JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 3 No 1 – April 2020 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Implementasi Algoritma Kriptografi AES CBC Untuk Keamanan Komunikasi Data Pada *Hardware*

Putri Alifia Rizky[1], Sopian Soim[2], Sholihin[3*]

[1,2,3]Jurusan Teknik Elektro, Program Studi Sarjana Terapan Teknik Telekomunikasi, Politeknik Negeri Sriwijaya, Jln. Srijaya Negara Bukit Besar, Palembang, Indonesia
Alamat, Palembang, Indonesia

e-mail: alifiarizky08@gmail.com[1], sopiansoim@gmail.com[2], sholihin@polsri.ac.id[3*]

Received : July, 2024	Accepted : July, 2024	Published : August, 2024

Abstract

The development of information technology is growing rapidly, data communication security is becoming very important. This research develops the Advanced Encryption Standard (AES) cryptographic algorithm with Cipher Block Chaining (CBC) operating mode to increase data communication security. The goal is to produce an AES-CBC algorithm that is more effective and efficient in protecting data. Research methods include literature study, hardware and software design, system integration, testing, data collection and analysis. Implementation is carried out on Arduino-based hardware and LoRa as a communication intermediary. The test results show that the AES-CBC algorithm successfully encrypts and decrypts various types of plaintexts into secure ciphertext. Using CBC mode is proven to improve security over standard AES by encrypting each block of data based on the previous block. Implementations on hardware have also been successful, adding variety to cryptographic research. In conclusion, the development of the AES-CBC algorithm and its implementation in hardware makes a significant contribution to improving the security of data communications, both in academic and practical environments.

Keywords: *Advanced Encryption Standard, Chiper Block Chaining, Cryptography, Data Communication Security*

Abstrak

Perkembangan teknologi informasi semakin berkembang dengan pesat, keamanan komunikasi data menjadi sangat penting. Penelitian ini mengembangkan algoritma kriptografi Advanced Encryption Standard (AES) dengan mode operasi Cipher Block Chaining (CBC) untuk meningkatkan keamanan komunikasi data. Tujuannya adalah menghasilkan algoritma AES-CBC yang lebih efektif dan efisien dalam melindungi data. Metode penelitian meliputi studi literatur, perancangan perangkat keras dan lunak, integrasi sistem, pengujian, pengambilan data, dan analisis. Implementasi dilakukan pada perangkat keras berbasis Arduino dan LoRa sebagai perantara komunikasi. Hasil pengujian menunjukkan bahwa algoritma AES-CBC berhasil mengenkripsi dan mendekripsi berbagai jenis plaintext menjadi ciphertext yang aman. Penggunaan mode CBC terbukti meningkatkan keamanan dibandingkan AES standar dengan mengenkripsi setiap blok data berdasarkan blok sebelumnya. Implementasi pada perangkat keras juga berhasil, menambah variasi dalam penelitian kriptografi. Kesimpulannya, pengembangan algoritma AES-CBC dan implementasinya pada perangkat keras memberikan kontribusi signifikan dalam meningkatkan keamanan komunikasi data, baik dalam lingkungan akademis maupun praktis.

Kata Kunci: *Keamanan Komunikasi Data, Kriptografi, Rantai Blok Chiper, Standar Enkripsi Tingkat Lanjut*

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi saat ini memungkinkan seseorang untuk berkomunikasi dengan mudah dan bertukar informasi dengan cepat secara bebas dari segi ruang dan waktu. Meningkatnya kebutuhan ini juga terjadi peningkatan permintaan untuk mengembangkan sistem keamanan data yang lebih efisien dalam mengelola informasi yang diungkapkan. Hal ini memicu pertumbuhan ilmu yang berfokus pada metode pengamanan data, yang dikenal sebagai kriptografi[1]. Kriptografi itu ilmu yang memiliki tujuan untuk melindungi keamanan pesan pada saat pesan yang dikirim dari satu tempat ke tempat lain[2].

Algoritma kriptografi terus berkembang untuk meningkatkan keamanan data melalui proses enkripsi dan proses dekripsi menggunakan algoritma tertentu. Proses enkripsi ini bisa mengubah pesan asli (plaintext) menjadi pesan yang terenkripsi (ciphertext), sementara dekripsi mengembalikan pesan terenkripsi menjadi pesan asli[3]. Kedua proses ini memerlukan kunci untuk memastikan keamanan. Penelitian ini memakai algoritma kunci simetris, menggunakan kunci yang sama untuk enkripsi dan dekripsi[4]. Algoritma yang dipakai adalah Advanced Encryption Standard (AES) yaitu sebuah algoritma kriptografi yang efektif dalam menjaga keamanan data. AES merupakan jenis kriptografi blok simetris yang mampu melakukan enkripsi dan dekripsi[5].

