

04/S/TEKKOM-KCBR/PK.03.08/25/JUNI/2024

**PENGEMBANGAN SISTEM PENGAMANAN PINTU RFID BERBASIS
INTERNET OF THINGS DENGAN ALGORITMA ENKRIPSI AES-128**

SKRIPSI

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer



oleh
Dhimaz Purnama Adjhi
NIM 2003411

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

HALAMAN HAK CIPTA

**PENGEMBANGAN SISTEM PENGAMANAN PINTU RFID BERBASIS
INTERNET OF THINGS DENGAN ALGORITMA ENKRIPSI AES-128**

oleh

Dhimaz Purnama Adjhi

NIM 2003411

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Teknik pada Program Studi Teknik Komputer

© **Dhimaz Purnama Adjhi** 2024

Universitas Pendidikan Indonesia

Juli 2024

Hak Cipta dilindungi oleh Undang-undang.

Skripsi ini tidak diperbolehkan seluruhnya atau sebagian, dengan dicetak ulang,
difotokopi, atau cara lainnya tanpa izin dari penulis.

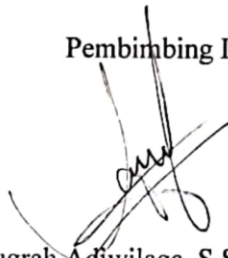
HALAMAN PENGESAHAN

DHIMAZ PURNAMA ADJHI

PENGEMBANGAN SISTEM PENGAMANAN PINTU RFID BERBASIS *INTERNET OF THINGS* DENGAN ALGORITMA ENKRIPSI AES-128

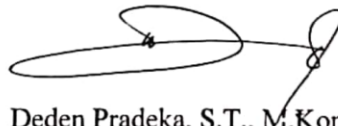
disetujui dan disahkan oleh pembimbing:

Pembimbing I



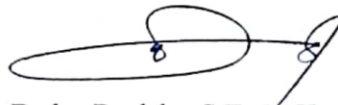
Anugrah Adiwilaga, S.ST., M.T.
NIP. 920200819880813101

Pembimbing II



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

Mengetahui,
Ketua Program Studi Teknik Komputer



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

**HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME**

Saya yang bertanda tangan dibawah ini:

Nama : Dhimaz Purnama Adjhi
NIM : 2003411
Program Studi : Teknik Komputer

Dengan ini saya menyatakan bahwa skripsi dengan judul "Pengembangan Sistem Pengamanan Pintu RFID berbasis *Internet of Things* dengan Algoritma Enkripsi AES-128" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Juli 2024

Yang membuat pernyataan,

Dhimaz Purnama Adjhi

NIM. 2003411

HALAMAN UCAPAN TERIMA KASIH

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT, yang telah melimpahkan rahmat, hidayah, serta karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini. Keberhasilan ini merupakan buah dari limpahan kasih sayang-Nya yang tak terhingga, serta rahmat-Nya yang senantiasa menyertai langkah-langkah penulis dalam menyelesaikan perjalanan akademis ini. Penulis juga ingin mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan selama penulisan skripsi ini. Oleh sebab itu, dengan segala kerendahan hati dan penuh rasa hormat, penulis bermaksud menyampaikan terima kasih kepada:

1. Mamah, Ayah, Adik, serta seluruh keluarga besar penulis yang senantiasa memberikan dukungan doa dan dorongan motivasi moral.
2. Bapak Deden Pradeka, S.T., M.Kom., selaku Ketua Program Studi Teknik Komputer dan dosen pembimbing kedua.
3. Bapak Anugrah Adiwilaga, S.ST., M.T., selaku dosen pembimbing pertama.
4. Seluruh dosen dan civitas akademika Universitas Pendidikan Indonesia yang telah memberikan segala kebaikan dan jasa selama masa perkuliahan.
5. Seluruh rekan seperjuangan di dalam komunitas "Tidak Semua UGM Part 0.1", Rastra Wardana Nanditama dan Mohamad Rizal Hanafi. Kerjasama, dukungan, serta semangat dalam menjalani perjalanan akademis bersama-sama telah memberikan warna yang berarti dalam perjalanan penulisan skripsi ini.
6. Fany Muhammad Fahmi, Abdi Surya, dan Ivan Rajwa, selaku teman kuliah terbaik yang gemar sekali memberikan tampungan kamar kost dan *transfer knowledge* kepada penulis.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat berbagai kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari semua pihak untuk penyempurnaan karya ini di masa mendatang. Akhir kata, semoga skripsi ini dapat memberikan manfaat serta kontribusi yang positif dalam bidang ilmu yang dipelajari.

