Web-Based Payroll Data Security Application Using the AES Cipher Method at the Mangga Dua Store Kebumen

Pandu Cahyo Sukoco [*, a,1] , Afwan Anggara [b,2]
[a,b] Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia
[1] cahyosukoco86@gmail.com, [2]angga_afw@uty.ac.id[*]

Abstract

Mangga Dua Store is a shop that is engaged in selling clothes, pants, and other products. In processing salary data, Mangga Dua Store employees only processing data in the form of text files in Microsoft Excel without any file protection which causes misuse of data by unauthorized people. To solve this problem, data protection is needed using a method to encrypt employee salary data. This study is conducted to protect employee salary data using the AES 128 Cipher Method. This research resulted in a Web-Based Payroll Data Security Application Using the AES 128 Cipher Method by performing encryption and decryption to protect employee salary data. Based on the results of research and discussions that have been carried out, it shows that the Data Security Application Using the Aes Cipher Method 128 employee salary data at the Mangga Dua Store can be encrypted and decrypted. So that it can avoid any misuse or manipulation of data that can be done by unauthorized people which can result in losses of the Mangga Dua Store.

Keywords: *Advance Security Standard*, Payroll Application, *Website*, *PHP*, Data Security.

I. INTRODUCTION

Mangga Dua Store is a shop that was pioneered by Muhtadin which is engaged in selling products in the form of clothes, pants, shoes, bags, and socks. Mangga Dua shop has 9 employees. The salary received by employees every month is in accordance with the UMR with bonuses every year based on the discipline and work spirit of the employees. In processing employee salary data, Mangga Dua Shop only processes salary data in the form of text files from Microsoft Excel without adequate file protection. [1] employee salary data is confidential data that can only be managed by the treasurer or head of the office. Therefore, the company tries to secure the data in order to avoid misuse or manipulation of data by unauthorized people which can result in losses to the company.

Technological developments cannot be separated from applications.[2]states the application is a ready-made program that can be used to execute commands from the application user with the aim of getting more accurate results in accordance with the purpose of making the application. The application has several platforms, namely desktop, web, and mobile. The website is an information presentation service that uses the concept of a hyperlink, which makes it easier for users to get information [3]. According to [4], the web is the entire web page contained in a domain that contains information. The application will be in direct contact with the data. [5] said data is a raw material that can later be processed further to become something more meaningful.

A company has data that is very risky for its security, especially payroll data. Salary is a receipt as a form of compensation from the employer to the employee for a job or service that has been performed and stated or valued in the form of money that is determined or based on an agreement or legislation and is paid based on a work agreement between the entrepreneur and the employee. [6].

Payroll applications will include the AES Cipher algorithm to improve employee data security. [7] states that the Advanced Encryption Standard is included in the type of cryptographic algorithm which has symmetrical properties and is a block cipher. This algorithm uses the same key at the time of encryption at the time of input and output in the form of blocks with a certain number of bits. The Advanced Encryption Standard algorithm is divided into 3 options, namely AES-128, AES-192, and AES-256.

Advanced Encryption Standard (AES) is a cryptographic algorithm that has become the current standard for symmetric key encryption algorithms. In the AES 128 cryptographic algorithm, 1 plaintext block is 128-bit, which is first converted into a 4x4 hexadecimal matrix called state. Each state element is 1 byte in size. The encryption process in AES is a transformation of the state repeatedly in 10 rounds [8].

As for the development of payroll applications, a system design is needed which includes the stages of the process using a Flowchart, which is a standard to describe a process [9]. Stages of database design using Entity-Relationship Diagram (ERD). [10] ERD is a tool used to model data structures by describing entities and relationships between relationships (entities) in an abstract (conceptual) manner. The next stage is to model the

system data flow using DFD. DFD is a diagram that uses symbols to reflect processes, data sources, data flows, and entities in a system. [11].

