Stochastic Approach in Government Service and Transactional Management Using Two-Tier Encryption-Decryption Process

Francis S. Cambaya and Albert A. Vinluan

***Abstract*—The Stochastic Approach in Government Service and Transactional Management Using Two-Tier Encryption-Decryption Process is designed to provide an undeterministic approach in performing encryption using Blowfish and Andvance Encryption Standard. With the help of stochastic methods namely: Poisson, Drunkards Walk and Queue, a tool for computing the cryptographic protocols to be used were developed during the process. To validate the cryptographic method to ensure security and performance for encryption and decryption, the study conducted test through visualization and experimental attacks on both AES and blowfish. The attacks are used are Scytale ciphertext-only attack, avalanche effect and Vigenère Analysis. The AES and blowfish visualization as well as the attacks were accomplished using CrypTool 2.1. Authentication and access control was applied in the developed encrypting file system through the development of a web-based application using Java. The IDE used was Netbeans 8.2. The combined use of user credentials and file encryption/decryption framework was able to implement authentication and access control in the process of government services and transactional management system.**

***Index Terms*—Stochastic encryption, two-tier encryption-decryption, cryptography.**

I. Introduction

The advent of computing technology becomes the antecedent of the migration of paper based to digital transformation of information. With the consistent growth of the use of internet across the globe, one of the major concerns in the digital world is security [1]. Cryptography deals with constructing and analyzing protocols that prevent unwanted third parties or the public from reading private messages. It was developed to provide security for the senders and receivers to confidentially transmit and receive data through public channels through a process called Encryption/Decryption [2].

In the early years of modern digital age, cryptography was considered synonymous with encryption [3]. Encryption is the conversion of information from a readable state to non-readable state or a seemingly nonsense message [4]. In encryption, the source of an encrypted message shares the decoding technique needed to recover the sent message only with intended recipient in order to prevent unwanted persons from doing the same [5]. An encryption process transforms original plaintext information into an unreadable data called ciphertext so that only the person who has the secret key can access the original information [6].

The Philippines, based on various cybersecurity reports, may not be as prepared compared to other countries. In 2017, the country ranked 10th among Asia Pacific countries when it comes to cybersecurity readiness, according to the Global Cybersecurity Index (GCI). The Philippines took the 37th spot out of 233 countries prone to cybersecurity threats – a huge jump from the previous quarter's 43rd rank [7]. In its ICT Manifesto for the Philippines for 2016 and Beyond, Microsoft pointed out the need for teamwork between the industry and government agencies to enhance cyber security [8].

In this study, the researcher decided to choose the Police Files of all police precinct and sort out what are those files that needs proper encryption-decryption process before transmission due to its vulnerability. The pacific towns of Southern Leyte are composed of nine (9) municipalities with their corresponding police precinct. It is therefore necessary to have strong security protocols to protect these messages from attackers and to guarantee authentication, confidentiality and data integrity [9]. Cryptographic techniques should be used to increase the confidence of users to use such computer networks. Several cryptographic techniques are developed for achieving secure communication [10]. Specifically, this study answered the following problems:

- What parameters can be used to develop the stochastic approach of government services and transactional management using two-tier encryption-decryption process in government services?
- How can randomize selection algorithms and encryption/decryption techniques be used in designing a stochastic approach in two-tier encryption/decryption process model?
- How to validate the cryptographic method to ensure security and performance for encryption and decryption?
- How to apply authentication and access control in the developed encrypting file system?

II. Methods

The Stochastic Approach in Government Service and Transactional Management Using Two-Tier Encryption-Decryption Process was conceptualized by utilizing the descriptive and experimental methods of research design to gather information about the present system for transactional management of the Police Station in the pacific towns of Southern Leyte.

Manuscript received May 21, 2019; revised July 12, 2019.

Francis S. Cambaya and Albert A. Vinluan are with the School of Graduate Studies, AMA University, Quezon City, Philippines (e-mail: bhorjs@gmail.com, aavinluan@neu.edu.ph).

A. Parameters Used in Stochastic Approach

Stochastic approach in programming is a framework for problems that involve uncertainty [11]. Random number generator in Java programming language was used to implement the stochastic approach in choosing between the three (3) random probability algorithms. The current date and time when the file is uploaded by the user for encryption are the variables used. The part of the date variable used for the random number generator is the day implicitly converted into integer. The time variable in the input would be accepted but only the time in terms of seconds would be used in the stochastic approach during the 1st tier. The day of the month is the part of the variable date used when Poisson distribution is triggered.

