Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Health-chat App: Secured Patient's Health Information App-based (SPHIA) using Integrated Data Encryption Algorithm (IDEA)

Christine Charmaine G. San Jose[1]
[1] *Isabela State University, CCSICT Echague Campus, Philippines, christinecharmaine.g.sanjose@isu.edu.ph*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The era of the digital landscape had caused evident progress, unfortunately this also became an avenue for untoward activities such as data breach, data manipulation, hacking and others. The Philippine Government had already enacted and promulgated numerous Laws that protects the rights of every individual, and one of this is the Data Privacy Act of 2012. This act protects the health data and is considered as sensitive personal information that penalizes Institution in the event of leakage of such information.

To resolve this pressing concern, the Health-chat App Mobile application was developed to safeguard patient's health information. The Integrated Data Encryption Algorithm (IDEA) is the merging of two strong algorithms, the Data Encryption Standard (DES) and Blowfish algorithm to protect sensitive information on health. The IDEA displays strength on its security with the calculated avalanche effect of 52.41% as compared when the original algorithm was used.

Based on the result, the application is a new platform that can be used to safeguard health sensitive information that protect and uphold the individual's right to privacy.

Keywords: Data Encryption Standard, Blowfish Algorithm, Avalanche Effect, Security, Data Privacy

INTRODUCTION

In the era of e-commerce, information has become a valuable commodity [1]. A study by The Economist indicates that data or information is the most crucial and valuable asset in today's digital landscape. The challenge of safeguarding information from cybercriminals is a significant concern for both online businesses and government entities. An effective security strategy has proven to be dependable in maintaining the integrity and safety of information.

The Philippine Government though the National Privacy Commission has been vigorous on the implementation of the Republic Act (R.A.) 10173 which was well known as the Data Privacy Act of 2012 [2]. As a proof to this, Institutions are compelled to designate its Data Protection Officer (DPO) that supervises and monitors the adherence of this Act.

Research on the International Journal for Computer Applications addresses the ethical and legal considerations surrounding medical data mining. The mining of healthcare-related data represents both a highly beneficial and a complex field within the realm of data mining and knowledge discovery. Medical datasets play a crucial role in medical research. Ethical issues, particularly those related to confidentiality, have led to the establishment of strict regulations in this type of research. The advantages and disadvantages of these new regulations are being discussed globally. The implementation of regulations requiring individual informed consent will be expensive for physicians. Efforts are underway to reach a consensus that adequately addresses ethical concerns while still promoting research [3].

For healthcare professionals, public health authorities, and policymakers, maintaining secure records poses a significant challenge. Measures such as the application of cloud storage, strong password protection, and encryption are options that healthcare providers can implement to enhance the security of portable electronic health records.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

One survey conducted by [4] revealed that 73% of doctors communicate via text with other physicians about work-related matters. However, mobile devices are susceptible to being lost, damaged, or stolen. It is crucial to emphasize the need for encrypting mobile devices that are used to send confidential information.

The Integrated Data Encryption Algorithm (IDEA) is an integration of two well-known algorithms, the DES (Data Encryption Standards) and Blowfish Algorithm. The integration of the two algorithms displays a strong security characteristic which is evident in the calculated avalanche effect. The IDEA Algorithm will be used to encrypt and decrypt the message sent by Medical Practitioners.

This paper is geared towards development, integration and security evaluation of Health-chat App: A Secured Patient's Health Information App-based (SPHIA) using Integrated Data Encryption Algorithm (IDEA). The study focuses on Mobile-app SPHIA (Secured Patients Health Information App) and integration of IDEA Algorithm (Integrated Data Encryption Algorithm).

The health-chat App is a mobile application that allows the users particularly Medical Doctors and Staffs to exchange communication in a secured environment. Messages sent on the system are encrypted and can only be readable once the receiver of the message will decrypt the message after supplying the correct password to the application.

IDEA-SPHIA ARCHITECTURE

The figure below shows the procedure in realizing the project. The developed IDEA algorithm will be integrated to the developed SPHIA mobile application. The system will be used to secure patients' health information through exchange of communication among Physicians and Medical Staff of a hospital.

