Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data

Amir Mahmud H1*, Bayu Angga W1, Tommy2, Andi Marwan E2, and Rosyidah Siregar3

1Departement of Computer Science, Faculty of Technology and Computer Science, Universitas Prima Indonesia, Indonesia
2Department of Computer Science, Faculty of Technic and Computer Science, Universitas Harapan, Indonesia

E-Mail: *amirmahmud@unprimdn.ac.id

Abstract. A file security is one method to protect data confidentiality, integrity and information security. Cryptography is one of techniques used to secure and guarantee data confidentiality by doing conversion to the plaintext (original message) to ciphertext (hidden message) with two important processes, they are encrypt and decrypt. Some researchers proposed a hybrid method to improve data security. In this research we proposed hybrid method of AES-blowfish (BF) to secure the patient's medical report data into the form PDF file that sources from database. Generation method of private and public key uses two ways of approach, those are RSA method f RSA and ECC. We will analyze impact of these two ways of approach for hybrid method at AES-blowfish based on time and Throughput. Based on testing results, BF method is faster than AES and AES -BF hybrid, however AES-BF hybrid is better for throughput compared with AES and BF is higher.

1. Introduction
The development of internet technology nowadays in digital era becomes the point of attention, especially issues which are about data confidentiality, integrity and information security [1]. The internet utilization in the current era can facilitate human, one of them is easy to deliver data, so needs of data security will be vital and significant [2]. Cryptography is one of techniques that used for secure and ensure data confidentiality [3]. Technically, cryptography is conversion of plaintext (original message) to ciphertext (hidden message) with two important processes to secure message, those are encryption and decryption [4]. Cryptographic techniques are divided into two categories: Symmetric and Asymmetric Key Cryptography. Symmetric key Cryptography referred to as a Private Key Cryptography using key encryption and decryption at the same data. Symmetric techniques like DES, IDEA, Blowfish, RC4, RC2, RC5, Triple DES, and AES. Blowfish algorithm is faster than other algorithms, but AES algorithm is more secure and superior than DES [5]. While Asymmetric Key Cryptography is known as Public Key Cryptography which uses two different keys for encryption and decryption [6], like RSA, Rabin Cryptosystem, ElGamal Cryptosystem and Elliptic Curve Cryptosystem (ECC). ECC is faster than RSA. Some researchers have applied hybrid method to overcome weaknesses of cryptographic algorithms, such as the Fast method of Chaos-based, AES,
RSA and ElGamal[7]. AES-RSA [8], RSA-AES [9], [10], RSA-AES and RSA [11], AES-DES-RSA [12], AES-Blowfish [5] AES-DES [13].

Some researcher have applied hybrid method to resolve the weakness of cryptography algorithm, like research [12], did a performance comparison on algorithms AES, DES, RSA with a hybrid method of AES-DES-RSA with four parameters, namely avalanche effect encryption time, CPU usage and Throughput. [5] developed a hybrid method of AES-Blowfish algorithm with the use of Elliptic Curve Cryptography (ECC) for the management and key exchange, testing was done in the format of text files, image files, audio files and video files. [10] proposed a hybrid method of AES-RSA data security in order to support cloud computing, [9] implemented RSA-AES hybrid methods for security of data exchange between two clients using web services as an intermediary with encrypt content blocks that can only be decrypted by the client side, and not on the web server.

RSA and AES hybrid methods propose [11] to increase data security. AES Method for encryption and decryption data process based on key generation method using RSA-128 bytes. [14] proposed a method of hybrid RSA-AES for encryption at the IP address stored in the DSN by comparing results with RSA algorithms hybrid RSA-AES. [13] proposed a hybrid method of AES-DES for the security of data transmission based on 128-bit key with testing on file format text, image, audio and video.

In this study, we aimed to analyze the performance of a public and private key generation RSA and ECC method to secure the patient's medical report on data sourced from a database. Both of them approach key generation method, we analyze the influence of time and Throughput at the encryption process and decryption algorithm on hybrid AES-Blowfish. This paper is served as follows: part 2 and part 5 is conclusion.

