



Implementation Aes-128 Encryption For Enhanced Data Security In Central Sulawesi Provincial Inspectorate

Imam Wahyudi*¹, Syahrullah¹, Dwi Shinta Anggreni¹, Rahmah Laila¹

¹Information Technology Department, Faculty of Engineering, Tadulako University, Jl. Soekarno Hatta No KM 9 Palu 94148 Central Sulawesi, Indonesia

*imamwahyudi140201@gmail.com

Abstrac. One technique to secure data is to use the Advanced Encrypt on Standard (AES) 128 method. The Advanced Encrypt on Standard (AES) method can be applied in improving data security, especially at the Central Sulawesi Provincial Inspectorate. The data in question are audit reports of BOS funds (School Operational Assistance), reports of special investigations into violations of regional finances and reports of violations of civil servant discipline (PNS). The data must have a high level of security, so that it is not easily known by irresponsible parties and will have a negative impact and be misused. The conclusion in this study was obtained that, the AES-128 algorithm can be used as an alternative to the process of improving data security, namely by encryption and decryption. The results of encryption can be guaranteed as long as the symmetry key encryption is not leaked to irresponsible parties.

Keywords; *Advanced Encrypt on Standard (AES)128, Data security, encryption and description, report.*

(Received 2024-02-13, Accepted 2024-04-24, Available Online by 2024-06-11)

1. Introduction

The development of information technology is currently propagating in various fields, both in government agencies and in private companies. Data security is the only thing that must be considered so that it is not easy to know or leak to other parties. If you use the advanced Encrypt on Standard (AES) 128 algorithm, the encrypted data can be guaranteed security. Security measures of a system to protect data transferred or transmitted over telecommunication networks can be applied to secure data known as cryptography. [15,16]

Cryptography uses a variety of techniques in an attempt to secure data. Cryptography is the science and art of keeping messages confidential by converting messages into forms in which they no longer understand their meaning. Cryptographic techniques are used to encrypt files so that only the recipient who has the secret key can read and understand the file. Cryptography has an important role in maintaining the confidentiality, integrity, and authentication of data in the digital world that converts clear messages (plaintext) into encrypted messages (ciphertext) [6,8].

There are several techniques to disguise files including the Advanced Encrypt on Standard (AES) method. The Advanced Encryption Standard (AES) algorithm is a block cipher algorithm and has symmetry properties that use symmetry keys during the encryption and decryption process. [1,20]

AES is used as the latest cryptographic algorithm standard published by NIST (National Institute of Standard and Technology) as a replacement for the outdated DES (Data Encryption Standard) algorithm. The AES algorithm is a cryptographic algorithm that can encrypt and decrypt data with varying key lengths, namely 128 bits, 192 bits, and 256 bits. [3,17]

There are 4 rounds of transformation in the process of encryption and decryption consisting of *SubBytes*, which serve to exchange the contents of bytes using the substitution table. *ShiftRows*, The process of shifting blocks per row on an array of states. *MixColumn*, The process of multiplying a block of data (randomization) in each state array with the formula $A(x) = \{03\}x2 +$

$\{01\}x^2 + \{01\}x + \{02\}$, *AddRoundKey*, Combines state array and round key with XOR relationship.[1] Combines status arrays and round buttons with XOR relationships. In the decryption process of AES: *InvShiftRows algorithm* , slide the bits to the right on each line block. *InvSubBytes*, Each element in the state is mapped with an Inverse S-Box table. *InvMixColumn*, Each column in the state is multiplied by the AES matrix. *AddRoundKey*, Concatenates an array of states and round keys with an XOR relationship. [11,4] At the beginning of the encryption process, inputs that have been copied to the state will undergo an *AddRoundKey* transformation. After that the state will undergo *SubBytes*, *ShiftRows*, *MixColumns*, and *AddRoundKey* transformations repeatedly as many times as rounds (Nr). This process in the AES algorithm is referred to as the spherical function. In the final round, states are not awarded the *MixColumns* transformation. [5,9]

