Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 6, No. 3, September 2018, pp. 309~316
ISSN: 2089-3272, DOI: 10.11591/ijeei.v6i3.493

Securing Electronic Medical Records Using Modified Blowfish Algorithm

Theda Flare G. Quilala[1], Ariel M. Sison[2], Ruji P. Medina[3]
[1,3]Technological Institute of the Philippines, 938 Aurora Blvd., Cubao, Quezon City, Philippines
[2]Emilio Aguinaldo College, 1113-1117 San Marcelino St., Paco, Manila 1000, Philippines

Article Info

Article history:

Received May 17, 2018
Revised Aug 23, 2018
Accepted Sep 6, 2018

Keyword:

Cryptography
Encryption
Health record
Patient protection
Security

ABSTRACT

EMR helped improve services to patients by delivering organization and accuracy of patient information, but issues regarding security breaches and medical identity theft are growing concerns. This paper enhance the current EMR system by integrating modified encryption. The simulation used modified Blowfish algorithm in an EMR system that focuses on four goals: 1) define the requirements, 2) design and identify features, 3) develop the EMR incorporating added security mechanism using modified Blowfish algorithm, and 4) test the application with sample data. Based on the results, the incorporation of the encryption was successful based on testing and checking done on the input terminal and the database server. Data inputted on the EMR system was successfully encrypted before transmission and decrypted only on the terminal for viewing. Performance results show that without encryption, saving took an average of 87.8ms while encrypted, it acquired 88.8ms, a difference of 1ms can be noted. The minimal difference is because of the size of the data. The average decryption time of all records using modified algorithm took 1342ms while using plaintext took 1322ms. The decryption time is higher by 20ms due to the application of the decryption algorithm.

Corresponding Author:

Theda Flare G. Quilala,
Technological Institute of the Philippines,
938 Aurora Blvd., Cubao, Quezon City, Philippines.
Email: tfgquilala@gmail.com

1. INTRODUCTION

An Electronic Medical Record (EMR) is a controlled document that contains essential and sensitive patient's information [1]. Protecting patient privacy is deemed valuable as evidenced by restrictions imposed regarding sharing of information and the security of physical repositories [2] [3]. As a fundamental right, laws per country control and regulate the access to medical information to protect patient's confidentiality.

There is an increasing desire to use the public infrastructure like the Internet to store, send, or receive private information for availability and sharing of public and private digital data. Because of this, data security breaches and medical identity theft are growing concerns, with thousands of cases reported every year [4]. Issues like this have driven industry professionals and researchers to dedicate attention to information security for protection against unauthorized access and attacks [5].

One way of guaranteeing the protection of patient's information is through the application of cryptography. Cryptography is the study of information hiding and achieving security by encoding messages to make them non-readable [6] [7]. The use of cryptography addresses data privacy preservation and security of electronic health record from modification and unauthorized access during transmission [1], [8]-[10].

Tarlac State University (TSU) is envisioned to be a premier University not only in Tarlac but the Asia Pacific Region. Its mission is to not only provide high-quality instruction, enhance research undertakings and strengthen collaboration with institutions but also seeks to ensure safe and healthy working

conditions for its employees and students [11]. The TSU medical clinic was established to provide free medical support to students, faculty, and staff of the University. Currently, the medical clinic is using the paper-based system for storing the medical records in files. But to take advantage of information technology, the clinic requests the Management Information System Office (MISO) of the University for digitization of medical records - from the previous handwritten or typed. Studies regarding the superiority of EMR versus paper-based approaches intend to improve the quality of documentation in recorded patients' information by enhancing organization and standardization of clinical data [12] [13]. Most enhancements are due to the increasing difficulty in handling medical data to gain accuracy and efficiency in the recording. The EMR is envisioned to help the medical clinic in the management of their records.

OpenEMR, GNUmed, OpenMRS, OSCAR, GNU Health and others are one of the many open source applications in healthcare. A study has evaluated the data security of these applications, and the most identified form of protection ranges only from utilizing passwords and some backup mechanisms while storage and secure communications are lacking [14]. EMR, though considered as the central element of health IT infrastructure, have drawbacks in implementation such as exposure to cyber-attack [15]. Individuals may attempt to steal a patient's identity, resulting in financial implications for the patient [4]. Secure communication is a priority requirement for EMR, so the use of encryption approaches and traffic shaping algorithms are placed to ensure secure access to data [16]. Data in transit or data in motion, movement of data from locations for instance across the internet or through a private network, is considered less secure [17]. Data in transit achieves less emphasis and found to be not as protected therefore security measures must be placed for protection because data is susceptible to eavesdropping when in motion, so encryption is needed [18], [19].