AES algorithm was developed by Joan Daemen and Vincent Rijment in 2001 through a contest organized by the National Institute of standards and technology (NIST). AES relies on patterns, basic principles related to substitution permutations system. AES has four methods: shift the Mix of columns, rows, substitute byte, and add an all-around sub-key [12].

AES encryption process using button on a special called the round keys. This key is applied with other operations such as Sub Shift Bytes, Rows etc in plaintext (original data) to get the cipher text (encrypted data). For the process of decryption, the inverse process is used at the stage of transformation. The process starts from the InvSubByte, InvShiftRows, and ends in InvMixColumns. Therefore, the S-box to encryption and decryption is different. In the process of decryption, the S-box used is reverse S-box substitution and operations permutations in block size 128 bits, and the key sizes from 128, 192, or 256 bits [12].

Blowfish is one of encryption method that is included in the Symmetric Cryptosystem. Symmetric key cipher block algorithm was designed in 1993 by Bruce Schneider to replace the DES (Data Encryption Standard). Blowfish is a block cipher, the encryption process and the decryption, Blowfish divides a message into blocks of equal size in length, i.e. 64 bits. This algorithm consists of two parts, namely the expansion of the key (the key expansion) and data encryption. Key expansion is stage to expanding the key length is 32 bits to 448 bits into several subkey arrays (subkey) with a total 4168 bytes. Data encryption occurs in as many as 16 rounds of feistily network where each round consists of a permutation lock and substitution of data. All operations are addition and XOR on 32-bit variables. Other operations are merely additional of four tables search (lookup table) for each round. Blowfish uses a large subkey where each keys must be computed before encryption or decryption of data begins.

RSA algorithm was invented by Ron Rivest, Adi Shamir and Leonard Aldeman and it is public key encryption. RSA method is widely used to secure data transmission with public key for encryption and decryption based on two prime numbers. The second prime number is to keep secret and only the authorized user can decode the message, the following steps [5].(a) Establishment of Key: Step 1 : take the two prime numbers tell a and b, Step 2 : Calculate n such that n = a * b, Step 3 : Calculate total n, (n) = (a-1) * (b-1), Step 4 : choose value e s.t 1 < e < (n) and e and (n) must relative prime,
Step 5: Count $d$ in such a way, $de = 1 \pmod{n}$. (b) Message Encryption, $C = me \pmod{n}$, where $m$ is plaintext. (c) Message Decryption, The plaintext calculated from text password by $M = cd \pmod{n}$.

Elliptic Curve Cryptography (ECC) is a system for public-key cryptography that makes the use of elliptic curve equation. The algorithm was designed and proposed by Neal Koblitz and Victor S. Miller. ECC method is considered more superior than other methods, because it uses a key that is much smaller, but it can provide the same level of security with an asymmetric algorithm using larger keys. With the smaller size of the key and the same high level of security, the implementation of ECC becomes more efficient.

SHA-256 is one of cryptographic hash functions designed by the NSA (U.S National Security Agency). SHA stands for Secure Hash Algorithm. Cryptographic hash function is a mathematical operation is performed on a digital data; by comparing the computed "hash" (the output of the execution algorithm) to the hash value that is known and expected, one can determine the integrity of data. SHA-256 hash computed by the words of 32 bits [9].

2. Proposed model framework

In the research, we propose hybrid cryptography method of AES and Blowfish, both of these symmetric methods will increase the time process of encryption and decryption on the patient's medical record data taken from databases with the format portable document file (PDF). Figure 1 and figure 2 are an illustration process Framework hybrid cryptography and decryption which we are proposing. Document activation uses SHA 256 while the key generation of private process and public key uses two ways of approaching, namely the method of RSA and ECC.

