Development and Evaluation of the Two-Factor Authentication for Credit Card Systems Security using the Modified AES Algorithm

Felicisimo V. Wenceslao, Jr., *Member, IAENG*

***Abstract*— Credit cards are used to electronically purchased goods and services offered over the Internet. However, the existing security system in credit card payments is a one-factor authentication. This system poses security threats and possible exploits among hackers. The application of a two-factor authentication in credit card systems security over Web-enabled transactions was proposed. In this system, a web application was specifically developed employing the modified AES algorithm using multiple S-Boxes. Results from simulation tests showed that the run-time performance of the combined first-factor authentication and second-factor authentication yielded an average of nine seconds. The SMS delivery was considered as a critical factor in the overall run-time performance of the proposed system. For its usability, the proposed system was perceived with a description of "excellent" based on the computed SUS score.**

***Index Terms*— Two-factor authentication, credit card system security, AES algorithm, System Usability Scale**

I. INTRODUCTION

MANY people have opted to use credit cards as a medium of paying purchased of various commodities they bought particularly through e-commerce. Simply stated, a credit is a method of selling services and goods to the buyer, who at the time of the transaction, does not have the money at hand. Credit cards provide a convenient alternative to cash allowing the individual to carry an infinitive amount of money stored in only a card [1].

However, there are certain risks involved in using credit cards as medium for payment. It can be easily exploited by someone who possesses trade secrets in credit card frauds. Committing credit card exploit can be done by either physical or electronic exploitation. Under the physical exploitation, the culprit has physical hold of the exploited credit card. This can be achieved either through skimming and possession of a stolen or lost card. Skimming is a technique where information stored in the card's magnetic strip is stolen when your card is swiped during a transaction with the aid of a data capturing device. The criminals are then able to reproduce fake cards that are used to make purchases using the account [2]. Any third party individual who may hold a stolen or lost card can make use of the card to purchase products and services as if he is the owner of the card.

On the other hand, another way of exploiting credit cards and could commit fraud is done electronically. Email scams and fake websites are two of the most widely used techniques. Email scams or phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers[3]. Once they have possession of these, they can proceed to electronic purchase using the captured information.

In securing online transactions, the process of authentication is imperative. By definition, authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be [4]. Once the identity of the human or of the machine is validated, the access to a process is granted. There are three universally recognized authentication factors that exist today: knowledge - what the user knows (e.g. passwords); possession - what the user has (e.g. tokens); and inherence - what the user is (e.g. biometrics) [5].

A two-factor authentication (2FA) is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system [6]. It is aimed at providing stronger security mechanisms for login that ordinarily utilizes password-based authentication by deploying secondary authentication tokens. It is not a new concept especially in the banking industry. The first authentication factor is the physical ATM cards the customer slides into the machine. The second factor is the PIN they enter. Without both, authentication cannot take place [7]. However, unlike ATM cards where the PIN is not physically visible on the face of the card, a credit card has all the information needed for a possible transaction. The security code for credit cards is normally found at the back portion being indicated as the Card Verification Value or CVV. Without additional security mechanisms, a lost credit card can be easily used by someone posing as the card owner.

In [8], they conducted an empirical study on the implementation of 2FA in online banking. In their study, they noted that user has to login using his username and password. When confirmed, the user can then perform any operation like money withdrawal, checking the balance and

Manuscript received January 16, 2019; revised October 28, 2019.

F. V. Wenceslao, Jr. is with the Institute of Information and Computer Studies at Northern Iloilo Polytechnic State College, Estancia, Iloilo 5017 Philippines (e-mail: fvwenceslao@yahoo.com).

others. To improve the system, the authors proposed to incorporate the 2FA that would strengthen its security. They used the mobile phone to act as a security token for authentication. A token number is generated using the SHA algorithm and XOR operation. The token number is a six-digit random numbers composed of the user mobile number, IMEI number, pin number and IMSI number. As a measure, the account is blocked when the user gives an invalid token numbers for more than three times. This scheme also ensures that the person performing the online banking transaction is the legitimate owner of the account because he is presumed to be the person in possession of the mobile device whose information were previously submitted to the bank.

