Matrix: Jurnal Manajemen Teknologi dan Informatika
Volume 12 Issue 2 Year 2022 Pages 102-108

DOI: http://dx.doi.org/10.31940/matrix.v12i2. 102-108
URL: http://ojs2.pnb.ac.id/index.php/matrix

# Application of the Blowfish Algorithm in securing patient data in the database

***Pahrul Irfan*** [1]***, Rifqi Hammad*** [2*]***, Andi Sofyan Anas*** [3]***, Fatimatuzzahra*** [4]***,***
***Nanang Samudra*** [5]

[1,2,3,4,5] *Bumigora University, Indonesia*

*Corresponding Author: *rifqi.hammad@universitasbumigora.ac.id*

**Abstract:** Patient data is one of the datasets managed by the hospital. Patient data in the form of examination results and other data is important data that is private and confidential. Therefore, patient data needs to be secured so that there is no misuse of data by parties who are not responsible for things that can harm the data owner. One of the several methods that can be used to secure data is cryptography. Cryptography itself has several algorithms, one of which is blowfish. This study applies the blowfish algorithm to secure patient data in the database to reduce the possibility of data misuse by irresponsible parties. This study succeeded in implementing the blowfish algorithm for securing patient data. The data stored in the database is the result of encryption using the blowfish algorithm, the results of which are difficult to understand because there is a combination of symbols and text. The application of the algorithm affects the data storage time in the database, which originally took 0.12 seconds to save data and now takes 0.28 seconds to store data.

**Keywords:** data patient, cryptography, blowfish, database

**History Article:** Submitted 22 June 2022 | Revised 6 July 2022 | Accepted 22 July 2022

**How to Cite:** P. Irfan, R. Hammad, A. S. Anas, Fatimatuzzahra, and N. Samudra, "Application of the Blowfish Algorithm in securing patient data in the database," Matrix: Jurnal Manajemen Teknologi dan Informatika, vol. 12, no. 2, pp. 102-108, 2022.

## Introduction

The utilization of information technology in the current era has an important role in the success of an organization [1] because information technology can help all organizational activities such as administration and others [2]. Such is the case with organizations in the health sector that utilize information technology in providing services in the health sector [3]. The hospital is one of the health organizations that utilize information technology. In managing its data, it uses digital storage media in the form of a database [4].

The data managed by the hospital is in the form of patient data, examination results data, and others. Patient data is very important data, so it needs to be protected because it is private and confidential [5] [6]. This data can be stolen through system hacks carried out by irresponsible and misused elements, such as identity theft and filing false insurance claims [7]. This is like what happened in 2020 when Indonesian citizen data related to COVID-19 was stolen by unauthorized parties and then sold on the dark web via the RapidsForum forum [8].

To anticipate the misuse of data by unauthorized parties, it is necessary to provide security for the data. This security can be done in the form of data encryption so that the data is difficult to open or read [9]. The method that can be used to perform encryption is called cryptography [10]. Data cryptography is one of the techniques used to secure data by encrypting it [11] so that it can be turned into other random data [12]. Cryptography has several algorithms that are used in the data security process, such as the Caesar cipher, vigenere cipher [13], Blowfish, and others. Blowfish is one of the cryptographic algorithms used to encrypt and decrypt data that operates with the input and output of data blocks of varying sizes, ranging from 32 bits to 448 bits [14].

In this study, the algorithm method used to overcome the problem of misuse of patient data is the blowfish algorithm, in which the algorithm will be embedded in the information system used to manage patient data. so that the data stored in the database will be different from the data entered. This is because the data is encrypted. It is hoped that the application of the blowfish algorithm will reduce the misuse of patient data that can harm the data owner. To support the research carried out, there are several studies related to the security of patient data and the use of the blowfish algorithm as data security, such as that conducted by Erwin Gunandhi and Agung Sudrajat entitled "Securing Medical Record Data Using Vigenere Cipher Cryptography". This study resulted in a medical record data security system using the vigenere cipher method [15]. The difference between the research conducted by Erwin and this research is that this study uses the blowfish method as the algorithm used in encrypting patient health data.