![Diagram](image-url)

**Figure 1.** The proposed hybrid encryption architecture.

In figure 1 is a proposed hybrid encryption process, medical record data will be encrypted using AES and Blowfish, follows the process used: Generate data of medical record into a format portable document file (PDF); Apply a hashing document with the method of SHA 256 resulting signature; Generate a public and a private key using two ways of approaching, namely: RSA and ECC; Encryption of patient's medical record file with AES and Blowfish uses key; Sends files (1) encrypted file (2) encrypted key and (3) the signature to the recipient.
In figure 2 describes the hybrid decryption process proposed, patient record data which has been already encrypted will be decrypted again so that it can be read by the recipient, the following decryption process: The recipient will receive a three-block file password: (1) block key, (2) signature block and (3) the encrypted file; Implement private key on block to open the public key, apply the public keys to open the file signature; Enter AES key and Blowfish key to unlock the encryption file so that it results Hashing document file; Then it is compared with the result of hashing signature by hashing the document, if it works then your medical record file will perform normally. If not, then the files will appear in encrypted.

The main objective in this study is to analyze the effect of key generation RSA and ECC against AES-Blowfish hybrid methods to secure the patient's medical record file based on speed time and Throughput. In General, throughput is the rate of production or rate at which something can be processed. In the context of Encryption throughput is the rate at which data are increasingly encrypted. It is better to have a high encryption throughput. As a high encryption level (throughput) and safe, it is used to transmit data securely over the network. We have taken the approach to calculate the throughput using the formula: (Total number of Bits that are accessed)/(Total CPU time).

3. Result and Discussion
An experiment is done with the platform specification of intel core i5 2.5 GHz CPU, 8 Gb of RAM and using an operating system WIN 10 64-bit from the client side, whereas the specification of the database server uses Intel Xeon Processor E3-1200 v5 Series; Core i3, 64 GB DDR4 Memory with 7 operating system Centos Linux and applications are created using C# 2010. In testing, before medical record data, process of encryption is done, medical record data will be processed from a database by using query then the results will be displayed in the form of a report with the PDF format, the PDF report files in encrypted with AES and Blowfish which 256 SHA hashing functions applied for integrity. Key generation method of private and public keys uses RSA and ECC method, both of these methods will be analyzed its effects on the results of the encryption based on speed and Throughput. In table 1 is a result of data encryption processes on medical record of the patient, from the results of testing method of Blowfish (BF) is faster than AES, this result is appropriate literature, whereas AES-BF hybrid methods proposed to take higher than AES methods.
The effect application of the public and the private key on a hybrid AES-BF is proposed to give different results from the two ways of approaching which are used. On the ECC method is faster than RSA method, the results of the comparison of the two methods are shown in figure 1 using the method of RSA and ECC method using figure 2. Decryption process results in the method proposed can be seen in table 3 and figure 3 and figure 4 is a graphics display comparison results of both ways of approaching duplicate medical record file into PDF format.

Table 1. Hybrid encryption runtime approach.

| File Name          | File Size (kb) | Encryption Runtime (t) | RSA Generate Key | ECC Generate Key |
|--------------------|----------------|------------------------|------------------|------------------|
|                    |                | BF                     | AES              | AES-BF           |
| Medical Report 1   | 372.67         | 124.22                 | 165.89           | 244.22           |
| Medical Report 2   | 367.33         | 122.44                 | 164.11           | 242.44           |
| Medical Report 3   | 424.00         | 141.33                 | 183.00           | 261.33           |
| Medical Report 4   | 214.67         | 71.56                  | 113.22           | 191.56           |
| Medical Report ..  | 296.67         | 98.89                  | 140.56           | 218.89           |

Table 2. Hybrid decryption runtime approach.

| File Name          | File Size (kb) | Decryption Runtime (t) | RSA Generate Key | ECC Generate Key |
|--------------------|----------------|------------------------|------------------|------------------|
|                    |                | BF                     | AES              | AES-BF           |
| Medical Report 1   | 372.67         | 135.89                 | 177.55           | 255.8867         |
| Medical Report 2   | 367.33         | 134.11                 | 175.77           | 254.1067         |
| Medical Report 3   | 424.23         | 153.00                 | 194.66           | 272.9967         |
| Medical Report 4   | 214.67         | 83.23                  | 124.89           | 203.2277         |
| Medical Report ..  | 296.67         | 110.56                 | 152.23           | 230.5587         |