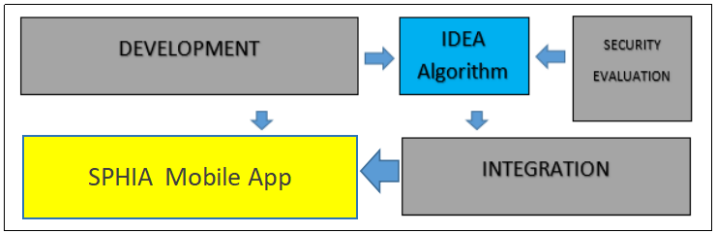

Figure 1. *IDEA-SPHIA Architecture*

IDEA Algorithm

The Figure 2 shows the IDEA Algorithm Structure. The algorithm composed of the merging of two strong Algorithm: The Data Encryption Standard and Blowfish Algorithm.

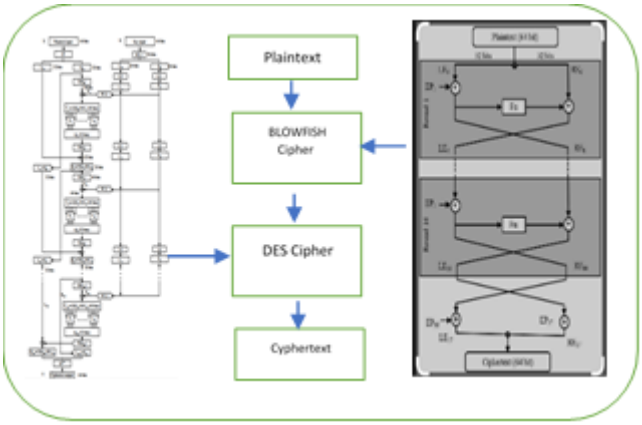

Figure 2. *IDEA Algorithm Structure*

Blowfish Algorithm

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Blowfish algorithm was designed by an American Cryptographer, Bruce Schneier in the year 1993. The algorithm he designed is a symmetric block cipher that replaces the outdated Data Encryption Standard. The blowfish processes using 64-bit variable length symmetric block cipher. The algorithm was unpatented and can be freely used by anyone [5], [7]. The computation involved in the blowfish as shown below consist of the following: a) Blocksize: 64-bits, b) Keysize: 32 bits, c) Number of Subkeys: 18 [P0 - P17], d) Number of Rounds: 16 and e) Number of Substitution Boxes: 4

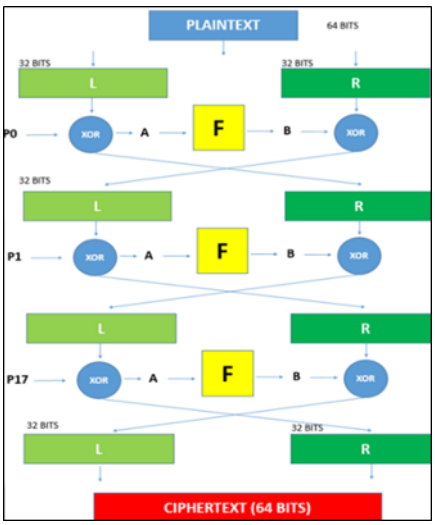

Figure 3. *Blowfish Cipher Architecture*

32-bit hexadecimal representation of initial value of sub-keys

P[0]	:	243f6a88	P[9]	:	38d01377
P[1]	:	85a308d3	P[10]	:	be5466cf
P[2]	:	13198a2e	P[11]	:	34e90c6c
P[3]	:	03707344	P[12]	:	c0ac29b7
P[4]	:	a4093822	P[13]	:	c97c50dd
P[5]	:	299f31d0	P[14]	:	3f84d5b5
P[6]	:	082efa98	P[15]	:	b5470917
P[7]	:	ec4e6c89	P[16]	:	9216d5d9
P[8]	:	452821e6	P[17]	:	8979fb1b

Figure 4. *Blowfish Eighteen Sub-keys [P0...P17]*

The F function on Figure 5 simply divides the 32 bits into four equal parts consisting of 8 bits per Sbox (Sbox1..Sbox4). Operation such as XOR and addition of bits is performed to the four Sboxes and concatenation of the result to form 32 bits value of B.