This research will focus on improving security in payroll applications. The AES Cipher Algorithm will be used to maximize the level of security in the application. Because of the importance of employee data, there must be an algorithm to secure the data from misuse.

II. METHOD

This study uses the Cipher AES method to improve security. Increased security according to needs and in accordance with the analysis and design that has been made.

A. System Requirements Analysis

In general, the purpose of developing the system is to improve security in processing salary data. Improved security using the Advanced Encryption Standard (AES) algorithm. This algorithm is expected to be a security in payroll applications so that there is no misuse or manipulation of data by unauthorized persons which can result in losses.

This research requires data related to employee data and employee salary data at the Mangga Dua Shop. The data obtained can be seen in the following table.

Table I. Employee Data

No	Nama Lengkap	Jabatan
1	H. Muhtidin	Direktur
2	Nur Mei Lia	Manajer
3	Ariyadi	Wakil Manajer
4	Mudatsir	Sekertaris
5	Puji Daryanti	Karyawan
6	Emawati	Karyawan
7	Fajar	Karyawan
8	Yanti	Karyawan
9	Aminudin	Karyawan
10	Nani	Karyawan

B. System Design

The proposed system will be built based on a website where this system can display information on the results of processing employee salary data at the Mangga Dua Shop where the information can be encrypted using the Advanced Encryption Standard (AES) method to protect information on the results of processing employee salary data.

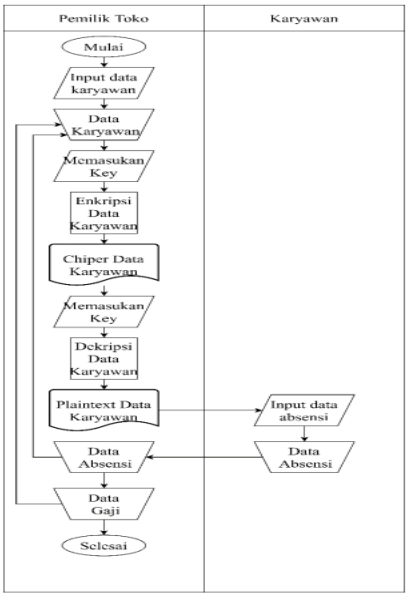

Figure 1. System Design

The database design that was built can be seen in Figure 2.

