

## Application of advanced encryption standard in the computer or handheld online year-round registration system

Jomar L. Calpito, Paul L. Olanday, Alain C. Gallarde

Instruction Department, Southern Isabela College of Arts and Trades, Isabela, Philippines

### Article Info

#### Article history:

Received Jul 26, 2021

Revised May 31, 2022

Accepted Jun 10, 2022

#### Keywords:

3DES

Advanced encryption standard

Cipher

Data encryption standard

ISO 25010

Symmetric-key cryptography

### ABSTRACT

With various severe security threats for web applications, ensuring security on the database layer itself is imperative. Hence, this study aims to protect data saved on the computer or handheld online year-round (CHOY) registration system using the advanced encryption standard (AES) to strengthen data security within the app so that even potential attackers gain access to the app's database; they cannot obtain valuable information because it is scrambled and unreadable. The proponents based the study's conceptual framework on the symmetric and asymmetric key algorithms and procedures manual on enrollment of Southern Isabela College of arts and trades (SICAT) and ISO 25010. The study consists of three elements: developing the CHOY web app imbued with AES, testing it in terms of online registration and spam prevention, and evaluating it using the ISO 25010 in terms of compatibility, reliability, and security. The evaluation results show that implementing the AES in the CHOY web app meets the ISO 25010 criteria mentioned above.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Jomar L. Calpito

Instruction Department, Southern Isabela College of Arts and Trades

Provincial Road, Calaocan, City of Santiago, Isabela 3311, Philippines

Email: jomar.l.calpito007@gmail.com

## 1. INTRODUCTION

This study focuses on applying the advanced encryption standard (AES) in encrypting and decrypting the database content of the computer or handheld online year-round (CHOY) web app. In addition, the researchers tested the app regarding online registration and encryption/ decryption capabilities, and the Southern Isabela College of arts and trades (SICAT) stakeholders evaluated it regarding compatibility, reliability, and security. Even before the pandemic, most institutions and businesses depend on web applications to collect/display information and extend their programs and services to their clients. Usually, they are developing their web apps based on the three-tier model, where the frontend, backend, and business logic are separated [1]. The first tier is the clients using a web browser, the second is the server-side application, and the third is the repository (database). However, these tiers have their vulnerabilities. Potential attackers might exploit one of these, and the whole application can be compromised [2]. The open web application security project (OWASP) released a document to further enhance an entity's web application security. It reflects widespread agreement on the most severe security threats to web applications [3]. Among the top 10 web application security risks identified in the document are injection, sensitive data exposure, cross-site scripting (XSS), broken authentication, broken access control, extensible markup language (XML) external entities (XXE), security misconfiguration, use of components with known vulnerabilities, insufficient logging and monitoring, and insecure deserialization. These attacks can access the database, resulting in data loss, corruption, disclosure to unauthorized parties, money laundering, or identity theft.

In response to the threats web applications face, researchers worldwide developed techniques and theories to prevent those. For instance, to detect XSS attacks, Pan and Mao [4] attempted to build templates for document object model (DOM)-based XSS detection using existing tools and solutions. Shalini and Usha [5] created a method to detect XSS attacks. They proposed a model that can see XSS on the client's browser without the need for third-party engagement. The experimental findings show that the proposed method is quite successful. Because the approach is platform-agnostic, it stopped possible exploits by prohibiting the malicious script from reaching the JavaScript engine instead of making potentially dangerous hypertext markup language (HTML) changes. Regarding structured query language (SQL) injection prevention, Singh *et al.* [6] suggested that privileges on the database must be minimized, implement consistent coding standards, and use SQL server firewall. Kamtuo and Soomlek [7] introduced SQL injection commands dataset extraction, pre-processing, and usage of machine learning model analysis for detection, testing, and training. Al-Sayid and Aldlaen [8] introduced the use of a web application firewall. However, these initiatives have common drawbacks; it does not have node verified signature. Hence, Yunus *et al.* [9] introduced the blockchain concept to overcome SQL injection through node verification with internet protocol (IP) addresses to address the earlier issue. On the other hand, there is a massive investment in cryptography to ensure confidentiality, data integrity, and availability. Moreover, researchers worldwide are continuously working on cryptography algorithms to secure sensitive information [10].

The study and research of techniques for encrypted communication are known as cryptography. More generally, protocols are developed and assessed to overcome adversaries' power and extend to different facets of information security, like data privacy, protection, authentication, and non-repudiation [11]. In addition, it is a science and art of shielding knowledge from unauthorized entities by turning it into something that its attackers cannot recognize while being processed and transmitted [12].

In computing, the three types of cryptographic techniques are as shown in: the symmetric-key cryptography, which involves a single key for the sender and receiver to encrypt or decrypt plaintext; the hash functions, which reduces the length of an arbitrary input string to a fixed-length string; and public-key cryptography, which encrypts and decrypts texts using two keys (public and private) [13], [14]. In this pandemic, most institutions rely on web applications to extend their services to their stakeholders. Hence, it is critical to secure the information collected from these web applications. Potential attackers may access the database and use its content for illegal purposes.

Aside from firewalls and other preventive measures, it is best to establish a form of defense at the data within the database itself, specifically in its columns, tables, or tablespaces [15]. Institutions can imbue their databases with database encryption algorithms so that if potential attackers breach the database, authorized users with the correct encryption keys are the only ones who can read the data stored. These algorithms scramble the database contents, rendering it useless for unauthorized intruders.

Researchers concluded that both symmetric and asymmetric information could secure information over any medium through the years. However, there are differences in implementation and speed, among others. For example, the last key calculations are more secure than the former. Hence its implementation is complex and significantly slower [16]. On the other hand, while the former is less secure, it offers algorithms like AES with no weaknesses. Also, it is significantly faster, cheap, has low power consumption, and is easy to implement [17].

Examples of symmetric-key algorithms include the advanced encryption standard (AES), data encryption standard (DES), Blowfish, and triple DES. During the 1970s, the DES algorithm was widely used to provide a standard way to secure sensitive commercial and unclassified data. Later, the National Institute of Standards and Technology (NIST) replaced DES and paved the way for the AES, a more stable encryption standard best suited for protecting commercial transactions over the internet [18]. The triple-DES is the enhanced version of DES, where data is encrypted thrice using DES, and Blowfish is an algorithm created in 1993.