In table 2 above, is the result of the decryption process using the hybrid method of AES-BF the time where the process is higher than data encryption, but the decryption key using the private key RSA and public method takes more than a method of ECC.
For the results of the performance in terms of Throughput shown in table 3 and table 4, Throughput Performance Analysis for the encryption process and duplicate is measured in Bits per Second. The process of encryption and decryption of data files of patient is on medical record, BF method is faster than AES, AES-BF but a combination is higher than AES. Results for Throughput, method of AES-is more efficiently than BF and AES, whereas AES is better than BF. The results of the comparison in the form of a graph are like in figure 5 and 6.

4. Result and Discussion

An experiment done with the platform specification intel core i5 2.5 GHz CPU, 8 Gb of RAM and is using an operating system WIN 10 64-bit from the client side, whereas the specification of the database server using Intel Xeon Processor E3-1200 v5 Series; Core i3, 64 GB DDR4 Memory with 7 operating system Centos Linux and applications are created using C # 2010.

In testing, before medical record data encryption, medical record data will be processed from a database by using query then the results will be displayed in the form of a report with the PDF format, the PDF report files in encrypted with AES and Blowfish which 256 SHA hashing functions applied for integrity. Key generation method of private and public keys using RSA and ECC method, both of these methods will be analyzed its effects on the results of the encryption based on speed and Throughput. In table 1 is a result of data encryption processes medical record of the patient, from the results of testing method of Blowfish (BF) faster than AES, this result appropriate literature, whereas AES is better than BF. The results of the comparison in the form of a graph are like in figure 1 using the method of RSA and ECC method using figure 2. Decryption process results in the method proposed can be seen in table 3 and figure 3 and figure 4 is a graphics display comparison results of both approaches duplicate medical record file into PDF format.

| File Name            | File Size (kb) | Encryption Runtime (t) |
|----------------------|----------------|------------------------|
| Medical Report 1     | 372.67         | 124.22 165.89 244.22 111.22 152.89 231.22 |
| Medical Report 2     | 367.33         | 122.44 164.11 242.44 109.44 151.11 229.44 |
| Medical Report 3     | 424.00         | 141.33 183.00 261.33 128.33 170.00 248.33 |
| Medical Report 4     | 214.67         | 71.56 113.22 191.56 58.56 100.22 178.56 |
| Medical Report ..    | 296.67         | 98.89 140.56 218.89 85.89 127.56 205.89 |

Table 3. Hybrid encryption runtime approach.
Figure 7. Graph of RSA encryption Key.

Figure 8. Graph of encryption ECC Key.

Table 4. Hybrid decryption runtime approach.

| File Name           | File Size (kb) | Decryption Runtime (t) | RSA Generate Key | ECC Generate Key |
|---------------------|----------------|------------------------|------------------|------------------|
|                     |                | BF         | AES          | AES-BF         | BF         | AES          | AES-BF         |
| Medical Report 1    | 372.67         | 135.89     | 177.55      | 255.8867      | 119.55     | 157.89      | 232.89         |
| Medical Report 2    | 367.33         | 134.11     | 175.77      | 254.1067      | 117.77     | 156.11      | 231.11         |
| Medical Report 3    | 424.23         | 153.00     | 194.66      | 272.9967      | 136.66     | 175.00      | 250.00         |
| Medical Report 4    | 214.67         | 83.23      | 124.89      | 203.2277      | 66.89      | 105.23      | 180.23         |
| Medical Report ..   | 296.67         | 110.56     | 152.23      | 230.5587      | 94.22      | 132.56      | 207.56         |

In table 4 above, is the result of the decryption process using the hybrid method of AES-BF the time where the process is higher than data encryption, but the decryption key using the private key RSA and public method It takes more than a method of ECC.

Figure 9. Graph of decryption RSA Key.