PENGEMBANGAN SISTEM PENGAMANAN PINTU RFID BERBASIS INTERNET OF THINGS DENGAN ALGORITMA ENKRIPSI AES-128

Dhimaz Purnama Adjhi

2003411

ABSTRAK

Berkembangnya pasar sistem *Radio-Frequency Identification* (RFID) dan kemajuan teknologi *Internet of Things* (IoT) telah memberikan dampak signifikan dalam sistem pencatatan dan autentikasi seperti sistem pengamanan pintu RFID berbasis IoT. Namun, sistem RFID dengan integrasi IoT memunculkan tantangan keamanan baru, terutama dalam serangan *network sniffing* dan *Man-in-the-Middle* (MiTM). Penelitian ini bertujuan untuk mengembangkan sistem pengamanan pintu RFID berbasis IoT dengan mengimplementasikan kriptografi *Advanced Encryption Standard* (AES-128), mengevaluasi kinerjanya, dan meminimalisir kerentanan *insecure data transfer and storage* pada protokol komunikasi MQTT. Menggunakan metode penelitian *Design Research Methodology* (DRM) dan metode pengembangan sistem *Agile*, sistem ini dikembangkan serta diuji dengan metode *Black-box Testing*. Hasil penelitian menunjukkan bahwa implementasi algoritma enkripsi AES-128 berhasil mengamankan data penting seperti UID kartu/tag RFID pada sistem pengamanan pintu RFID berbasis IoT, mencegah penyalahgunaan hak akses, dan mengurangi risiko serangan *network sniffing* dan *MiTM*. Adapun temuan selebihnya dari penelitian ini ialah sistem yang dikembangkan oleh penulis berfungsi dengan baik yang memenuhi kebutuhan fungsionalitas, memperoleh data proses kecepatan enkripsi AES-128 di beberapa *microcontroller*, serta hasil pengujian ketahanan enkripsi AES-128 yang dihasilkan. Inovasi ini diharapkan menjadi standar industri untuk ruangan dengan tingkat keamanan tinggi seperti ruangan server, ruangan balita di rumah sakit, laboratorium, gudang, dan brankas. Dengan demikian, penelitian ini berkontribusi pada pengembangan paradigma keamanan yang lebih tangguh dalam protokol komunikasi MQTT melalui penerapan enkripsi data AES-128, meningkatkan integritas dan kerahasiaan data dalam sistem pengamanan pintu RFID berbasis IoT.

Kata Kunci: Sistem Pengamanan Pintu; RFID; IoT; MQTT; AES-128

DEVELOPMENT OF RFID DOOR SECURITY SYSTEM BASED ON INTERNET OF THINGS WITH AES-128 ENCRYPTION ALGORITHM

Dhimaz Purnama Adjhi

2003411

ABSTRACT

The growing market for RFID systems and advancements in IoT technology have had a significant impact on recording and authentication systems such as IoT-based RFID door security systems. However, RFID systems with IoT integration pose new security challenges, especially in network sniffing and MiTM attacks. This research aims to develop an IoT-based RFID door security system by implementing AES-128 cryptography, evaluating its performance, and minimizing the vulnerability of insecure data transfer and storage using the MQTT communication protocol. Using the DRM research method and the Agile system development method, this system was developed and tested using the Black-box Testing method. The results showed that the implementation of the AES-128 encryption algorithm successfully secures important data such as the UID RFID tag on the IoT-based RFID door security system, prevents misuse of access rights, and reduces the risk of network sniffing and MiTM attacks. The remaining findings of this research are that the system developed by the author works well that meets the functionality needs, obtaining data on the AES-128 encryption speed process on several microcontrollers, as well as the results testing the durability of the resulting AES-128 encryption. This innovation is expected to become an industry standard for rooms with high security levels such as server rooms, toddler rooms in hospitals, laboratories, warehouses, and safes. Hence, this research contributes to the development of a more robust security paradigm in the MQTT communication protocol through the application of AES-128 encryption, improving data integrity and confidentiality in IoT-based RFID door security systems.