In [9], they proposed the Secure Online Transaction Algorithm (SOTA) that sought to use two-factor authentication with the random codes. This can be utilized to identify users and establish secure way of purchasing items online. The proposed SOTA uses mobile devices to log into card accounts via an application to view the randomly generated code. This is then inputted on an online retailer's website when prompted in order to authenticate the individual making the purchase. This minimizes the possibility that an illegitimate user can use someone else's information to make fraudulent purchases. Without a valid code, identity thieves cannot use the stolen card information to make purchases.

It is for this reason that we proposed to improve credit card system security over Web-based transactions by adding another layer of security to the existing mechanism. This paper implemented the modified Advanced Encryption Standard (AES) algorithm using a two-factor authentication in credit card security system as the second layer of security. It also evaluated the processing performance and the usability characteristic of the proposed system to determine its acceptability.

II. METHODOLOGY

This study employed the previously developed modified version of the AES algorithm using multiple SBoxes [10]. As such, this study was implemented in two (2) phases. The first phase was the design and development of a two-factor authentication system for credit cards security. At the core of the proposed system is the modified AES algorithm using multiple SBoxes.

The second phase involved the evaluation of the system product. A simulation was conducted to test the performance as well as the usability of the system prototype. There were 100 respondents involved in the testing. These respondents included students and faculty members at the Institute of Information and Computer Studies of Northern Iloilo Polytechnic State College in Estancia, Iloilo, Philippines. We purposively selected the respondents based on the survey we conducted in which respondents were identified having experienced using credit cards in online procurement.

Prior to the start of the evaluation, a system prototype walk-through was presented to the respondents for them to be familiar with some of the user interfaces that are deemed essential to learn. Once everything was set, they were asked to register their account details as shown in Figure 2. Subsequently, they were requested to start the process of buying products from the webstore specifically created for this purpose. As the participants respond to the different interfaces, various checkpoints were recorded by the system to determine its operational performance being denoted in mm:ss.00. We also asked the participants to make two transactions, hence there were a total of two hundred transactions.

A. An Overview of the Modified AES Algorithm Using Multiple Substitution Boxes

The AES algorithm is a symmetric key cryptography. Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key [11]. Symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm.

In our previous study, we modified the AES algorithm using multiple SBoxes by changing the MixColumns function with a second substitution box, hence the name AES2SBox. We assumed that the MixColumns function requires more computational resources in software implementation as compared to the other functions. Replacing the MixColumns function by an alternative process had increased the speed performance of the AES algorithm. The four functions in the internal rounds of the AES2SBox are consisted of SubBytes, ShiftRows, SubBytesXOR and AddRoundKey. As with the original AES algorithm that drops the MixColumns function, the final round in the AES2SBox also drops down the SubBytesXOR function to produce the ciphertext. Reversing the execution of the process will produce the plaintext.

Moreover, we were able to show that in both encryption and decryption, the AES2SBox was more efficient by 27.638% and 108.369% respectively than the original AES algorithm. However, when we tested its security characteristics using the Avalanche Effect, the obtained changes in the bit sequence were only computed at 25.000% and 19.351% for two sets of plaintext which were slightly lower than the minimum expected output of at least 50% bit flip when 1 bit input is altered. Figure 1 shows the modified AES algorithm structure using multiple S-Boxes.

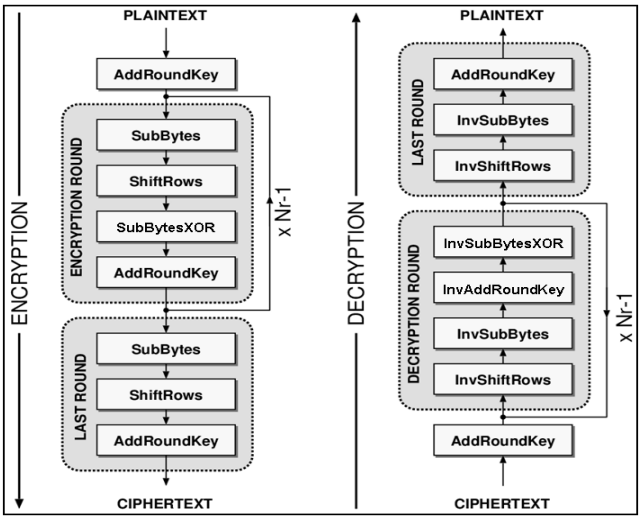

Fig. 1. Modified AES Algorithm Using Multiple S-Boxes.

