UNIVERSITAS
GADJAH MADA
Purwarupa Pengamanan Komunikasi Radio Pintu Otomatis dengan Enkripsi AES-128
Benaya Gedalya Harenito, Drs. Bambang Nurcahyo Prastowo, M.Sc.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

PURWARUPA PENGAMANAN KOMUNIKASI RADIO PINTU OTOMATIS DENGAN ENKRIPSI AES-128

Diajukan oleh:
Benaya Gedalya Harenito
21/480029/PA/20834

Sistem pengunci pintu otomatis berbasis komunikasi radio frekuensi (RF) 433MHz rentan terhadap serangan replay attack karena sifat transmisi yang terbuka dan mudah disadap. Penelitian ini mengembangkan purwarupa sistem pengamanan komunikasi radio pintu otomatis menggunakan enkripsi AES-128 yang terintegrasi dengan mekanisme *timestamp* berbasis modul RTC DS3231 untuk meminimalisir *replay attack*. Sistem terdiri dari Arduino Pro Mini sebagai *transmitter* (remot) dan Arduino Uno sebagai *receiver* (kontroler pintu) yang berkomunikasi melalui modul FS1000A. *Payload* data berukuran 16 *byte* yang berisi *command*, *timestamp*, *device* ID, *checksum*, dan *padding* dienkripsi menggunakan AES-128 sebelum transmisi. Pada sisi receiver, sistem melakukan dekripsi dan validasi timestamp dengan membandingkan selisih waktu terhadap RTC lokal dalam jendela waktu yang telah ditentukan.

Pengujian dilakukan dengan mensimulasikan *replay attack* menggunakan perangkat *attacker* yang mengirimkan paket statis berulang kali selama 5 menit dengan interval 20 detik. Hasil menunjukkan sistem tanpa timestamp menerima seluruh 15 paket replay sebagai *legitimate*, sedangkan sistem dengan timestamp berhasil membatasi jumlah paket yang diterima secara linear tergantung besar jendela waktu: 6 paket pada jendela 60 detik, 5 paket (50 detik), 4 paket (40 detik), 3 paket (30 detik), 2 paket (20 detik), hingga hanya 1 paket pada jendela 10 detik. Analisis kinerja menunjukkan waktu rata-rata enkripsi 522.8 mikrodetik dan dekripsi 817.6 mikrodetik.

Penelitian ini membuktikan bahwa integrasi timestamp pada enkripsi AES-128 efektif sebagai mekanisme preventif terhadap *replay attack*, dengan *trade-off* berupa risiko *false rejection* pada jendela waktu yang terlalu sempit akibat *drift* waktu RTC atau delay transmisi RF. Pemilihan jendela waktu optimal harus mempertimbangkan keseimbangan antara aspek keamanan dan keandalan operasional sistem.

Kata Kunci: AES-128, enkripsi, radio frekuensi, replay attack, timestamp, RTC DS3231, sistem tertanam, pintu otomatis

UNIVERSITAS
GADJAH MADA

Purwarupa Pengamanan Komunikasi Radio Pintu Otomatis dengan Enkripsi AES-128
Benaya Gedalya Harenito, Drs. Bambang Nurcahyo Prastowo, M.Sc.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

PROTOTYPE OF AUTOMATIC DOOR RADIO COMMUNICATION SECURITY WITH AES-128 ENCRYPTION

Proposed by:
Benaya Gedalya Harenito
21/480029/PA/20834

Automatic door lock systems based on 433MHz radio frequency (RF) communication are vulnerable to replay attacks due to the open and easily intercepted nature of transmission. This research develops a prototype security system for RF-based automatic door communication using AES-128 encryption integrated with a timestamp mechanism based on the RTC DS3231 module to minimize replay attacks. The system consists of an Arduino Pro Mini as the transmitter (remote) and an Arduino Uno as the receiver (door controller) communicating through the FS1000A module. A 16-byte data payload containing command, timestamp, device ID, checksum, and padding is encrypted using AES-128 before transmission. On the receiver side, the system performs decryption and timestamp validation by comparing the time difference against the local RTC within a predetermined time window.

Testing was conducted by simulating replay attacks using an attacker device that repeatedly transmitted static packets for 5 minutes at 20-second intervals. Results showed that the system without timestamp accepted all 15 replay packets as legitimate, while the system with timestamp successfully limited the number of accepted packets linearly depending on the time window size: 6 packets at 60-second window, 5 packets (50 seconds), 4 packets (40 seconds), 3 packets (30 seconds), 2 packets (20 seconds), down to only 1 packet at 10-second window. Performance analysis revealed average encryption time of 522.8 microseconds and decryption time of 817.6 microseconds.

Furthermore, the use of a narrow time window introduces the risk of false rejection, defined as the rejection of legitimate commands caused by RTC time drift or RF transmission delays. Therefore, the selection of an optimal time window must balance security effectiveness against replay attacks and the operational reliability of the system.

Keywords: AES-128, encryption, radio frequency, replay attack, timestamp, RTC DS3231, embedded system, automatic door