Vol. 1, No. 1, Desember 2024, page. ab-cd

ISSN 2598-3245 (Print), ISSN 2598-3288 (Online)

DOI

Available online at http://eltikom.poliban.ac.id

**Perancangan dan Implementasi Keamanan Sistem Informasi Desa Namo Buaya Menggunakan MetodeAES (*Advanced Encryption Standard*)**

**128-bit berbasis Web**

Efendi1\*, Cut Mutia2, Dan Cukri Rahmi Niani2

1) Departement of …., Universitas Teuku Umar, Aceh Barat, Indonesia

e-mail: [efendi.tif20@email.com](mailto:efendi.tif20@email.com), [cutmutia@email.com](mailto:cutmutia@email.com), [cukrirahminiani@email.com](mailto:cukrirahminiani@email.com)

Received: Desember 2024 – Revised: xx month year – Accepted: xx month year

**ABSTRACT**

*The advancement of information technology has had a significant impact on various sectors, including village government administration. Namo Buaya Village stores a lot of important data such as population data, village assets, and budgets that require protection from unauthorized access. However, the lack of an adequate security system makes the data vulnerable to the risk of leakage and misuse. This study aims to design and implement a web-based security system using the Advanced Encryption Standard (AES) 128-bit method to protect important data in Namo Buaya Village. The methods used include encryption and decryption of files in .txt, .doc, .pdf, and .xls formats. The implementation of this system is designed so that important data can be accessed securely via the web with encryption, ensuring that only users who have the correct key can access the information. This system was tested to ensure the level of security provided by the 128-bit AES algorithm, and compared to other encryption methods such as Triple DES. The test results showed that the system successfully secured files, and 128-bit AES provided better security and efficiency in the encryption and decryption process than other algorithms.*

**Keywords**: AES 128-bit, Data Security, Cryptography, Namo Buaya Village, Web-Based Information System.

**ABSTRAK**

Kemajuan teknologi informasi telah memberikan dampak signifikan pada berbagai sektor, termasuk administrasi pemerintahan desa. Desa Namo Buaya menyimpan banyak data penting seperti data kependudukan, aset desa, dan anggaran yang memerlukan perlindungan dari akses yang tidak sah. Namun, minimnya sistem keamanan yang memadai membuat data tersebut rentan terhadap risiko kebocoran dan penyalahgunaan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan berbasis web menggunakan metode Advanced Encryption Standard (AES) 128-bit untuk melindungi data penting Desa Namo Buaya. Metode yang digunakan meliputi enkripsi dan dekripsi file dengan format .txt, .doc, .pdf, dan .xls. Implementasi sistem ini dirancang agar data penting dapat diakses dengan aman melalui web dengan enkripsi, memastikan bahwa hanya pengguna yang memiliki kunci yang benar yang dapat mengakses informasi. Sistem ini diuji untuk memastikan tingkat keamanan yang diberikan oleh algoritma AES 128-bit, serta dibandingkan dengan metode enkripsi lainnya seperti Triple DES. Hasil pengujian menunjukkan bahwa sistem berhasil mengamankan file dengan efektif, dan AES 128-bit memberikan keamanan lebih baik serta efisiensi dalam proses enkripsi dan dekripsi dibandingkan algoritma lain.

**Kata kunci** : AES 128-bit, Keamanan Data, Kriptografi, Desa Namo Buaya, Sistem Informasi Berbasis Web

# Introduction

K

Perkembangan teknologi informasi telah membawa dampak signifikan di berbagai sektor, termasuk administrasi desa, dengan pengamanan data menjadi aspek yang sangat penting. Desa Namo Buaya, yang terletak di Kecamatan Sultan Daulat sekitar 11 kilometer dari Kota Subulussalam, menghadapi tantangan besar dalam melindungi data penting seperti data kependudukan, aset desa, anggaran, dan informasi sensitif lainnya. Sistem penyimpanan data yang masih offline tanpa cadangan memadai, serta rendahnya pemahaman masyarakat tentang keamanan data, membuat informasi vital ini rentan terhadap ancaman akses tidak sah atau penyalahgunaan [1], pentingnya perlindungan data pribadi menjadi sorotan utama di era digital untuk mencegah kebocoran data yang dapat merugikan individu dan masyarakat secara luas. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan penerapan algoritma enkripsi Advanced Encryption Standard (AES) 128-bit, yang merupakan metode kriptografi simetris yang terbukti efektif dalam menjaga kerahasiaan data. AES mampu mengamankan informasi pada kecepatan tinggi dengan kunci kriptografi berukuran 128, 192, hingga 256 bit [2]. Sistem berbasis web dirancang untuk mengenkripsi dan mendekripsi file dengan format tertentu (txt, doc, pdf, xls) serta menghasilkan ciphertext dalam format \*.rda, memastikan data hanya dapat diakses oleh pihak yang memiliki kunci dekripsi. Penelitian ini juga membandingkan kinerja dan keamanan AES dengan algoritma lain seperti Triple DES untuk membuktikan keunggulannya dalam konteks efisiensi dan perlindungan data. Implementasi teknologi ini tidak hanya meningkatkan keamanan data sensitif, tetapi juga memperkuat kepercayaan masyarakat terhadap sistem administrasi desa, mendorong pengelolaan yang transparan, serta menciptakan infrastruktur administrasi yang lebih modern dan aman. Selain itu, penelitian ini memberikan manfaat tambahan, seperti mendorong adopsi teknologi keamanan data oleh masyarakat desa, meningkatkan literasi teknologi, dan memberikan pengalaman praktis bagi peneliti dalam menerapkan solusi nyata untuk masalah keamanan data. Dengan langkah ini, Desa Namo Buaya diharapkan dapat membangun sistem administrasi yang efisien, transparan, dan terlindungi, yang pada akhirnya berdampak positif pada kesejahteraan masyarakatnya.