B. Design and Development of the Two-Factor Authentication in Credit Card Systems Security using the Modified AES Algorithm

In this paper, we proposed for a mechanism that reinforces the credit card system security in web-enabled transactions by implementing a two-factor authentication through an SMS-based token. The SMS token will be used as another layer of security that the cardholder has to respond. The unique identification of the SIM card effectively enables the cell phone owner to possess an authentication token, which can be registered and used by different applications. SMS is an effective means for places where cell phones are widely used in the community[12].

Various modules were created to comprise the proposed system. The encryption module runs in the client-side application while the decryption module runs in the server-side application. The other significant components are the random key generator that produces the passkey, the SMS component that transmits the token and the cleaner module that checks for the integrity of the passkey.

In the implementation of this project, we acknowledged the full functionality of the credit card company's internal security policies and procedures. Thus, the security implementation of the first-factor authentication was only included for consistency with the second-factor authentication.

Registration Module

The Registration Module is a custom-made registration form aimed at soliciting important information from the credit card owners. During the registration for the application of the credit card, a security question and its corresponding answer must be provided by the card owner. The "answer to the security question" and the passkey will generate a ciphertext that will serve to authenticate the ownership of the cardholder. As such, most existing application forms will be revised to include items that will capture the needed security question and its corresponding answer. The application form will also require the entry of the mobile phone number of the cardholder. Figure 2 shows the user registration form.

Fig. 2. User Registration Form.

Passkey Generation Module

As the title suggests, the passkey generation module creates a randomly-generated value. While the function tends to create simple randomness of the generated values, its main purpose is to combine it with the "answer" to the security question to produce a ciphertext. For purposes of documentation, figure 3 shows the user interface for the passkey generation module. However, in the actual system prototype this interface is a server process and is therefore not visible to the user.

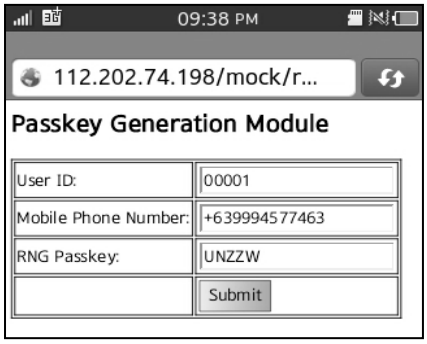

Fig. 3. Passkey Generation Module User Interface.

SMS Module

The SMS module is the system's component that transmits the passkey as an SMS text message. The passkey is an important element in the two-factor authentication as it serves as a security token. Its purpose is to generate a ciphertext by converting the plaintext into a non-readable format. Figure 4 shows that actual SMS text message with the passkey as the security token.

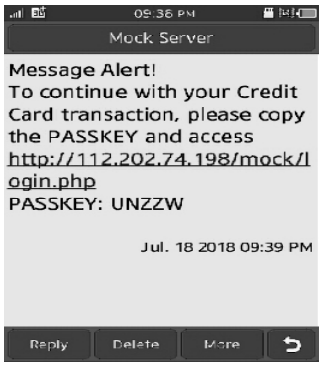

Fig. 4. SMS Text Message with Passkey as Security Token.

Client-side Encryption Module

A client-side encryption module was developed to generate a ciphertext. The ciphertext is the output of the processes employing the AES2SBox algorithm. It can be accessed using any device that is connected to the Internet. It can be noted that since this project covers the use of credit cards for web-enabled transactions, it is therefore safe to state that during the transaction, the owner/user has a concurrent connection to the Internet. The ciphertext, after being created, will be submitted to the server for decryption and subsequently authenticated with information previously stored in the database. Figure 5 shows the Client-side Encryption Module.

Fig. 5. Client-side Encryption Module.