In 1994, Bruce Schneier designed Blowfish algorithm as an alternative encryption algorithm to the out-of-date DES. It is a symmetric block cipher that accepts a 64-bit input block cipher and a varying key size of 32 to 448 [20]. Blowfish is one of the fastest, compact, easy to understand, easy to implement, free alternative to existing encryption algorithms and features variable security level except when changing keys [21]. Blowfish has been used as the cryptographic algorithm to impose increase security for encryption of file records and electronic documents that contain medical information [22]-[24].

Even though blowfish is remarkable, it still uses the 64-bit input block size which would allow higher chances of having duplicate blocks during encryption of files which can lead to a leak in information. Each round in the key expansion needs around four kB which makes it unsuitable for devices with small memory. The modified blowfish algorithm was developed to address vulnerabilities of Blowfish such as the input block size, and memory storage space of the key. The modification in block size would allow encryption of file with reduced chances of having identical blocks. The number of s-boxes is reduced from four to two to provide less memory consumption while maintaining the original structure for migration ease. The modified algorithm reduced the number of S-boxes, so a derivation technique was added to remove symmetry.

This paper intends to enhance the current system by integrating an encryption scheme in an EMR system. A simulation will present the use of the modified Blowfish algorithm in the EMR. It focuses on four primary objectives namely: 1) to define the requirements needed in the development of the EMR, 2) to design and identify features to be included, 3) to develop EMR incorporating an added security mechanism using modified Blowfish algorithm, and 4) to test the application with sample data. The use of cryptography in EMR will be beneficial to health care patients as this addresses issues of data privacy preservation and encryption of patient health records for transmission over the network infrastructure.

2. RESEARCH METHOD

RAD is based on prototyping and iterative development. Rapid Application development focuses on gathering customer requirements through workshops or focus groups, early testing of the prototypes by the customer using iterative concept, reuse of the existing prototypes (components), continuous integration and rapid delivery. Since RAD fits into the time frame, this model was adopted in the system development.

An interview was conducted both on the medical clinic and management information system office for data gathering. After series of question and answers, requirements were formulated. Sample data were taken from the medical records of employees in Tarlac State University (TSU) and medical record sample. Since health records are considered private, the actual name of the persons involved will be replaced with dummy names during the testing phase. Data privacy will be strictly imposed. The structure of the database is taken from the existing database of TSU medical records system.

Simulation work using medical records on the algorithm will be carried out by using .net framework (pronounced dot net). VB.NET (Visual Basic) is an object-oriented programming language developed by Microsoft that runs on the .NET Framework on a Microsoft Windows operating system. An HP computer

system with Intel® Core™ i5-7200U processor performing at a speed of 2.50 GHz with windows platform and 8GB installed memory will be used to carry out the proposed work.

3. RESULTS AND ANALYSIS

3.1. Requirement Definition

Interview was used for data gathering and after series of question and answers, requirements were formulated. Registered users must be able to login to the EMR by providing username and password. The administrator is the superuser who can access all modules. The administrator can add, edit, and view information of any EMR system user. Nurse account shall be able to add, edit, and see the medical profile which includes the patient personal information and medical history. The nurse can input initial details during the consultation which consists of the general appearance and vital signs of the patient. The doctor account can view information of the patient and add the result of the diagnosis. The nurse account can record the physical examination of employees for their Annual Physical Exam (APE). The nurse account can log the physical examination of students for their pre-employment medical exam. The nurse account can record lab examination such as hematology, blood chemistry, urinalysis, ultrasound, 2D echo with doppler, stress, and other test results. The system can provide a medical certificate of the patient. The nurse asses the patient and can add a patient in the queueing system if the patient needs Doctors' assistance for onsite consultation. The system shall be able to provide medical services internally or on-site. The system shall be able to provide transmission encryption using the modified Blowfish algorithm.