Keywords: Door Security System; RFID; IoT; MQTT; AES-128;

DAFTAR ISI

HALAMAN PENGESAHAN	i
HALAMAN PERNYATAAN	ii
HALAMAN UCAPAN TERIMA KASIH	iii
ABSTRAK	iv
DAFTAR ISI	vi
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xiii
DAFTAR PERSAMAAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Penelitian	1
1.2 Rumusan Masalah Penelitian	4
1.3 Batasan Penelitian	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
1.5.1 Manfaat Teoritis	5
1.5.2 Manfaat Praktis	6
1.6 Struktur Organisasi Skripsi	6
BAB II KAJIAN PUSTAKA	8
2.1 Peta Literatur	8
2.2 Sistem Pengamanan Pintu RFID berbasis IoT	8
2.2.1 <i>Microcontroller</i> ESP32	12
2.2.2 RFID MFRC 522 HF	13
2.2.3 <i>Relay Module</i> 5V dan <i>Doorlock</i> Solenoid 12V.....	15
2.2.4 Protokol Komunikasi MQTT	17
2.2.5 Web dan <i>Database</i> Server.....	20
2.3 <i>Cyber Security</i> pada Sistem berintegrasi IoT	20
2.3.1 <i>Network Sniffing</i> dan MiTM (<i>Man-in-the-Middle</i>)	22
2.3.2 Wireshark dan Ettercap	24
2.4 <i>Advanced Encryption Standard</i> (AES-128)	24
2.4.1 Proses Pembangkitan Kunci.....	27
2.4.2 Proses Enkripsi.....	31

2.4.3	Proses Dekripsi	37
2.5	<i>Kernel</i> Sistem Operasi FreeRTOS.....	39
2.6	Penelitian Terdahulu.....	39
BAB III METODE PENELITIAN		43
3.1	Desain Penelitian	43
3.1.1	Klarifikasi Penelitian.....	44
3.1.2	Studi Deskriptif I.....	44
3.1.3	Studi Preskriptif	44
3.1.4	Studi Deskriptif II	45
3.2	Metode Pengembangan Sistem	45
3.2.1	<i>Plan</i>	46
3.2.2	<i>Design</i>	47
3.2.3	<i>Develop</i>	48
3.2.4	<i>Test</i>	48
3.2.5	<i>Deploy</i>	49
3.2.6	<i>Review</i>	49
3.3	Metode Pengujian Sistem.....	49
BAB IV TEMUAN DAN PEMBAHASAN		51
4.1	Pengembangan Sistem Perangkat Keras	51
4.1.1	<i>Block Diagram</i>	51
4.1.2	<i>Wiring Diagram</i>	52
4.1.3	<i>Architecture Diagram</i>	53
4.1.4	Desain PCB (<i>Printed Circuit Board</i>).....	53
4.1.5	Hasil Akhir Sistem Perangkat Keras.....	54
4.2	Pengembangan Sistem Perangkat Lunak	56
4.2.1	Skenario Protokol Komunikasi MQTT.....	57
4.2.2	<i>Flowchart</i> Sistem	58
4.2.3	<i>Use Case Diagram</i>	64
4.2.4	<i>Entity Relationship Diagram</i>	65
4.2.5	<i>Sequence Diagram</i>	66
4.2.6	<i>Activity Diagram</i>	67
4.2.7	Hasil Akhir Sistem Perangkat Lunak.....	68
4.3	Pengujian dan Evaluasi Sistem.....	71
4.3.1	<i>Black-box Testing</i> pada Fungsionalitas Sistem.....	71