2. Method

The research method used is descriptive research, which aims to explain or describe the phenomenon by developing an application to encrypt and decrypt data using the AES-128 algorithm based on desktop applications, this study explores topics without specific hypotheses which ultimately serve as a fundamental starting point for improving data security. [2,12]

3. Research and Discussion

3.1. Planning

AES (Advanced Encryption Standard) is a cryptographic algorithm that is highly relied upon in securing data. By using 128-bit blocks, AES provides a robust encryption and decryption process through a series of operations such as *SubBytes*, *ShiftRows*, *MixColumns*, and *AddRoundKey*. AES is used extensively in encrypting and decrypting files to protect sensitive information. In addition, protection from crypto attacks and attention to performance and efficiency are also required. Taking those challenges into account, AES remains a powerful tool in protecting sensitive data across a wide range of application environments.

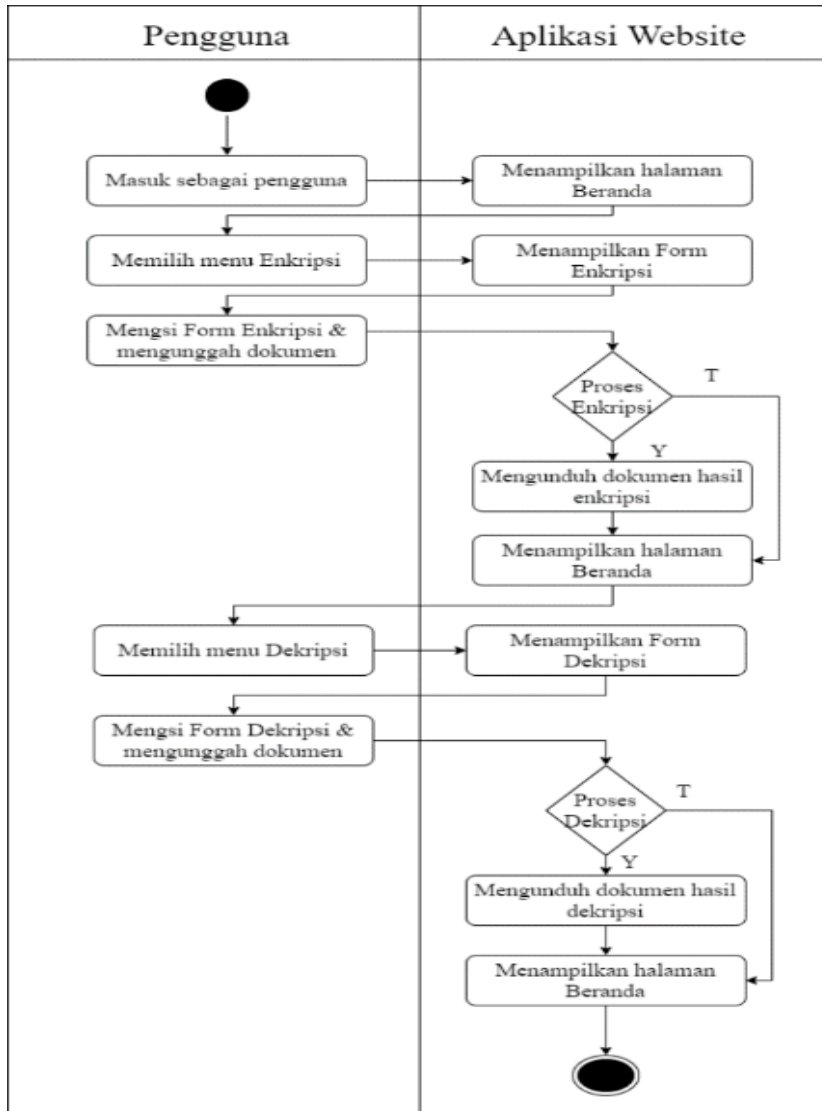
3.2. Analysis.