Advanced Encryption Standard menjadi salah satu algoritma kriptografi modern yang banyak dipakai. AES dikembangkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat, memakai kunci rahasia yang sama pada saat proses enkripsi dan dekripsi. AES diterima luas oleh berbagai organisasi dan digunakan dalam aplikasi keamanan jaringan, perlindungan perangkat lunak, dan penyimpanan data yang aman [6].

Jaringan komputer dan internet telah mempermudah proses dan aktivitas pertukaran informasi. Namun, masalah utama adalah data yang ditransmisikan melalui jaringan komputer umumnya berupa plaintext. Ini sangat berisiko karena pihak yang tidak berwenang dapat dengan mudah menyadap dan membaca informasi tersebut [7]. Berbagai masalah yang terkait dengan keamanan informasi bisa diatasi dengan proses enkripsi, yang telah dikenal luas melalui metode enkripsi Advanced Encryption Standard (AES). Metode enkripsi ini menyediakan kunci privat yang digunakan pada saat proses enkripsi dan proses dekripsi [8].

Pengujian ini memakai metode AES-128 yang dimodifikasi dengan operasi CBC dan disebut dengan AES-128 CBC. AES-128 CBC adalah jenis mode operasi kriptografi yang digunakan bersama dengan algoritma AES-128 untuk mengubah data menjadi ciphertext (teks yang dienkripsi)[9]. Manfaat AES-128 CBC antara lain bisa meningkatkan keamanan yang lebih tinggi untuk data dengan pola serupa dan memberikan perlindungan terhadap masalah kriptoanalisis saat ini. Namun, penting untuk dipahami bahwa vektor inisialisasi (IV) harus ditentukan secara akurat dan unik untuk setiap kasus yang diajukan agar sistem tetap stabil [10].

Beberapa penelitian telah dilakukan untuk memanfaatkan algoritma AES dalam mengamankan data pada perangkat keras. Endrayanto melakukan penelitian dengan menerapkan AES-128 pada modul IoT Particle Photon yang tidak memiliki akselerator perangkat keras. Hasil penelitian tersebut menunjukkan bahwa penggunaan AES-128 dapat berjalan dengan baik, dengan waktu enkripsi terlama yang dibutuhkan adalah 398 ms [11].Selain itu, pada penelitian lain, AES 128-bit juga telah diterapkan untuk mengamankan data pada perangkat IoT yang digunakan dalam sistem budidaya hidroponik [11].Penelitian-penelitian sebelumnya ini memberikan gambaran tentang keberhasilan penerapan algoritma AES dalam meningkatkan keamanan data pada perangkat keras.

Pengujian ini algoritma AES-CBC akan diimplementasikan pada perangkat keras berbasis Arduino dan LoRa sebagai perantara komunikasi[12]. Implementasi algoritma AES-CBC ke dalam perangkat keras ini dapat menjadi salah satu cara untuk mengembangkan penelitian kriptografi, mengamankan komunikasi data, dan menambah inovasi baru dalam bidang kriptografi. Biasanya, kriptografi ini di implementasikan ke dalam website atau aplikasi, tetapi dengan mengimplementasikan ke dalam perangkat keras, penelitian ini dapat menambah variasi dan inovasi baru dalam bidang kriptografi [8].

2. METODE PENELITIAN

Bagian ini memberikan penjelasan mengenai langkah-langkah proses penelitian yang menggambarkan penggunaan logika untuk memastikan hasil dengan sesuai harapan.

