Secure Electronic Document with QR Code and RSA Digital Signature Algorithm

by Kadek Amerta Yasa

Submission date: 02-May-2023 11:38AM (UTC+0700)
Submission ID: 2081736555
File name: ith_150-Watt_Peak_Solar_Panel_in_Denpasar_Based_on_NASA_Data.pdf (1.56M)
Word count: 3159
Character count: 16578

Secure Electronic Document with QR Code and RSA Digital Signature Algorithm

Kadek Amerta Yasa, Putu Gde Sukarata, Gusti Putu Mastawan Eka Putra, I Made Riyan Adi Nugroho and I Nyoman Gede Arya Astawa
Department of Electrical Engineering, Politeknik Negeri Bali, Bali, Indonesia

Keywords: Security, Encryption, Digital Signature, QR Code, RSA, Secure Electronic Document.

Abstract: Falsification of electronic documents has become a challenge in these modern days. Lack of security is a factor in the occurrence of falsification of electronic documents. There are several methods have been founded which can be used to solve these problems, one of which is digital signature. However, most existing digital signature use insecure data format and encryption is rarely used. In this paper, we propose a Secure Electronic Document (SeED) model by adding QR Code and Digital Signature that are encrypted with RSA (Rivest, Shamir and Adleman) algorithm. We implemented the proposed SeED model in a website-based population data processing system and showed that the system is effective for generating electronic documents and validating them more securely.

1 INTRODUCTION

The development of technology is very fast changing the way we do a process. This has led to the emergence of the idea of utilizing technology such as e-government (Hu and Ma, 2010). E-government according to, is an ICT revolution in public government to increase the effectiveness, efficiency and transparency of services. In contrast to traditional governance methods where paper-based documents are more dominant, e-government services use more electronic documents in their implementation (Hu and Ma, 2010). Electronic document is a document that contains information or data stored electronically. These electronic documents are usually issued by official institutions, so the information or data on electronic documents can be cited as proof (Savrai, 2017).

Researchers have proposed to perform encryption to hide digital signature data. Sangita and Santosh proposed a solution, A Modified RSA Algorithm to Enhance Security for Digital Signature (Jaju and Chowhan, 2018). Rochman et.al proposed a solution, Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents (Rochman, 2017). Okfalisa et.al proposed a solution, Implementation of Advanced Encryption Standard (AES) and QR Code Algorithm on Digital Legalization System (Okfalisa, 2018). Setiawan and Kesuma proposed a solution, Design of Secure Electronic Disposition Applications by Applying Blowfish, SHA-512, and RSA Digital Signature.

Algorithms to Government Institution (Setiawan, 2018). Ahamed and Mustafa proposed a solution A Secure QR Code System for Sharing Personal Confidential Information (Ahamed, 2019). However, these solutions do not consider cases where data updates occur on the system.

Therefore, in this paper we propose a SeED model by adding QR Code and Digital Signature that are encrypted with RSA algorithm. RSA is used because it has better encryption and key generation speeds (Aufa, 2018). QR Code is used to store encrypted document data which can later be used for verification of printed documents. And for the data update issue on the system, the proposed model is equipped with metadata that containing document change data. This metadata is stored in a document database.

The SeED model will be divided into three components, namely components for generating secure electronic documents, components for validating secure electronic documents, and components for validating printed documents. We implemented the proposed SeED model in a website-based population data processing system and showed

Yasa, K., Sukarata, P., Putra, G., Nugroho, I. and Astawa, I.
Secure Electronic Document with QR Code and RSA Digital Signature Algorithm.
DOI: 10.5220/0010965600003260
In *Proceedings of the 4th International Conference on Applied Science and Technology on Engineering Science (iCAST-ES 2021)*, pages 1370-1375
ISBN: 978-989-758-615-6; ISSN: 2975-8246

that the system is effective for generating electronic documents and validating them more securely.