At this stage, the analysis was carried out by observing and interviewing auditors of the Central Sulawesi Provincial Inspectorate to encrypt and describe the file. This encryption process aims to improve the performance of the data security system, by converting sensitive information into an unreadable format without the appropriate encryption key. By implementing an effective encryption process.

3.3. System Design.

This user activity diagram used to illustrate structured activities and actions between user and system interactions[13,14] can be seen in the following figure:

Figure 1. User Activity Diagram.



A flowchart is a systematic presentation of the process and logic of information handling activities or a graphical depiction of the steps and sequence of procedures of a program. A flowchart is a chart that shows the flow in a program or system procedure logically. [18,19] The algorithm design of the application program, will be explained using flowcharts.

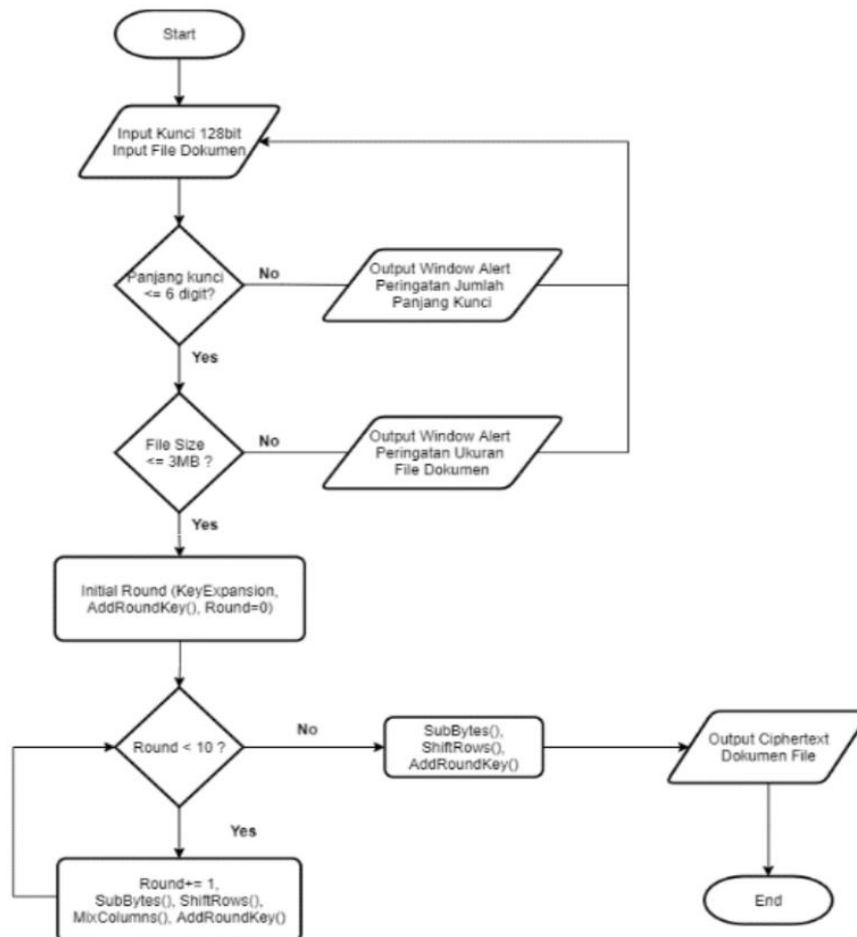


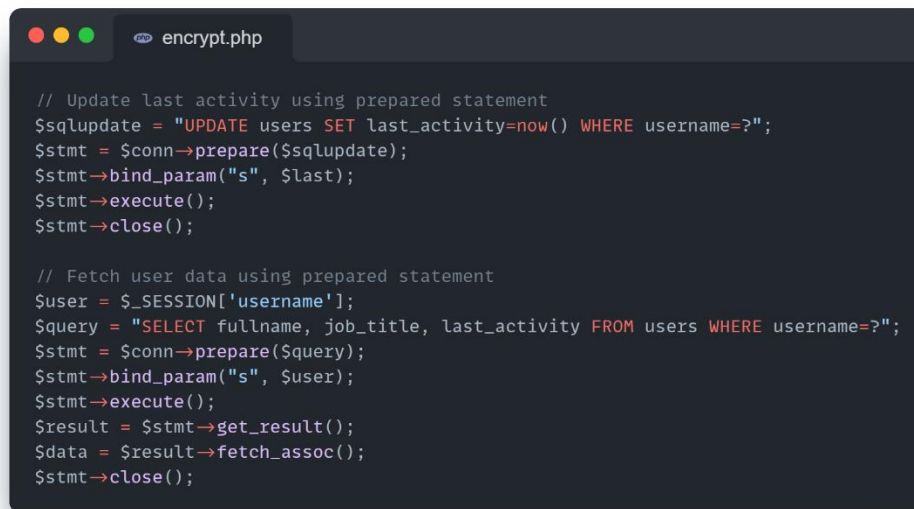
Figure 2. AES 128-bit encryption and Decryption Flow Diagram

3.4. Prototype.

This prototype stage is done to build a user interface with the admin, which shows the process of the application flow. Create a Prototype using the figma app.

3.5. Implementation