Another research is a study conducted by Nuniek Fahriani and Indah Kurniawati entitled "Patient Data Security with the Blowfish Algorithm on HOTSPOTDT". This study resulted in an application that was used to encrypt medical record files from patients at the HOTSPOTDT hospital [16]. The difference between the research conducted by Nuniek and Indah and the research to be conducted is that the research to be conducted does not encrypt medical record files but encrypts the data entered by the user into the database to reduce the misuse of the data stored in the database.

Another research is a study conducted by Erick Erwin Nylis and Purwanto entitled "Implementation of Email Security Using the Web-Based Blowfish Method at UPT Puskesmas Pondok Kacang Timur". This study resulted in an application that was used to encrypt email messages related to technical services provided or carried out by the UPT Puskesmas Pondok Kacang Timur [17]. The difference with the research that will be carried out is that in the research to be carried out, encryption is carried out on the data entered by the user into the database, so that the data available in the database is encrypted and difficult to understand, while in the research conducted by Erick and Purwanto, encryption is carried out on e-mail messages.

In addition to the three studies previously mentioned, there are also studies related to data protection using blowfish conducted by Harlen Gilbert Simanullang and Arina Prima Silalahi with the title "Blowfish Algorithm To Improve Mysql Database Security". This research produces an application that can be used to perform encryption and decryption with the blowfish algorithm [18]. The difference with the research that will be carried out by Harlen and Arina with this research is that this research produces an additional feature that is embedded in the patient data management application where every data input process into the database, the data will be encrypted automatically where the data stored is data that has been encrypted

## Methodology

This study uses the blowfish algorithm method for encrypting patient data. The flow of the application of blowfish in this study can be seen in Figure 1.

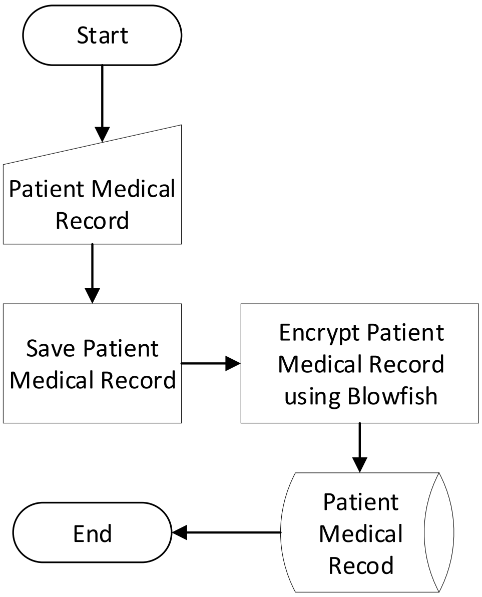

Start
Patient Medical Record
Save Patient Medical Record
Encrypt Patient Medical Record using Blowfish
Patient Medical Recod
End

**Figure 1.** Blowfish Algorithm Implementation Flow

Figure 1 shows that the encryption process is carried out on the data before it is entered into the database. Blowfish is a cryptographic algorithm that is quite strong and has a large enough space and various lengths. Blowfish also keep their keys secret [19]. The encryption process using blowfish in this study can be seen in Figure 2.

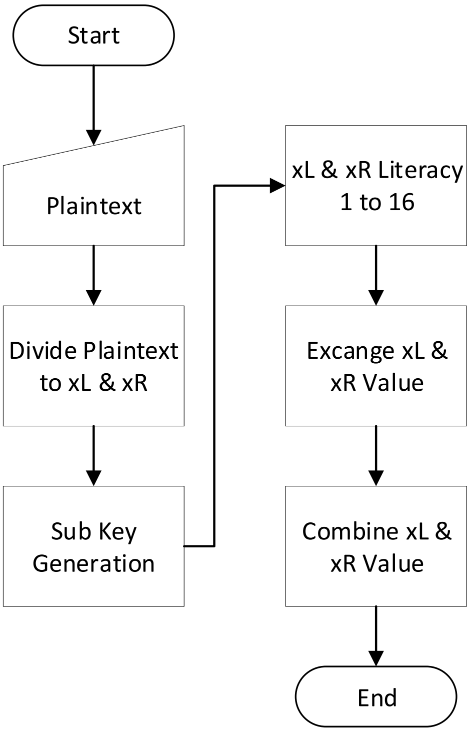


**Figure 2.** Encryption Flow

Figure 2 shows the encryption process used in the study with the blowfish algorithm. There are several steps involved in this process, namely:

1. The data to be stored in the database (plaintext) will be divided into 2, namely xL and xR
2. Key generation by creating an array P from P0 to P17 in hexadecimal form and converting it into binary form

3. Making S arrays, each of which is 255 in hexadecimal form and converted in the form of binary numbers, the plaintext is converted into binary form and divided into 2 (two) namely xL and xR, then enters the first round where i = 0 where xL is XoR right with P0 which was previously created in the P array, this xL is divided by 4 into 8 bits, namely a,b,c,d, then look for F(function) with equation (1) [20].

$$F(XL) = (((S0.a + S1.b \bmod 2^{32}) XoR\ S2.c) + S3d \bmod 2^{32}) \quad (1)$$

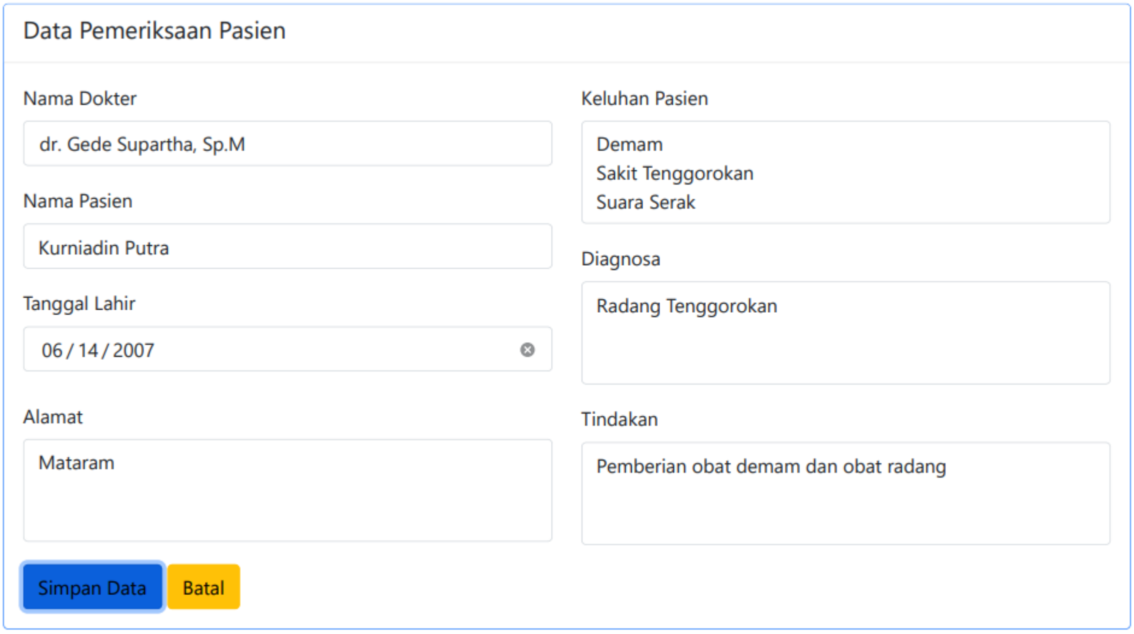
After finding the value of F, then next look for the value of xR. Finding the value of xR can be done by using the equation (2) [20]

$$XR = F(XL) XoR\ XR \quad (2)$$

After finding the xR value, the process of exchanging xL values with xR is carried out for up to 16 liters. This process generates new xL and xR values, each of which has 32 bits.
4. xL and xR values are exchanged again, then XoR values xL with P16 and xR with p17
5. Finally, combine the xL and xR values so that you get the ciphertext result

## Results and Discussions

The encryption process with blowfish on patient data changes the shape of the data stored in the database. For example, the data entered into the system is shown in Figure 3.