# Preparing Articles

The articles must consist of at least eight pages. Do not change the font size or line spacing to insert more text on a limited number of pages. Use italics for emphasis; do not use underscores.

To insert an image in Word, place the cursor at the insertion location and use Insert | Picture | From file or copy the image into the Windows clipboard and select Edit | Paste Special | Picture (with the "float over text" option unselected). The editorial team of the Jurnal ELTIKOM will make the final editing for your article.

## The body of The Paper

Abstracts should be explained at the beginning of the manuscript. The abstract section must clearly state the research's background, problems, objectives, results, and conclusions. The Introduction section must explicitly state the problem, update, and research objectives. The introduction must also be equipped with state-of-the-art research accompanied by the latest primary library sources. The Research Methods section contains a detailed description of the research carried out. Readers are expected to be able to replicate the research conducted by the author. The Results and Discussion section can be divided into two subsections: the Results subsection and the Discussion subsection. The Results subsection only displays the results of the evaluation or tests performed. The Discussion sub-section contains a discussion of the results of the tests. The discussion can contain the test's impact or the test's findings, comparison with other studies, and so on. The conclusion contains whether the research objectives were achieved and other important matters. In addition, the conclusions must provide suggestions for future research on sustainability.

If you write an original research paper, the main body of the paper should be numbered in consecutive order as follow: I. Introduction, II. Research Method, III. Result and Discussion, IV. Conclusion, Acknowledgment, and References. You may present the result and discussion (analysis) as a separate sub-section. The Acknowledgment section is optional. The minimum number of references is 15 references.

If you write a review paper, the main body of the paper should be numbered in consecutive order as follow: I. Introduction, II. Related/Previous Work, III. Research Method, VI. Findings, V. Discussion, VI. Conclusion, Acknowledgment, and References. The Research Method section should describe (and not be limited to) review objectives and research questions, search strategy and criteria, data collection and selection, and methodological quality assessment. The Acknowledgment section is optional. The minimum number of references is 60 references.

## Abbreviations and Acronyms

Define abbreviations and acronyms when first used in the content, although it has been defined in the abstract. Common abbreviations such as IEEE, SI, AC, and DC do not need to be defined. The abbreviation that uses a dot should not be given space: write "C.N.R.S.," not "C. N. R. S. " Do not use the abbreviation in the title of the article unless it cannot be avoided (for example, "ELTIKOM" in the title of this article).

## Other Recommendation

Use one space after a dot and comma. Separate the complex modifier with a connecting sign: "Zero-Field-Cooled Magnetization." Avoid using ambiguous sentences, such as, "Using (1), the final value has been calculated." [It is not clear who or what uses (1).] It is better to write down, "The final value is calculated using (1)," or "using (1), we calculate the final value."

Use a dot as a decimal separation: "0.25" and not "0,25". Use "cm3," not "cc." Moderate the sample dimension as "0.1 cm × 0.2 cm," not "0,1 × 0,2 cm2." When writing the range of values, write down "7 to 9" or "7-9," not "7 ~ 9.

The statement in the brackets is given a dot outside the closing brackets (like this). (A dot). Serial commas are more recommended: "A, B, and C" and not "A, B, and C."