On this page, there is a table that lists documents belonging to users, which have previously been processed. On the Encryption Page, admins can encrypt digital files by filling out an encryption form and uploading the file document from internal storage, file upload date, file description, and entering a password as the symmetry key used to encrypt the document. The encoding view of document encryption is shown in Figure 5 below:

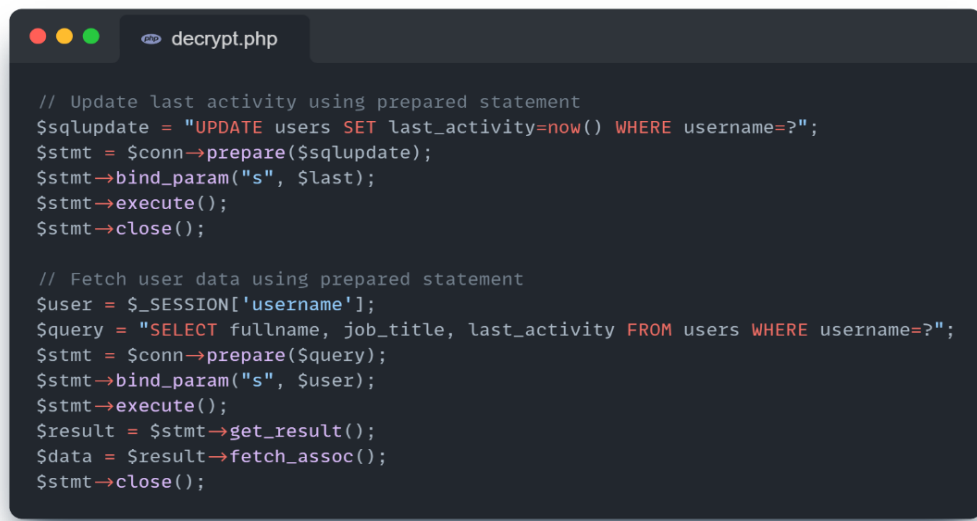
A screenshot of a code editor window titled 'encrypt.php'. The code is written in PHP and uses PDO for database operations. It contains two main sections: one for updating the last activity of a user and another for fetching user data. The update section uses an UPDATE statement with a prepared statement to set the last activity to the current time for a specific user. The fetch section uses a SELECT statement with a prepared statement to retrieve the full name, job title, and last activity of a user based on their session ID.

```
// Update last activity using prepared statement
$sqlupdate = "UPDATE users SET last_activity=now() WHERE username=?";
$stmt = $conn->prepare($sqlupdate);
$stmt->bind_param("s", $last);
$stmt->execute();
$stmt->close();

// Fetch user data using prepared statement
$user = $_SESSION['username'];
$query = "SELECT fullname, job_title, last_activity FROM users WHERE username=?";
$stmt = $conn->prepare($query);
$stmt->bind_param("s", $user);
$stmt->execute();
$result = $stmt->get_result();
$data = $result->fetch_assoc();
$stmt->close();
```