An integer from the time in seconds variable ranging from 0 to 59 will be randomly selected. The time in seconds is used so the program can choose between Poisson, drunkards walk and queue. These three stochastic processes are shuffled every time sending a file for encryption is invoked. The Poisson distribution needs two (2) inputs to generate a Poisson random variable. The inputs for the Poisson distribution are time in seconds and day of the month in date variables. The Poisson random variable is used in randomly choosing between AES or BlowFish encryption algorithms. The output of Queue is either zero (0) or one (1). The output of the Drunkard's Walk is either left or right which will also be converted to either (0) or one (1). The outputs of both Queue and Drunkard's Walk will also be used in stochastically implementing either AES or BlowFish.

B. Random Probability and Encryption/Decryption Algorithms

Poisson distribution [12] helps in describing the chances of occurrence of several events in some given time interval or given space conditionally that the value of average number of occurrence of the event is known. The number of successes that are resulting from a Poisson experiment is termed as a Poisson random variable [13].

The following is the formula for the Poisson Distribution used for the computation of Poisson probability:

$$P(X, \mu) = \frac{(e^{-\mu})(\mu^{x})}{x!}$$

where:

e : this is a constant whose value is equal to 2.71828 approximately. Basically, it is the base value of the system of natural logarithm.

μ : it is the mean value of the number of successes that are occurring in the region specified.

x : it is the actual number of the successes that are occurring in the region specified.

P (x, μ) : it is the probability or we can say the Poisson probability of the condition of occurrence of exactly 'x' number of successes in the conducted Poisson experiment, when it is given that the mean value of the number of occurring successes is μ.

A drunkard or random walk is a mathematical object, known as a stochastic or random process that describes a path that consists of a succession of random steps on some mathematical space such as the integers [14]. It assumes:

• Probability of a left-step (tails) is q

• Probability of a right-step (heads) is p

where $p + q = 1$

Consider a walk which consists of a total of n steps or turns. Let X be a random variable whose value, r, is the number of those n steps which are to the right. Given a total of n steps, each of which has a probability p of being a right-step, the probability of there being r right-steps is given by the Binomial distribution [15]:

$$P(X = r) = \binom{n}{r} p^r q^{n-r}$$

Queue is a kind of abstract data type or collection in which the entities in the collection are kept in order and the principal (or only) operations on the collection are the addition of entities to the rear terminal position, known as enqueue, and removal of entities from the front terminal position, known as dequeue [16]. Queueing theory is results are often used when making decisions about the resources needed to provide a service. In this case, the said service is which encryption algorithm to use.

C. Encryption Algorithms

The type of encryption as to Blowfish or AES is decided only upon the result of any of the stochastic process using Poisson distribution, Drunkard's Walk and Queue. Each of the three-stochastic procedures has their own rules to be applied as to how a certain data will be encrypted.

AES is an encryption standard that replaced DES in 2001 [17]. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. In the encryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final ciphertext [18]. Figure 1 shows the AES flowchart and discussed in the proceeding pseudocodes. For both encryption and decryption, the cipher begins with an AddRoundKey stage.

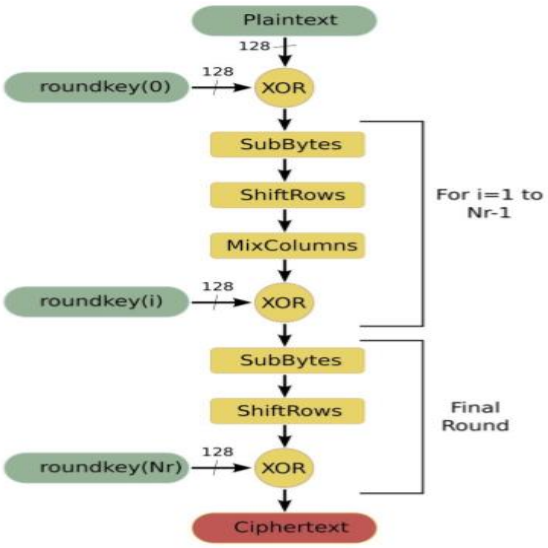

Fig. 1. AES flowchart.

Blowfish symmetric [19] block cipher algorithm encrypts block data of 64-bits at a time. The algorithm follows fiestal network [20] and is divided into two main parts. The first part is key-expansion. Before proceeding to any encryption, these keys should be computed. The second part is data encryption.

The p-array consists of 18, 32-bit sub-keys: P1, P2, P18.