Researchers were able to increase the efficiency and security of existing algorithms by modifying them or combining them with new algorithms. Using numerous approaches, Farhan and Ali [19] improved MD5 with a 1024-bit input block message and a 160-bit output message. Databases are protected using two tactics, according to his research: maintaining data integrity by employing hash algorithms and improved MD5 to generate passwords for users, ensuring data secrecy, and encrypting vital data with the AES algorithm. As a result, verifying the database's security is as simple as collecting each constraint's configured hash value (MD5 improvement) and comparing it to the original version. Because of the additional tables storing the hash values for each entry and the attached file size in the method containing the keys to the size ( $2^{32}$ ), the extended MD5 is slower than the basic MD5. Ali and Farhan [20] improved the MD5 function for e-document verification by adding a dynamic variable length and a high efficiency that simulates the maximum level of security. Unlike the logistic system, which was used to encode ribonucleic acid (RNA) by generating a random matrix based on a new key created using the initial permutation (IP) tables used in the data encryption standard (DES) with the linear-feedback shift register (LFSR), this work proposes several

structures to improve the MD5 hash function. The tests show that it has a high level of resistance to hackers while still, that can last a reasonable amount of time. Kadhim and Khalaf [21] proposed a new method for real-time security chatting based on a new block cipher algorithm that achieves peer-to-peer security for each communication connection. This system is divided into two parts: the first is concerned with the server, and the systems begin to establish connections between subscribers, generate keys, distribute dynamic keys, and guarantee that this subscriber is registered in the system. On the other hand, the second portion is concerned with data security and services by encrypting them with AES. The suggested approach enhances communication secrecy while manipulating the communication and data transfer process elegantly.

Ali and Farhan [22] proposed a revolutionary approach for improving the data storage of a rapid quick response code (QR code). By integrating secret information inside a QR code message, the suggested algorithm incorporates a clear and straightforward plan for circumventing this obstacle. The QR code has been modified to include levels that aid in sharing secure messages of various sizes and the authentication of documents for verification and validation. The newly proposed QR code does not reconstruct the QR code's design or structure in this study. Instead, it improves security by using the Huffman compression method to minimize the size of the input data and the XOR function to encrypt the data using a changeable encryption key. The experimental results demonstrate the method's advantage over prior methods. Many known attacks can be thwarted by developing a new QR code model that meets security criteria while retaining the QR code's speed advantages. Naif *et al.* [23] developed a secure system based on a chaotic system combined with a lightweight AES modification. The sequences chaos keys used in the lightweight AES and SHAKE128 were generated using the 5-D chaos system (a mix of logistic and Lorenz chaotic systems). The Lightweight AES has been developed to minimize the processing complexity of AES while increasing processing speed (by 145 percent), making it appropriate for use in IoT devices and sensors with low power consumption.

In the end, researchers worldwide determined the best and most efficient encryption algorithm for data security. Kannan *et al.* [24] claimed that AES is faster and more secure than the DES because the NIST selected the former as a replacement for the latter. Sapna [25] showed that the AES has excellent security, efficient power consumption, and cost and has more key length than DES. Finally, Singh *et al.* [26] implemented DES, 3DES, AES, and RSA in VB.net to test input data size, time, and throughput algorithms. The results proved that AES is excellent in terms of performance and security. While it uses more power than DES, it uses far less than 3DES and RSA, making it the best option among the algorithms studied.

The National Institute of Standards and Technology (NIST) started selecting some symmetric-key encryption algorithms to secure sensitive (unclassified) federal information to fulfill its regulatory obligations in 1997. NIST verified the approval of 15 candidate algorithms in 1998 and sought the cryptographic research community for assistance in evaluating them. After NIST reviewed the preliminary research findings, MARS, RCTM, Serpent, Twofish, and Rijndael were chosen as runners-up. NIST selected Rijndael as the new Advanced Encryption Standard following a study of additional public analyses of the finalists [27]. Vincent Rijmen and Joan Daemen made the winning algorithm, hence the word "Rijndael" [28].

AES is a block cipher that encrypts/ decrypts using the same key. AES will encrypt and decrypt 128-bit blocks using various cipher keys up to 256 bits, which is the most remarkable bit size and is impenetrable by brute force based on computational power since the number of possible key combinations increases exponentially with key size [29] as shown in Table 1.

Table 1. AES key size and possible combinations

Key size	Possible combinations
1 bit	2
2 bits	4
4 bits	16
8 bits	256
16 bits	65536
32 bits	$4.2 \times 10^9$
56 bits (DES)	$7.2 \times 10^{16}$
64 bits	$1.8 \times 10^{19}$
128 bits (AES)	$3.4 \times 10^{38}$
192 bits (AES)	$6.2 \times 10^{57}$
256 bits (AES)	$1.1 \times 10^{77}$

The AES has ten rounds to change from plaintext to ciphertext. To convert a text, each round is very close. The expand key rule governs how AES performs encryption and decryption. The algorithm will encrypt from round 1 to round 10. After that, the algorithm would decrypt in the opposite direction. The key is represented as words W0 to W43. Forty-four words contain 4 bytes each in this sample, and the matrix key is saved as text (expanded key) [24].

A few blocks or steps in the encryption process are suppressed in Figure 1. AES encrypts data or plaintext using 128-bit blocks as input, which a square matrix can interpret. At each encryption stage, the individual matrix is copied into a state array, which is changed. As a result, it is copied from an input matrix.

With the AES implementation in the CHOY web app, clients can register online using the form provided by the app. Afterward, the app generates a key and converts the record fields into ciphertext, then saves it to the repository (the database). In this way, even if the database server is breached, potential attackers can only obtain meaningless data. On the other hand, the app can easily decrypt the information in the database to make it readable for administrators (school registrar), as shown in Figure 2.