3.2. Design and Modules

Based on the gathered requirements and after deliberation, the final design of the customized EMR composed of the following features:

a. Main Module: This module shows the list of patients. The user can search and view information of patients under the main module.
b. Medical Profile Module: This module consists of patients' personal information and medical history including hospitalization records, childhood illnesses, family medical history, and allergies.
c. Consultation and Diagnosis Module: The consultation module contains the patients' general appearance, vital signs, and body mass index information at the time of consultation. This module will show the patients' medical history. This module is also where the result of the diagnosis will be encoded.
d. Physical Examination Module: Under this module, the purpose of the physical examination can be classified according to Annual Physical Exam (APE) for employees or students' pre-employment physical exam. General appearance, vital signs, eye test, and review of general system functions is recorded here. The result of diagnostic procedure test is also documented here. A medical certificate is provided when needed for this module.
e. Laboratory Module: Result of different laboratory tests required for the physical exam are encoded here. A laboratory test can be, but not limited to the Hematology, Blood Chemistry, Urinalysis, Ultrasound, Stress, 2D Echo with Doppler, and other tests.
f. Patient queueing: Patient queueing module allows organized numbering of the patient for an on-site consultation. Patients are numbered in order of appearance as per assessment by the nurse on duty.
g. User management and privileges: The user management module allows the administrator to handle account privileges. This module will enable the administrator to add, edit and view users that can access the EMR.
h. Audit Trail: This module records all transactions done in the EMR as audit trail logs. This feature is included for accountability purposes since EMR records are considered private and confidential.
i. Database Back-up and restoration: Back up and restoration module will enable the user to back up the database in a specified location set by the user from time to time to minimize risk in case of unforeseen events. This module can also restore the saved database from any location.
j. Login Module: This module allows authorized users to login into the EMR system.

3.3. Security Mechanism

The modified Blowfish algorithm is included as the encryption mechanism as an added security mechanism. Figure 1 explained the process of encryption and decryption.