This paper is written as follows: Each section (1, 2, 3, 4, and 5) is describing about introduction, theoretical foundation, proposed model, and implementation. The 6th part explaining about analysis and test result. The last one is conclusion.

2 THEORETICAL FOUNDATION

2.1 Electronic Document

Electronic document is a document that contains information or data stored electronically. These electronic documents are usually issued by official institutions, so the information or data on electronic documents can be cited as proof. Electronic documents can be grouped into two groups, namely safe and simple. A safe electronic document refers to the document that is generated, saved or processed by using a safe information system and bears a safe electronic signature. A simple electronic document refers to the document that is generated, saved or processed by using an unsafe information system and simple electronic signature. In this paper, we will create a model to create a safe or secure electronic document.

2.2 Digital Signature

A digital signature is a mathematical scheme for showing the authenticity of a digital message or document. For security, digital signatures are stored in cipher-text form. Several studies use cryptographic algorithms to form cipher-text, such as DES, AES, Blowfish, and RSA. In this paper, the cryptographic algorithm used to create cipher-text is the RSA algorithm. The RSA algorithm has 3 important processes: key generation, encryption, and decryption.

2.3 QR Code

QR Code is a two-dimensional image that represents data, especially text data. With the ability to store in two dimensions of QR Code certainly can store more data and varied rather than the barcode. QR Code has the ability to encode and store information in the form of a printable pattern. The type of data that can be stored in QR Code is (Okfalisa et. al, 2018) including Numerical mode, Alphanumeric mode, 8-bit mode byte, and Kanji Mode.

3 PROPOSED MODEL

In this section, we discuss our proposed SeED model which consist of three model: Secure electronic document generator model; Validate of electronic document model; and validate of secure printed document model.

3.1 Secure Electronic Document Generator Model

This model serves to create or generate secure electronic documents. Each document has its own private key and public key. Public and private key have been generated when input the document data. This model consists of four stages, namely encrypt document data; generate QR Code; generate digital signature and generate secure electronic document. The encrypt document data stage aims to encrypt document data using a public key. The encryption process is carried out using the RSA algorithm. Cipher-text with document id will be processed at generate QR code and digital signature stage. At the stage of generating a QR code, the cipher-text and document id will be encoded into a QR Code. At the stage of generating digital signature, the cipher-text and document id will be generated into a digital signature. The last step in this model is to generate a secure electronic document. This stage aims to create or generate an electronic document and add a digital signature and QR code in it. The resulting secure electronic document can be further processed according to needs, such as downloading or sending via email. The flow of this model can be seen in Figure 1.

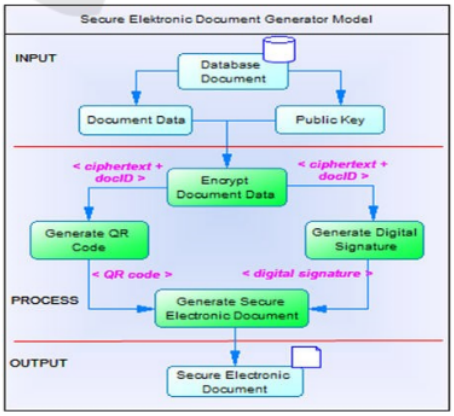

Figure 1: Secure Electronic Document Generator Model.

3.2 Validate of Electronic Document Model

This model serves to validate a secure electronic document. This validation process aims to detect whether the document is original or not, and whether there has been a data change in the document or not. This validation model consists of four stages, namely get digital signature, get document data, encrypt document data, and compare. The get digital signature process aims to get the digital signature in the file. In addition to getting a digital signature, this stage is also used to get a document id which is used as input for the get document data process. The next stage is get document data, this stage aims to retrieve document data and public keys from the database. The next stage is Encrypt Document Data; this stage aims to encrypt document data using the public key obtained from the get document data stage. The last stage is compare, this stage aims to make a comparison between the digital signature and the cipher-text obtained from the encrypt document data stage. If the digital signature with cipher-text has the same value, then the document is declared valid and there is no change in data, otherwise the document is declared invalid or data has been changed. The flow of this model can be seen in Figure 2.