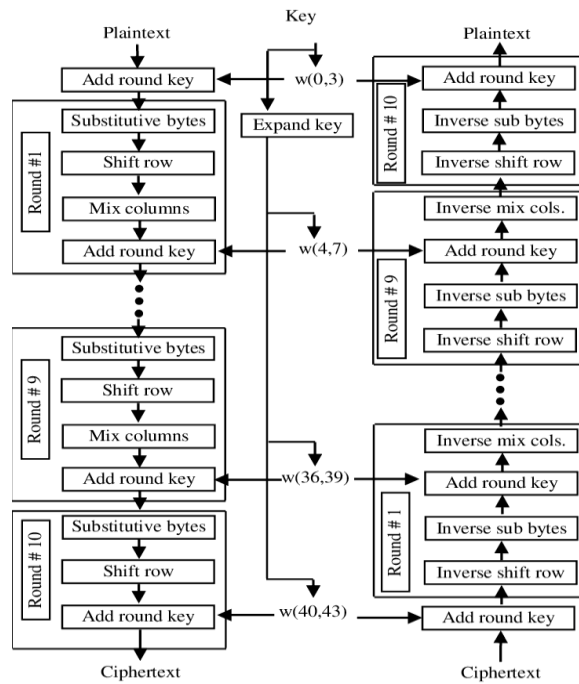


Figure 1. AES encryption and decryption block diagram

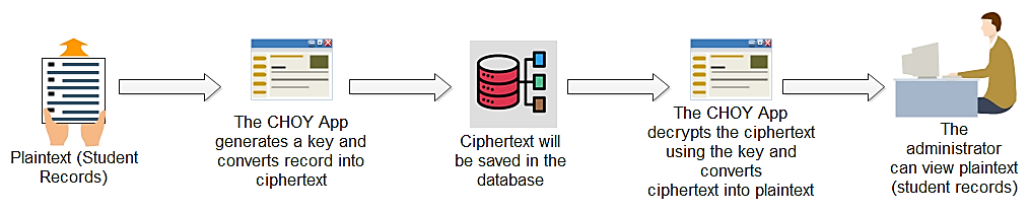


Figure 2. Encryption and decryption process

The main focus of this study is the application of the AES in developing the CHOY web app. Specifically, it aimed to: i) develop the CHOY web application applying the AES; ii) examine the app's functionality in terms of online registration and spam prevention; and iii) access the web app's technical elements in terms of compatibility, reliability, and security using the ISO 25010.

## 2. RESEARCH METHOD

### 2.1. Conceptual framework of the study

The proponents of this study used the symmetric-key method, AES, ISO 25010 standards, and the procedures manual on enrollment and admission of Southern Isabela College of Arts and Trades (SICAT) to establish the conceptual framework. The basis for the encryption/ decryption of the framework is the AES algorithm, implemented in the CHOY web app, shown in Figure 3.

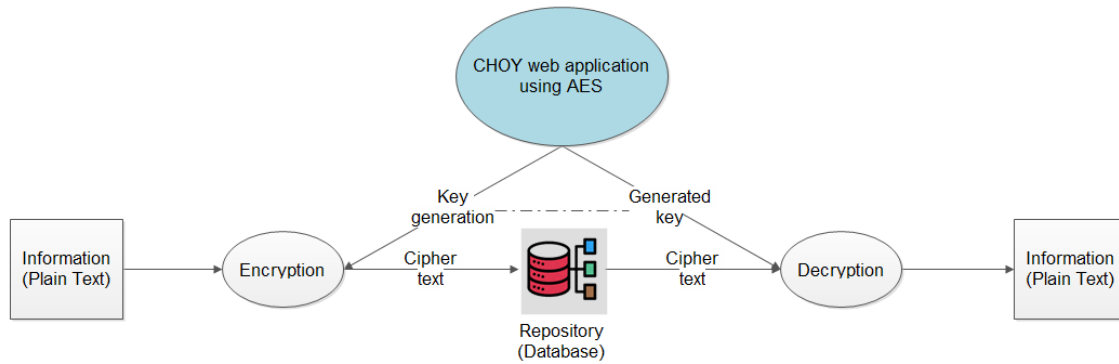


Figure 3. Conceptual framework of the study

To summarize, Figure 3 shows that administrators and clients can enter information in the CHOY web app, and the AES algorithm will encrypt it before saving it in the database. If there is a need to view the saved student records, the app retrieves the ciphertext in the database and decrypts it using only the administrators' pre-set key. With this, the app converts cipher into plain text, readably by administrators.

**2.2. AES as basis in encryption and decryption**

The AES largely relies on the number of rounds, as shown in Figure 1, and each round consists of four sub-processes: substitute byte, ShiftRows, MixColumn, and AddRoundKey transformation. To encrypt a plaintext, the earlier-mentioned sub-processes are performed orderly. To decrypt a ciphertext, the sub-processes are performed reversely, starting from the AddRoundKey transformation. For encryption and decryption, the following are performed:

**2.2.1. Substitute bytes transformation**

The first process in each round is the substitute bytes transformation. It substitutes one byte for another using a non-linear S-box. For instance, this process will replace a hexadecimal value A9 to D3, derived from the intersection of A and 9 as presented in Table 2 and Figure 4 [30].

Table 2. The AES S-box Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	CO
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
4	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	3	F6	OE	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	OF	B0	54	BB	16

**2.2.2. Shiftrows transformation**

After SubByte, ShiftRows is the following phase that impacts the state. This move's basic principle is to cyclically transfer state bytes from row zero to the left of each row. The bytes of row zero remain unchanged in operation, and no permutation is performed. Only one byte is circularly pushed to the left in the first row, then two bytes have been relocated to the left in the second row. Three bytes have been relocated to the left in the last row [31]. The size of the new state remains unchanged at 16 bytes, but the location of the bytes in the state has been moved as shown in Figure 5 [30].

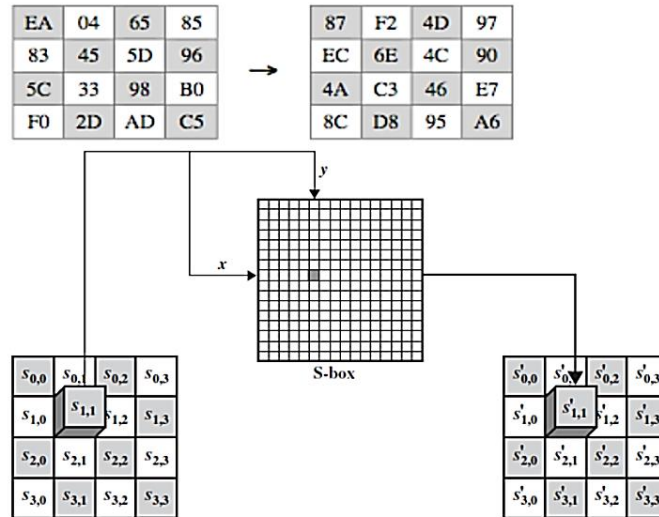


Figure 4. The substitute-byte transformation

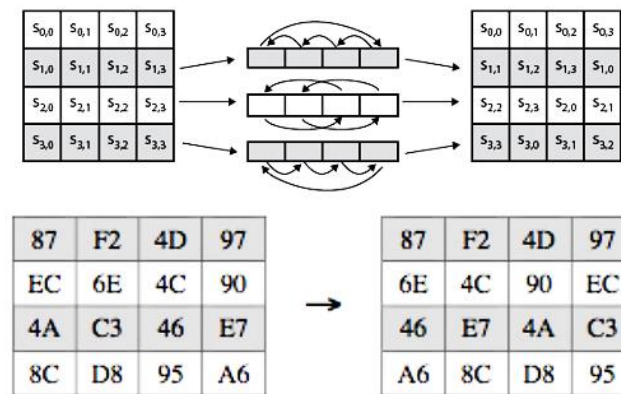


Figure 5. ShiftRows transformation

**2.2.3. Mix columns transformation**

Each byte of one row is multiplied by each value (byte) of the state column in the matrix transformation process. Simply put, each state column must multiply by each matrix transformation row. The multiplication results are merged with eXclusive OR (XOR) in producing a new set of four bytes intended for the following state. This phase does not change the size of the state; it remains at its original size of 4x4, as illustrated in Figure 6 [30].

