

## INTISARI

*Cybercrime* telah menjadi ancaman yang lebih besar saat ini, karena semakin banyak serangan yang menargetkan berbagai industri, seperti infrastruktur nasional dan operasi industri. Kebutuhan akan komunikasi antarperangkat yang aman telah meningkat seiring dengan pertumbuhan Internet of Things (IoT), terutama di industri. Kriptografi sangat penting untuk komunikasi yang aman dan kerahasiaan data yang terjamin. Kriptografi yang ringan diperlukan karena banyak perangkat IoT tidak memiliki daya pemrosesan untuk menggunakan teknik enkripsi yang rumit.

Studi ini berfokus pada implementasi algoritma kriptografi AES-128 pada mikrokontroler STM32 untuk mengamankan enkripsi dan dekripsi file berukuran besar. Karena meningkatnya kebutuhan, terutama dalam *cyber security*, sistem IoT industri, perangkat dengan sumber daya terbatas memerlukan penggunaan kriptografi yang ringan. Algoritma AES-128 dalam mode Cipher Block Chaining (CBC) dipilih karena memiliki kemampuan enkripsi yang kuat dan dapat menangani volume data yang besar. Sistem ini menggunakan memori eksternal (*micro SD card*) untuk mengatasi keterbatasan memori mikrokontroler, memproses data dalam blok-blok 16 byte.

Pengujian pada berbagai jenis file, termasuk PDF, PNG, dan JPG, menunjukkan keberhasilan enkripsi dan dekripsi file hingga 3 MB, serta mempertahankan integritas data. Pengujian performa menunjukkan bahwa waktu enkripsi dan dekripsi meningkat secara linear dengan ukuran file, dengan throughput rata-rata 3,27 KB/s untuk enkripsi dan 3,26 KB/s untuk dekripsi pada micro SD card Class 6, serta throughput rata-rata 3,60 KB/s untuk enkripsi dan 3,57 KB/s untuk dekripsi pada micro SD card UHS Speed Class 3. Studi ini menunjukkan bahwa enkripsi AES-128 berbasis mikrokontroler dapat digunakan untuk file berukuran besar dan menawarkan solusi yang aman dan efisien untuk sistem berdaya rendah.

**Kata kunci – AES-128, Mikrokontroler, STM32, Enkripsi, Dekripsi**

## ABSTRACT

Cybercrime is becoming a bigger threat in today's data-driven world, as more attacks target different industries, such as national infrastructure and industrial operations. The necessity for secure device-to-device communication has increased with the Internet of Things (IoT) growth, especially in different industries. Cryptography is essential for secure communication and data confidentiality to be guaranteed. Lightweight cryptographic solutions are necessary because many IoT devices lack the processing power to use complex encryption techniques.

This study focuses on implementing the AES-128 cryptographic algorithm on an STM32 microcontroller to secure file encryption and decryption for large files. Due to growing concerns about cybersecurity, particularly in industrial IoT systems, resource-constrained devices require lightweight cryptographic solutions. The AES-128 algorithm in Cipher Block Chaining (CBC) mode was chosen because it has strong encryption capabilities and can handle large data volumes. The system used external memory (micro SD card) to overcome the microcontroller's memory limitations, processing data in 16-byte blocks.

Tests on various file types, including PDF, PNG, and JPG, demonstrated successful encryption and decryption of files up to 3 MB, maintaining data integrity. Performance testing indicated that both encryption and decryption times increased linearly with file size, with an average throughput of 3.27 KB/s for encryption and 3.26 KB/s for decryption on Class 6 micro SD card, and an average throughput of 3.60 KB/s for encryption and 3.57 KB/s for decryption on UHS Speed Class 3 micro SD card. The study confirmed the feasibility of microcontroller-based AES-128 encryption for large files, offering a secure and efficient solution on low-powered devices.

**Keywords – AES-128, Microcontroller, STM32, Encryption, Decryption**