Figure 3. Document Encryption

Admins can decrypt digital files consisting of file source, encrypted file name, file path, file status, and options. The coding display for document decryption can be seen in Figure 6 below:

A screenshot of a code editor window titled 'decrypt.php'. The code is written in PHP and uses PDO for database operations. It contains two main sections: one for updating the last activity of a user and another for fetching user data. The update section uses an UPDATE statement with a prepared statement to set the last activity to the current time for a specific user. The fetch section uses a SELECT statement with a prepared statement to retrieve the full name, job title, and last activity of a user based on their session ID.

```
// Update last activity using prepared statement
$sqlupdate = "UPDATE users SET last_activity=now() WHERE username=?";
$stmt = $conn->prepare($sqlupdate);
$stmt->bind_param("s", $last);
$stmt->execute();
$stmt->close();

// Fetch user data using prepared statement
$user = $_SESSION['username'];
$query = "SELECT fullname, job_title, last_activity FROM users WHERE username=?";
$stmt = $conn->prepare($query);
$stmt->bind_param("s", $user);
$stmt->execute();
$result = $stmt->get_result();
$data = $result->fetch_assoc();
$stmt->close();
```

Figure 4. Document Description

4. System Testing

4.1. Testing the Encryption Process

Through the Encryption Menu, Encryption is changing the message or encoding data from the original message (plaintext) that is transformed into a form that is not clear to understand and even understand. Advanced encryption standard algorithms have a 128-bit key length consisting of AddRoundKey, SubBytes, ShiftRows and MixColumns[10]. The encryption process can be seen in Figure 7 below;

```

encrypt-process.php

$file = rand(1000, 100000) . "-" . $file_name;
$new_file = strtolower(str_replace(' ', '-', $file));
$final_file = "file_encrypt/" . $new_file;

$sql1 = "INSERT INTO file VALUES ('', '$user', '$new_file', '$new_file.rda', '', '$size2', '$key', now(), '1', '$deskripsi')";
$query1 = mysqli_query($koneksi, $sql1) or die(mysqli_error($koneksi));

$sql2 = "SELECT * FROM file WHERE file_url = ''";
$query2 = mysqli_query($koneksi, $sql2) or die(mysqli_error($koneksi));

$url = $new_file . ".rda";
$file_url = "file_encrypt/$url";

$sql3 = "UPDATE file SET file_url = '$file_url' WHERE file_url = ''";
$query3 = mysqli_query($koneksi, $sql3) or die(mysqli_error($koneksi));

$file_source = fopen($file_tmpname, 'rb');
$file_output = fopen($file_url, 'wb');

$mod = $size % 16;
$banyak = ($mod == 0) ? ($size / 16) : (($size - $mod) / 16) + 1;

if (is_uploaded_file($file_tmpname)) {
    ini_set('max_execution_time', -1);
    ini_set('memory_limit', -1);
    $aes = new AES($key);

    for ($bawah = 0; $bawah < $banyak; $bawah++) {
        $data = fread($file_source, 16);
        $cipher = $aes->encrypt($data);
        fwrite($file_output, $cipher);
    }
}

```

Figure 5. The document encryption process

After the system successfully reads the contents of the document, all characters contained in the document will be converted into blocks of hexadecimal numbers measuring 128 bits which will then be converted into a two-dimensional matrix measuring 4x4 called the state matrix. Before entering the first round, the state matrix is the first XOR, precisely with the 0 round key (rk0) or passkey.

