage consist of literature study and business modeling; The analysis and design stage contains the general system description, the unique coding of the dean, the AES encryption process, the QR Code Encode and the watermark of the certificate. The analysis results are then used in system design by using Unified Model Language (UML) tool, data modeling, and interface design. Stages continued with the implementation and testing process. The implementation is restricted by some rules, viz. The encryption algorithm used is AES-128 with ECB as electronic codebook mode. The parameter of the QR Code is using PHP QR Code library, such as the output format in PNG, ECC Level is Middle, the Image size is 6, and the frame size is 2. The object file format target must be in JPG/JPEG, PNG, and GIF. The output file format is in JPG/JPEG. The maximum width of the output file is 2126 and 1414 for max height. The quality image of the output file is 79. Finally, the conclusions and suggestions are given as

closing the research. This explanation can be depicted in Fig.1.

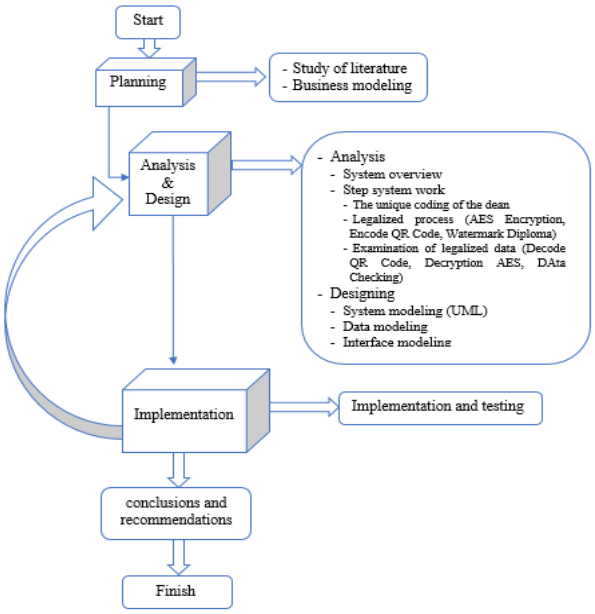

Fig. 1. Research methodology

4. Analysis and discussion

4.1 Analysis and discussion

4.1.1 System analysis

In general, the LID system is as same as the conventional legalization process. Where begins with a request from the owner of a certificate to the educational institution that issued the certificate. After the request is received by the admin of the administration then the file is forwarded to the official who certifies the copy of the certificate. Once the file is in the hands of the official, the file will be directly signed and still need the stamp of approval. Compared with the conventional legalized process, LID systems have little difference. Besides can be done online, there are other differences in the stages of the ratification process, where once the file has been signed by the official, the file can be directly used by the applicant by downloading the file. In contrast to the conventional way that, after being signed by the certifier, the file still needs to be stamped with the educational institution.

4.1.2 Step system work

The step begins with the submission process, the applicant who is here is the alumni requesting the legalization of the certificate with two options which to use the certificate photo file that has been provided from the system (uploaded by admin) or use the certificate photo file uploaded by the applicant himself. Then, the file will go to the admin workspace (administration admin) which will be reviewed whether to proceed to the dean or rejected (returned). Procedural applicable in UIN Suska Riau environment, only Dean can do the file legalization. In this process, the encryption is done by providing a combination code of the certificate number, the unique code of the certifier officer, and the time when the process is performed. Next encryption result of the code combination will be made its QR Code. QR Code will be affixed to the photo of the certificate that will be used on examination of the originality of legalized data through code matching process.

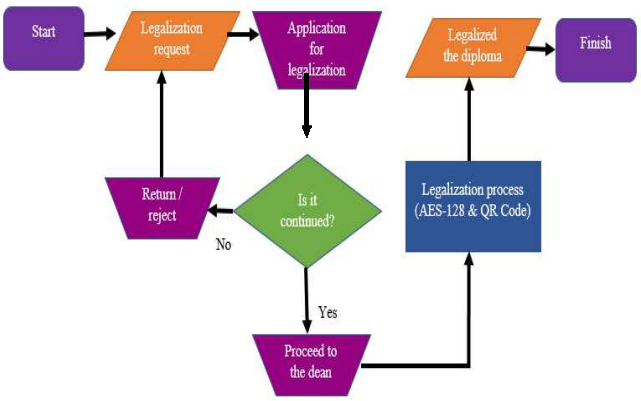

Fig. 2. Step system work

4.1.3 Legalization process

The legalization process is done by the certifier officer to the incoming certificate file. This process is the main process that produces certified copies of certificates. In this process, the certificate photo file will be affixed with a QR Code image that contains the legalized data checking address link and AES-encrypted AES-128 encryption code. Further translational links are made into a QR Code image embedded on the photo certificate.