Figure 10. Graph of decryption ECC Key.

For the results of the performance in terms of Throughput shown in table 3 and table 4, Throughput Performance Analysis for the encryption process and duplicate is measured in Bits per Second. The process of encryption and decryption of data files of patient medical record, BF method faster than AES, AES-BF but a combination higher than AES. Results for Throughput, method of AES more efficiently than BF and AES, whereas AES better than BF. The results of the comparison in the form of a graph like figure 5 and figure 6.
Table 5. Hybrid encryption throughput approach.

| File Name         | File Size (kb) | Encryption Throughput RSA Generate Key | ECC Generate Key |
|-------------------|----------------|----------------------------------------|------------------|
|                   |                | BF          | AES          | AES-BF        | BF          | AES          | AES-BF        |
| Medical Report 1  | 372.67         | 403378      | 242027       | 145216        | 355922      | 213553       | 128132        |
| Medical Report 2  | 367.33         | 397598      | 238559       | 143135        | 350822      | 210493       | 126296        |
| Medical Report 3  | 424.23         | 459187      | 275512       | 165307        | 405165      | 243099       | 145859        |
| Medical Report 4  | 214.67         | 232359      | 139415       | 83649         | 205022      | 123013       | 73808         |
| Medical Report .. | 296.67         | 321116      | 192669       | 115602        | 283337      | 170002       | 102001        |

Figure 11. Graph of hybrid encryption throughput approach.

In table 3 is the result of Hybrid encrypting Throughput of medical record data of the patient, the establishment of a public key and a private key using the RSA method produces a higher computing time compared methods of ECC. Throughput results of Hybrid method AES-BF proposed better than BF and AES method, whereas the application of the private key and public key RSA method is still higher than the method of ECC it is not much different from the results of the encryption process.

Table 6. Hybrid decryption throughput approach.

| File Name         | File Size (kb) | Decryption Throughput RSA Generate Key | ECC Generate Key |
|-------------------|----------------|----------------------------------------|------------------|
|                   |                | BF          | AES          | AES-BF        | BF          | AES          | AES-BF        |
| Medical Report 1  | 372.67         | 3025335     | 2337759      | 2337837       | 2269001     | 1753319      | 1753394       |
| Medical Report 2  | 367.33         | 2981985     | 2304261      | 2304339       | 2236489     | 1728196      | 1728271       |
| Medical Report 3  | 424.23         | 3443899     | 2661195      | 2661273       | 2582924     | 1995896      | 1995971       |
| Medical Report 4  | 214.67         | 1742691     | 1346625      | 1346703       | 1307018     | 1009969      | 1010044       |
| Medical Report .. | 296.67         | 2408367     | 1861011      | 1861089       | 1806275     | 1395758      | 1395833       |

Figure 12. Hybrid decryption throughput approach.
Based on testing performed, RSA method takes computing with average time process of encryption 94.62 seconds and decryption 106.29 seconds at BF method. AES method for encryption process is 136.34 second and 147.96 seconds for decryption while the hybrid method for encryption is 214.62 second and for decryption is 226.29 second, while ECC method with encryption time is 81.62 second and Decryption is 89.96 second at BF method. Encryption of AES method is 123.36 second and 147.96 seconds for decryption while the hybrid method for encryption is 214.62 second and for decryption is 226.29 second, while ECC method with encryption time is 81.62 second and decryption is 89.96 second at BF method. AES-BF hybrid takes higher than BF and AES in which time of encryption process is 201.62 second and 203.29 to decryption process.

The value of average Throughput on testing is as shown in table 3 Encryption Throughput and table 5 Decryption Throughput, AES- BF Hybrid methods is better than BF and AES with average throughput time BF encryption is 307416 bps and decryption is 2305618 bps. The average throughput of AES encryption is 188449 bps and decryption is 1781614 bps and AES-BF hybrid encryption is 110670 bps and decryption is 1781692 bps on RSA method. While the average ECC method of throughput BF method for encryption is 271249 bps and decryption is 17281692 bps. The average throughput of the AES encryption is 162749 bps and decryption is 1336210 bps and AES- BF hybrid encryption is 97650 bps and decryption is 1336285 bps.