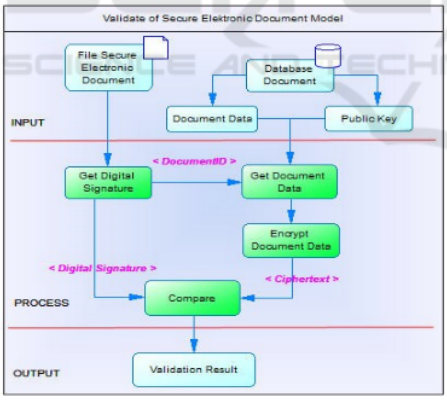

Figure 2: Validate of Secure Electronic Document Model.

3.3 Validate of Secure Printed Document Model

This model aims to perform validation for printed documents. This validation model consists of four stages, namely: QR code scan; get document data; decrypt QR code data; and manual compare. The QR code scan stage aims to retrieve the QR code data that printed on the document. Besides getting QR code data, this stage is also used to get the document id which is used as input for the get document data process. The next stage is get document data, this stage aims to retrieve document data and private keys from the database. The next stage is Decrypt QR Code data, in this stage aims to re-convert from cipher-text into readable document data. The last stage is manual compare, which is the process of comparing decrypted document data, document data from the database and document data from printed documents. If the data has the same value, the document is considered valid and data is not changed. The flow of this model can be seen in Figure 3.

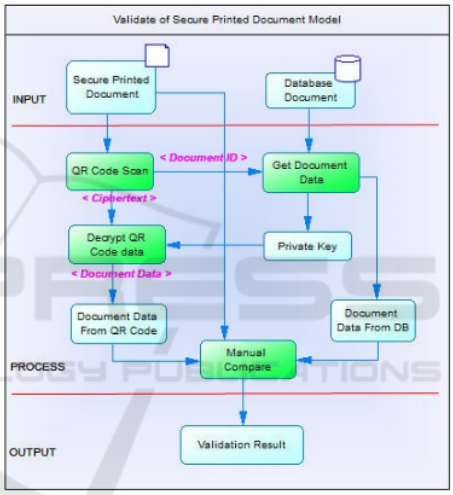

Figure 3: Validate of Secure Printed Document Model

4 IMPLEMENTATION

We implemented the SeED model in a website-based population data processing system. On the frontend side, the system is developed with the vue.js framework. The backend side, we use the LIM framework and MySQL as the system database. Waterfall model was followed during implementation. The SeED model is implemented in the three main features of the application, namely the family card generation feature, the digital family card validation feature, and the printed family card validation feature.

4.1 Family Card Generation Feature

There are several data that are entered as family card data, including name, nik, place of birth, date of birth, gender, and address. Using the EasyRSA library (Enterprises, 2019) private and public keys are generated 2048-bit long. Family card data along with private and public keys are stored in a database with a unique document id.

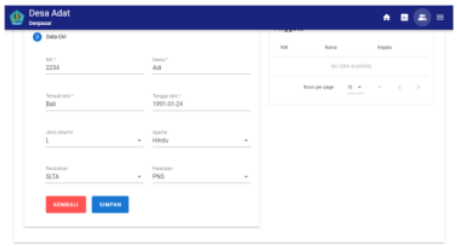

Figure 4: Insert Family Card Data and Generate Key.

Family card and public key data are retrieved from the database using the document id. Family card data is arranged into plain text with semicolon delimiters, such as names; NIK; place of birth; Date of birth; sex; address. The family card data is then encrypted using a public key with the EasyRSA library. The results of the encryption called cipher-text are then combined with the document id with the # sign separator (cipher-text#documentID). The combination of the cipher-text with the document id is used as a digital signature and encoded into a QR code. The encoded process is assisted by endroid/qr- code (Van den Enden, 2020) library. The QR code and digital signature are then added to the family card document to be printed in pdf format.