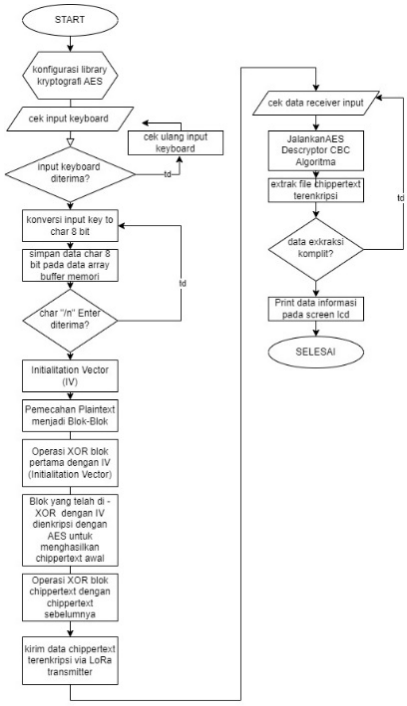
Gambar 1: Kerangka Metode Penelitian (*Research Method*)

Berdasarkan gambar 1 yaitu, diagram alur metodologi penelitian yang ditampilkan dapat dijelaskan sebagai berikut :

a. Studi Literatur :
   Untuk tahapan ini, dilakukan kajian literatur relevan dengan topik penelitian, yaitu pengembangan algoritma kriptografi AES dengan mode CBC untuk keamanan komunikasi data.
b. Persiapan Perangkat Hardware dan Software :
   Tahap ini mencakup perancangan dan pengembangan perangkat keras serta perangkat lunak yang dibutuhkan untuk implementasi sistem kriptografi.
c. Integrasi Hardware dan Software :
   Setelah persiapan perangkat keras dan lunak, dilakukan integrasi keduanya menjadi satu kesatuan sistem yang utuh.
d. Pengujian Sistem :
   Sistem yang telah diintegrasikan akan melalui proses pengujian untuk mengevaluasi kinerja, keamanan, dan keandalan sistem kriptografi yang dikembangkan.
e. Pengambilan Data :
   Data-data yang diambil dari hasil pengujian sistem akan dikumpulkan untuk selanjutnya dianalisis.
f. Analisis :
   Tahap analisis dilakukan untuk mengevaluasi hasil pengujian sistem dan membandingkannya dengan tujuan penelitian yang telah ditetapkan.
g. Kesimpulan :
   Untuk tahap akhir, dirumuskan kesimpulan dari hasil pengujian yang telah dilakukan.

Metode penelitian ini diharapkan bisa memberikan panduan yang jelas dalam mengembangkan sistem kriptografi AES-CBC untuk meningkatkan keamanan komunikasi data, sesuai dengan topik penelitian yang diangkat[[13]

2.1 Perancangan Perangkat Lunak



Gambar 2: *Flowchart* Perancangan Perangkat Lunak (*Software*)

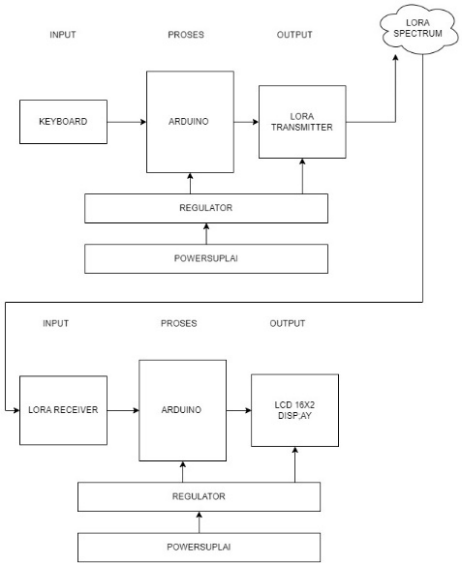
Pada Gambar 2 terdapat Flowchart perancangan perangkat lunak (Software) ini adalah rancangan perangkat lunak yang melibatkan proses enkripsi dan transmisi data menggunakan algoritma kriptografi AES (Advanced Encryption Standard)[14]. Berikut penjelasan umum mengenai alur kerja dari diagram ini :

a. Proses dimulai dengan konfigurasi library kriptografi AES.
b. Perangkat menerima input keyboard, kemudian melakukan konversi input key menjadi char 8 bit.

c. Data karakter 8 bit disimpan dalam buffer memori.
d. Inisialisasi vektor (IV) untuk operasi enkripsi.
e. Enkripsi data menggunakan algoritma XOR blok pertama dengan IV, kemudian blok selanjutnya dengan hasil enkripsi sebelumnya.
f. Hasil enkripsi dikirim melalui transmitter LoRa.
g. Pada sisi penerima, data yang diterima di-decrypt menggunakan algoritma JalankanAES Descriptor CBC.
h. Hasil dekripsi kemudian ditampilkan pada layar LCD.

Secara umum, flowchart ini menggambarkan proses pengiriman data terenkripsi menggunakan AES melalui transmisi wireless LoRa. Beberapa tahapan penting seperti konfigurasi, enkripsi, transmisi, dan dekripsi terlihat jelas dalam diagram alir ini.