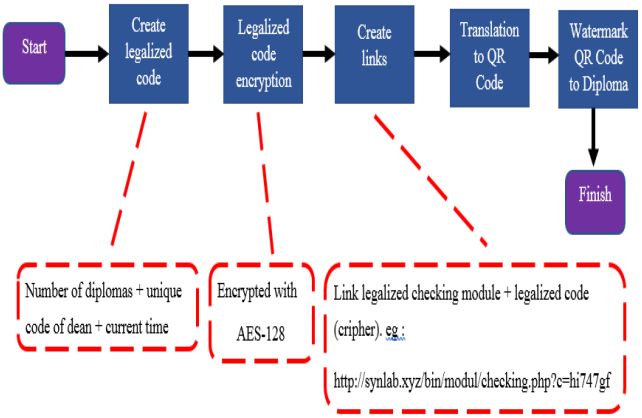

Fig. 3. Legalization process

4.1.4 Legalized data checking

The process of examining legalized data is done by scanning the QR Code in the photo certificate by using a special camera application or smartphone. The results of

the scan will be obtained a link that leads to the legalized checking module available on the LID. In the link, there is a variable that contains the encrypted code which then the code will be decrypted with AES-128 to get the original legalized code. Once the legalized code is obtained it will be checked whether the code is contained in the database or not, if not the system will tell that the data does not exist, on the contrary, the next can be done for withdrawal of existing legalization databases on the database to be displayed along with the certificate photo.

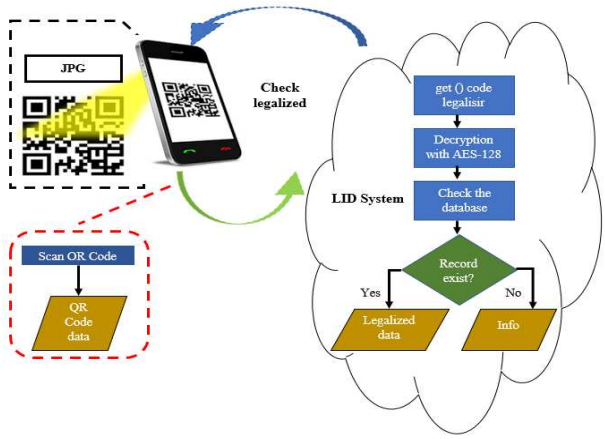

Fig. 4. Legalized data checking

4.2 Result and testing

4.2.1 System implementation

The following are the description of system implementation. Figure 5 illustrates the legalization request process which began with data input process such as students graduation number, name, students identity number (nim), submission date, request number of certified to copy, status and date of status issued and photo. The legalized process form is executed by the dean as an authorized official. The dean application form can be seen in Figures 6. Then the examination process is begun. The system will check the legalized code in the database (Please see Figure 7). As the result, the examination status will be declared as shown in Figure 8a as "data not found" and 8b as "data found".

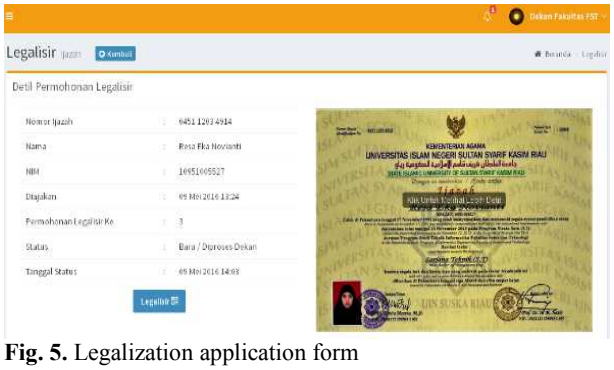

Fig. 5. Legalization application form

Fig. 6. Legalized form by officials

Fig. 7. Legalized examination process

Fig. 8. a. Data not found

Fig. 8. b. Data not found

4.2.2 System testing

The testing of LID system was done in several stages, including the functional module testing through the application of black box testing, system performance testing by examining the execution time and memory load used during the process, and the latest testing is User Acceptance Test (UAT) to identify the user responses on the system applications. The above testing mode was performed in two implementation environments, namely Web-based standard computer

