DEVOTION
Journal of Research and Community Service

Volume 3, Number 12, October 2022
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

IMPLEMENTATION OF WEB-BASED DOCUMENT SIGNING AND DATA VALIDATION SYSTEM

Raihan Febian Bahy[1], Muhammad Faris Ruriawan[2], Yudha Purwanto[3]
[123] Fakultas Teknik Elektro, Universitas Telkom Bandung, Indonesia
Email: raihanbahy29@gmail.com[1], muhammadfaris@telkomuniversity.ac.id[2], omyudha@telkomuniversity.ac.id[3]

KEYWORDS
Cryptography, Base64, MD5, Validation

ABSTRACT

The physical form of documents has changed a lot, previously documents can only be used if they have been printed, now documents can also be used in digital form only. However, along with the change in the physical form of the document, it also does not close the crimes that occur, such as falsifying documents, especially in the ratification or signing section. The digital document validation process combines digital document signing techniques with cryptographic algorithms, the cryptographic algorithm used is the Base64 algorithm. By combining the Base64 cryptographic algorithm and MD5 hashing, it is hoped that a method will be created to validate secure digital documents while maintaining the C.I.A (Confidentiality, Integrity, and Availability) aspects in the world of cryptography. Henceforth, the result of this final project is the creation of a digital platform or website that functions to validate digital documents by combining Base64 cryptographic techniques and MD5 hashing algorithms as data security protection. This document validation application has features such as user management, input, edit, delete, and the main features of document validation with a success rate of 100% from black box testing and white box testing. As for the performance test, the fastest time is when the system deletes data, with an average time of 0.14s, while the longest time is when the system updates data, with an average time of 0.70s

INTRODUCTION

The prolonged Covid-19 pandemic forces every individual to minimize physical contact with other individuals to reduce the spread. The impact of this restriction is the paralysis of all operational activities from all fields (Johassan, n.d.). All service-based activities such as public services cannot be carried out face-to-face. To maintain existence and complete paralysis, all institutions have begun to switch their operational systems from offline to online (Yuniati & Sidiq, 2020). Due to this pandemic, important activities in the service world such as document validation are also affected. As we also know that this activity is an important process in the service world, because documents are an important tool if we want to make transactions in the serviceworld (Mahrup, 2022).

With the change in this service system, the potential for criminal acts such as document forgery, signature forgery, and various other crimes related to a document is high. Therefore, we need a way so that the document validation process, especially digital documents cannot be falsified. For example, by combining the document validation process with cryptographic techniques, cryptography is a solution to data security problems (Fikriyah, 2011).

Therefore, this research is focused on the design and creation of web-based applications that can be used to validate digital documents by combining the validation

process and encrypted cryptographic techniques, as a solution to the secure digital document validation process

METHOD RESEARCH

In 2008 Budi Maryanto did a research to describes a one- way hash function to encrypt data (Maryanto, 2008). Some examples of one-way hash functions are MD2, MD4, MD4, SHA, RIPMEND, and WHIRLPOOL. The hash function is a common hash function that is often used. Its use also varies depending on the needs and objectives of the application made. An example is MD5 which is often used for the login system of an application (Huda & Kom, 2019). Later in 2012, Saipul Bahri, Diana, and Susan Dian PS explained about data security using MD5 cryptographic techniques (Bahri, Diana, & Dian PS, 2012). This study aims to make data owners to secure their data easier without having to know the queries that need to be typed or run by using MD5 encryption.

Next is from Ahir Yugo Nugroho research in 2015 (Nugroho, 2017). This study discusses the use of the Base64 algorithm in making text data security applications. In this study, it is explained that Base64 is an algorithm that is flexible enough to be used as an application algorithm, especially applications related to data security. Next is from Rachmat Suryadithia research in 2013 (Suryadithia, 2013). This study discuss what factors are the benchmarks in the use of QR Codes in the era of digitalization as it's today. Wijaya and Rahmat (Wijaya, 2012) did research on Base64 algorithm. This research discusses about making an application that is used to encode and decode using the Base64 algorithm as the algorithm used to perform the encode and decode process.