2.3 Perancangan Perangkat Keras



Gambar 3: Flowchart Perancangan Perangkat Keras (Hardware)

Pada Gambar 3, terdapat Flowchart perancangan perangkat keras (Hardware), berdasarkan flowchart yang ditampilkan dalam gambar, dapat disimpulkan bahwa perancangan perangkat keras (hardware) untuk sistem kriptografi data komunikasi terdiri dari beberapa komponen utama, yaitu[15] :

a. Input :
- Keyboard : Digunakan untuk memasukkan teks atau data yang akan dienkripsi.
- Arduino : Sebagai komponen pemroses utama yang akan mengenkripsi data menggunakan algoritma kriptografi.

b. Proses :
- LoRa Transmitter : Modul transmitter yang menggunakan teknologi LoRa untuk mengirimkan data terenkripsi melalui kanal komunikasi nirkabel.
- Regulator : Komponen untuk mengatur catu daya yang diperlukan oleh perangkat.
- Power Supply : Menyediakan sumber daya listrik untuk seluruh komponen perangkat keras.

c. Output:
- LoRa Receiver : Modul penerima yang menggunakan teknologi LoRa untuk menerima data terenkripsi dari transmitter.
- Arduino : Menerima data terenkripsi dari receiver dan melakukan proses dekripsi menggunakan algoritma kriptografi.
- LCD (I2C) : Menampilkan hasil dekripsi data untuk pengguna.

Perangkat keras yang dirancang dengan komponen-komponen tersebut, diharapkan mampu melakukan proses enkripsi dan dekripsi data komunikasi secara efektif dan aman menggunakan algoritma kriptografi yang ditetapkan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Rangkaian Alat

Gambar 4: Perangkat Keras Alat Kriptografi

Gambar 4 menampilkan hasil rangkaian dari alat kriptografi berbasis mikrokontroler yang mengimplementasikan algoritma AES dengan mode pengoperasia CBC. Komponen utama dari rangkaian ini adalah board mikrokontroler yang bertugas untuk menjalankan proses enkripsi dan dekripsi data. Di sebelah kiri board mikrokontroler, terdapat modul display LCD yang berfungsi sebagai antarmuka pengguna, menampilkan informasi seperti teks asli, kunci, serta hasil enkripsi atau dekripsi. Sedangkan di sebelah kanan board mikrokontroler, terdapat modul keypad yang memungkinkan pengguna untuk memasukkan teks asli dan kunci enkripsi atau dekripsi.

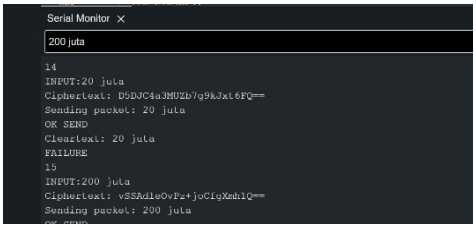
Selain itu, pada bagian bawah gambar terlihat rangkaian catu daya yang berfungsi untuk menyuplai daya ke seluruh komponen dalam alat kriptografi ini. Di sisi kiri dan kanan board mikrokontroler juga terdapat konektor input/output (I/O) yang bisa digunakan untuk menghubungkan alat kriptografi dengan perangkat lain, seperti komputer atau jaringan komunikasi, guna keperluan pengiriman dan penerimaan data terenkripsi.

Secara keseluruhan, rangkaian alat kriptografi yang ditunjukkan pada Gambar 11 mengintegrasikan berbagai komponen, seperti mikrokontroler, LCD, keypad, catu daya, dan konektor I/O, untuk mengimplementasikan proses enkripsi dan dekripsi data menggunakan algoritma AES-CBC. Alat ini dirancang untuk memudahkan pengguna dalam melakukan operasi kriptografi pada data yang perlu diamankan.

3.2 Hasil Pengujian

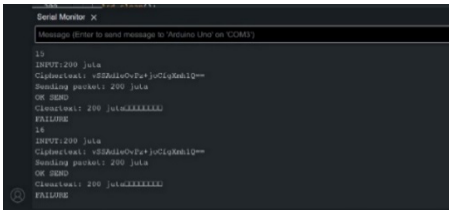
Berikut ini adalah hasil pengujian perangkat lunak dan perangkat keras alat kriptografi yang telah dilakukan pengujian :

a. Gambar 5 menunjukkan pengguna sedang memasukkan teks asli (plaintext) melalui keypad yang tersedia pada alat kriptografi yaitu 200 juta.