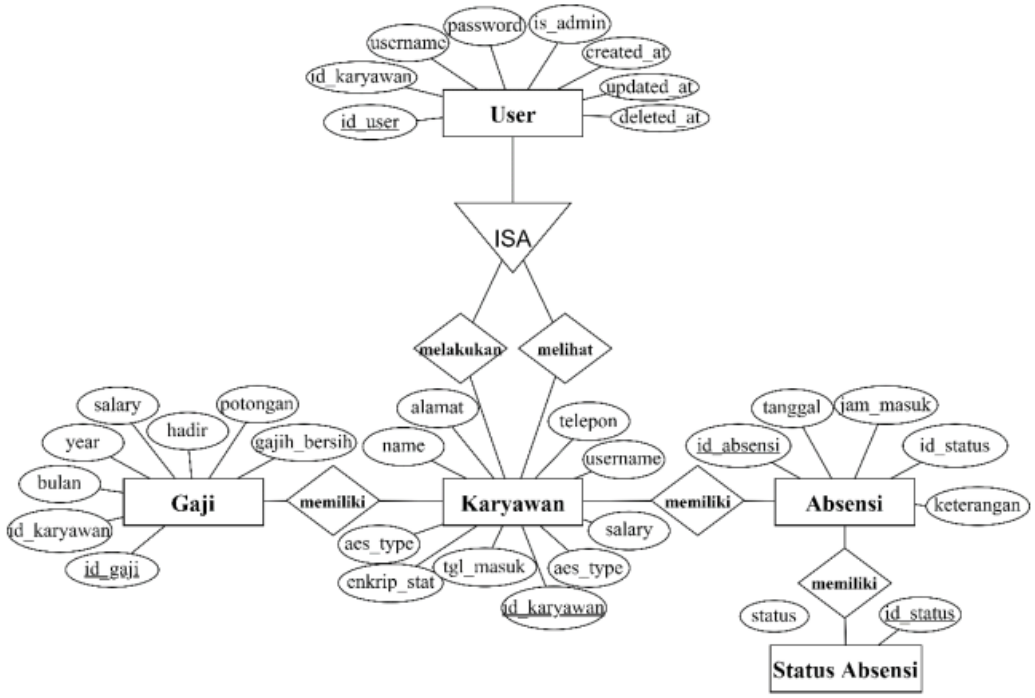

Figure 2. Entity Relationship Diagram

To describe the system process data flow that includes processes for owners and employees. The owner can process employee data, employee attendance data, and employee attendance data and can encrypt and decrypt employee data to protect employee information changes from irresponsible parties. Meanwhile, employees can perform attendance on the system as shown in Figure 3.

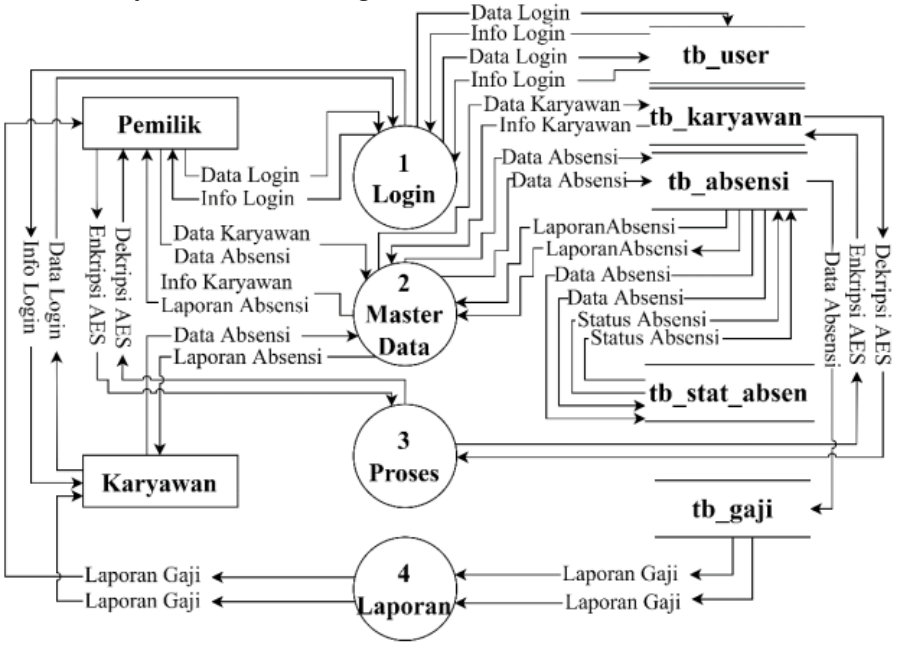

Figure 3. Data Flow Diagram Level 1

III. RESULT AND DISCUSSION

This research will produce a payroll application. The payroll application has security features that are supported by the AES Cipher Algorithm. So that the application can protect data from misuse.

A. Employee Page

The employee page is a page that can only be accessed by the shop owner. On this page, shop owners can manage employee data in the form of inserting, updating, and deleting employees.