In this research, we will combine the validation process and encrypted cryptographic technique. In our implementation, the validation was done by converting the data from the document using the MD5 hashing algorithm and save the data into database. The data from database could be converted to QR code and can be used to validate the document, by scanning the QR code. Basically, MD5 is a common hash that can be used on any cryptographic platform. MD5 have enough security to secure any encrypted string for further use. That's why in this research use MD5 algorithm combined with QR Code to secure any inputted data from user (Fadhillah et al., 2022).

RESULT AND DISCUSSION

A. Design System

This system is designed to input the document number along with the supporting data, the results of the inputted data will be displayed along with a QR Code for the validation process. For the document number that has been inputted, it will go through a hashing and encryption process, and then the results of the encryption will be.

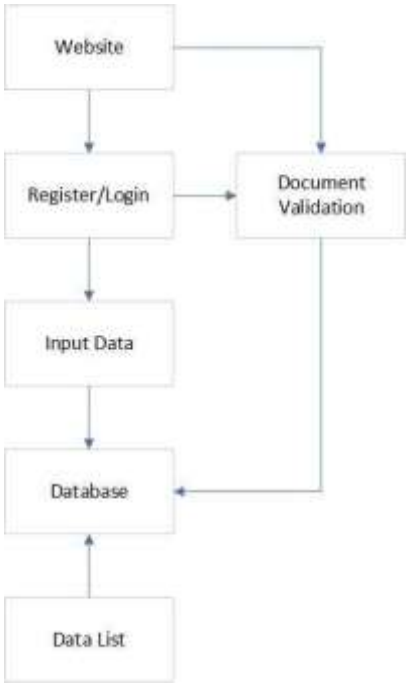

Figure 1
Block Diagram

Converted into a QR Code form for the user to use in validation process. In our implementation, we used MD5 hashing and Base64 encoding.

The website is used as a platform to process document data input and validate digital documents, and as a medium for interaction between the user and the system. The Register/Login feature functions as user management when the user will process data input and document validation. The data input feature here functions to input the document number along with its supporting data which will be validated by the user.

The database functions as a storage for user input data that has been hashed and encrypted. The database here also functions as a storage list of users who have registered. The document validation feature serves as a feature to validate documents that have been entered by the user by utilizing the QR Code that has been created based on the document number entered by the user.

Figure 2
QR Code generated Input Data

The data list feature displays all the input results that have been inputted by users. In addition, the user can also save the results of the QR Code that has been created by the system. The QR code generated can be seen at Figure 2.

The validation function was done by scanning the QR code generated. In our implementation, the website, if opened in mobile apps or on a device with camera, could detect the QR code generated from a prior inputted document. In this case, if the document number and QR code matching the data on the database, the document was declared valid. However, if it was not matching any of the data on the database, the document was declared invalid, and further assessment for the document might be required.

Figure 3
A document is matching the database and declared valid

B. White Box Testing

In this testing, all source code will be analyzed and seen, whether it is in accordance with the application logic and desired expectations. This test focuses on the performance and logic of MD5 hashing, Base64 encryption, and the validation process of documents that has been inputted by the user to check the suitability of the data. Therefore, it must be ensured whether the inputted data can be processed by the system logic or not.

Table 1
White Box Testing Input Data

Scenarios	Expected Results	Results Obtained
User opens input data page from view data page	Input data pageopens	Input data pageopens
User fills the form on the input data page	The forms on theinput data page filled	The formsonthe input data page filled
User click the submit button	Inputted data willbe stored in the database, document numberis hashed withMD5 and encrypted with Base64 algorithm,then stored in the database and generated into aQR Code	Inputted data will be stored in the database, document number is hashed with MD5 and encrypted with Base64 algorithm, then store in the database and generated into a QR Code
User back to view data page	View data pageopens	View data pageopens

Table 1 shows the white box testing result from input data page. After the user click the submit button, the data will be stored in the database, while the document number data

will be hashed with MD5 and encrypted with Base64. Then after that the encryption results will be stored in the database and generated into a QR Code

Table 2
White Box Testing Documents Validation

Scenarios	Expected Results	Results Obtained
User opens documents validation page from view data page	Documents validation page opens	Documents validation page opens
Scanner tab opens	Scanner tab can scan the QR Code	Scanner tab can scan the QR Code
Document number form filled	Document number form filled with encrypted results from database	Document number form filled with encrypted results from database
User click the submit button	The validation page opens and shows the validation results	The validation page opens and shows the validation results

Table 2 shows the white box testing result from validate documents page. Users only need to scan the QR Code that was previously obtained, then the contents of the QR Code will be immediately filled in the document number form. Next, when user click the submit button, the application will move to a page that shows the validity of the scanned document.