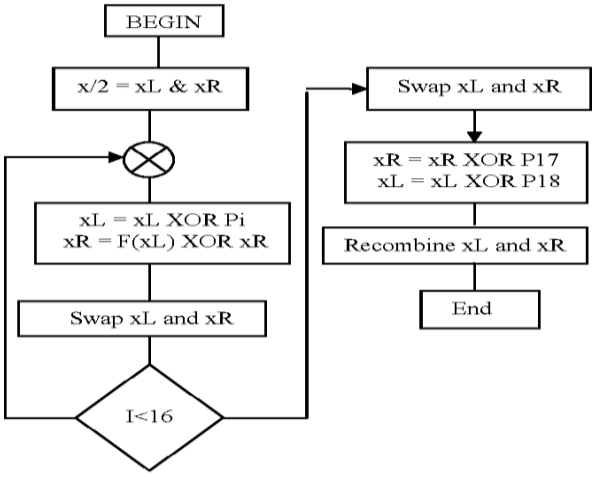

Fig. 2. Blowfish flow chart.

Fig. 2 shows the blowfish flowchart. P-array and then the four S-boxes, in order, with a fixed string. It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

The developed system itself handles the automatic decryption of specific file. The issue as to how can the algorithm automatically detects or determines what kind of encryption used and the key associated with it is solved through a control module embedded on the software design.

D. Validating Security and Performance

The researcher conducted experimental research in the validation of security and performance. CrypTool 2.1 was used as a third party analysis for the experiment. Blowfish and AES simulation were used to validate the performance of both algorithms. For the security of the algorithms, Avalanche Effect Visualization, Scytale ciphertext-only attack and Vigenère Analysis (attack) were conducted.

E. Authentication and Access Control

The researcher described the characteristics of the developed system through creation of diagrams, pseudocodes, system screen shots and program outputs. The system was used to generate actual user authentication through human-to-computer interactions. Credentials provided by the user are compared to those on file in a database of authorized users' information both on the local operating system and through a cloud server. If the credentials match, and the authenticated entity is authorized to use the resource, the process is completed and the user is granted access. The study used the Dynamic System Development Methodology throughout the course of the system development. DSDM is an agile project delivery framework, initially used as a software development method. DSDM is one of several Agile methods for developing software and non-IT solutions, and it forms a part of the Agile Alliance. The Dynamic Systems Development Method provides a framework of controls and best practice for Rapid Application Development (RAD).

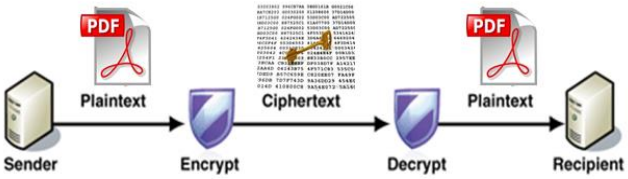

Fig. 3. System architecture.

After the business requirements are specified at a high level and the information requirements out of the system are identified. Once this is done, the basic architectural framework of the desired system is prepared. Figure 3 shows the system architecture. This guided the researcher in the development of the system anchored with the requirements of the locale.

III. RESULTS

A. Parameters Used in Stochastic Approach

Stochastic approach uses mathematical programs where some of the data incorporated into the objective or constraints is uncertain. The stochastic programming that the researcher implemented used unknown numbers but probability distribution is present.

A user has no definite time and date of using the encryption program since duties in a police station may be at any time. The time in seconds and the day of the month in date are parameters actually used in program. The said parameters set uncertainties but still set ranges. The possible range values for day of the month are between 1 to 31 while the range values for the seconds in time are between 1 to 60. The current date and time when the file is uploaded by the user for encryption are the variables used. The part of the date variable used for the random number generator is the day implicitly converted into integer ranges values from 1 to 31. The time variable in the input would be accepted but only the time in terms of seconds would be used in the stochastic approach for the 1st tier. The seconds have values ranging from 1 to 60.

The number of seconds determines the number of times that Poisson distribution, drunkard's walk and queue is shuffled. When the number of shuffles had been accomplished, an output between 1 to 3 representing the three (3) random probability algorithms would be determined.

For the Poisson distribution, day and seconds as inputs would yield an output parameter between 1 to 100. Using the Poisson random probability algorithm, an output between 1 to 50 selects blowfish for encryption while and 51 to 100 selects AES.

For the drunkard's walk random probability algorithm, a loop would be performed. The number of the loop's recursion is dependent on the seconds input. The output of this stochastic approach is either 0 or 1. If the output is 1, then AES is invoked and 0 is for blowfish.

For the queuing stochastic approach, the day and the seconds serve as inputs. The out of the algorithm is either 0 or 1. AES is used when the output is 1 and blowfish if the output is 0.