device and Sony Xperia Miro (st23i) smartphone device. Herein, the smartphone is used to run QR Code transfer application to the third party (QR Code Reader v.2.2.3). System application has some menu function, such as log in process menu, legalized menu (alumni access), legalized submission menu, legalized information menu (alumni access), legalized download button menu, legalized menu (administrative/admin access), legalized request review menu, legalized menu (dean access), legalizing certificate menu, legalized checking menu with smartphones, legalized checking menu in LID web for original/fake/deleted legalization, unique codes menu for Deans and logging out system menu. Black box testing found that the entire menu and function was running well and correctly.

Meanwhile, for system performances testing several benchmarks are installed on the target source code in menu legalization process and legalization checking process. Three benchmark models performed on legalization process includes AES algorithms benchmarks, legalized module benchmarks, and legalized page benchmarks. Meanwhile, legalization checking process applied two benchmarks model namely AES algorithm benchmark and legalized checking module. The average execution time and memory load of benchmarks applied to 15 simulation data in each process can be seen in Table 1.

Table 1. Average benchmark.

Main Process	Object	Time Execution (ms)	Memory Load (MB)
Legalization Process	AES Encryption	1.18157	0.95601
	Legalized Module	704.013	0.97829
	Legalized Page	762.566	0.77327
Legalization Checking Process	AES Decryption	1.28200	0.54662
	Checking Module	114.386	0.54868

For 15 data, AES encryption benchmark spent the fastest execution time from 0.0059104 seconds to the slowest in 0.001703024 seconds thus provided average value was 0.001181571 seconds (s) or 1.181571 in milliseconds (ms). The fluctuated of execution time in AES benchmark testing can be depicted in Figure 10. Next, legalized module benchmark spent the fastest execution time in 0.47792602 seconds and the slowest is in 1.48998284 seconds thus provided an average value is 0.704013634 seconds or 704.013634 milliseconds. Lastly, the legalized page menu benchmark provided the fastest execution time is 0.58162999 seconds and the slowest is 1.65834403 seconds or spent in average as 0.762566141 seconds or 762.566141 milliseconds. The execution time performance of legalized module and page menu is explained in Figure 10.

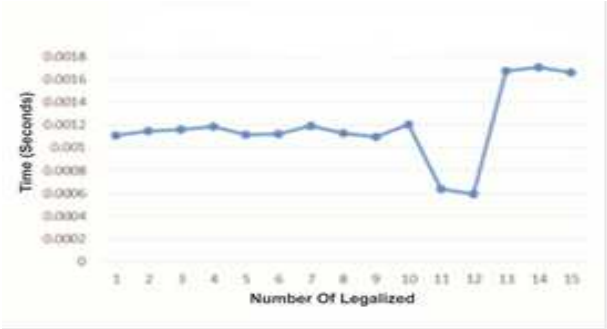

Fig. 9. Execution time for AES encryption testing

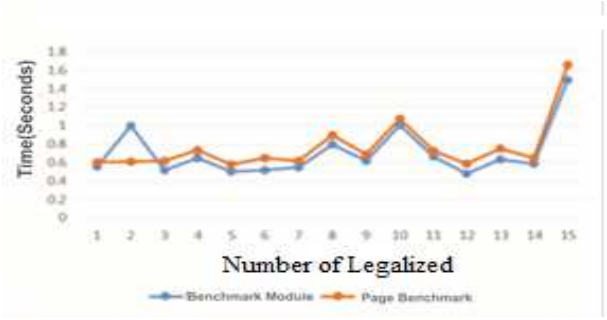

Fig. 10. Execution time for module and page benchmark testing

Memory load for AES encryption benchmark during the legalization process provided the smallest one is in 0.9539948 MB and the biggest is in 0.956019093 MB thus proposed the average value is 0.95601 MB. Legalized Module benchmark spent memory load from 0.9762878 MB as the smallest and 0.9804382 MB as the biggest one thus average value around 0.978295873 MB. Meanwhile, legalized page menu benchmark spent memory load in 0.7643204 MB up to 0.7919862 MB thus average value around 0.773273 MB. The graphical performance of memory load in the legalization process can be depicted in Figure 11.