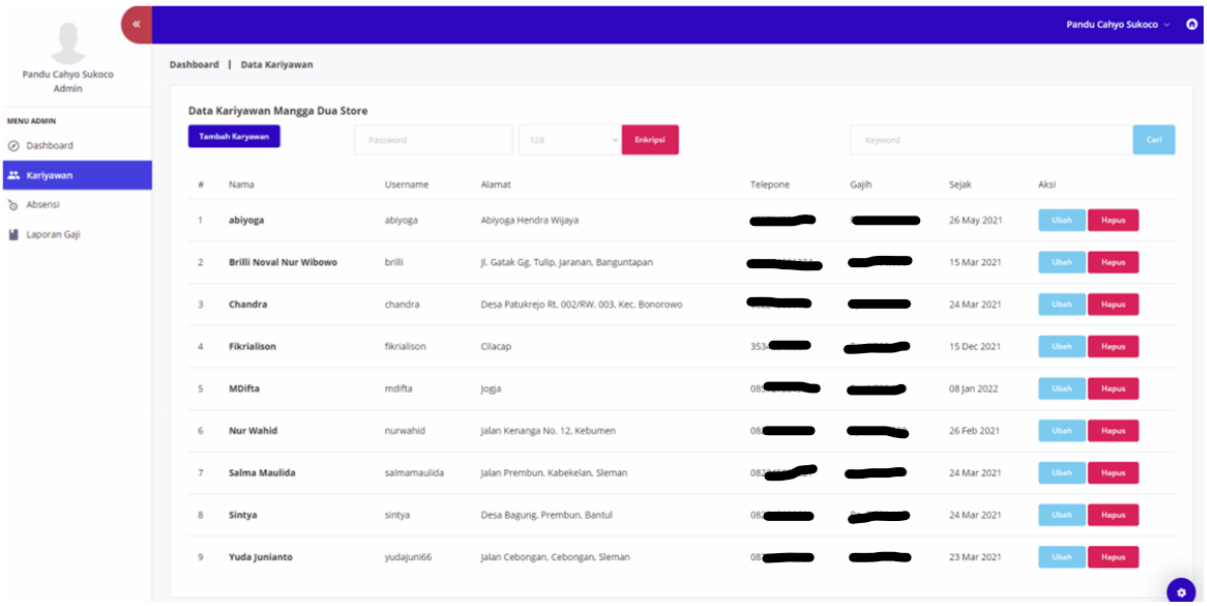

Figure 4. Employee Page

B. *Salary Report Page*

This page is a page that displays salary reports that have been issued to employees. On this page, the owner can print salary reports.