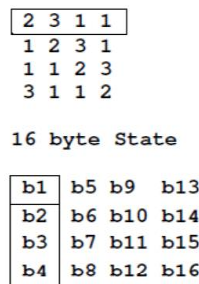


Figure 6. Multiplication matrix

**2.2.4. AddRoundKey transformation**

During this phase, the state (input data and key) are grouped in a 4×4 byte matrix [32]. The allocation of the 128-bit key and input data into the byte matrices is shown in Figure 6. When it comes to encrypting data, AddRoundKey can provide significantly more protection. The relationship between the key and the ciphertext is the basis for this operation. The primary key is utilized in originating the subkey in each round using the key scheduling of Rijndael. It has the same scale for subkey and state. The subkey is created by using bitwise XOR to combine each byte of the state with the corresponding byte of the subkey as shown in Figures 7 and 8 [33].

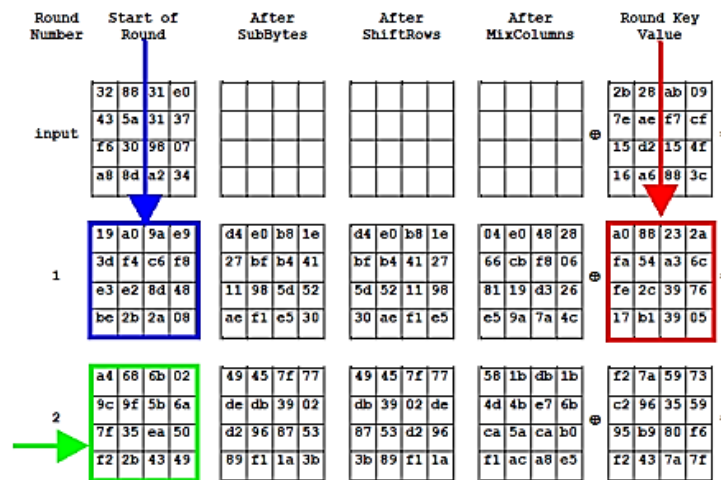


Figure 7. AddRound key

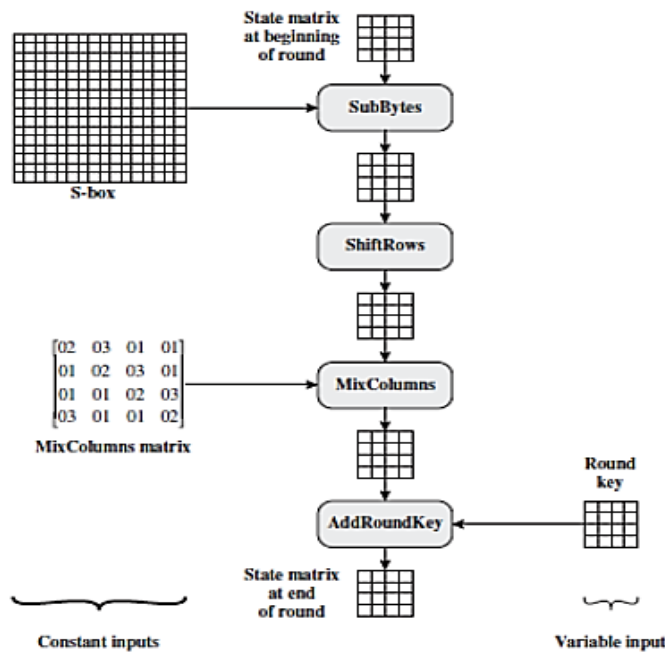


Figure 8. Inputs for single AES round

After these processes, the plaintext is now encrypted and is unreadable to others. With this, potential attackers will obtain scrambled, useless information in the database if they managed to penetrate the web server. To decrypt the ciphertext, the processes mentioned above must be performed reversely using the key used to encrypt it, as shown in Figure 1.

**2.3. System development model**

The development of the online registration will follow the rapid application development (RAD) methodology. It is a type of incremental model. In the RAD paradigm, the components or functions are constructed as if they were mini-projects. The projects are timed, delivered, and then put together into a working prototype. It can immediately provide something for the customer to see and use and feedback on their delivery and requirements. The model has been divided into four (4) stages: analysis and quick design; web application development, including building, demonstration, and refining; application testing; and application evaluation. Figure 9 shows the stages of online registration development using the AES algorithm.

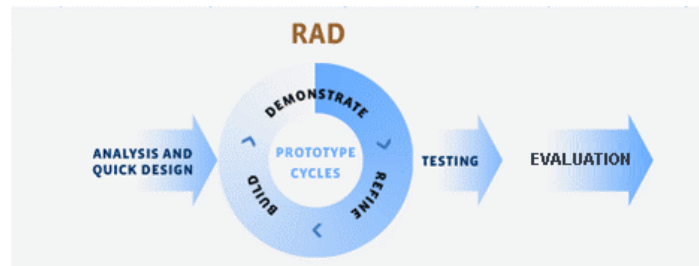


Figure 9. The rapid application development model used in the development of CHOY

**2.3.1. Analysis and quick design**

The analysis had been conducted to determine the information requirements. This include questions such as on what platform the system must be deployed based on the institution's clients. Also, researchers analyzed the problems by providing the present manual procedure diagram in Figure 10.

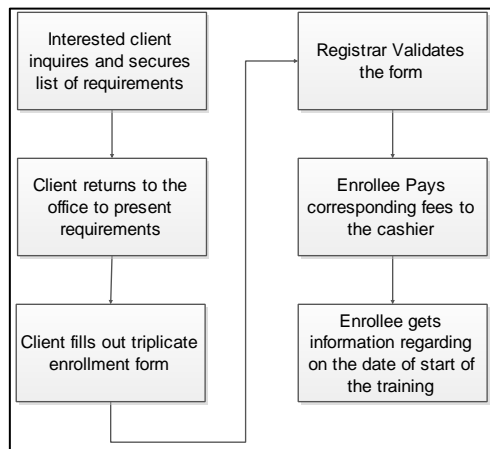


Figure 10. Manual procedure on registration of clients

The manual procedure for registering clients is as follows: interested clients from distant cities or municipalities will go to the registrar's office for inquiries. They will get vital information such as schedules, fees, and requirements. After securing all the required documents, clients will return to the registrar's office for validation. Afterward, clients will fill out a triplicate form for the cashier, accounting, student copy, and the main form for the registrar's office. After validating the form, the enrollee pays corresponding fees to the cashier and gets informed on training. A fishbone diagram has been constructed based on the manual process, as shown in Figure 11.