5. Conclusion
Our primary goal in this study is to analyze the generation performance of public and private key at RSA and ECC method to secure the patient's medical report data in the form of a PDF file that sourced from a database. From the testing results, ECC method is faster than RSA method as shown in tables. Table 1 is comparison of encryption processing time and table 2 is comparison of decryption processing time on BF, AES and AES-BF hybrid method. Thus it can be drawn as the conclusion of ECC method which gives highest strength per bit of any crytosystem with the smaller size of the key by generating a faster calculation, power consumption and low memory, it also provides a methodology to get protocol implementation and high speed key authentication, efficient and measurable.

References
[1] Rani R, Sharma G, 2017, “Review Paper on Data Hiding In 3D Barcode Image Using Steganography”, International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017, 2271—2276, ISSN No. 0976-5697
[2] Ghodke M, Mali N. 2016, FPGA Based network security using cryptography. International Research Journal of Engineering and Technology. 3(3):469–71
[3] Bhuvaneshwari M, Tenmozhi S. 2016, “A VLSI architecture for security based stenographic processor with AES algorithm”. International Journal of Electrical and Computer Engineering; 1–6
[4] Sukhraliya V, Chaudhary S, Solanki S. 2013, “Encryption and decryption using ASCII values with substitution array approach”. International Journal of Advanced Research in Computer and Communication Engineering. 2(8):3094–7
[5] A. P Shaikh, V. kaul, 2014, “Enhanced Security Algorithm using Hybrid Encryption and ECC”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3; PP 80-85
[6] Garg SK. 2014, “Modified encryption and decryption using symmetric keys at two stages: Algorithm SKG 1.2”. International Journal of Advanced Research in Computer Science and Electronics Engineering. 4(6):778–80
[7] M Enriquez, D W Garcia and E Arboleda, 2017, “Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA and ElGamal Cryptosystems”, Indian Journal of Science and Technology, Vol 10(27), DOI: 10.17485/ijst/2017/v10i27/105001. 1-4
[8] Ch.Vijayalakshmi, L.Lavanya, Ch.Navya, 2016, “A Hybrid Encryption Algorithm Based On AES and RSA, International Journal of Innovative Research in Computer and Communication Engineering”, Vol. 4, Issue 1, 909-917
[9] K G Kadam and V Khairnar, 2015, “Hybrid RSA-AES Encryption for Web Services, International Journal of Technical Research and Applications”, Special Issue 31(September, 2015), PP. 51-56

[10] B Kumar, J Boaddh and L Mahawar, 2016, “A hybrid security approach based on AES and RSA for cloud data, International Journal of Advanced Technology and Engineering Exploration”, Vol 3(17), 43-49

[11] Palanisamy, V. and Jeneba Mary, A, 2011, “Hybrid Cryptography By The Implementation Of RSA and AES, International Journal of Current Research”. Vol. 33, Issue, 4, pp.241-244.

[12] S.N.Ghosh, et al. 2015, “Performance Analysis of AES, DES, RSA And AES-DES-RSA Hybrid Algorithm for Data Security”, International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 5, 83-88

[13] J R Patel, R S. Bansode and V Kaul, 2012, “ybrid Security Algorithms for Data Transmission using AES-DES”, International Journal of Applied Information Systems (IJIAS), Volume 2–No.2, 15-21

[14] R Behl, G Sehgal, M Kumar, P Gupta, S Garg, 2015, “Experimental comparison between Hybrid RSA-AES and RSA algorithms in IP security”, IJMTER, 588-594

[15] Por, L. Y., Beh, D., Ang, T. F., Ong, S. Y., 2013, “An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm”, The International Arab Journal of Information Technology, Vol. 10, 51-60

Acknowledgments
This research was supported by Universitas Prima Indonesia, Universitas Harapan Medan, Indonesia and one of private hospital in Medan city.