4.2. Process Description Testing.

The transformation bytes used in the decryption process are AddRoundKey, InvShiftRows, InvSubBytes, and InvMixColumns. In the decryption process, for the first iteration, AddRoundKey, Inverse ShiftRows, and Inverse SubBytes transformations are performed. The cipher text will perform the AddRoundKey transformation. [7] The successful description process can be seen in the following encoding image:

```

decrypt-process.php

$idfile = $conn->real_escape_string($_POST['fileid']);
$pwdfile = $conn->real_escape_string(substr(md5($_POST["pwdfile"]), 0, 16));
$query = "SELECT password, file_url, file_name_source, file_size FROM file WHERE id_file='$idfile' AND password='$pwdfile'";
$result = $conn->query($query);

if ($result->num_rows > 0) {
    $data = $result->fetch_assoc();

    $file_path = $data["file_url"];
    $key = $data["password"];
    $file_name = $data["file_name_source"];
    $size = $data["file_size"];

    $file_size = filesize($file_path);

    $query2 = "UPDATE file SET status='2' WHERE id_file='$idfile'";
    $conn->query($query2);

    $aes = new AES($key);

    $fopen1 = fopen($file_path, "rb"); // Open the encrypted file for reading
    $fopen2 = fopen("file_decrypt/$file_name", "wb"); // Open the decrypted file for writing
}

```

Figure 6. The decryption process was successful

The test results obtained through this study in the form of digital document encryption results and decryption processes are valid and can be seen in the system test results as follows:

Table 1. System Test Results

Feature	Feature functions	Result
Login (admin)	Admin login so not just anyone can access admin features	Valid
File encryption	Enter data and upload encrypted files	Valid
File description	Describe encrypted files	Valid
File list	View encrypted files and file descriptions	Valid
Login (user)	User login to access other features in the app	Valid
List of files and downloads	Displays the results of the file described for download	Valid

5. Conclusion

The use of the 128-bit Advanced Encryption Standard (AES) algorithm is a strategic step for the Central Sulawesi Provincial Inspectorate in ensuring data security. By implementing AES-128, the Inspectorate can encrypt sensitive data with a high level of security, reducing the risk of unauthorized access or information theft. However, the success of a data security strategy is not solely determined by the choice of encryption algorithm alone. Factors such as effective key management, implementation of strict security policies, and increased awareness of information security also need to be considered. In addition, potential future research in the field of data security includes the development of stronger encryption algorithms, more efficient key management, security in cloud computing environments, and increased user awareness of information security policies. The Central Sulawesi Provincial Inspectorate can continue to improve their data security and keep sensitive information safe from threats.

Reference

- [1] Cristy, N., & Riandari, F. (2021). *Niolinda Cristy 1 , Fristi Riandari 2 [Implementation of Advanced Encryption Standard (AES 128 bit) method to secure financial data. 4(2), 75.*
- [2] Clivent gerhard sondakh et al. (2024), *Implementation of data layer in Blockchain network using SHA256 Hashing Algorithm*
- [3] Hermawan, A., Halim, A., Susilawati, D., Putri, I. A., Informatics, J. T., Science, F., Technology, D., & Dharma, U. B. (n.d.). *Journal of Informatics and Software Engineering Implementation of Advanced Encryption Standard and Caesar Cipher Algorithms on Encrypted Messages.*
- [4] Muharram, F. (2018). *Algorithm analysis on the process of encrypting and decrypting files using advanced encryption standards. Proceedings of the National Seminar on Computer Science and Information Technology, 3(2).*
- [5] Nurnaningsih, D., & Permana, A. A. (2018). *Design data security applications with Advanced Ency Standard (AES) algorithms. Journal of Informatics Engineering, 11(2), 177–186. <https://doi.org/10.15408/jti.v11i2.7811>*
- [6] Prameshwari, A., & Literature, N. P. (2018). *Implementation of Advanced Encryption Standard (AES) 128 algorithm for encrypting and decrypting document files. Explore Informatics, 8(1), 52. <https://doi.org/10.30864/eksplora.v8i1.139>*
- [7] Suranta, A. I., Virgia, D., & Sakti, S. Y. (2022). *Application of AES (Advance Encryption Standard) 128 Algorithm for Document Encryption at PT. Mount Geulis*