Gambar 5: Tampilan Awal Masukan Plain Teks

b. Gambar 6 memperlihatkan proses enkripsi yang dilakukan oleh mikrokontroler pada alat kriptografi. Dalam tahap ini, mikrokontroler mengimplementasikan algoritma AES dengan mode pengoperasian CBC untuk melakukan transformasi terhadap teks asli. Proses enkripsi ini mengubah teks asli menjadi ciphertext yang tidak terbaca.



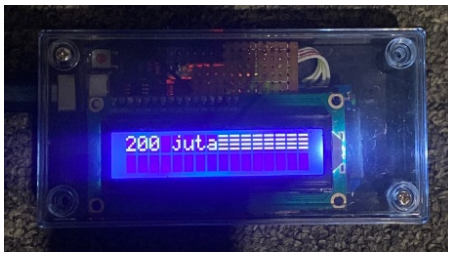
Gambar 6: Tampilan Proses Enkripsi

c. Hasil dari proses enkripsi ditampilkan pada Gambar 7, 8, 9, dan 10. Di gambar tersebut, bisa dilihat bahwa informasi yang ditampilkan di layar LCD alat kriptografi mencakup teks asli, kunci enkripsi, serta hasil enkripsi berupa ciphertext. Pengguna dapat dengan mudah memverifikasi kesesuaian antara input (teks asli) dan output (hasil enkripsi) yang dihasilkan oleh alat kriptografi. Tampilan ini memungkinkan pengguna untuk memeriksa keberhasilan proses enkripsi.

Gambar 7: Tampilan LED Saat *Text* Terenkripsi

Gambar 8: Tampilan *Chipertext*

Gambar 9: Tampilan *Extract* Teks Kembali



Gambar 10: Tampilan Hasil Akhir Kembali Jadi *Plaintext*

d. Gambar 11 menunjukkan proses akhir dekripsi yang dapat dilakukan oleh pengguna. Pada tahap ini, mikrokontroler dalam alat kriptografi akan melakukan proses dekripsi terhadap ciphertext menggunakan kunci dekripsi yang dimasukkan, sehingga dapat mengembalikan teks asli (plaintext) yang telah berhasil dienkripsi sebelumnya.

Gambar 11 Hasil Akhir Enkripsi

3.4 Hasil Uji Coba

Pada uji coba kali ini, penguji berhasil menguji berkali-kali dan berhasil, tabel di bawah ini adalah 5 data teks yang diambil , yang berisi plaintext dan chipertext. Berdasarkan hasil uji coba yang ditampilkan dalam tabel, dapat dilihat bahwa semua plaintext yang diuji berhasil dienkripsi dengan baik menggunakan algoritma kriptografi AES-CBC. Proses enkripsi mengubah plaintext menjadi ciphertext yang tidak dapat terbaca secara langsung, menunjukkan bahwa algoritma tersebut dapat meningkatkan keamanan data komunikasi. Hasil uji coba ini membuktikan efektivitas penerapan AES-CBC dalam menjaga kerahasiaan data, sehingga dapat menjadi solusi yang handal untuk diterapkan pada sistem komunikasi data yang membutuhkan tingkat keamanan yang tinggi.

Tabel 1: Tabel Hasil Uji Coba Proses Enkripsi

No	Plain Text	Chiper Text	Status
1.	polsribisa	Zik4u7JYBgVE7FgxmJZeUW	Enkripsi Berhasil
2.	palembang123	9nqQNJPXJyU912eQ+ybd8A	Enkripsi Berhasil
3.	Indonesia maju	vOegjV/EoivMjL04kqiJvw	Enkripsi Berhasil
4.	bismillahsukses	YQ/q5kVbMLF19/vaAzpW4dDfa0xLDtnzG6/ft74MIVA	Enkripsi Berhasil
5.	putrialifia	32FIAzqXns87Duaptv4jYQ	Enkripsi Berhasil