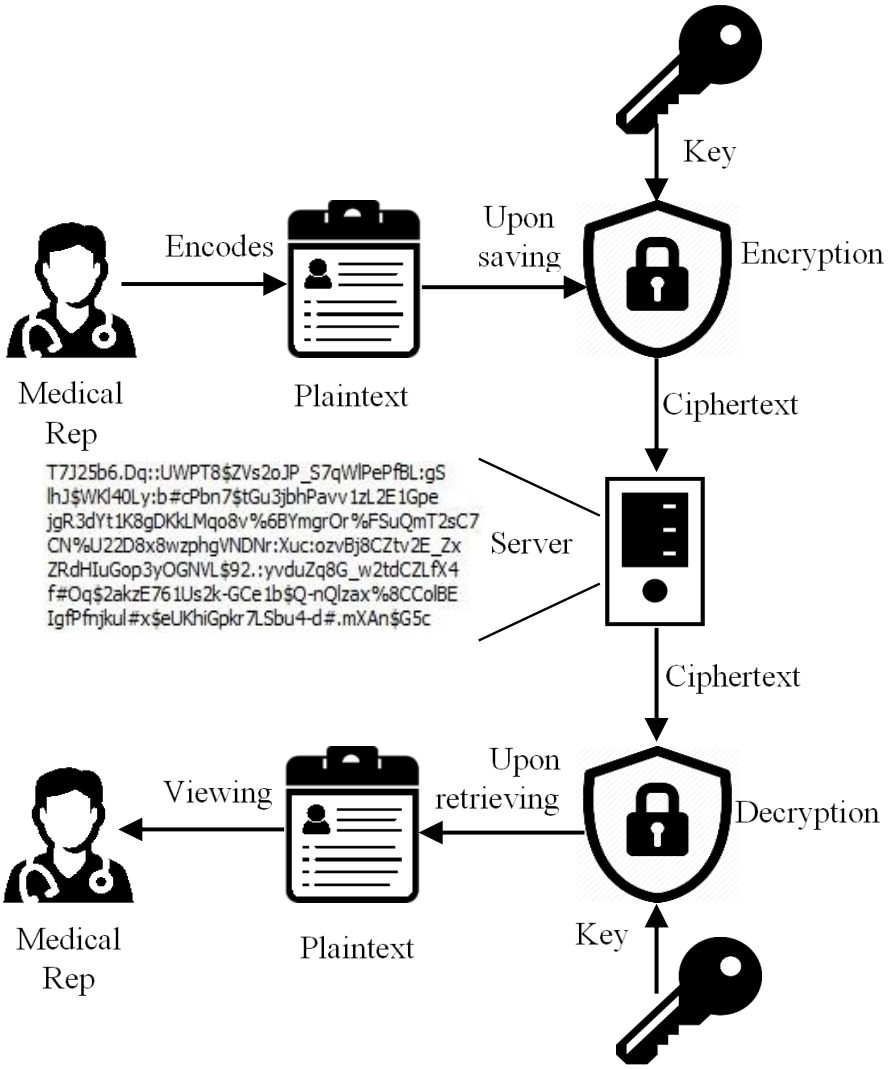

Figure 1. Medical data encryption and decryption process using modified blowfish

The representative or any authorized user encodes the medical related information in the EMR. The process of encryption starts the moment the record is saved. Before the data is transmitted to the server, the data is encrypted using the modified Blowfish algorithm with the key. The resulting ciphertext is sent instead of the plaintext to the server. Only selected private and sensitive information will be encrypted. During viewing, the encrypted medical information is fetched from the server and then decrypted using the modified Blowfish algorithm and key. Once the encrypted information is decrypted, the information is shown to the authorized user or representative as readable text.

The modified Blowfish reduced the size of keys from the previous 4168 bytes to 2128 bytes. The key expansion will still convert the 128-bit key length into several subkey arrays. These keys are generated dynamically before any data encryption or decryption occurs. The P-array consist of 20 32-bit subkeys. The four S-Boxes consist of 256 individual entries comprising 32-bits each. In the modified key expansion scheme, the total number of iterations is reduced to 266 to generate all required subkeys.

Calculation of the subkeys are done using the same Blowfish algorithm, but the algorithm reduced the size to two S-boxes. First, P-array followed by the four S-boxes is initialized using constant strings that consist of predetermined hexadecimal digits of pi. Next, P1 and P2 are XORed with the first and second 32 bits of the key, in a loop until all bits of the key is exhausted. Repeat the cycle until the whole P-array (P20) has been XORed against the key bits. Then, Blowfish algorithm is used in encrypting an all-zero string using the subkeys described in the previous steps. Next, the outcome of step 3 substituted values of P1 and P2. Then using the Blowfish algorithm again, encrypt the output of step 3 using the revised subkeys. Then,

results obtained in step 5 replaced P3 and P4. This process is continuously repeated replacing all entries of the P array, followed by the two S-boxes with the output of the continually varying Blowfish algorithm.

Figure 2 shows the new process of encryption of the modified blowfish algorithm. The structure of the original blowfish algorithm is still adopted, but the modified Blowfish reduce the number of iterations to 8.