C. Black Box Testing

In this testing, all features in the application are tested and seen whether they are in accordance with their functions and can run as expected. This test focuses on the performance of each feature in the application, such as buttons, form fields, tables, and hyperlinks of a page. Therefore, it must be ensured whether all the features can run and can be used according to the instructions from the user.

Table 3
Black Box Testing Input Data

Scenarios	Expected Results	Results Obtained
Input document number	Can input document number	Document number form filled
Input document name	Can input document name	Document name form filled
Input document author name	Can input document author name	Document author name form filled
Input document author identity number	Can input document author identity number	Document author identity number form filled
Input document signer name	Can input document signer name	Document signer name form filled
Signing date dropdown	Can input document signing date	Document Signing date form filled
Submit button	Can input the document to Database and generate a QR Code	Inputted result stored in database and new QR Code showed

Table 3 shows the black box testing result from input data page. Features such as document number form field, document name form field, author name form field, document author identity number form field, signer name form field, signing date dropdown, and submit button can execute all user commands. Therefore, the results of the black box testing on the register page can run smoothly and according to expectations, because the input results can be stored properly in the database.

Table 4
Black Box Testing Documents Validation

Scenarios	Expected Results	Results Obtained
Scanner	Can scan the QRCode	Scanner hassuccessfully read the QRCode
Input documentnumber	Can input document number	Document number formfilled
Scenarios	**Expected Results**	**Results Obtained**
Submit button	Can do documentvalidation process	Validation result appears

Table 4 shows the black box testing result from the document validation page. Features such as scanner, document number form field, and submit button can execute all user commands. Therefore, the results of the black box testing on the validation page can run smoothly and according to expectations.

Based on all the test scenarios carried out using the black box testing method, it can be concluded that this application has a 100% success rate, because every existing feature can work according to its functionality based on the testing carried out.

Figure 4
Performance Test Input Data

D. Performance Test

This testing is used to test all the performance from each feature contained in the application. The unit used is (/s)

Figure 5
Performance Test Validate Document

Fig. 4 shows the performance test result from input data feature in this application. In this testing, the system was tested by inputting the data from 30 different documents into the system. The time was measured based on the time data was inputted to the generated QR data. Therefore, there are several processes here: querying the inputted data to the database, queried the data into the hashing algorithm, encode the hashed data to encoded form, and generate the unique QR code from the data. Based on the testing, there are several delays caused by the amount of data. The fastest time is 0.47s and the longest time is 0.99s. The average time is 0.70s.

Fig. 5 shows the performance test result from document validation feature in this application. In this testing, the system was tested by measuring the time it took from the QR code scan until the data was validated. Based on the figure, there were several delays due to the large number of validated data. In document validation, the fastest time is 0.46s and the longest time is 0.73s. The average time is 0.52s.

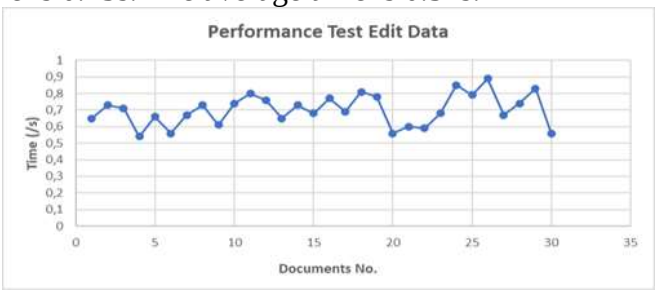

Figure 6
Performance Test Edit Data

Figure 6 shows the performance test result from edit data feature in this application. Based on the figure, there were several delays caused by the amount of data being updated. In edit data, the fastest time is 0.54s, and the longest time is 0.89s.