Server-side Decryption Module

The server-side decryption module performs the conversion of the ciphertext into the plaintext. The server receives the ciphertext from the client-side encryption module; checks the transaction code accompanying the ciphertext; retrieves the passkey and perform the decryption process. Once the plaintext is generated, the server retrieves the "security answer" from the database and performs a comparison with the plaintext. If a match is found, the entire transaction is consummated otherwise the entire transaction fails. The processes in the server-side decryption module are done automatedly at the background and thus, there is no visible user interface to the clients.

Cleaner Module

An independent module called "cleaner" checks the database to monitor whether a passkey has reached the 30-minute time limit to consummate a transaction. This process is important as it tests the integrity of the passkey. If a passkey is not yet processed within the maximum time limit, the cleaner module destroys the passkey by deleting it from the database. Any further transactions using the deleted passkey will no longer progress. The cleaner module is routinely executed every 15 minutes by way of the Task Scheduler. Like the server-side decryption module, its processes are intended to run at the background.

III. RESULTS AND DISCUSSION

A. Run-Time Performance

According to CardHub, a search engine website dedicated to credit card issues, credit card transactions which are processed through a variety of platforms, including brick-and-mortar stores, e-commerce stores, wireless terminals, and phone or mobile devices will take the entire process to approximately two to three seconds to complete [13]. However, it should be underscored that the processing time being mentioned is for the first-factor authentication. In this paper, the run-time performance refers to the average time that the transaction is completed comprising of the first-factor authentication and second-factor authentication.

The average processing time for the first-factor authentication was 00:02.73. In the first round of transaction for the first-factor authentication, the average processing time was 00:02.81 with the longest time-check at 00:05.00 and the shortest time-check was at 00:02.00. Similarly, in the second round for the first-factor authentication, the average processing time was 00:02.65 with the longest time-check at 00:04.00 and the shortest time-check was 00:02.00. In the current credit card system, the processing time is completed or denied as soon as the needed security checks are performed. In this project, addition modules such as the passkey generation and SMS forwarding are included in the first-factor authentication. Although there are additional processes brought about by additional modules, processing time for the first-factor authentication is still within the approximate time limit as described by the CardHub.

For the second-factor authentication which starts from user login until evaluation of the decrypted text, the average processing time was 00:06.15. In the first round transaction for the second-factor authentication, the average processing time was at 00:06.56 with the longest checkpoint at 00:12.00 while the shortest checkpoint was recorded at 00:03.00. In the second-round, the average processing time was 00:05.76 with the longest checkpoint was recorded at 00:09.00 while the shortest checkpoint was at 00:03.00.

For the entire transaction, which covered both the first-factor and the second-factor authentications, the average processing time was 03:30.52. In the first round, the average processing time was 03:59.62 with the longest checkpoint recorded at 09:10.00 while the shortest checkpoint was at 01:34.00. In the second-round, the average processing time was 03:03.12 with the longest checkpoint at 04:33.00 while the shortest checkpoint was 01:32.00. Table 1 shows the average run-time processing performance of the proposed system.

TABLE I
RUN-TIME PERFORMANCE BASED FROM SIMULATION

Run-Time Performance		Authentication Factors		Entire Transaction
		First	Second	
First Round	Average	00:02.81	00:06.56	03:59.62
	Longest	00:05.00	00:12.00	09:10.00
	Shortest	00:02.00	00:03.00	01:34.00
Second Round	Average	00:02.65	00:05.76	03:03.12
	Longest	00:04.00	00:09.00	04:33.00
	Shortest	00:02.00	00:03.00	01:32.00
Overall Average		00:02.73	00:06.15	03:30.52

As observed in table 1, we noted that the overall average performance of the first-factor and the second-factor authentications was at 00:8.88, however the entire transactions were at an average of 03:30.52. There was a difference of 03:21.64 which is attributed to the delayed time delivery of SMS token by the mobile network service. From the collected data, the earliest SMS delivery receipt was at 01:45.00 while the latest SMS delivery that was received by the system was at 08:59.00 after the second timestamp for the first-factor authentication. Figure 6 shows the SMS delivery as a critical factor in the entire operations.