For legalization checking process, 31 data testing were simulated. AES decryption benchmark provided the fastest execution time in 0.01621246338 milliseconds and the lowest in 4.427195 milliseconds thus the average values in 1.282007 milliseconds. The performance of 31 data simulation can be depicted in Figure 12.

Meanwhile, checking module spent the fastest execution time in 0.022562027 seconds and the slowest one in 0.555138826 seconds thus the average time in 114.386128 milliseconds. The performance of simulation benchmark testing is explained in Figure 13.

Memory load for AES decryption benchmark during the legalization process provided the smallest one is in 0.5431519 MB and the biggest is in 0.5504684 MB thus proposed the average value is 0.546623229 MB. Meanwhile, checking module spent memory load in 0.5436478 for the smallest and 0.553215 MB for the highest thus provided the average value is 0.548683165 MB. The description of this performance is explained in Figure 14.

Fig. 11. Memory load for benchmark testing in the legalization process

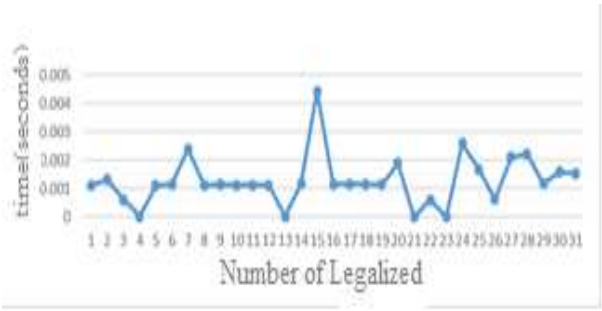

Fig. 12. Execution time for checking module

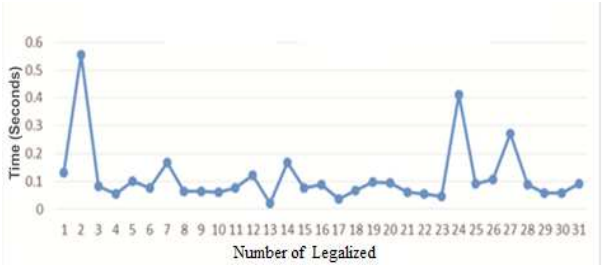

Fig. 13. Execution time for checking module

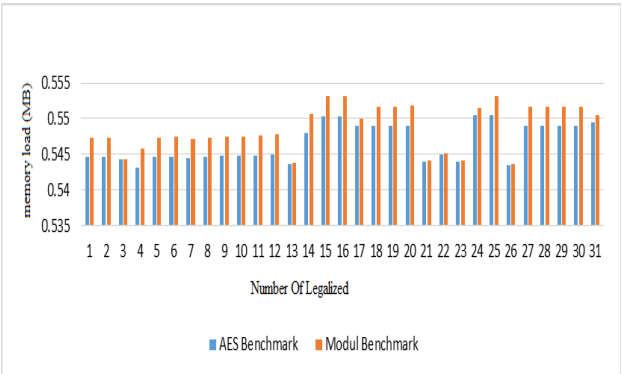

Fig. 14. Memory Load for Bechmark Testing in Legalization Checking Process

2.2.1 User Acceptance Test

User Acceptance Test (UAT) testing is conducted through the dissemination of the questionnaire for 100 respondents as graduate students, 25 official leaders, and 40 administrators. The questionnaire performed 7 questions using 4 Linkert scales, including very agree, agree, less agree and disagree statement. The questions related to the respondents' responses on LID application interface, the ease use of application and all functions, the functionality of application and all menu, the accuracy of information and data during the legalization process, the beneficial of LID system, the agreement statement in implementing this LID system, the future prospect of LID system. As the result, 91.667% respondents gave a very positive response and agree with this application.