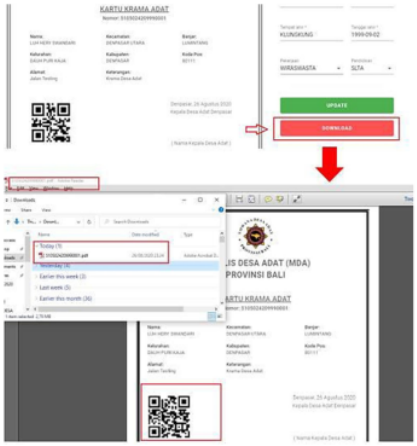

Figure 5: Generate Electronic Family Card.

4.2 Digital Family Card Validation Feature

Validation of the digital family card is done by uploading the family card file on the form provided. From the uploaded file, the system will take the digital signature on the file. The digital signature is then extracted to obtain encrypted family card data and document id. With the document id, the system will retrieve the family card data and public key in the database. The family card data obtained is then encrypted using a public key. The encryption results are then compared with the family card data encryption from the digital signature. If the results are the same, the system displays a valid document message, otherwise invalid document message.

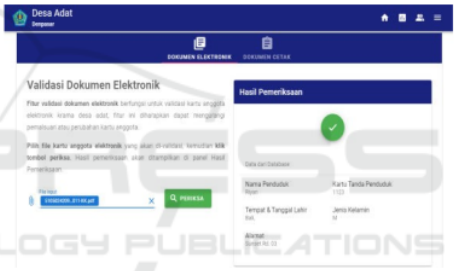

Figure 6: Valid Electronic Document Result.

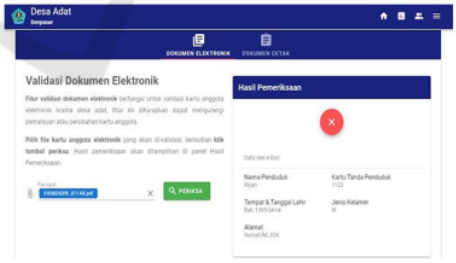

Figure 7: Invalid Electronic Document Result.

4.3 Printed Family Card Validation Feature

In addition to validating digital family cards, the system can also validate printed family cards. To read the QR code printed on the family card, the system is equipped with a QR code reader. For QR code reader we use vue-qrcode-reader (Gruhn, 2020) library.

The system will read the QR code printed on the family card. The data obtained is then extracted to obtain encrypted family card data and document id. With the document id, the system will retrieve the family card data and private key in the database. The private key is used to decrypt family card data from the QR Code. The decryption result then compares with the family card data from the database and printed family card data. If it has the same value, then the family card is valid, otherwise the family card is invalid.

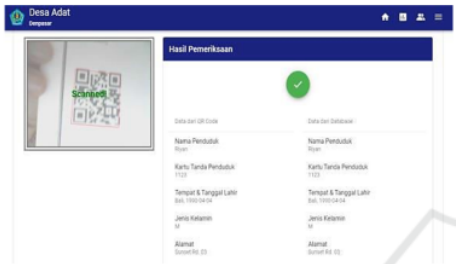

Figure 8: Valid Printed Document Result.

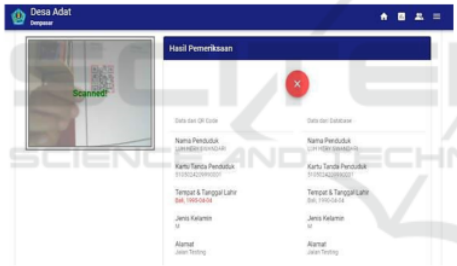

Figure 9: Invalid Printed Document Result.

5 ANALYSIS AND TEST RESULT

In the population data processing system, we conducted an experiment by making electronic documents from the following data:

Table 1: Data Testing.