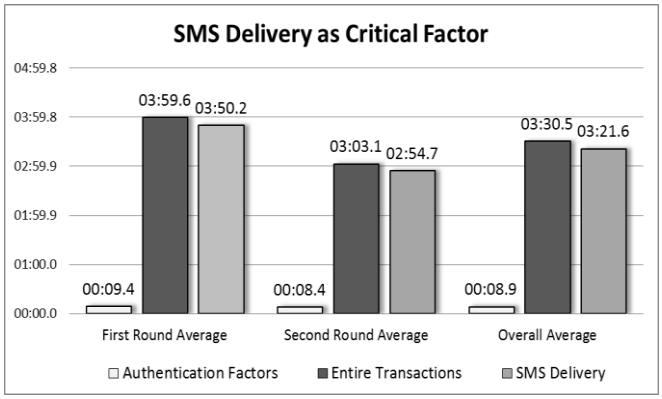

Fig. 6. SMS Delivery as Critical Factor and is Being Computed as the Difference between the Entire Transaction and the Authentication Factors.

Speculatively, there can be several factors that may have contributed to this issue. Factors may include the existing network infrastructure where the client is located during the time of transaction, network congestion and the time of access (whether if it's off-peak or peak hours) when the transaction was made. While the two major telecommunication service providers provide 4G signals available in some areas of the Philippines, the place of study is currently in 3G network. Although these issues are not within the scope of this study, but they are collectively considered as a critical factor in the run-time performance.

B. Perceived Usability of the Proposed System

Aside from the evaluation of the run-time performance of the proposed system, it was also subjected to perception evaluation of its usability. Testing for usability is an important element in the development and further improving the system product. It refers to the ease of access and/or use of a product or website and is one of the most traditional concepts in HCI research evaluations. As defined in [14], usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use". On web-based systems, usability is an essential condition for its operations. If the system is difficult to use, clients would leave.

In this study, the System Usability Scale (SUS) was employed. Developed by Brooke in 1996 [15], the SUS is one of the survey instruments that can be used to assess the usability of a variety of products or services [16]. As an evaluation metric, it is applied to a wide variety of web or technology-based applications to measure how easy or difficult they are to use in order to improve them. SUS is composed of a 10-item, five-point Likert scale with a weighted scoring range of 0–100 and is anchored with one as Strongly Disagree and five as Strongly Agree [17]. There are five positive statements (Q1, Q3, Q5, Q7 and Q9) and five negative statements (Q2, Q4, Q6, Q8 and Q10). SUS is considered to be one-dimensional. However, the factorial analysis showed that SUS has two factors: usability (Q1, Q2, Q3, Q5, Q6, Q7, Q8 and Q9) and learning (Q4 and Q10) [18].

As mentioned earlier, we have invited 100 participants to evaluate the usability characteristic of the proposed system using the SUS questionnaire. From the responses made by the participants, the best scored items were Q3 (M=4.87; SD=.223), Q7 (M=4.85; SD=.291) and Q5 (M=4.83; SD=.428). It can be assessed therefore that the proposed system is easy to use and can be learned quickly by users due to its well-defined and integrated functions. Moreover, the respondents felt that they no longer needed assistance from technical persons as shown by the results in Q4 (M=1.78; SD=.811) and Q10 (M=1.99; SD=.847) because it can be learned by them.

Furthermore, to be able to compute for the SUS score, the following formula is used [19]:

$$SUS\ Score = ((\sum odd\ items\ RS - 5) + (25 - \sum even\ items\ RS)) * 2.5 \quad (1)$$

A SUS score of over 68 would be considered above average [20]. In this study, the results showed that the SUS score was computed at 81.025 which can be interpreted as "Excellent" [16][19], indicating that the participants found the proposed system to be very usable due to its simple and clear interface design. Also, they found it to be easy-to-learn and simple to use. It provided pop-ups and tips that would allow the users to easily perform the tasks with confidence. Table II shows the data.