- Eternal Beauty. SKANIKA: Computer Systems and Information Engineering*, 5(1), 1–10.
- [8] R. Tullah, M. I. Dzulhaq, and Y. Setiawan, "Design of File Cryptography Applications with Advanced Encryption Standard (AES) Algorithm Method," *J. Sisfotek Glob.*, vol. 6, no. 2, pp. 24–30, 2016.
- [9] G. Gumira, Ernawati, and A. Erlanshari, "Implementation of Advanced Encryption Standard (AES) and Message Digest 5 (MD5) methods on document encryption (Case Study of LPSE UNIB)," *J. Recursive*, Vol. 4, No. 3, pp. 277–287, 2016.
- [10] V. Novianty, J. Algorithm, S. Tinggi, T. Garut, and I. Introduction, "Securing Cooperative Financial Databases," *J. Algorithms. High-tech colonel. Arrowroot*, vol. Vol. 12, pp. 1–7, 2015
- [11] A. Prameshwari and N. P. Sastra, "Implementation of Advanced Encryption Standard (AES) 128 Algorithm for Encryption and Decryption of Document Files," *Ekslorra Inform.*, vol. 8, no. 1, p. 52, 2018, DOI: 10.30864/explora.v8i1.139.
- [12] D. S. Purnia, M. F. Adiwisastro, H. Muhajir, and D. Supriadi, "Digital Divide Measurement Using Website-Based Descriptive Method," *EVOLUTION J. Science and Manaj.*, Vol. 8, No. 2, Sep 2020, doi: 10.31294/evolution.v8i2.8942.
- [13] T. Arianti, A. Fa'izi, S. Adam, and M. Wulandari, "Library Information System Design Using UML (Unified Modelling Language) Diagrams," vol. 1, 2022.
- [14] M. Syarif and E. B. Pratama, "Analysis of Blackbox Testing Software Test Methods and UML Diagram Modeling in Veterinary Service Applications Developed with Waterfall Models," vol. 5, no. 2, 2021.
- [15] HS, S. COMPUTER SECURITY GUIDE Security. [https://www.academia.edu/31730328/PANDUAN_KEAMANAN_KOMPUTE R_K_eamanan_komputer](https://www.academia.edu/31730328/PANDUAN_KEAMANAN_KOMPUTE_R_K_eamanan_komputer)
- [16] Wirdasari, d. *Get to know computer security techniques and attack models (Security Attack Models)*. Safe. Attack model. 4, 111–119 (2008).
- [17] A. Prameshwari and N. P. Sastra, "Implementation of Advanced Encryption Standard (AES) 128 Algorithm for Encryption and Decryption of Document Files," *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139
- [18] Umniy Salamah, Andi Purnomo "Cooperative Savings and Loans Application at PT. Mobile-Based Primantara Using FIFO Algorithm" *Journal of SISFOKOM (Information Systems and Computers)*, Volume 09, Number 01, PP 51 – 58
- [19] Fahry Fadila Risky, Darjat Saripurna, Iskandar Zulkarnain "Design of Solar Tracking Panel System to Determine the Direction of Solar Panels on the Sun with Microcontroller-Based Fuzzy Method"
- [20] Primartha, Rifkie. January 2013. The implementation of encryption and decryption of files uses the Advanced Encryption Standard (AES) algorithm. *Journal of Computer Science Research and Applications*, Vol. 2, No. 1: 13-18.