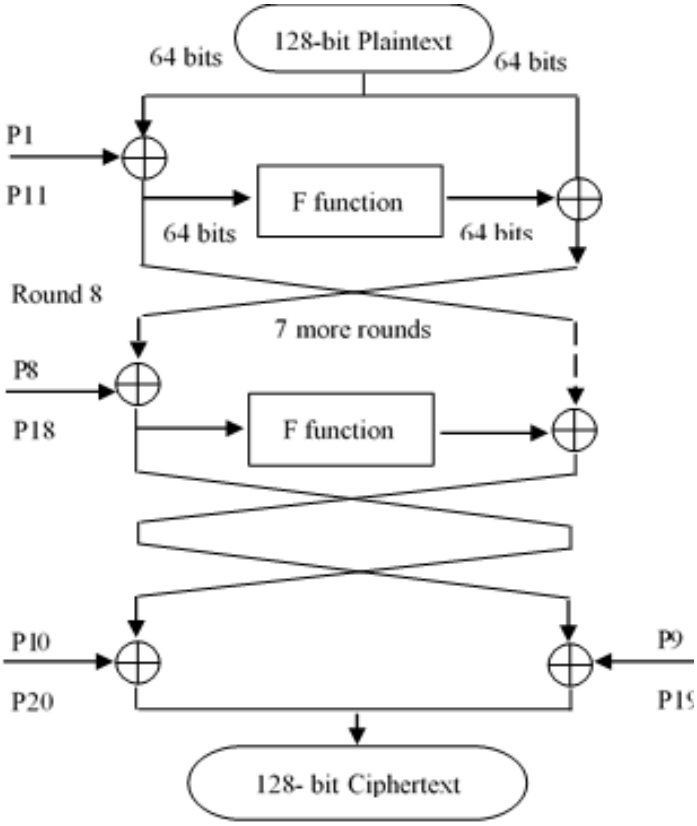

Figure 2. Modified blowfish algorithm architecture

The difference lies in the input block. The input block changes to 128-bit and will be split into two 64-bit equal segments LE0, RE0. Second, the first segment 64-bit block (LE0) is XORed to the first entry in the P-array (P1, P11) with two 32-bit entries. Third, input the two 32-bit data obtained to the F-function. The output from the F-function will then be XORed with the second segment (RE0) of the plaintext. Then, swap LE0 and RE0. This cycle will continue up to the eighth round. After the eighth round, exchange LE8 and RE8 reversing the last swap. Then, RE8 is XORed to P-array (P9, P19) and LE8 is XORed to P-array (P10, P20). Finally, we recombine LE9 and RE9 to get the ciphertext. The decryption process is the reverse of the encryption process.

Figure 3 also shows the details of the construction of the new F-function in the modified blowfish. The F-function now accepts a 64-bit data stream and will be divided into eight 8-bits where a is the first 8 bits, b is the second 8 bits, up to the last 8 bits. Transform each 8-bit data bits into a 32-bit data. The first four 8-bit data stream utilizes the first S-box while the next four 8-bit data stream uses the second S-box. The output from the S-boxes are then XORed or added to obtain the final 32-bit value per S-box and then concatenated to obtain the 64-bit output as shown in the Equation 1

$$F(LE0) = ((S1(a) + S1(b) << 1 \bmod 2^{32}) \oplus S1(c) >> 1) + S1(d<<1) \bmod 2^{32} \mid ((S2(e) + S2(f) << 1 \bmod 2^{32}) \oplus S2(g) >> 1) + S2(a<<1) \bmod 2^{32} \quad (1)$$

The S-boxes are derived at runtime from S-box 1 by a simple rotation by one position of either the input or the output or either by left or right. Below defined the details of the derivation process:

$$S2(x) = S1(x) << 1 \quad (2)$$

$$S3(x) = S1(x) >> 1 \quad (3)$$

$$S4(x) = S1(x << 1) \quad (4)$$

The researcher changed the structure of the F-function as can be seen from the equation above.

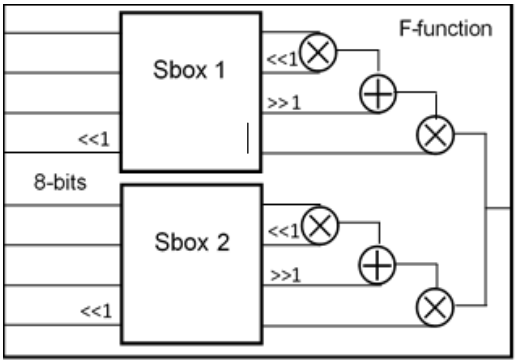

Figure 3. Modified F-function

Sample data was encoded to test the application. Figure 4 shows the sample encoded medical profile with details such as the name, gender, birthdate, address, and others. As can be seen in the viewing module, the text is readable.