As shown in Figure 11, there are four (4) causes of the slow and unsecured method of student registration. One is the lack of security of data. Enrollment forms can be tampered with, resulting in unreliable information. It is also time-consuming because students must fill out a triplicate form, and afterward, the person-in-charge checks their profile form. The third is the large volume of paper work. In the



manual registration process, the enrollees must fill the triplicate form, and it is added to the burden of the registrar's personnel because they have to reproduce these forms. In addition to these are the attachments, such as requirements that need to be organized. Lastly, there are problems in data entry, usually in the form of unreadable writings and inevitable changes in information (e.g., change in marital status). The proposed process flow for administrators is shown in Figure 12.

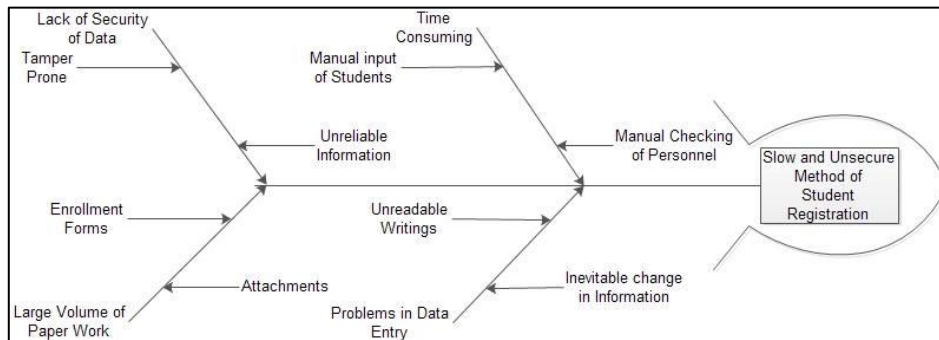


Figure 11. Fishbone diagram of the present registration system

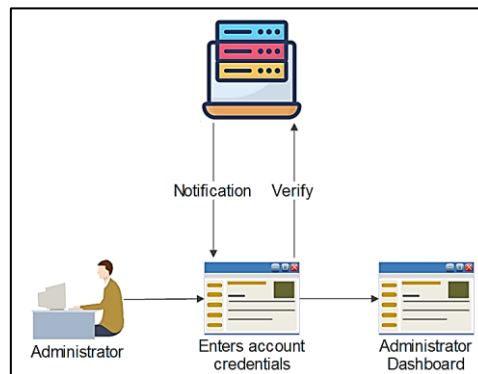


Figure 12. Process flow for administrator

Administrators must provide valid account credentials (username and password) in accessing the web app. It validates the entered credentials by decrypting the stored accounts on the database and checks whether the account entered exists or not. If yes, then the administrator can access the administrator dashboard, where he/ she can monitor students' applications. The AES decrypts information from the database before displaying it on the Administrator dashboard. The process flow for clients is illustrated in Figure 13. Clients must enter their complete personal information to accomplish the online registration. Subsequently, the AES algorithm encrypts the information before saving it in the database.

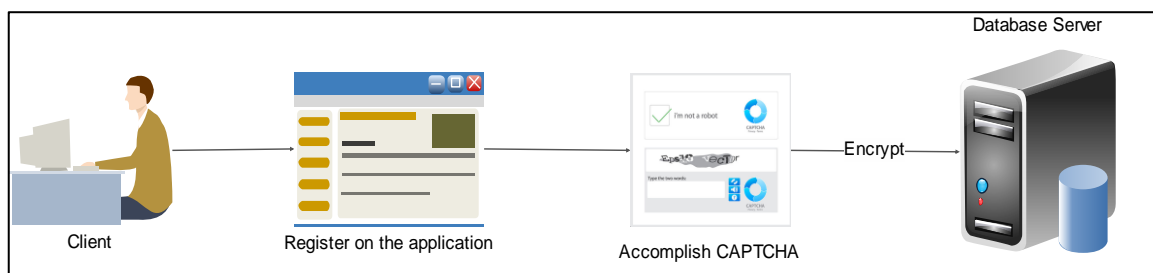


Figure 13. Process flow for clients

### 2.3.2. Development

The online registration was developed using Adobe Dreamweaver as the source code editor to keep track of the appearance of the web application while coding. For the HTTP and database server, XAMPP was considered since the application was developed on a windows platform. The application's interface and functionality were built using hypertext preprocessor (PHP) as the programming language and hypertext mark-up language (HTML) and JavaScript. The web server was APACHE, and the database server was MySQL. The device used in the web application development is a desktop computer with an Intel Celeron Processor of 2.4 GHz, 250GB Hard Disk, and 2GB DDR3 Memory running a 64-bit Windows 10 operating system.

### 2.3.3. Testing and evaluation

The following testing activities were conducted to ensure that the online registration works accordingly: the graphical user interface testing, in which the user interface is tested on a variety of devices to guarantee that every component of the interface is visible on a variety of devices and screen sizes; web app performance testing where all modules were tested to determine its response time; and Compatibility testing where the app was tested on various devices to ensure every component/functionalities are working on all types of devices. More importantly, online registration was tested in terms of information security and spam prevention. It is to ensure that the information saved on the repository is encrypted and spam can be prevented. To assess the technical features of the produced application in compatibility, reliability, and security, ISO 25010 was used [34]. Faculty, employees, and clients of the Southern Isabela College of Arts and Trades, a TESDA-administered school in the City of Santiago, Isabela, are included in the evaluation.

## 3. RESULTS AND DISCUSSION

### 3.1. Development and testing of CHOY applying the AES

The information based on analysis served as a basis for determining the web application's modules. Clients can access the online registration portion of the web app in which they need to provide their basic information such as full name and contact numbers, among others. Completely automated public Turing test to tell computers and humans apart (CAPTCHA) was used to prevent spamming by ensuring that the app would not be swamped with records from robots, as seen in Figure 14.