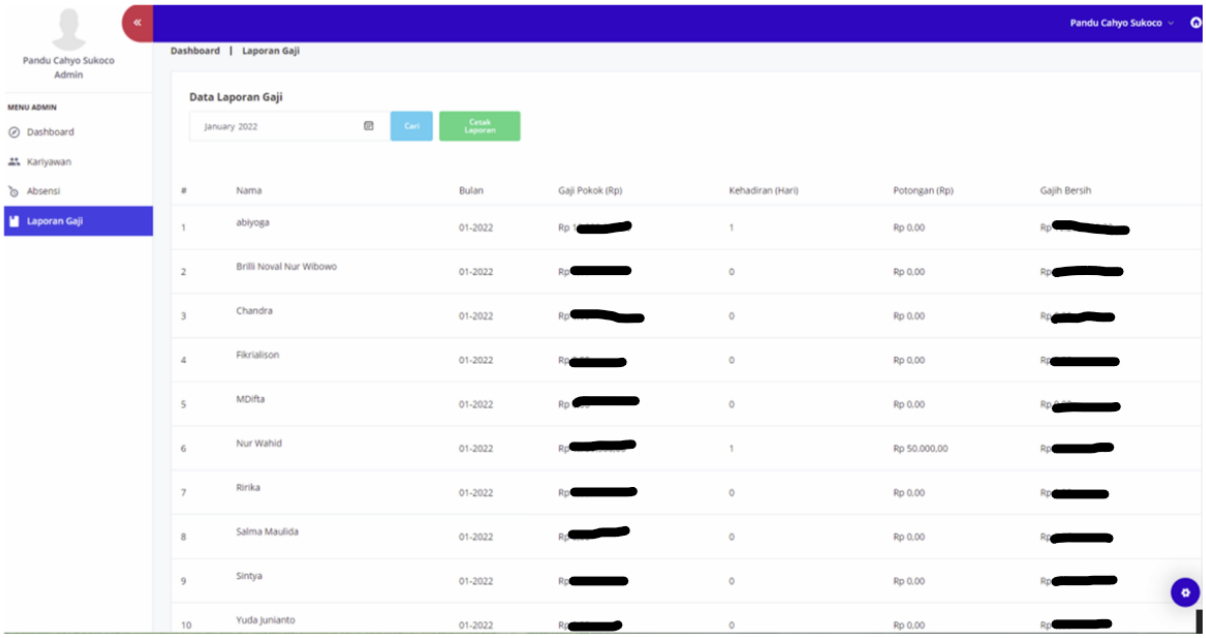

Figure 5. Salary Report Page

C. *Encryption Process*

The encryption process is carried out on employee data including salary data. Encryption is done with AES 123. The results of the encryption are shown in the image below.

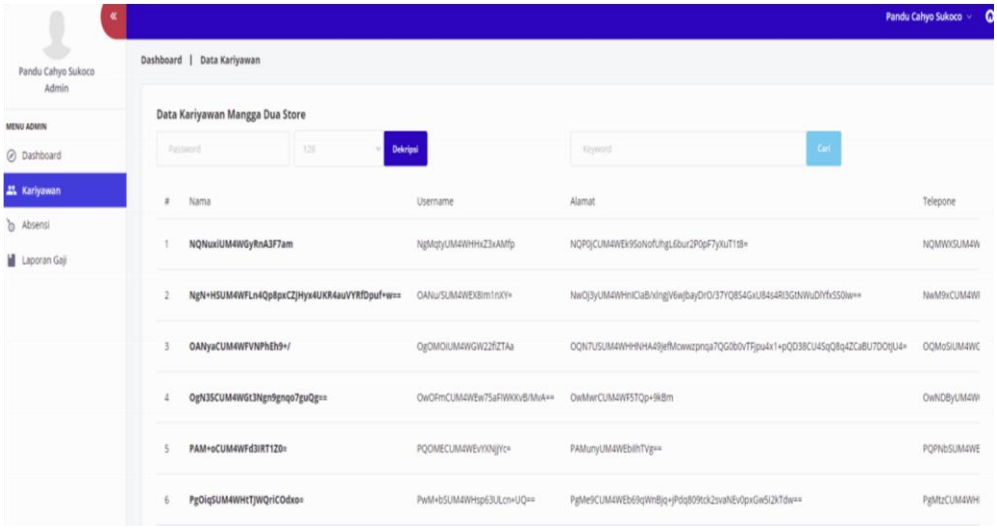

Figure 6. Salary Data Encryption Results

Calculation simulation in *Advanced Encryption Standard-128* done with plaintext and cipher key as follows:

Plain Text : JONATHANJOESTAR0

Key : 6521000000000000

1) PreRound

Encryption is first done by changing the plain text and key to be used into a 4x4 table as follows:

Table II. Plain Text

J	T	J	T
O	H	O	A
N	A	E	R
A	N	S	0

Table III. Cipher Key

6	0	0	0
5	0	0	0
2	0	0	0
1	0	0	0

Then the contents of the table above are converted into hexadecimal to produce the following table:

Table IV. Plain Text Hexadecimal

4a	54	4a	54
4f	48	4f	41
4e	41	45	52
41	4e	53	30

Table V. Cipher Key Hexadecimal

36	30	30	30
35	30	30	30
32	30	30	30
31	30	30	30

2) Initial Round

Initial Round (*AddRoundKey*) is the process of changing the data in the plaintext hexadecimal table and the cipher key is converted into binary and XOR is calculated. The result of the XOR is converted back to hexadecimal. The results of the change process can be seen in the table below.