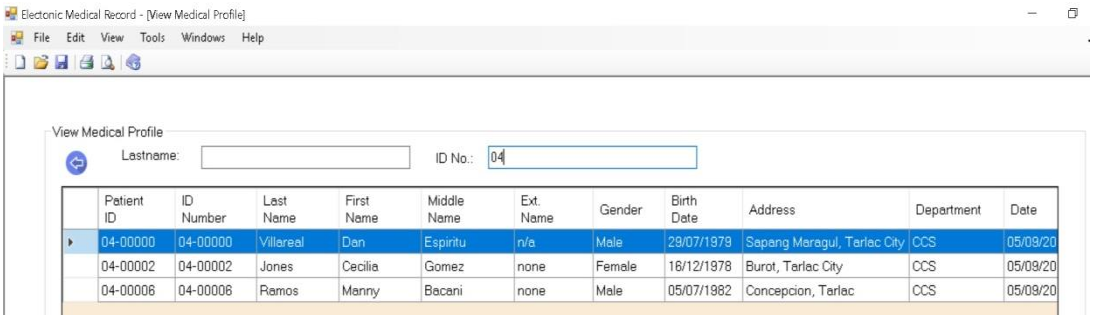

Figure 4. Sample medical profile of patient using the EMR system

Sample medical record is viewed on the database server to check if the encryption of data works accordingly. Figure 5 shows the screenshot of the data saved on the server. As seen, specific fields are encrypted. Hence, this assures that even if a breach occurs, the data are still encrypted and still considered safe.

Figure 5. Sample encrypted data as seen on database server

Performance of the modified algorithm is measured using time in milliseconds. The average time was noted without the use of encryption (plain text only) and using the modified Blowfish encryption using five sample medical profiles. Table 1 shows the comparison. As can be seen, if without encryption, saving took an average of 87.8ms while if encrypted it obtained 88.8ms. A slight variation in the average time (1ms) can be noted for the five records. The changes in time are very minimal because the size of the data to be encoded is small.

Table 1. Time Comparison of Saving Data in Milliseconds Using Sample Medical Data

	Time	
Record Number	Without Encryption (Plaintext)	With Encryption (modified Blowfish)
1	87	89
2	87	89
3	86	87
4	88	88
5	91	91
Average	87.8	88.8

In viewing the medical data, time in milliseconds was also noted without decryption (plain text only) and using the modified Blowfish decryption algorithm. Table 2 shows the comparison. Viewing of all five medical profiles was repeated five times. As can be noted, the average time without decryption or using plaintext only is 1322ms while average decryption time of information using the modified algorithm took 1342ms. The decryption time is higher by 20ms. Viewing time of all records is anticipated to increase as the number of records to display increases because all records are decrypted at the same time.

Table 2. Time Comparison of Viewing Data in Milliseconds Using Sample Medical Data

	Time	
Trial Number	Without Encryption (Plaintext)	With Encryption (modified Blowfish)
1	1305	1348
2	1290	1300
3	1302	1314
4	1289	1309
5	1424	1439
Average	1322	1342

4. CONCLUSION AND FUTURE WORKS

EMR helped improve services provided to patients by offering organization and accuracy in dealing with patient information. The information requirement gave enough information to build the EMR software and serves as a guide. The features included were the answers on how the system might help in the enhanced acquisition of information from the EMR. Since most EMR lacks application of encryption, the study addressed issues in data security by applying an encryption algorithm using the modified Blowfish algorithm. Finally, the EMR system was tested by encoding sample data and checking the application of the encryption mechanism by inspecting data saved on the server. Performance of saving and viewing medical data in plaintext and using modified Blowfish encryption is also measured using time expressed in milliseconds. Performance results show that if without encryption, saving took an average of 87.8ms while if encrypted it acquired 88.8ms, a difference of 1ms can be noted. The minimal difference is observed because the size of the data encoded is small. The average decryption time of all records using modified algorithm took 1342ms while using plaintext took 1322m. The decryption time is higher by 20ms because of the application of the decryption algorithm. For this study, all text fields are encrypted. For future works, the processing time of encrypting text files as an additional supplementary attachment may be considered as well as encryption of non-text data.

REFERENCES

[1] J.E. Camargo, D.F. Sierra, and Y.F. Torres, "Study of cryptographic algorithms to protect electronic medical records in mobile platforms", *Indian J. Sci. Technol.*, vol. 8, no. 21, pp. 1–7, 2015.

[2] I.D. Patdu and A.B. Marcelo, "Health Information Privacy in the Philippines : Trends and Challenges in Policy and Practice Privacy in the Developing World — Philippines Monograph Series", 2013.