TABLE II
PERCEIVED USABILITY OF THE PROPOSED SYSTEM USING THE SYSTEM USABILITY SCALE (SUS)

Questions	Mean	Standard Deviation
1. I think that I would like to use this system frequently.	4.18	1.282
2. I found the system unnecessarily complex.	2.98	.921
3. I thought the system was easy to use.	4.87	.223
4. I think that I would need the support of a technical person to be able to use this system.	1.78	.811
5. I found the various functions in this system were well integrated.	4.83	.428
6. I thought there was too much inconsistency in this system.	2.22	.836
7. I would imagine that most people would learn to use this system very quickly.	4.85	.291
8. I found the system very cumbersome to use.	2.89	1.222
9. I felt very confident using the system.	4.67	.514
10. I needed to learn a lot of things before I could get going with this system.	1.99	.847
System Usability Scale (SUS) Score	81.025	

IV. CONCLUSION

This paper presents the development and evaluation of a two-factor authentication mechanism in credit card systems security in Web-enabled transactions using the modified AES algorithm. The first-factor authentication includes the usual information provided from the credit card. The second-factor authentication includes the possession of a security token in a form of a passkey transmitted to the credit card owner's registered mobile phone number. At the core of the web application are the client-side encryption module and the server-side decryption module which make use of the modified AES algorithm using multiple S-Boxes. The design of the system would require an "answer to the security

question" by the cardholder and security token cum passkey to generate a ciphertext. The ciphertext is converted back to the plaintext by the system's several functionalities and is compared to stored information from the database to authenticate the identity of the user.

Based on the results of the simulation, we found out that the first-factor authentication, even equipped with additional functionalities such as random number generation that is essential to creating a passkey that serves as a security token, and an SMS module, its run-time performance was still within the acceptable time limit. On the other hand, the second-factor authentication is not far behind at an acceptable average. Cumulatively, both factors had an acceptable run-time performance. However, the SMS delivery was seen to be a critical factor when the transaction is viewed as a whole because it became the cause of delay in the overall performance of the proposed system.

The proposed system was evaluated using the System Usability Scale metric. For its usability, it was perceived to be very usable. The proposed system was easy to use, and allows users to effectively complete their tasks. It also allows users to become productive quickly without the assistance of technical personnel as shown in the computed mean for Q3 and Q4. This conforms to the study of Martínez-Falero et al. [21] wherein their developed system was viewed as easy for IT experts and forest managers to use without the help of technical personnel. Furthermore, the learnability factor was perceived to be acceptable as the proposed system was able to provide feedback to users such as error messages and information on how to fix problems. It was also easy to understand and organized.

REFERENCES

[1] L. Delamaire, H. Abdou and J. Pointon, "Credit Card Fraud and Detection Techniques: A Review", *Banks and Bank Systems*, vol. 4, no. 2, pp. 57-68, 2009.

[2] ANZ Internet Banking. (2013, October 28). *Types of Frauds*. [Online]. Available: https://www.anz.com.au/security/fraud-detection/types/

[3] R. Kay. (2004, January 19). *Phishing*. [Online] Available: http://www.computerworld.com/article/2575156/security0/ phishing.html.

[4] L. Rosencrance. (2015). *Authentication.* [Online] Available: http://searchsecurity.techtarget.com/definition/authentication.

[5] E. D. Cristofaro, H. Du, J. Freudiger and G. Norcie. (2013, September 20). *Two-Factor or Not Two-Factor? A Comparative Usability Study of Two-Factor Authentication*. [Online] Available: https://arxiv.org/abs/1309.5344

[6] F. A. Aloul, S. Zahidi, and W. El-Hajj, W. "Two Factor Authentication Using Mobile Phones", in *Proc. 2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641-644. DOI:10.1109/AICCSA.2009.5069395

[7] O. S. Adeoye, "Evaluating the Performance of Two-Factor Authentication Solution in the Banking Sector," *International Journal of Computer Science Issues*, vol. 9, no 4, pp. 457-462, 2012.

[8] P. Y. Pawar, S. Acharya, A. Polawar, P. Baldawa and S. Junghare, "Internet Banking Two Factor Authentication Using Smartphone", *International Journal of Scientific & Engineering Research*, vol. 4, no. 3, pp. 1-4, 2013.