Figure 7 shows the performance test result from delete data feature in this application. Based on the figure, there are several delays. This is due to the large number of deleted data. In delete data the fastest time is 0.1s and the longest time is 0.2s. Based on these results, it can also be seen that the editing process data is the process that has the longest time, because the system must update the data in the database against the

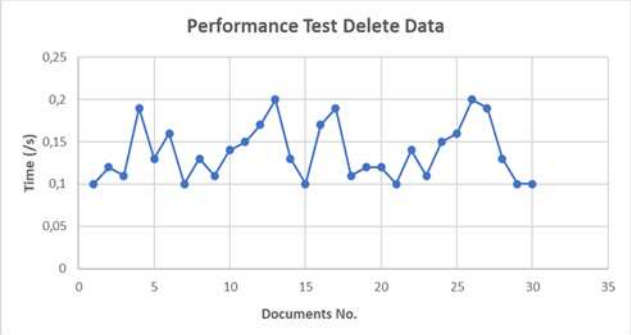

Figure 7
Performance Test Delete Data

Data that was previously inputted by the user based on the results of user input on the data edit page. The last performance test is the performance test of delete data. This test has an average time of 0.14s to run the process. Based on these results, it can also be seen that the process of deleting data is a process that has the fastest time, because the system is only ordered to delete the data contained in the database.

CONCLUSION

Based on the results of all tests that has been done on this application, this application can run as expected without encountering a problem that cause the system or algorithm and logic in this application to fail. Based on white box and black box testing that has been done on this application, the test success rate reaches 100%, this result is obtained because every function, feature, and scenario in this application can run smoothly according to expectations and functionality. In performance test, delete data has the fastest time to process, with an average time of 0.14s, while editing data has the longest time to process, with an average time of 0.70s.

REFERENCES

Bahri, Saipul, Diana, Diana, & Dian PS, Susan. (2012). Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5. *Skripsi Mahasiswa TI S1*.

Fadhillah, Yusra, Samosir, Khairunnisa, Angriawan, Randy, Jamaludin, Jamaludin, Ardiana, Dewa Putu Yudhi, Parewe, Andi Maulidinnawati A. K., Yuswardi, Yuswardi, Simarmata, Janner, Pakpahan, Andrew Fernando, & Multazam, Mochammad Tanzil. (2022). *Teknologi Blockchain dan Implementasinya*. Yayasan Kita Menulis.

Fikriyah, Hurriyatul. (2011). *Tindak pidana pemalsuan data dalam undang-undang no. 11 tahun 2008 tentang ite dan kajian hukum Islam*.

Huda, Miftahul, & Kom, M. (2019). *Open Systems Interconnection: Lapisan Data-Link* (Vol. 2). bisakimia.

Johassan, Deavvy M. R. Y. (n.d.). Komunikasi Di Masa Pandemi (Kajian Teori Paradigma Naratif Walter Fisher). *Media, Komunikasi Dan Informasi Di Masa Pandemi Covid-19*, 144.

Mahrup, Yudi Hasan. (2022). *Efektifitas Kerja Operator Sistem Informasi Administrasi Kependudukan (Siak) Berbasis Daring Di Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Subang*. Universitas Subang.

Maryanto, Budi. (2008). Penggunaan Fungsi Hash Satu-Arah Untuk Enkripsi Data. *Media Informatika*, *7*(3), 1–10.

Nugroho, Ahir Yugo. (2017). Pembuatan aplikasi kriptografi algoritma base 64 menggunakan

php untuk mengamankan data text. *Seminar Nasional Informatika (SNIf)*, *1*(1), 134–139.
Suryadithia, Rachmat. (2013). Faktor-Faktor yang Mempengaruhi Penggunaan QR Code pada Era Digitalisasi dengan Metode Usability. *Paradigma*, *15*(2), 170–179.
Wijaya, Anderias Eko. (2012). Pembuatan Aplikasi Encode dan Decode Berbasis Web Menggunakan Algoritma Base64 untuk Konfirmasi Pengiriman Pin. *Jurnal Teknologi Informasi Dan Komunikasi*, *2*(1), 320575.
Yuniati, Trihastuti, & Sidiq, Muhammad Fajar. (2020). Literature review: Legalisasi dokumen elektronik menggunakan tanda tangan digital sebagai alternatif pengesahan dokumen di masa pandemi. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1058–1069.