[3] R. Chavda and R. Aluvalu, "Encryption Based Access Control Model In Cloud : A Survey", *J. Telemat. Informatics*, vol. 4, no. 1, pp. 15–21, 2015.
[4] J.K. Taitsman, C.M. Grimm, and S. Agrawal, "Protecting Patient Privacy and Data Security", *N. Engl. J. Med.*, vol. 368, no. 11, pp. 977–979, Mar. 2013.
[5] R. Singh Chhillar, "Data Hiding Using Steganography and Cryptography", *Int. J. Comput. Sci. Mob. Comput.*, vol. 44, no. 4, pp. 802–805, 2015.
[6] M. Bhattacharya, K. Pal, G. Ghosh, and S.S. Mandal, "Generation of novel encrypted code using cryptography for multiple level data security for Electronic Patient Record", *Proc. - 2015 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2015*, pp. 916–921, 2015.
[7] T.N. Babu, D.L.P. Kaja, K. Tejaswi, Y. Harish, and A. Cryptography, "Ortho Linear Feedback Shift Register Cryptographic System", *J. Telemat. Informatics*, vol. 3, no. 2, pp. 27–33, 2015.
[8] M.A. Sadikin and R.W. Wardhani, "Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application", in *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 2016, pp. 387–392.
[9] H. Abdulrahman, N. Poh, and J. Burnett, "Privacy preservation, sharing and collection of patient records using cryptographic techniques for cross-clinical secondary analytics", *IEEE SSCI 2014 - 2014 IEEE Symp. Ser. Comput. Intell. - CICARE 2014 2014 IEEE Symp. Comput. Intell. Healthc. e-Health, Proc.*, pp. 148–153, 2015.
[10] S. Fong-In, S. Kiattisin, A. Leelasantitham, and W. San-Um, "A partial encryption scheme using absolute-value chaotic map for secure electronic health records", in *The 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE)*, 2014, pp. 1–5.
[11] "Tarlac State University", [Online]. Available: http://www.tsu.edu.ph/.
[12] G.L. Laing, J.L. Bruce, D.L. Skinner, N.L. Allorto, D.L. Clarke, and C. Aldous, "Development, implementation, and evaluation of a hybrid electronic medical record system specifically designed for a developing world surgical service", *World J. Surg.*, vol. 38, no. 6, pp. 1388–1397, 2014.
[13] L. Pan, X. Fu, F. Cai, Y. Meng, and C. Zhang, "A compact electronic medical record system for regional clinics and health centers in China: Design and its application", *Proc. - 2016 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2016*, pp. 1010–1015, 2017.
[14] M.L.M. Kiah, A. Haiqi, B.B. Zaidan, and A.A. Zaidan, "Open source EMR software: Profiling, insights and hands-on analysis", *Comput. Methods Programs Biomed.*, vol. 117, no. 2, pp. 360–382, Nov. 2014.
[15] J. Mungara and C. Rao, "Need for Electronic Health Record", *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 3, pp. 887–890, 2017.
[16] M. Grana and K. Jackwoski, "Electronic Health Record: A review", in *2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 2015, pp. 1375–1382.
[17] N. Lord, "Data Protection: Data In Transit Vs. Data At Rest", 2018. [Online]. Available: https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest. [Accessed: 03-Mar-2018].
[18] F. Els and L. Cilliers, "Improving the information security of personal electronic health records to protect a patient's health information", in *2017 Conference on Information Communication Technology and Society (ICTAS)*, 2017, pp. 1–6.
[19] P.A.A. Adedeji Kazeem B, "Improved Image Encryption for Application over Wireless Communication Networks using Hybrid Cryptography Technique", *Indones. J. Electr. Eng. Informatics*, vol. 4, no. 4, pp. 307–318, 2016.
[20] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", in *Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., December 9--11,1993 Proceedings*, R. Anderson, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 191–204.
[21] V. Kumar and A. Sharma, "A Survey on Various Cryptography Techniques", *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 4, pp. 307–312, 2014.
[22] S.S. Kondawar and D.H. Gawali, "Blowfish algorithm for patient health monitoring", *2016 Int. Conf. Inven. Comput. Technol.*, vol. 3, pp. 1–6, 2016.
[23] R. Ade, "Patient Controlled Encryption using Key Aggregation with Blowfish Algorithm", in *International Journal of Computer Applications*, 2015, no. Ncac, pp. 11–14.
[24] D.T. Dunsmuir *et al.*, "Development of mHealth Applications for Pre-Eclampsia Triage", *IEEE J. Biomed. Heal. Informatics*, vol. 18, no. 6, pp. 1857–1864, Nov. 2014.