Data	Name	NI K	PO B	DOB	Sex	Address
D1	Riyan	1123	Bali	1990-04-04	M	Sunset Rd. 03
D2	Adi	2234	Bali	1991-01-24	M	Sartika Rd. 22A
D3	Nugroho	3345	Bali	1995-05-04	M	Sudirman St. 1B
D4	Made	4456	Bali	1996-08-17	F	Kuta St. 120X
D5	Nyoman	5567	Bali	1980-01-04	F	Dalung Rd. 220Y

The results of the process of inserting data and generating private and public keys are as follows:

Table 2: Insert & Generating Key Result.

Data	Insert Data	Generate Key	Time (sec.)
D1	Success	Success	0.4042
D2	Success	Success	0.3188
D3	Success	Success	0.5163
D4	Success	Success	0.1069
D5	Success	Success	0.1712
Average Time			0.30348

The results of generating a secure electronic document are as follows:

Table 3: Generating Secure e-Document Result.

Data	Encrypt Data	QR Code	Dig. Signature	E-Doc	Time (sec.)
D1	Success	Success	Success	Success	0.3011
D2	Success	Success	Success	Success	0.2908
D3	Success	Success	Success	Success	0.2705
D4	Success	Success	Success	Success	0.2793
D5	Success	Success	Success	Success	0.2603
Average Time					0.2804

The results of the secure electronic document validation are as follows:

Table 4: Secure Electronic Document Validation Result.

Data	Get Dig. Sig.	Get Doc. Data	Encrypt Doc. Data	Compare	Time (sec.)
D1	Success	Success	Success	Success	0.1744
D2	Success	Success	Success	Success	0.1414
D3	Success	Success	Success	Success	0.0617
D4	Success	Success	Success	Success	0.062
D5	Success	Success	Success	Success	0.0645
Average Time					0.1008

The results of the printed electronic document validation process are as follows:

Table 5: Printed Electronic Document Validation Result.

Data	Scan QR Code	Get Doc. Data	Decrypt QR Code	Compare	Time (sec.)
D1	Success	Success	Success	Success	0.2544
D2	Success	Success	Success	Success	0.1814
D3	Success	Success	Success	Success	0.1217
D4	Success	Success	Success	Success	0.1062
D5	Success	Success	Success	Success	0.1545
Average Time					0.16364

We conducted evaluation experiment with creating and validating secure electronic documents. The experimental results show that the proposed method can make electronic documents safer and the validation process faster and easier. The RSA keys (private key and public key as a pair) are successfully generated and stored with an average time of 0.30348 seconds. QR code and digital signature to protect documents successfully generated and added with an average time of 0.2804 seconds. The digital signature has been read and validated successfully with an average time of 0.1008 seconds. The printed QR Code has been read and validated successfully with an average time of 0.16364 seconds.

6 CONCLUSIONS

This paper presents an innovative model to prevent falsification of electronic document. Here we design and apply the SeED model to a resident data processing system to protect family card documents from falsification. The RSA cryptographic algorithm is used to create digital signatures and secure QR codes. This digital signature and secure QR code are used to protect electronic documents. The SeED model can be applied to a variety of other real-world applications involving sensitive information.

ACKNOWLEDGEMENTS

This research was supported by Politeknik Negeri Bali. We thank our colleagues from this institution. We thank everyone who contributed to the completion of this paper in one way or another. Hopefully, this research can be useful.

REFERENCES

X. Hu and L. Ma (2010). A study on inter-governmental documents security transfer under e-government environment. *Proc. Int. Conf. E-bus. E-Government, ICEE 2010*, pp. 663–666, 2010, doi: 10.1109/ICEE.2010.173.

P. Savrai, A. Nazem, P. Sciences, and P. Sciences (2017), Evidentiary value of electronic document in domestic and international regulations. *Int. J. Law*, vol. 3, no. 3, pp. 15–20..