[9] J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler and S. Rizvi, "Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication", in *Proc. Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems*, Illinois, USA, 2017, pp. 93-99.

[10] F. Wenceslao, Jr., "Enhancing the Performance of the Advanced Encryption Standard (AES) Algorithm Using Multiple Substitution Boxes", *International Journal of Communication Networks and Information Security*, vol. 10, no. 3, pp. 496-501, 2018.

[11] W. Stallings, *Cryptography and Network Security Principles & Practice 5th Edition*. New York, NY: Prentice-Hall, 2011.

[12] e-Authentication Methods. (2007). *SMS based Authentication*. [Online]. Available: http://www.e-authentication.gov.hk/en/professional/sms.htm

[13] O. Papadimitriou. (2015). "*How Credit Card Transaction Processing Works: Steps, Fees & Participants*". [Online]. Available: http://www.cardhub.com/edu/credit-card-transaction

[14] ISO 9241-11:2018(E). (2018). *Ergonomics of Human-Computer Interaction – Part 11: Usability: Definitions and Concepts*. [Online]. Available: https://www.sis.se/api/document/preview/80003410/

[15] J. Brooke. SUS: A 'quick and dirty' usability scale. In P. W. Jordan, B. Thomas, B.A. Weerdmeester, and I.L. McClelland (Eds.) Usability Evaluation in Industry (189-194). London: Taylor and Francis, 1996.

[16] A. Bangor, P. Kortum & J. Miller. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies*, vol. 4, iss. 3, 2009, pp. 114-123.

[17] K. Finstad. (2010). The Usability Metric for User Experience. *Interacting with Computers*, vol. 22, iss. 5., 2010, pp. 323-327, Available: https://doi.org/10.1016/j.intcom.2010.04.004

[18] L. Padrini-Andrade, R. Balda, K.C.N. Areco, P. Bandiera-Paiva, M. Nunes, S.T.M. Marba, W.B. Carvalho, L.M.S. Rugolo, J.H.C. Almeida, R.S. Procianoy, J.L. Duarte, M.A.S. Rego, D. Ferreira, N. Alves Filho, R. Guinsburg, E.M.A. Diniz, J.P.F. Santos, D. Testoni, N.M. Silva, M.R.C. Gonzales, R.V.V. Silva, J. Meneses, W.A. Gonçalves-Ferri, R. Perussi-e-Silva & O. Bomfim. Evaluation of Usability of a Neonatal Health Information System According to the User's Perception. *Revista Paulista de Pediatria*, vol. 37, iss. 1, 2019. pp. 90-96. Available: https://dx.doi.org/10.1590/1984-0462/;2019;37;1;00019

[19] UIUX Trend. (2017, May 31). *Measuring and Interpreting System Usability Scale (SUS)*. [Online]. Available: https://uiuxtrend.com/measuring-system-usability-scale-sus/

[20] J. Sauro & J. R. Lewis. Quantifying the User Experience: Practical Statistics for User Research, 1st ed. San Francisco, MA, USA: Morgan Kauffman, 2012, p. 295.

[21] J. Martínez-Falero, E. Ayuga-Téllez, C. González-García, M. Grande-Ortíz, A. Garrido & A. Medina. (2017). Experts' Analysis of the Quality and Usability of SILVANET Software for Informing Sustainable Forest Management. *Sustainability*, vol. 9, iss. 7:1200, 2017. Available: 10.3390/su9071200.

ABOUT THE AUTHOR

Felicisimo V. Wenceslao, Jr. finished his Bachelor of Science in Computer Science at the Computer College of the Visayas, Iloilo City, Philippines (1993), his Master of Science in Information Technology at Hannam University, Republic of Korea (2005), Doctor of Education at NIPSC, Estancia, Iloilo, Philippines (2013) and his Doctor in Information Technology at the Technological Institute of the Philippines, Quezon City, Philippines (2016). He is currently an Associate Professor V and the designated Director of the Institute of Information and Computer Studies at Northern Iloilo Polytechnic State College, Estancia, Iloilo, Philippines. His research interests are in network security, mobile development, data mining, system development and e-learning. He is a member of the IAENG since 2013.