Table VI. Hexadecimal AddRoundKey

7c	64	7a	64
7a	78	7f	71
7c	71	75	62
70	7e	63	00

3) Round 1

Each *round* has several processes in the form of *SubSytes*, *ShiftRows*, *MixCollums* dan *AddRoundKey*. The *SubBytes* process is the result of *AddRoundKey* which is substituted with a preround which produces results as shown in the table below.

Table VII Hexadecimal Result SubBytes

10	43	da	43
da	bc	d2	a3
10	a3	9d	aa
51	f3	fb	63

The results of the *SubBytes* are then continued with the *ShiftRows* permutation process where *ShiftRows* is a permutation process by changing the position of the element in the state without changing its value. The results of the *SubBytes* transformation process on rows 1, 2, and 3 are rotated to the left with a different number of turns. The first row is rotated 1 time, the second row 2 times, the 3rd row is rotated 3 times, and the row 0 is not rotated.

Table VIII. Hexadecimal Result ShiftRows

10	43	da	43
bc	d2	a3	da
9d	aa	10	a3
63	51	f3	fb

The next process after the *ShiftRows* process is the *MixColumn* process wherein each column of the *state* matrix is carried out a multiplication operation. It spreads the influence of each bit on the *PlainText* and *CipherKey* on the resulting *CipherText* in the direction of the state matrix column. Each column of the state matrix is treated as a four-term polynomial in the Galois field multiplied by modulo (X8 + X4 + X + 1) as follows:

$$\begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \end{matrix} \quad \left| \begin{matrix} 1 & 1 & 2 \\ & 3 & \\ 3 & 1 & 1 \\ & 2 & \end{matrix} \right|$$

Figure 7. Matriks State

The *MixColumn* process that is carried out produces a hexadecimal value.

Table IX. Hexadecimal MixColumn Results

01	10	b2	ab
ac	48	44	e9
28	2d	57	d2
d7	1f	3b	51

The next process after the *MixColumn* process is the *AddRoundKey* process as before, but the XOR process with the corresponding *sub-key* for each iteration is *contained* in the *keyexpansion* by doing key expansion. The *sub-key* was used in round 1.

Table X. Hexadecimal Sub-Keys Round 1

33	03	33	03
31	01	31	01
36	06	36	06
35	05	35	05

Sub-keys are then calculated XOR with the results from *MixColumn* and generate *AddRoundKey*.

Table XI Hexadecimal AddRoundKey Round 1

32	13	81	a8
9d	49	75	e8
1e	2b	61	d4
e2	1a	0e	54

4) Round 2 to Round 9

The *round* 2 to *round* 9 processes are carried out the same as the *round* 1 process where each round starts with a sequence of *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey*.

5) Round 10

Round 10 is the final process of AES, which is 128-bit AES. *Round* 10 only has *SubBytes*, *ShiftRows*, and *AddRoundKey* processes without any *MixColumn* processes. This process then produces a *CipherText* that has gone through the AES algorithm. The results of the process in *round* 10.

Table I. Hexadecimal Results Round 10

b5	68	3b	25
d4	02	f7	b4
32	25	6a	a6
36	a0	01	3e

D. Decryption Process

The AES decryption algorithm uses the inverse transformation of all the basic transformations used in the AES encryption algorithm. The inverse transformations are *InvSubBytes*, *InvShiftRows*, and *InvMixColumns*. AddRoundKey is a self-inverse transformation provided that it uses the same key.

1) PreRound

The *CipherText* in this section is taken from the hexadecimal result of round 10 which is then calculated XOR using *AddRoundKey*.

Table II. AddRoundKey PreRound

49	d9	9a	d0
0b	46	0b	10
7d	39	55	30
45	6a	27	81

2) Round 10

The AES *round* 10 decryption process has several processes carried out sequentially, namely the *InvShiftRow*, *InvSubBytes*, *AddRoundKey*, and *InvMixColumn* processes. The results of the *InvShiftRow* process.