4. KESIMPULAN

Penelitian ini menunjukkan keberhasilan yang signifikan dalam implementasi algoritma kriptografi AES-CBC pada perangkat keras. Hasil pengujian membuktikan bahwa sistem mampu mengenkripsi dan mendekripsi berbagai jenis plaintext menjadi ciphertext yang aman, dengan proses yang berjalan lancar pada perangkat keras yang dirancang. Implementasi pada perangkat keras ini memberikan kontribusi baru dalam penelitian kriptografi, mengingat sebagian besar implementasi sebelumnya fokus pada website atau aplikasi perangkat lunak. Sistem yang dikembangkan menunjukkan integrasi yang baik antara komponen-komponen utama, meliputi input (keyboard, Arduino), proses (LoRa Transmitter, regulator, power supply), dan output (LoRa Receiver, Arduino, LCD), yang memungkinkan proses enkripsi-dekripsi data berjalan secara efektif. Penelitian ini berhasil menghasilkan solusi praktis untuk keamanan komunikasi data yang dapat diterapkan dalam berbagai konteks, baik di lingkungan akademis maupun industri. Meskipun demikian, masih terdapat ruang

untuk pengembangan lebih lanjut, seperti optimalisasi kinerja, peningkatan efisiensi energi, atau integrasi dengan teknologi keamanan lainnya, yang dapat menjadi fokus penelitian di masa depan.

DAFTAR PUSTAKA

[1] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016, [Online]. Available: http://ejournal.unisba.ac.id

[2] A. H. Kridalaksana *et al.*, "APLIKASI PENGAMAN SMS DENGAN METODE KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES) 128 BERBASIS ANDROID."

[3] Anggraeni Eka Putri, Aghistina Kartikadewi, and Lina Audina Abdul Rosyid, "Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang ," *Applied Information Systems and Management (AISM)* , vol. 3, no. 2, pp. 69–78, 2020.

[4] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.

[5] D. Pratomo, N. Budi Nugroho, and R. I. Ginting, "IMPLEMENTASI KRIPTOGRAFI UNTUK MENGAMANGKAN DATA PENJUALANAN DI PT. PAPPARICH MEDAN MENGGUNAKAN METODE AES 128," *Jurnal CyberTech*, vol. x. No.x, [Online]. Available: https://ojs.trigunadharma.ac.id/

[6] S. Oktavani *et al.*, "JURNAL MEDIA INFORMATIKA [JUMIN] Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," 2023.

[7] Janner Simarmata, *Pengamanan Sistem Komputer*, vol. 9797631222. Yogyakarta: Andi, 2006.

[8] F. Alfajar and M. Akbar, "Implementasi Keamanan Chat Realtime Menggunakan Aes-Cbc Dan Base64 Implementation Of Realtime Chat Security Using Aes-Cbc And Base64."

[9] Qinandea Nurmalasari, Ahmad Taqwa, and Sholihin, "Teknologi Virtual Reality Sebagai Media Pembelajaran Praktikum Elektronika Telekomunikasi," *Jurnal Ilmiah Komputasi Komputer & Sistem Informasi*, vol. 20, no. 3, 2021.

[10] M. Reza Rizky and T. Fatimah, "3 rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 30 Agustus 2023-Jakarta," vol. 2, no. 2, 2023.

[11] Noprianto and Vivi Nur Wijayaningrum, "END TO END ENKRIPSI MENGGUNAKAN ADVANCED ENCRYPTION STANDARD PADA PERANGKAT INTERNET OF THINGS," *Jurnal Sistem Informasi Dan Bisnis Cerdas (SIBC)*, vol. 14, Aug. 2021.

[12] L. S. Khotifah Puji Lestari, "Implementasi NodeMCU ESP8266 pada Alat Pelacak Kendaraan Menggunakan Global Positioning System dan MiFi Berbasis IoT," *Jurnal Teknologi Sistem Informasi dan Aplikasi*, vol. 6, no. 2, Apr. 2023.

[13] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[14] N. Febitri and H. Witriyono, “Application of AES 256 Cryptography Algorithm OCB Mode on Student Data Penerapan Algoritma Kriptografi AES 256 Mode OCB pada Data Mahasiswa,” *JURNAL KOMITEK*, vol. 3, no. 2, pp. 423–432, doi: 10.53697/jkomitek.v3i2.

[15] Adimas Fiqri Ramdhansya, Endro Ariyanto, and Hilal Hudan Nuha, “IMPLEMENTASI ADVANCED ENCRYPTION STANDARD (AES) PADA SISTEM KUNCI ELEKTRONIK KENDARAAN BERBASIS SISTEM OPERASI ANDROID DAN MIKROKONTROLER ARDUINO,” *Seminar Nasional Informatika 2014 (semnasIF 2014)* , vol. 1, no. No 1(2014), 2014.