M. S. Ahamed and H. Asiful Mustafa (2019). A Secure QR Code System for Sharing Personal Confidential Information. *5th Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2019*, pp. 11–1, doi: 10.1109/IC4ME247184.2019.9036521.

F. F. Rochman, I. K. Raharjana, and T. Taufik (2017). Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents. *Sci. J. Informatics*, vol. 4, no. 1, pp. 8–19, doi: 10.15294/sji.v4i1.7198.

H. Siawan and K. Rey Citra (2018). Design of secure electronic disposition applications by applying blowfish, SHA-512, and RSA digital signature algorithms to government institution. *2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018*, pp. 168–173, doi: 10.1109/ISRITI.2018.8864280.

S. A. Jaju and S. S. Chowhan (2018). A Modified RSA algorithm to enhance security for digital signature. *Int. Conf. Work. Comput. Commun. IEMCON 2015*,2015, doi: 10.1109/IEMCON.2015.7344493.

Okfalisa, N. Yanti, W. A. D. Surya, A. Akhyar, and A. A. Frica (2018). Implementation of Advanced Encryption Standard (AES) and QR Code Algorithm on Digital Legalization System. *E3S Web Conf.*, vol. 73, pp. 1–7, doi: 10.1051/e3sconf/20187313009.

F. J. Aufa, Endroyono, and A. Affandi (2018). Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. *Proc. - 2018 4th Int. Conf. Sci. Technol. ICST 2018*, vol. 1, pp. 1–5, doi: 10.1109/ICSTC.2018.8528584.

P. I. Enterprises (2019). EasyRSA. [Online]. Available: https://github.com/paragonie/EasyRSA.

J. van den Enden (2020). qr-code. [Online]. Available: https://github.com/endroid/qr-code.

N. Gruhn (2020). vue-qrcode-reader. [Online]. Available: https://github.com/gruhn/vue-qrcode-reader.

Secure Electronic Document with QR Code and RSA Digital Signature Algorithm

ORIGINALITY REPORT

19%	15%	13%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pdfs.semanticscholar.org Internet Source	3%
2	www.researchgate.net Internet Source	2%
3	Md. Salahuddin Ahamed, Hossen Asiful Mustafa. "A Secure QR Code System for Sharing Personal Confidential Information", 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), 2019 Publication	2%
4	Submitted to De Montfort University Student Paper	2%
5	www.lawjournals.org Internet Source	2%
6	www.semanticscholar.org Internet Source	2%
7	cps-vo.org Internet Source	1%

8	link.springer.com Internet Source	1 %
9	Submitted to Informatics Education Limited Student Paper	1 %
10	Farah Jihan Aufa, Endroyono, Achmad Affandi. "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm", 2018 4th International Conference on Science and Technology (ICST), 2018 Publication	<1 %
11	doaj.org Internet Source	<1 %
12	repository.poliban.ac.id Internet Source	<1 %
13	ijai.iaescore.com Internet Source	<1 %
14	Submitted to CSU, San Jose State University Student Paper	<1 %
15	I Made Ari Dwi Suta Atmaja, I Nyoman Gede Arya Astawa, Ni Wayan Wisswani, I Made Riyan Adi Nugroho et al. "Document Encryption Through Asymmetric RSA Cryptography", 2020 International Conference on Applied Science and Technology (iCAST), 2020 Publication	<1 %

16	www.cs.stevens-tech.edu Internet Source	<1 %
17	Naeem Howrie Ghayad, Ekhlas Abbas Albahrani. "A Combination of Two-Dimensional Hénon Map and Two-Dimensional Rational Map as Key Number Generator", 2019 First International Conference of Computer and Applied Sciences (CAS), 2019 Publication	<1 %
18	docshare.tips Internet Source	<1 %
19	jnte.ft.unand.ac.id Internet Source	<1 %
20	joiv.org Internet Source	<1 %
21	journals.ums.ac.id Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		