For the number of shuffling to always be more than five

(5) times, the program determines if day is <= 5. If day it is less than 5, the system implicitly return a value parameter of 5. If second is < day, then second is set to be the same as day.

The 1st tier of the government services and transactional management system is bounded up to the point when an output to choose between AES or blowfish had been established. The 2nd tier involves the implementation of either AES or blowfish in encryption and / or decryption.

B. Random Probability and Encryption/Decryption

From the assumed variables on the previous discussion, the probability of choosing (1)AES or (2)Blowfish is dependent on the percentage generated from the formula P (x, μ). Where:

e : receives a random value (numeric date)
d : receives a random value (time in seconds)

Such that: P (x, μ) = x as e; and μ = d

Using range, we created a lower and upper limit of *t* and *d*.

t (0 - 50%)
b (51 – 100%)

The researcher tested the source code using python codes. The result randomly changes depending on the time_rate variable which directly proportional to d. Based on the first run where time_rate is equal to 60 the result is 66.37 or 66 percent which belongs to b (upper limit).

Given d and e such that:

- The sum of *d* and *e* <= 31 but > 5
- Let 0[left], and 1[right], then we can say that left = *t* and right = *b*.
- From the result found, the last digit that occur is any of the variables (*t, and b*) which represents the encryption process.

Considering the randomized variables, namely, the day and seconds, the clock ticks 60 times in a minute and is captured during the process. While the date remains' constant for the entire day otherwise it changes on the succeeding days. The enqueue is dependent on the numeric equivalent of day in date while the process of dequeuing is dependent on the time in seconds captured. The following conditions are set to minimize any unexpected event, assume that e is the numeric date, d is the seconds, *a* is AES and b is blowfish:

- If *e* is less than 5 then *e* = 5, such that *e* is the number of randomized occurrences of *a* and *b*. The number of enqueue is dependent on *e*.
- If *d* is <= 0 then *d* = 5 which represents the process of *dequeuing e*.
- If *d* is greater than *e*, then *d* is always dependent to *e*. Otherwise *d* = 31.

The last to came out from the queue (*a, b*) is the candidate for encryption process.

For the 2nd tier, the type of encryption as to Blowfish or AES is decided only upon the result of any of the stochastic processes using Poisson distribution, Drunkard's Walk or Queue. Each of the three stochastic procedures has their own rules to be applied as to how a certain data would be encrypted.

The program written in Java generated an AES encryption algorithm that supports any combination of 128 bits key length of 128. In the encryption process, AES system goes through 10 rounds for I28-bit keys. Blowfish (Ashchenko, 2002) is a symmetric block cipher. It encrypts blocks of 128 bits and can operate with key sizes of 128, 192 or 256 bits. It belongs to the class of Feistel ciphers and it passes through 16 rounds. The process of decryption is very straightforward. The developed system itself handles the automatic decryption of specific file. Once the appropriate algorithm of either AES or Blowfish had been matched with the file, then the decryption process will take place yielding a plaintext in PDF file format as output.

C. Validating Security and Performance

The researcher used CrypTool 2.1 to conduct experiments for the validation of security and performance. Blowfish and AES simulation as well as the attacks simulation were used to validate the performance of both algorithms. Table I indicates the features and performance details of AES and blowfish.

TABLE I: FEATURES OF AES AND BLOWFISH

Features	AES	Blowfish
Creator	Joan Daeman, Vincent Rijmen in 1998	Bruce Schneier in 1998
Algorithm Structure	Substitution, Permutation Network	Feistel Network
Block Size	128 bit	64 bits
Rounds	10, 12, 14	16
Key length	128, 192 or 256 bits	32 bits to 448 bits
Computational Speed	Fast	Very Fast
Tunability	No	Yes
Encryption time	High	Very High
Decryption time	High	Very High
Memory Usage	Medium	Very Low

It is evident from Table I that Algorithmic structure of Blowfish is Fiestel Network developed by Cryptography researcher Horst Feistel (Mushtaque, 2004). The analysis shows that in case of symmetric algorithms, Blowfish is considered more secured than AES. Blowfish is able to provide long term data security without any backdoor vulnerability or ability to reduce the key size. In case of performance aspects, Blowfish is better. The confidentiality of Blowfish is high as compared to AES. Blowfish is tunable and encryption/decryption throughput is high as compared to AES algorithm. To further validate security of the blowfish and AES algorithms, Avalanche Effect Visualization, Scytale ciphertext-only attack and Vigenère Analysis (attack) were conducted. Using the ciphertext generated using blowfish and AES, the researcher invoked the Scytale Ciphertext-Only Attack. The generated decrypted ciphertext was not able to produce any readable form of the message. Both the blowfish and AES ciphertext was not properly decrypted using the said attack. Not even any part of the message falls into any dictionary word. The Vigenère analysis is a ciphertext-only attack that uses polyalphabetic substitution. Not even a single character between the actual key and the best key produced is the same.