Table XIV. InvShiftRow Round 10

49	d9	9a	d0
10	0b	46	0b
55	30	7d	39
6a	27	81	45

The results from the *InvShiftRow* process are then performed by *InvSubBytes* where in this process the results from the *InvShiftRows* process are substituted with the preround table. As for the results of *InvSubBytes*

Table XV. InvSubBytes Round 10

a4	e5	37	60
7c	9e	98	9e
ed	08	13	5b
58	3d	91	68

From the results of *InvSubBytes* then XOR with the *sub-key* in round 10 decryption to perform the *AddRoundKey* process on the *key expansion*. As for the *sub-key*

Table XVI. Sub-key Round 10

a4	e5	37	60
7c	9e	98	9e
ed	08	13	5b
58	3d	91	68

The *sub-key* is then calculated by XOR with the result of *InvShiftRows* which is the *AddRoundKey* process. Results of *AddRoundKey*.

Table XVII. Results of RoundKey Round 10

04	a8	27	34
70	05	20	c6
4c	5b	30	f2
0b	84	7d	f1

The result of the *RoundKey* is then multiplied by the matrix below and the result is *InvMixColumn*.

$$\begin{vmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0D \\ 0B & 0D & 09 & 0E \end{vmatrix}$$

Table III. InvMixColumn Round 10 Results

67	54	4a	54
4f	48	4f	41
4e	41	45	52
41	4e	53	30

3) Round 9 to Round 2

The entire *round* process is carried out the same as the process in *round* 10 where the initial process starts sequentially from the *InvShiftRows*, *InvSubBytes*, *AddRoundKey*, and *InvMixColumn* process.

4) Round 1

The process in *round* 1 is carried out the same as the process in *round* 10.

Table XIX. InvMixColumn Round 10 Results

4a	54	4a	54
4f	48	4f	41
4e	41	45	52
41	4e	53	30

IV. CONCLUSION

The existence of a web-based payroll data security application using the AES cipher method at the Mangga Dua store Kebumen can secure employee salary data at the Mangga Dua store Kebumen from misuse or data manipulation that can be carried out by unauthorized people which can result in losses at the Mangga Dua store Kebumen.

V. REFERENCES

[1] J. Prayudha, Saniman, and Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)", *Sains dan Komputer (SAINTIKOM)*, vol. 18, no. 2, pp. 119–129, 2019.

[2] H. Abdurahman, A. R. Riswaya, and A. Id, "Aplikasi Pinjaman Pembayaran Secara Kredit Pada Bank Yudha Bhakti STMIK Mardira Indonesia", Jurnal Computech & Bisnis, vol. 8, no. 2, pp. 61-69, 2014.

[3] B. Sidik, *Pemrograman Web dengan PHP7*, 1st ed. Bandung: Informatika, 2017.

[4] Yuhefizar, *Cara Mudah & Murah Membangun & Mengelola website*, 1st ed. Indonesia: Graha Ilmu, 2013.

[5] A. Kadir and Heryyanto, *Algoritma & pemrograman menggunakan C & C ++*. Yogyakarta: Andi, 2010.
[6] R. Wulandari, A. Giyantono, and A. Gunawan, "Rancang Bangun Penggajian Karyawan Berbasis Web Pada PT. Surganya Motor Indonesia," *CERITA*, vol. 3, no. 1, pp. 27–35, 2017.
[7] S. Kromodimoeljo, *Teori dan Aplikasi Kriptografi*. SPK IT Consulting, 2010.
[8] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, pp. 7–14, 2016.
[9] A. Kadir, *Algoritma & Pemrograman Menggunakan C & C++*, 1st ed. Yogyakarta: CV. Andi Offset, 2012.
[10] S. Mulyani, *Metode Analisis dan Perancangan Sistem*, 2nd ed. Bandung: Abdi Sistematika, 2016.
[11] J. A. Hall, *Accounting Information Systems*, 7th ed. Cengage Learning, 2010.