Data Pemeriksaan Pasien

Nama Dokter
dr. Gede Supartha, Sp.M

Nama Pasien
Kurniadin Putra

Tanggal Lahir
06 / 14 / 2007

Alamat
Mataram

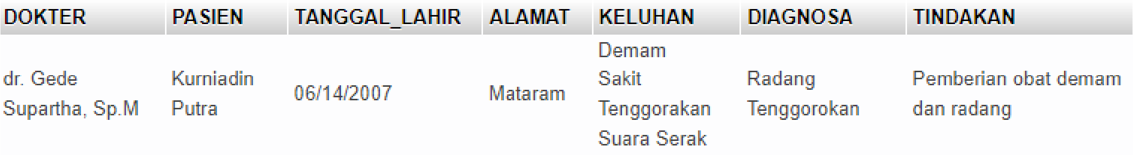
Keluhan Pasien
Demam
Sakit Tenggorokan
Suara Serak

Diagnosa
Radang Tenggorokan

Tindakan
Pemberian obat demam dan obat radang

**Figure 3.** Patient Data Form

In Figure 3, the patient data fields that will be stored are the doctor's name, patient name, date of birth, address, patient complaints, diagnoses, and actions. The fields will be encrypted using blowfish with the keyword "blowfish". The display on the database before the patient data is encrypted can be seen in Figure 4.



| DOKTER | PASIEN | TANGGAL_LAHIR | ALAMAT | KELUHAN | DIAGNOSA | TINDAKAN |
|---|---|---|---|---|---|---|
| dr. Gede Supartha, Sp.M | Kurniadin Putra | 06/14/2007 | Mataram | Demam<br>Sakit Tenggorakan<br>Suara Serak | Radang Tenggorokan | Pemberian obat demam dan radang |

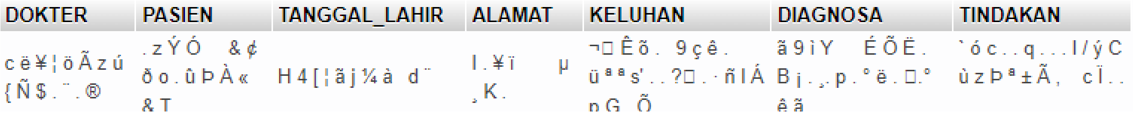
**Figure 4.** Data Before Encryption

Figure 4 shows the results of data storage without encryption. These results indicate that the data entry can still be misused because it displays the true meaning. Therefore, encryption is necessary. The results of the encryption can be seen in Table 1.

**Table 1.** Encryption Result

| **Attribute Name** | **Plain Text** | **Encrypt Result** |
|---|---|---|
| *Nama Dokter* | *dr. Gede Supartha, Sp.M* | cë¥¦öÃzú {Ñ$.<br>¨.®p©\ïH?ÜGÏ |
| *Nama Pasien* | *Kurniadin Putra* | .zÝÓ &¢ðo.ûÞÀ<br>«&Tk |
| *Tanggal Lahir* | *06/14/2007* | H4[¦ãj¼à d¨i<<br>¹¤. |
| *Alamat* | *Mataram* | I.¥ï µ¸K. |
| *Keluhan* | *Demam*<br>*Sakit Tenggorakan*<br>*Suara Serak* | ¬□Êõ. 9çê.<br>üªªs'..?□.<br>·ñlÁpG.Õ.<.Q□<br>Ö.û».¤.N |
| *Diagnosa* | *Radang Tenggorokan* | ã9ìY ÉÕË. Bi.¸.<br>p.°ë.□.°êã |
| *Tindakan* | *Pemberian obat demam dan radang* | `óc..q...l/ýCù<br>zÞª±Ã,□cÏ..Ì.<br>TxÊê. |

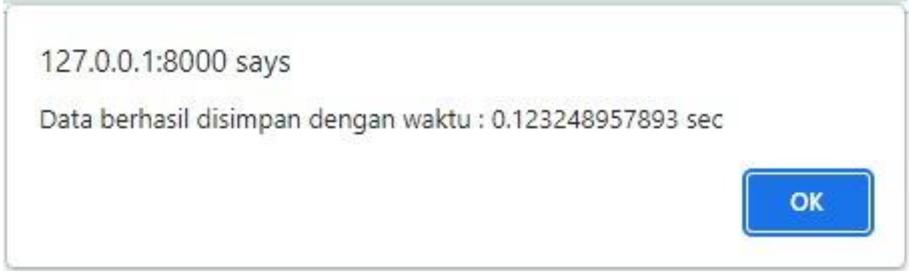
Table 1 shows the results of the encryption of the plaintext that will be stored in the database. So there is a change in the stored data, as can be seen in Figure 5.