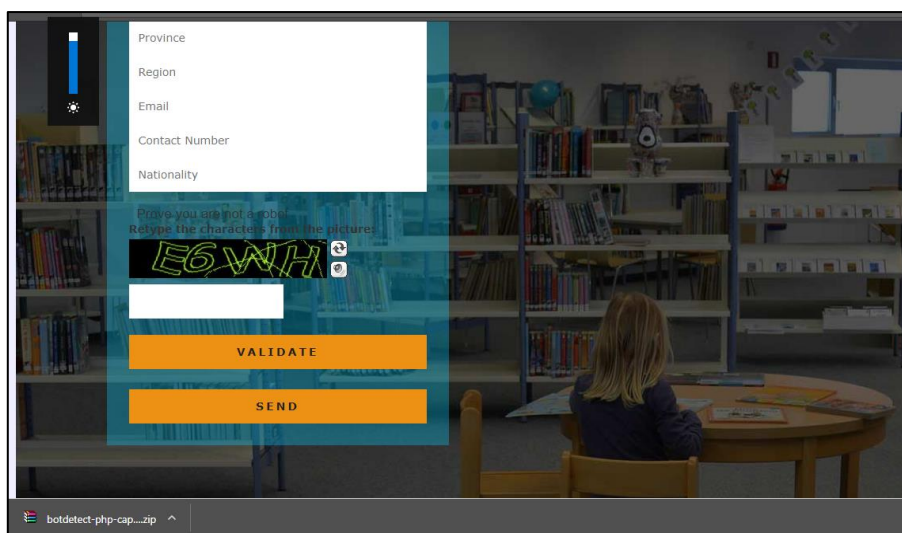


Figure 14. Client registration of CHOY

The advanced encryption algorithm encrypts all the information saved on the database regarding data security. For instance, if a specific client registers on the online registration, the saved information from the client will be encrypted. The record on the database is stored as a binary large object (BLOB) as shown in Figure 15.

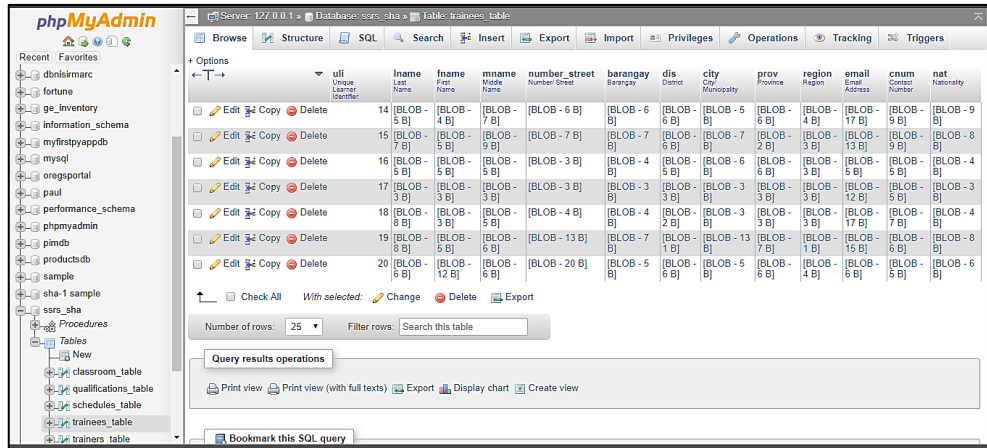


Figure 15. Live database content of CHOY

In a database management system, BLOB is a collection of binary data kept as a single object. If viewed or downloaded, the encrypted information will be shown. For instance, a sample plaintext "Olanday, Paul L." with hex key "37 33 20 36 39 20 36 33 20 36 31 20 37 34 20 34" will result in the following encrypted text: "JBc3QDfE156yGk4tipSK0H57aqc7XgVLIaHYoY3B6PM=". The web application will decrypt the encrypted information on the database by reversing the encryption process to make it readable for administrators, as shown in Figure 16. With this, even an attacker gains access to the database, he/ she cannot read any of its contents.

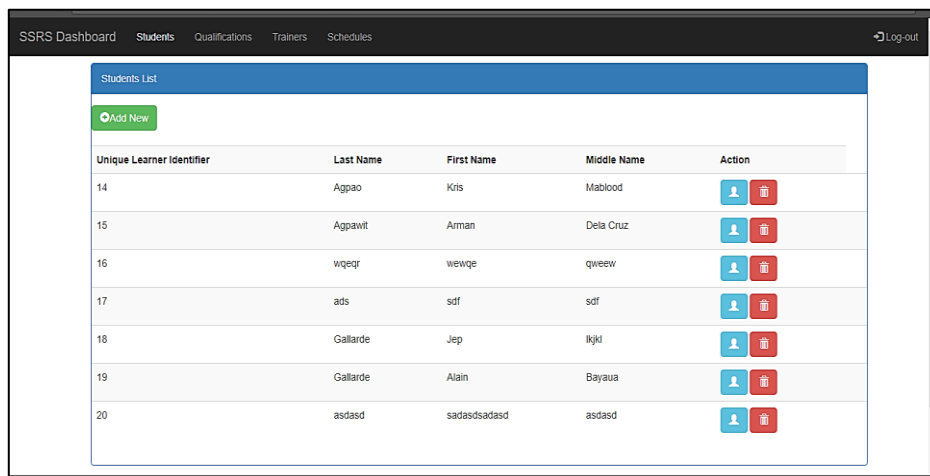


Figure 16. Decrypted information from the database on administrator dashboard

The administrator dashboard consists of four modules: i) students registration which contains all the registration of clients, ii) qualifications management, which is intended for adding, editing, and deleting qualifications or courses, iii) trainers management module allows profiling of trainers, and iv) schedule management where students, qualifications, and trainers are added in a particular schedule, thus making a student "officially enrolled".

### 3.2. Evaluation using the ISO 25010 standard

The study's proponents employed the ISO/IEC 25010 standard to assess the app's compatibility, reliability, and security elements. The compatibility evaluation demonstrated that CHOY could execute the needed functions as specified during the analysis phase and that users could access it via various devices, including cellphones, laptops, and desktops. Furthermore, as indicated in Table 2, the overall mean of 4.0 suggests that CHOY is commendable in coexistence and interoperability.

Table 2. Compatibility evaluation results

Criteria	Computed mean	Descriptive interpretation
<b>Compatibility</b>		
Coexistence. The application can efficiently perform its needed duties while sharing a shared environment and resources with other apps without causing problems.	4.02	Very Good
Interoperability. The online application that was created can be used on a variety of devices, including smartphones.	3.98	Very Good
Overall Mean	4.00	Very Good

Table 3 presents the reliability evaluation results. The overall mean of 4.0 shows that CHOY is reliable under normal operations. It also demonstrates that the app is operational and available when needed despite hardware or software failures. Finally, the web app can recover data that has been directly damaged, such as passwords and secret keys, and restore the program's desired state.