D. Authentication and Access Control

The system generated actual user authentication through human-to-computer interactions. An actual user can be mapped to other abstract user object in the system, and therefore be granted rights and permissions to the user and user must give evidence to prove his identity to the system. Access control is a process by which users are granted

access and certain privileges to systems, resources or information. In the access control of the developed system, the users must present credentials before they can be granted access.

REFERENCES

[1] S. Ranger, "The undercover war on your internet secrets: How online surveillance cracked our trust in the web," *TechRepublic*, 2015.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Chapman and Hall/CRC Press, 2014.

[3] O. Goldreich, *The Foundations of Cryptography*, vol. 2. Cambridge University Press, 2004.

[4] J. Gannon, *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington, D.C., Brassey's, 2001.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Prentice Hall, 2013.

[6] S. Saraireh, M. Saraireh, and Y. Alsbou, "Secure image encryption using filter bank and addition Modulo 28 with exclusive OR combination," *International Journal of Computer Science and Security (IJCSS)*, vol. 7, no. 2, 2013.

[7] Global Cybersecurity Index (GCI). *International Telecommunication Union*, Switzerland Geneva, 2017.

[8] K. LaCapria, *Anonymous 'Day of Rage' Protests*. [Online]. Available: www.snopes.com/news

[9] P. Révész, *Random Walk in Random and Non-random Environments*, 3rd ed. World Scientific Pub Co. 2013.

[10] V. Agrawal, S. Agrawal, and R. Deshmukh, "Analysis and review of encryption and decryption for secure communication," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, no. 2, 2014.

[11] M. Talagrand, "Upper and lower bounds for stochastic processes: modern methods and classical problems," *Springer Science & Business Media*, p. 4, 2014.

[12] F. Haight, *Handbook of the Poisson Distribution*, New York: John Wiley & Sons, 1967.

[13] A. Shapiro, D. Dentcheva, and A. Ruszczyński, "Stochastic programming: Modeling and theory," *Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM). Mathematical Programming Society (MPS)*, 2009.

[14] I. Tishby, O. Biham, and E. Katzav, "The distribution of first hitting times of random walks on Erdős-Rényi networks," *Journal Reference J. Phys. A: Math. Theor.* vol. 50, p. 115001, 2017.

[15] R. Laha and V. Rohatgi, *Probability Theory*, New York: John Wiley & Sons, 1979, p. 233.

[16] M. Ugarte, A. Militino, and A. Arnholt, *Probability and Statistics with R*, 2nd ed. CRC Press, 2016.

[17] H. Alanazi, B. Zaidan, A. Zaidan, A. Jalab Hamid, M. Shabbir, and Y. Al- Nabhani, "Comparative study between DES, 3DES and AES within nine factors," *Journal of Computing*, vol. 2, no. 3, pp. 152-157. 2010.

[18] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," *Cryptographic Hardware and Embedded Systems (CHES)*, vol. 3156. pp. 357-370, 2004.

[19] T. Atia, "Development of a new algorithm for key and S-Box generation in blowfish algorithm," *Journal of Engineering Science and Technology*, vol. 9, no. 4, pp. 432-442, 2014.

[20] J. Bhalla and P. Nagrath, "Nested digital image watermarking technique using blowfish encryption algorithm," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, 2013.

Francis Segador Cambaya was born in San Juan Southern Leyte, Philippines in 1979. He is currently a graduating student of AMA University, the Philippines taking up doctor in information technology. He finished his master's degree in the University of Cebu, Philippines with the degree of master in science teaching major in computer science. He earned his baccalaureate degree in AMA University with the degree of bachelor of science in computer science. He is an assistant professor in the College of Computer Science and Information Technology at Southern Leyte State University, San Juan, Southern Leyte, Philippines.

Albert Alcause Vinluan was born in 1978. He completed his doctor in information technology at AMA Computer University in Quezon city, Philippines in 2014. He finished his master of science in computer science at AMA Computer University in 2007 and master of science in information technology at the University of La Salette in 2005 at Santiago, Philippines. He is presently the dean of the College of Computer Studies and at the same time the program coordinator of the Computer Science Department at New Era University, Philippines. Dr. Vinluan is a member of the Philippine Society of Information Technology Educators.