| DOKTER | PASIEN | TANGGAL_LAHIR | ALAMAT | KELUHAN | DIAGNOSA | TINDAKAN |
|---|---|---|---|---|---|---|
| cë¥¦öÃzú<br>{Ñ$.¨.® | .zÝÓ &¢<br>ðo.ûÞÀ«<br>&T | H4[¦ãj¼à d¨ | I.¥ï µ<br>¸K. | ¬□Êõ. 9çê.<br>üªªs'..?□.·ñlÁ<br>pG Õ | ã9ìY ÉÕË.<br>Bi.¸.p.°ë.□.°<br>êã | `óc..q...l/ýC<br>ùzÞª±Ã, cÏ.. |

**Figure 5.** Encryption Results in Database

Figure 5 shows the encryption results that have been stored in the database. The encryption process affects the speed of data storage. This can be seen from the time it takes to save data to the database. The time needed to store data without any encryption process is shown in Figure 6.

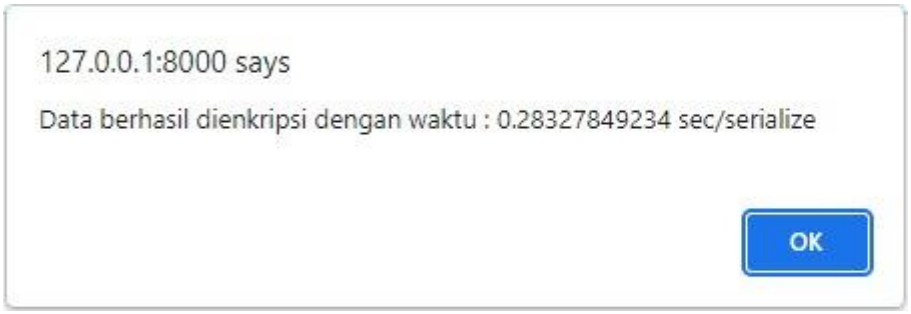


127.0.0.1:8000 says

Data berhasil disimpan dengan waktu : 0.123248957893 sec

**Figure 6.** Time Required Before Encryption

Figure 6 shows the time required by the system to store data without any encryption process is 0.12 seconds. Meanwhile, the encryption process takes a little longer. This is shown in Figure 7.



127.0.0.1:8000 says

Data berhasil dienkripsi dengan waktu : 0.28327849234 sec/serialize

**Figure 7.** Time Required After Encryption

Figure 7 shows the time required by the system to store data is 0.28 seconds. There is a difference of about 0.16 seconds between before and after encryption. This time difference occurs because of the encryption process carried out.

## Conclusion

Based on the research conducted, the application of the blowfish algorithm in securing patient data can be carried out and produces ciphertext that is quite difficult to understand, but with the application of the algorithm, the data storage process becomes slightly longer than before, from 0.12 seconds to 0.28 seconds. As for suggestions for future research, it is to develop this blowfish algorithm again and it can also be combined with other cryptographic methods to produce ciphertext that is more difficult to crack so that the data remains safe and is not misused by unauthorized parties.

## References

[1] R. Hammad, A. C. Nurcahyo, A. Z. Amrullah, P. Irfan, and K. A. Latif, "Optimization of data integration using schema matching of linguistic-based and constraint-based in the university database," *J. Manaj. Teknol. dan Inform.*, vol. 11, no. 3, pp. 119–129, 2021.

[2] Y. Farida and L. N. Desinaini, "Designing a microsoft access-based administration letters and archives system at BPJS of employment regional office of East Java," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 11, no. 1, pp. 42–54, 2021.

[3] A. M. Ningtyas and I. K. Lubis, "Literatur Review Permasalahan Privasi Pada Rekam Medis Elektronik," *Pseudocode*, vol. 5, no. 2, 2018, doi: 10.33369/pseudocode.5.2.12-17.