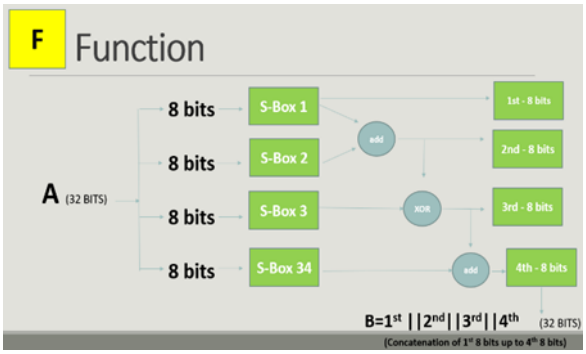

Figure 5. *The Function "F" Process*

DES Algorithm

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Data Encryption Standard was officially developed in 1976 and was used for nearly 18 years. It was the most popular encryption technique because of its robust internal design. The DES algorithm was then replaced by Advanced Encryption Standard (AES) in 2001. Numerous enhancements to the algorithm were conducted to improve DES [8], [9]. This enhancement resulted to a more secure DES algorithm.

DES Algorithm is considered as a block cipher, it operates on plaintext consisting of 64 bits per block and will produce a 64 bits ciphertext [6]. Suppose a plaintext: ISUECCSICT is to be encrypted using DES algorithm, the first step is to substitute the plaintext to its hexadecimal value using the ASCII CODE such that the plaintext I=49, S=53, U=55, E=45 until the last letter of plaintext T=54. After substitution to hexadecimal, each value will be converted to its Binary Digit then the next process is for the first 64-bit block to undergo the Initial Permutation using IP Table shown on Figure 6. The table 1 illustrates how plaintext is being processed using the ASCII Code.

Table 1. *Simulation of Plaintext using DES Algorithm*

Plaintext	**I**	**S**	**U**	**E**	**C**	**C**	**S**	**I**	**C**	**T**
Hexadecimal value using ASCII CODE	49	53	55	45	43	43	53	49	43	54
Binary Digit	0100 1001	0101 0011	0101 0101	0100 0101	0100 0011	0100 0011	0101 0011	0100 1001	0100 0011	0101 0100

Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	51	41	33	25	17	9	1
59	53	43	35	27	19	11	3
61	55	45	37	29	21	13	5
63	57	47	39	31	23	15	7

Figure 6. *DES Initial Permutation (IP) Table*

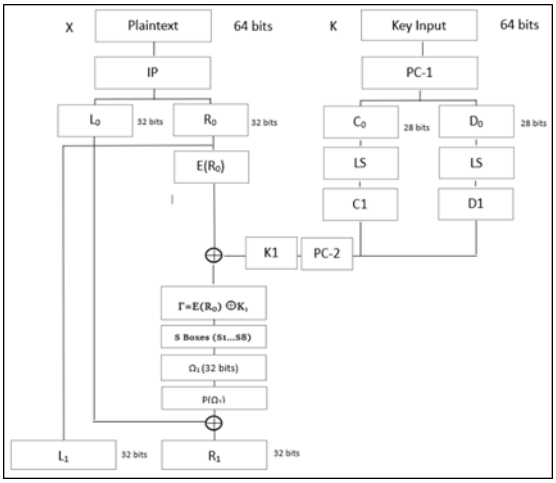

Figure 7. *DES Computational Structure for first level of L_0, R_0*

Several computations as shown on Figure 7 will be performed for the Data Encryption Standard (DES) algorithm.

RESULTS AND DISCUSSION

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SPHIA Application

One of the Software used to develop the SPHIA App is the Android Studio, it is the official integrated development environment for Android operating system for google. Another example is Kotlin, a contemporary and well-established programming language designed to simplify developers' tasks. It is known for being concise, secure, and compatible with Java as well as other programming languages.

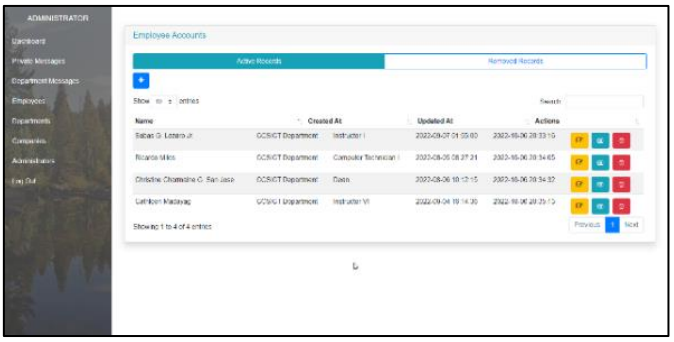

Figure 8. *SPHIA Admin Dashboard*

The figure shows the Dashboard where the admin has the capability to view and access the different menus, manage users account and manage record.