5. Conclusion

Some conclusions and suggestions that can be obtained from this research are:

1. Implementation of AES algorithm as code encryption in the legalization process and QR Code as translation tool of ciphertext into an image in LID system application has been successfully done.
2. Based on the result of functionality, capacity testing, and user response, this application can be used as well as in assisting digital legalization process in a college. This LID system is beneficial for both the applicant/graduate students and the administration in facilitating the legalization process and improving the service.
3. As the result of execution time and memory load testing, this LID system has good performance, efficient, light, and fast execution responses (less than one second and less than one megabyte). This LID system also can run in a fairly standard infrastructure environment.

For future work, this LID system can be applied to the other method such as the CBC model. The legalization process checking can be done without internet access, for example by applying the Least Significant Bit (LSB) method. Moreover, this LID system can also be used for other documents.

Acknowledgment

We would like to thank University State Islamic University of Sultan Syarif Kasim Riau (UIN Suska Riau); administration and management at Faculty Science and Technology for time and place during the survey; our team in Department Informatics Engineering and Information System, and the reviewers who have provided comments and suggestions to improve the manuscript. Many thanks for your cooperation and support.

References

1. Erasmus University Rotterdam, 2015. [Online]. Available: https://www.eur.nl/sites/corporate/files/2017-11/webbrochure2015_Cheating-plagiarism_EN.pdf. [Accessed 2018].
2. A. Singhal and R. S. Pavithr, "Degree Certificate Authentication using QR Code and Smartphone," *International Journal of Computer Applications,* vol. 120, no. 16, pp. 38-43, 2015.

3. R. Patel, A. Ombale, Y. Patel and C. Raut, "E-Secured Documents & Sharing Via Qr Code," *International Journal of Recent Trends in Engineering & Research (IJRTER),* vol. 3, no. 3, pp. 31-34, 2017.
4. F. F. Rochman and I. K. Raharjana, "Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents," *Scientific Journal of Informatics,* vol. 4, no. 1, pp. 8-19, 2017.
5. H. A. Ahmed and J. W. Jang, "Higher Educational Certificate Authentication System Using QR Code Tag," *International Journal of Applied Engineering Research,* vol. 12, no. 20, pp. 9728-9734, 2017.
6. 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.
7. D. L. Tresnani and R. Munir, "Implementasi Sistem Absensi Pegawai Menggunakan QR Code pada Smartphone Berbasis Android," Teknik Informatika, Institut Teknologi Bandung, Bandung, 2011.
8. A. M. Wilson, "QR codes in the library: Are they worth the effort? Analysis of a QR code pilot project," *Journal of Access Services 9,* 2018.
9. J. H. Change, "An introduction to using QR codes in scholarly journals," *Sci Ed,* vol. 1, no. 2, pp. 113-117, 2014.
10. M. Zhang, D. Yao and Q. Zhou, "he Application and Design of QR Code in Scenic Spot's eTicketing System A Case Study of Shenzhen Happy Valley," *International Journal of Science and Technology,* vol. 2, no. 12, pp. 817-822, 2012.
11. R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," *International Journal of Engineering Research and Applications,* vol. 3, no. 4, pp. 1922-1926, 2013.
12. N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," *International Journal of Security and Its Applications,* vol. 9, no. 7, pp. 241-246, 2015.
13. K. Rege, N. Goenka, P. Bhutada and S. Mane, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA," *International Journal of Computer Applications,* vol. 71, no. 22, pp. 10-13, 2013.
14. E. Martiana, N. Rosyid and U. Augestia, "Application of Automatic Clustering in Document Searching Machine," *Telkomnika,* vol. 8, no. 1, 2010.
15. H. Eldira, E. K. Martiana and N. R. Mubtada, "The Application of Hill Climbing Automatic Clustering in Web mining for English Document Searching," EEPIS Project, Surabaya, 2011.
16. R. A. Mollin, Codes: The Guide To Secrecy From Ancient To Modern Times, Boca Raton: Chapman and Hall/CRC, 2005.
17. H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," *Journal Of Computing,* vol. 2, no. 3, 2010.

* Corresponding author: okfalisa@gmail.com