[4] H. D. Siregar, F. S. Sulaiman, and N. Falih, "Literatur Review Permasalahan Pengamanan pada Database," in *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, 2021, pp. 521–530.

[5] A. Riski, A. Kamsyakawuni, and M. Z. Ari, "Implementasi Vigenere Cipher Pada Pengamanan Data Medis," *J. Ris. dan Apl. Mat.*, vol. 2, no. 1, pp. 23–30, 2018.

[6] N. O. Akande, C. O. Abikoye, M. O. Adebiyi, A. A. Kayode, A. A. Adegun, and R. O. Ogundokun, "Electronic Medical Information Encryption Using Modified Blowfish Algorithm," in *Computational Science and Its Applications – ICCSA*, 2019, pp. 166–178.

[7] L. Sutandra, "Pengaruh Sistem Pengamanan Data Pasien di Rumah Sakit Menuju Era Revolusi Industri 4.0," *J. Heal. Sci. Physiother.*, vol. 1, no. 2, pp. 106–114, 2019.

[8] C. Indonesia, "Deretan Peristiwa Kebocoran Data Warga RI Sejak Awal 2020," *CNN Indonesia*, 2020. https://www.cnnindonesia.com/teknologi/20200623160834-185-516532/deretan-peristiwa-kebocoran-data-warga-ri-sejak-awal-2020 (accessed May 05, 2022).

[9] I. Riadi, A. Fadlil, and F. A. Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *J. Inform. Sunan Kalijaha*, vol. 7, no. 1, pp. 33–45, 2022.

[10] D. Erdriani and D. Devita, "APLIKASI MATRIK PADA ILMU KRIPTOGRAFI DENGAN MENGGUNAKAN MATLAB," *J. KomtekInfo*, vol. 8, no. 2, pp. 154–162, 2021.

[11] Hermansa, R. Umar, and A. Yudhana, "Analisis Sistem Keamanan Teknik Kriptografi dan Steganografi Pada Citra Digital (Bitmap)," in *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana*, 2019, pp. 520–528.

[12] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 11, no. 3, p. 155, 2020.

[13] V. C. Hardita and E. W. Sholeha, "Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher dan Simbol Baca Dalam Mengamankan Pesan," *J. Saintekom*, vol. 11, no. 1, pp. 34–43, 2021.

[14] M. Rizka, "Perpaduan Diffie Hellman dan Blowfish sebagai Sistem Keamanan Dokumen," *J. Infomedia Tek. Inform. Multimed. Jar.*, vol. 6, no. 2, pp. 86–90, 2021.

[15] E. Gunadhi and A. Sudrajat, "Pengamanan Data Rekan Medis Pasien Menggunakan Kriptografi Vigenere Cipher," *J. Algoritm. Sekol. Tinggi Teknol. Garut*, vol. 13, no. 2, pp. 295–301, 2016.

[16] N. Fahriani and I. Kurniawati, "Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT," *J-COSINE*, vol. 5, no. 2, pp. 140–148, 2021.

[17] E. E. Nylis and P. Purwanto, "Implementasi Pengamanan Email Menggunakan Metode Blowfish Berbasis Web Pada UPT Puskesmas Pondok Kacang Timur," *J. SKANIKA*, vol. 1, no. 2, pp. 570–576, 2018.

[18] H. G. Simanullang and A. P. Silalahi, "Algoritma Blowfish Untuk Meningkatkan Keamanan Database Mysql," *J. Method.*, vol. 4, no. 1, pp. 10–14, 2018.

[19] B. H. Nuboba, I. G. N. A. C. Putra, and I. K. G. Suhartana, "Rancang Bangun Aplikasi Enkripsi dan Dekripsi Objek 3 Dimensi menggunakan Algoritma Blowfish," *J. Elektron. Ilmu Komput. Udayan*, vol. 8, no. 3, pp. 307–316, 2020.

[20] H. Rosianto and L. Anifah, "Implementasi Algoritma DES Berbasis Blowfish untuk Enkripsi dan Dekripsi Data," *J. Tek. Elektro*, vol. 6, no. 2, pp. 121–128, 2017.