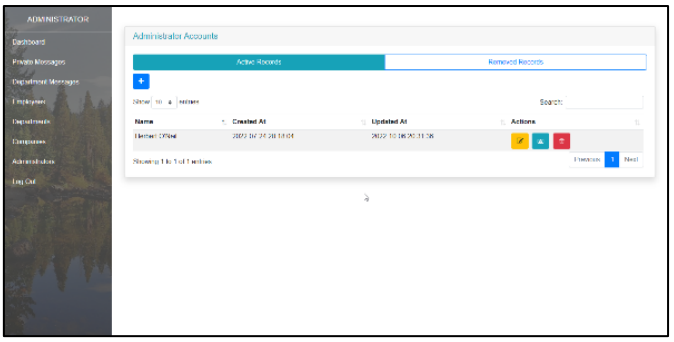

Figure 9. *Manage Record*

The figure shows the page where the admin could manage record of the users of the system. It has the capability to add, update, delete and save records.

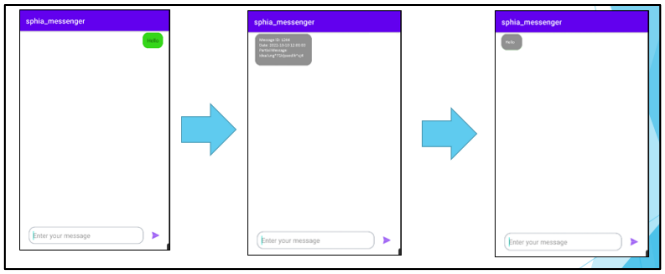

Figure 10. *Encryption/ Decryption Message*

The figure shows the encryption and decryption process where the IDEA Algorithm has been incorporated to the system. It is a platform that exchange of messages is encrypted and is hidden to any intruder. This process safeguards the confidentiality of the messages among employee that includes the Medical Doctors, Nurse, Staff of the Agency.

Security Evaluation of IDEA Algorithm

The result of the security evaluation conducted shows that the IDEA Algorithm through the integration of DES and Blowfish algorithm is more secure through the computation of its avalanche effect as shown in Table 4 with a mean

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

value of 52.41 as compared when this algorithm was individually used as shown on Table 2 and Table 3 with a mean value of 49.05 and 47.01 respectively.

Table 2. *DES Avalanche Effect*

Plaintext 1	*Plaintext 2*	*Key*	*Ciphertext 1*	*Ciphertext 2*	*Avalanche Effect*
The Quick Brown Fox Jumps over the Lazy Dog	the quick brown fox jumps over the lazy dog	TQBFJOTLD	74d87aac5df1504a436ae20f8fba88f06a6390902528f152ff1a68b214fc4c19a51f8695076a0009d47cd0ca55adc426	b98f77eaeddbb9fdd529a3de05ff84a1f0579ed5086cfa8af254ed66ba6c60a92caa575548eac440b36593e2706d4990	42.45
CCSICT	ccsICT	ICT	03763d0937e3a509	3c2b11d59665d277	53.13
Hello World!	hELLO wORLD!	PROGRAMMER	a461ff3ea2ea4357e91195532653ec7f	6bb25695a8b3bac6974f429b182d1ab9	51.56
				MEAN	**49.05**

Table 3. *Blowfish Avalanche Effect*

Plaintext 1	*Plaintext 2*	*Key*	*Ciphertext 1*	*Ciphertext 2*	*Avalanche Effect*
The Quick Brown Fox Jumps over the Lazy Dog	the quick brown fox jumps over the lazy dog	TQBFJOTLD	cbffa58b1d9750541f39e580053e43f90e3019cad77d9b2d5a9fe12c4d6eb2b1de80882a48f5ac2c6467861aaf84d4ed	d8ac05bdb18551da95b95a28d824e4aa09310b6deddff0595a9fe12c4d6eb2b1a5c1c14333f907047ae53589206a59c1	28.52
CCSICT	ccsICT	ICT	219b773ebf58d7d1	3c2b11d59665d277	59.38
Hello World!	hELLO wORLD!	PROGRAMMER	d62f18318f42221d0df88626ddef2140	5ab657c87f20d010c5c6798a7e6690f2	53.13
				MEAN	**47.01**