Table 3. Reliability evaluation results

Criteria	Computed mean	Descriptive interpretation
<b>Reliability</b>		
Maturity. Under regular operation, the designed application and its components meet the requirements for reliability.	4.00	Very Good
Availability. When needed, the application is operational and accessible.	4.05	Very Good
Fault Tolerance. Despite the presence of hardware or software flaws, the application performs as expected.	3.95	Very Good
Recoverability. In the event of an anomaly, the program can recover the data directly affected (for example, passwords and secret keys) and restore the system to its ideal state.	3.98	Very Good
Overall Mean	4.00	Very Good

Table 4 illustrates the security evaluation results, which reveal that CHOY ensures that data is only available to permitted users. It also protects computer programs and data from unwanted access or modification. The software includes built-in activity logs to document the action or events. This allows the actions of a given entity to be tracked back to it. Identifying a subject or resource can also be demonstrated as the one claimed. Because of the AES implementation, the overall mean of 4.04 indicates that the CHOY web app is secure.

Table 4. Security evaluation results

Criteria	Computed mean	Descriptive interpretation
<b>Security</b>		
Confidentiality. The application ensures that information is available only to those who have authorized access.	4.17	Very Good
Integrity. The application protects computer programs and data from unwanted access or alteration.	4.10	Very Good
Non-repudiation. The application uses activity logs to confirm that activities or events can be have occurred and cannot be denied later.	3.95	Very Good
Accountability. The application uses logs to trace an entity's actions.	3.93	Very Good
Authenticity. The app can identify a subject or resource to be the one claimed.	4.07	Very Good
Overall Mean	4.04	Very Good

#### 4. CONCLUSION

Per the methodology used and findings from this study, the proponents made the following conclusions: i) the CHOY web application serves as an avenue for potential learners to enroll regardless of their distance and the institution. It also serves as a powerful tool for administrators in automating repetitive tasks such as manually checking the enrollment forms, reducing problems in data entry, and making the overall enrollment process faster and more efficient, ii) the Advanced Encryption Standard can be applied in an online registration like the CHOY web app to further enhance the records' security. Even potential attackers gain access to the database, they can only obtain useless information because database contents are scrambled and unreadable. Therefore, the developed web application passes the testing series conducted in online registration and information security, and iii) the features of the CHOY web app were presented and evaluated to/by the stakeholders. The result shows that the overall mean comprises three criteria:

compatibility, reliability, and security garnered a score of 4.01, which has a descriptive interpretation as "Very Good." Hence, the AES implementation in the CHOY web application is effective and is accepted by the end-users.

The following recommendations were made based on the study's results and conclusions: i) the CHOY web application must cover all aspects of the enrollment process, specifically the cashiering and accounting processes. It must also be implemented as soon as possible, ii) the researchers of this study can enhance the AES algorithm to strengthen further the security of information stored in the database, and iii) the researchers can devise their own or use two or more algorithms to encrypt user information stored in the database to ensure data security further.

## ACKNOWLEDGMENTS

The researchers would like to thank the faculty, staff, and other Southern Isabela College of Arts and Trades stakeholders, especially the Vocational School Superintendent, Dr. Danilo P. Pacis, for the funding and support. They also like to express their utmost gratitude to everyone who helped make this study possible, especially those who have strong advocacy for educating new researchers for free.




## REFERENCES

- [1] S. Madan and S. Madan, "Security standards perspective to fortify web database applications from code injection attacks," in *ISMS 2010 - UKSim/AMSS 1st International Conference on Intelligent Systems, Modelling and Simulation*, Jan. 2010, pp. 226–230, doi: 10.1109/ISMS.2010.50.
- [2] T. Holz, S. Marechal, and F. Raynal, "New threats and attacks on the world wide web," *IEEE Security and Privacy*, vol. 4, no. 2, pp. 72–75, Mar. 2006, doi: 10.1109/MSP.2006.46.
- [3] OWASP, "OWASP Top 10," *OWASP Top 10- 2021*, 2021. <https://owasp.org/Top10/#welcome-to-the-owasp-top-10-2021> (accessed Mar. 23, 2021).
- [4] J. Pan and X. Mao, "DomXssMicro: A micro benchmark for evaluating DOM-based cross-site scripting detection," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 208–215, doi: 10.1109/TrustCom.2016.0065.
- [5] S. Shalini and S. Usha, "Prevention of cross-site scripting attacks XSS On Web Applications in the client side," *International Journal of Computer Science Issues*, vol. 8, no. 4, pp. 650–654, 2011.
- [6] N. Singh, M. Dayal, R. S. Raw, and S. Kumar, "SQL injection: Types, methodology, attack queries and prevention," in *Proceedings of the 10th INDIACOM: 2016 3rd International Conference on Computing for Sustainable Global Development, INDIACOM 2016*, 2016, pp. 2872–2876.
- [7] K. Kamtuo and C. Soomlek, "Machine learning for SQL injection prevention on server-side scripting," in *20th International Computer Science and Engineering Conference: Smart Ubiquitous Computing and Knowledge, ICSEC 2016*, Dec. 2017, pp. 1–6, doi: 10.1109/ICSEC.2016.7859950.
- [8] N. A. Al-Sayid and D. Aldlaen, "Database security threats: A survey study," in *2013 5th International Conference on Computer Science and Information Technology, CSIT 2013 - Proceedings*, Mar. 2013, pp. 60–64, doi: 10.1109/CSIT.2013.6588759.
- [9] M. A. M. Yunus, M. Z. Brohan, N. M. Nawi, E. S. M. Surin, N. A. M. Najib, and C. W. Liang, "Review of SQL injection: Problems and prevention," *International Journal on Informatics Visualization*, vol. 2, no. 3–2, pp. 215–219, Jun. 2018, doi: 10.30630/Joiv.2.3-2.144.
- [10] K. Arora and L. Harikrishnan, "Implementation of advance encryption standard (AES) to securely store and maintain research data," *International Journal of Engineering Technology, Management and Applied Sciences*, vol. 5, no. 4, pp. 127–130, 2017.
- [11] A. Verma, P. Gupta, and M. Deshmukh, "An efficient encryption technique for images using symmetric key cryptography and binary trees," *SSRN Electronic Journal*, 2018, doi: 10.2139/ssrn.3171511.
- [12] B. B. Zaidan, A. A. Zaidan, A. K. Al-Frajatand, and H. A. Jalab, "On the differences between hiding information and cryptography techniques: An overview," *Journal of Applied Sciences*, vol. 10, no. 15, pp. 1650–1655, Jul. 2010, doi: 10.3923/jas.2010.1650.1655.
- [13] N. Jirwan, A. Singh, and S. Vijay, "Review and analysis of cryptography techniques," *International Journal of Scientific and Engineering Research*, vol. 4, no. 3, pp. 1–6, 2013.
- [14] R. Sobti and G. Geetha, "Cryptographic hash functions - a review," *IJCSI International Journal of Computer Science Issues*, vol. 9, no. 2, pp. 461–479, 2012, [Online]. Available: <https://www.researchgate.net/publication/267422045>.
- [15] D. Anwar and D. Riyazuddin, "Transparent data encryption- solution for security of database contents," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 3, 2011, doi: 10.14569/ijacsa.2011.020305.
- [16] N. Kumar, R. Poovarasana, S. Harish, and D. Jagadish, "A comparative analysis of symmetric and asymmetric key cryptography," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 5, pp. 357–377, 2017.
- [17] P. Prasithsangaree and P. Krishnamurthy, "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2003, vol. 3, pp. 1445–1449, doi: 10.1109/glocom.2003.1258477.
- [18] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," *Global Journal of Computer Science and Technology Network, Web & Security*, vol. 13, no. 15, pp. 60–69, 2013, [Online]. Available: <https://computerresearch.org/index.php/computer/article/view/272/272>.
- [19] A. Mohammed Ali and A. K. Farhan, "Enhancement of QR Code capacity by encrypted lossless compression technology for verification of secure e-document," *IEEE Access*, vol. 8, pp. 27448–27458, 2020, doi: 10.1109/ACCESS.2020.2971779.
- [20] A. K. Farhan and M. A. A. Ali, "Database protection system depend on modified hash function," in *Conference of Cihan University-Erbil on Communication Engineering and Computer Science*, 2017, p. 84.
- [21] A. Kadhim and S. Khalaf, "New approach for security chatting in real time," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 4, no. 3, pp. 30–36, 2015.
- [22] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020, doi: 10.1109/ACCESS.2020.2989050.