Table 1

Unit For Magnetic Properties

|  |  |  |
| --- | --- | --- |
| Symbol | Quantity | Convert from Gaussian and CGS EMU to SI a |
| Φ | magnetic flux | 1 Mx → 10−8 Wb = 10−8 V·s |
| *B* | magnetic flux density,  magnetic induction | 1 G → 10−4 T = 10−4 Wb/m2 |
| *H* | magnetic field strength | 1 Oe → 103/(4π) A/m |
| *m* | magnetic moment | 1 erg/G = 1 emu  → 10−3 A·m2 = 10−3 J/T |
| *M* | magnetization | 1 erg/(G·cm3) = 1 emu/cm3  → 103 A/m |
| 4π*M* | magnetization | 1 G → 103/(4π) A/m |
| σ | specific magnetization | 1 erg/(G·g) = 1 emu/g → 1 A·m2/kg |
| *j* | magnetic dipole  moment | 1 erg/G = 1 emu  → 4π × 10−10 Wb·m |
| *J* | magnetic polarization | 1 erg/(G·cm3) = 1 emu/cm3  → 4π × 10−4 T |
| χ*,* κ | susceptibility | 1 → 4π |
| χρ | mass susceptibility | 1 cm3/g → 4π × 10−3 m3/kg |
| μ | permeability | 1 → 4π × 10−7 H/m  = 4π × 10−7 Wb/(A·m) |
| μr | relative permeability | μ → μr |
| *w, W* | energy density | 1 erg/cm3 → 10−1 J/m3 |
| *N, D* | demagnetizing factor | 1 → 1/(4π) |

Vertical lines are optional in the table.

If you use Word, use Microsoft Equation Editor or Mathtype (http://www.mathtype.com) to write the similarities in your article. Make sure the "Float Over Text" format is not selected.

## Equation

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please, no other font). Treating the equation as a graphic may be necessary to create multileveled equations and insert them into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents—Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign.

|  |  |
| --- | --- |
|  | (1) |

Ensure that the equation's symbol has been defined before the equation is written or immediately after the equation. Make sure the symbol is tilted in a paragraph. Refer with "(1)," not "EQ. (1) "or" Equation (1), "except at the beginning of the sentence:" Equation (1) is .... ".

# Figure and Table

## Figure

The following is a list of types of images received by the Jurnal ELTIKOM. This type is categorized based on the manufacture and use of color / gray:

### Color

The figure can use any color, but it is more advised to use grayscale. The recommended color range is grayscale, RGB (red/green/blue), and CMYK (Cyan/Magenta/Yellow/Black). RGB is usually used for graphics on the screen, whereas CMYK is used for printing purposes. All color images must be made in RGB or CMYK format. Grayscale images must be inserted in the form of grayscale.

### Multifigure

A figure consisting of more than one figure is displayed side by side, stacked with points (a), (b), and so on.

### Size on page

The maximum figure size is the same as the width of the page.

### Resolution

The resolution of the recommended figure is a minimum of 300dpi x 300dpi.

### Label

The label is at the bottom of the figure—the number of sequential figures from 1 according to the example in Figure 1. Use the "Times New Roman" font with the size of 8 pt.

### Laying Figures

The figure must be placed at the top or bottom of the page. The figure is not allowed to be placed in the middle of the page.

### Reference Figures

When referring to figures in the article, use "Figure 1". Figures must be given a number with Arabic numbering.

### Font in figure

If the figure has text, the author needs to use "Times New Roman" with adjusted fonts (8-11 pt).

## Table

### Size on page

The maximum Table size is the same as the width of the page.

### Label

The label is at the top of the table. The number of sequential tables from 1 according to the example in Table 1. Use the "Times New Roman" font with the size of 8 pt.

### Laying Tables

The table must be placed at the top or bottom of the page. The table is not allowed to be placed in the middle of the page.

### Reference Table

When referring to a table in the article, use "Table 1". Tables must be given a number with Arabic numbering.

### Font in Table

The author needs to use "Times New Roman" with adjusted fonts (8 pt).

# Conclusion

The conclusion summarizes the article's main points but does not copy the abstract as a conclusion. A conclusion might emphasize the importance of work results or suggestions for further development.

Attachment

Attachment, if necessary, can be displayed before Acknowledgement.

Acknowledgment

Acknowledgments are also a part that is not mandatory. If outsiders are involved in making this article, then it can be written in this section.

References

The reference source written in the Bibliography must be cited in the content. 80% of the references must consist of primary references from the last ten years. We strongly recommend using reference management applications such as Mendeley, Endnotes, Zootero, and others. We use the IEEE format as the reference format.

1. I. A. Ilyas and S. Widodo, "Kriptografi File Menggunakan Metode AES Dual Password," Prosiding KOMMIT, 2014
2. C. T. Lesmana, E. Elis, and S. Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia: The Urgence Of The Personal Data Protection Law In Ensuring The Security Of Personal Data As The Fulfillment Of The Right To Privacy Of The Indonesian Community," in Prosiding Seminar Nasional Hukum, Kebijakan Publik, Hak Asasi Manusia dan Keadilan (Sentuhan Keadilan), vol. 1, pp. 37–41, June 2022.