Plaintext 1	*Plaintext 2*	*Key*	*Ciphertext 1*	*Ciphertext 2*	*Avalanche Effect*
The Quick Brown Fox Jumps over	the quick brown	TQBFJOTLD	6AEBA2C0BDFE67DC4DD01E3827F5E554938742973AA	9B61B59463B70BAE96B67860A90E5F301C836CBA3A37	52.15

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the Lazy Dog	fox jumps over the lazy dog		14856505433EDAA0C621AD9137C53FD91B098BFE59A944BC3106BAEF955AFB1438AF3A1DADA7466E9528AA9D9B1391246A02166A8854D366DE49ABBFE6F91BF11B49F95D566BC76372D3F3AABB461B3BEEDDC	60396DD540DCE103380A4511D9362686E2EC5AB0BA3BD9F9A590C91FBBA3C611BF72654405684099204D58E8F292E525AB5B5F2B7405FB0CBD9221B1DFCC2CCBB50454F14ED635B95171CFB32D00606A712D	
CCSICT	ccsICT	ICT	5D3377782C8C844AE6B9F0F6E4620ED81107582OA6BCCFD1	B1BEBB25DE261A4D76979511CCFB41BBBAF13E558F534934	53.12
Hello World!	hELLO wORLD!	PROGRAMMER	751CFF62792055E9D478BEA0EF6A928BACAA6C33B0C1C0E951029A9D3E64A23D27A8A51BC5C2DCA9	1105BA2E485623E2D0F553B200D76FC774908C4E9AAE47FC1D8298D85810939E0E51A0FAE5C48F61	51.97
				MEAN	**52.41**

Table 4. *IDEA (Integrated Data Encryption Algorithm using DES and Blowfish)*

CONCLUSION

The Health-chat App was developed to primarily address the foregoing problems on patients medical health record from misuse by safeguarding communications through the use of encryption on mobile application. The encryption algorithm used is the Integrated Data Encryption Algorithm (IDEA) which is the merging of two famous algorithms, the DES Algorithm and the Blowfish Algorithm. The algorithm displays strong security which is evident in the calculated Avalanche Effect. This algorithm was successfully integrated into the developed mobile application - SPHIA (Secure Patients Heath Information App). The SPHIA is a mobile application which was developed using several software such as Visual Studio Code, Android Studio and Kotlin. The system consists of two privileges for users such Admin that is capable to Manage Account and Manage Record while the Employee has the capability to access the system through log-in window, send and receive encrypted messages and decrypt messages.

The IDEA algorithm was also evaluated in terms of its security by calculating its avalanche effect. Based on the result, the IDEA produced a higher avalanche effect as compared when this algorithm was individually used.

This new platform addresses the problem on the confidentiality of the messages sent online. Messages are encrypted and decrypted, this means that exchange of messages among Medical Doctors, Medical Staff and Nurses are hidden from intruder. Moreover, this application is applicable to any agency where there is high value on confidentiality of exchange messages on everyday transaction.

REFRENCES

[1] Snow, G.M., (2011) NCJRS, National Criminal Justice Reference Service, Administered by the Office of the Justice Programs, U.S. Department of Justice. https://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

[2] National Privacy Commission, Implementing Rules and Regulations of Republic Act No. 10173, Also Known as the "Data Privacy Act of 2012", https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[3] Ghosh, S., Bhuiyan, T., Jabiullah, I., (2019) “A Steganographic Apps-based Patient‟s Information Encryption-Decryption”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8, Issue-2S6.
[4] Poissant, L., Pereira, J., Tamblyn, R., Kawasumi, Y., (2005), The impact of electronic health records on time efficiency of physicians and nurses: A systematic review. J Am Med Inform Assoc.
[5] Schneier, B., (1994), “Description of a new variable-length key, 64-bit block cipher (Blowfish),” in Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., Proceedings, R. Anderson, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 191–204.
[6] Rhee, M., (2003), Internet Security, Cryptographic principles, algorithms and principles, pp.149, John Wiley & Sons, Ltd ISBN 0-470-85285-2
[7] Quilala, R., Sison, A., & Medina, R., (2018), Enhanced Blowfish Algorithm, Indonesian Journal of Electrical and Computer Science, 2018
[8] Amorado, R., Sison, A., Medina, R., (2019), Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques, 2nd International Conference on Information Science and Systems, Page 252-256
[9] Ozkaynak F., Muhamad, M.I., (2018), "Alternative substitutional box structures for DES," 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1--4.