- [23] J. R. Naif, G. H. Abdul-Majeed, and A. K. Farhan, "Secure IOT system based on chaos-modified lightweight AES," in *2019 International Conference on Advanced Science and Engineering, ICOASE 2019*, Apr. 2019, pp. 12–17, doi: 10.1109/ICOASE.2019.8723807.
- [24] M. Kannan, C. Priya, and S. VaishnaviSree, "A comparative analysis of DES, AES, and RSA crypt algorithms for network security in cloud computing," *Journal of Emerging Technologies and Innovative Research*, vol. 6, no. 3, pp. 574–582, 2019.
- [25] N. B. Sapna Singh, "A comparative study of some symmetric and asymmetric key cryptography algorithms," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 04, no. 03, pp. 1028–1031, 2015, doi: 10.15680/ijirset.2015.0403043.
- [26] A. Singh, M. Marwaha, B. Singh, and S. Singh, "Comparative study of DES, 3DES, AES and RSA," *International Journal Of Computers & Technology*, vol. 9, no. 3, pp. 1162–1170, Jul. 2013, doi: 10.24297/ijct.v9i3.3342.
- [27] J. Nechvatal *et al.*, "Report on the development of the advanced encryption standard (AES)," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 3, p. 511, May 2001, doi: 10.6028/jres.106.023.
- [28] P. Rewagad and Y. Pawar, "Use of digital signature and rijndael encryption algorithm to enhanced security of data in cloud computing services," in *IJCA Proceedings on Emerging Trends in Computer Science and Information Technology*, 2012, vol. 2, pp. 5–7.
- [29] M. Reza Z'aba and M. A. Maarof, "A Survey on the cryptanalysis of the advanced encryption standard," in *Proceedings of the Postgraduate Annual Research Seminar*, 2006, pp. 97–102.
- [30] R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, and M. Sanap, "AES algorithm using 512 bit key implementation," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 3, pp. 3516–3522, 2014.
- [31] N. Selmane, S. Guilley, and J. L. Danger, "Practical setup time violation attacks on AES," in *Proceedings - 7th European Dependable Computing Conference, EDCC-7*, May 2008, pp. 91–98, doi: 10.1109/EDCC-7.2008.11.
- [32] U. Kretzschmar, "AES128 – A C implementation for encryption and decryption," *Texas Instruments*, Texas ,2009. [Online]. Available: <https://community.element14.com/technologies/security/m/files/2440>.
- [33] H. Lee, K. Lee, and Y. Shin, "AES implementation and performance evaluation on 8-bit microcontrollers," *International Journal of Computer Science and Information Security*, vol. 6, no. 1, pp. 70–74, 2009, [Online]. Available: <http://arxiv.org/abs/0911.0482>.
- [34] iso25000, "Product Quality - ISO/IEC 25010," iso25000. <https://iso25000.com/index.php/en/iso-25000-standards/iso-25010> (accessed Feb. 23, 2021).

## BIOGRAPHIES OF AUTHORS






**Jomar L. Calpito**    is currently an Instructor and, at the same time, the Acting Registrar of the Southern Isabela College of Arts and Trades, a TESDA-administered school. He aims to continuously improve the processes within the institution and later within the agency. He finished his master's degree in Information Technology at the Isabela State University and is currently pursuing his doctorate in IT. He is also engaged in various scholarly works, especially in data security, image processing, frameworks, and simulated mockups for TVET. He can be contacted at email: [jomar.l.calpito007@gmail.com](mailto:jomar.l.calpito007@gmail.com).



**Paul L. Olanday**    is the former Registrar of the Southern Isabela College of Arts and Trades. With his dedication and commitment to improving the institution, he became the Vocational Instruction Supervisor, overseeing quality TVET training in the school. He received his master's degree in IT at the Isabela State University. Also, he is engaged in scholarly works related to improving the processes within the institution and later within the agency. He can be contacted at email: [plolanday@tesda.gov.ph](mailto:plolanday@tesda.gov.ph).



**Alain C. Gallarde**    is currently an Assistant Professor IV of the Southern Isabela College of Arts and Trades. He received his master's degree in IT at the Isabela State University. He aims to finish his doctorate, and his research interests involve developing frameworks for quality TVET, automation, and simulated mockups. He is selected as the TAGSANAY regional level awardee and serves as a coach in various ICT-related skills competitions. Also, he is a lead trainer and assessor in Trainers Methodology I and Computer Systems Servicing NC II. He can be contacted at email: [acgallarde@tesda.gov.ph](mailto:acgallarde@tesda.gov.ph).