4.3.2	Hasil Proses Kecepatan Enkripsi dan Pengiriman Data.....	74
4.3.3	Variabel Koefisien Korelasi Pearson pada Enkripsi	75
4.4	Pengaruh Implementasi Algoritma Enkripsi AES-128	79
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI		83
5.1	Simpulan.....	83
5.2	Implikasi	83
5.3	Rekomendasi	84
DAFTAR PUSTAKA		85
LAMPIRAN.....		92

DAFTAR TABEL

Tabel 2.1 Perbandingan Sistem Pengamanan Pintu RFID secara Lokal dan IoT ...	9
Tabel 2.2 Perbedaan QoS pada MQTT	19
Tabel 2.3 Spesifikasi Varian Algoritma Enkripsi AES.....	26
Tabel 3.1 Perencanaan Teknologi Perangkat Lunak yang Digunakan	46
Tabel 3.2 Perencanaan Komponen Perangkat Keras yang Digunakan	47
Tabel 4.1 Hasil Akhir Web <i>Dashboard</i> pada Sistem Pengamanan Pintu RFID ...	69
Tabel 4.2 Hasil Pengujian Sistem menggunakan Metode <i>Black-box Testing</i>	71
Tabel 4.3 Kecepatan Enkripsi AES-128 terhadap beberapa <i>Microcontroller</i>	74
Tabel 4.4 Kecepatan Pengiriman Data <i>Ciphertext</i> AES-128 terhadap <i>Broker</i>	75
Tabel 4.5 Kriteria Klasifikasi Koefisien Korelasi pada AES-128	75
Tabel 4.6 Hasil Keseluruhan Pengujian Korelasi Pearson untuk AES-128.....	77

DAFTAR GAMBAR

Gambar 1.1 Data Pertumbuhan Pasar RFID (Das & Chang, 2023).....	1
Gambar 2.1 Peta Literatur Penelitian	8
Gambar 2.2 BF-870 <i>WebBased</i> RFID <i>MultiDoor</i> (Armada-IT, 2024).....	10
Gambar 2.3 <i>Flowchart</i> Pengamanan Pintu RFID berbasis IoT secara Umum	11
Gambar 2.4 <i>Pinout</i> GPIO ESP32 (RandomNerdTutorials, 2018)	12
Gambar 2.5 <i>Chip Tag</i> RFID pada eKTP Indonesia, Contactless Card	13
Gambar 2.6 <i>Block Diagram</i> Sistem RFID bertipe Pasif	14
Gambar 2.7 <i>Pinout</i> RFID MFRC 522 HF (LastMinuteEngineers, 2024).....	15
Gambar 2.8 Aktuator <i>Doorlock</i> Solenoid 12V	16
Gambar 2.9 <i>Relay Module</i> 5V.....	16
Gambar 2.10 <i>Delay Average</i> MQTT terhadap HTTP (Windryani dkk., 2019)	17
Gambar 2.11 Cara Kerja MQTT berdasarkan QoS.....	18
Gambar 2.12 <i>Layer Architecture</i> pada Sistem berintegrasi IoT	21
Gambar 2.13 Ilustrasi <i>MiTM Attack</i> Bekerja (Imperva, 2020).....	23
Gambar 2.14 Ilustrasi Detail <i>ARP Spoofing</i> bekerja pada <i>MiTM Attack</i>	23
Gambar 2.15 Perbedaan Kriptografi Simetris dan Asimetris	25
Gambar 2.16 Tabel Konversi ASCII (Kurniawan, 2019)	27
Gambar 2.17 Proses Cara Kerja Pembangkitan Kunci AES-128	28
Gambar 2.18 Inisialisasi <i>Cipherkey</i> - Pembangkitan Kunci AES-128	29
Gambar 2.19 Proses <i>Rotword</i> - Pembangkitan Kunci AES-128.....	29
Gambar 2.20 Proses <i>SubBytes</i> - Pembangkitan Kunci AES-128.....	30
Gambar 2.21 Proses <i>Rcon</i> - Pembangkitan Kunci AES-128	30
Gambar 2.22 Operasi <i>XOR</i> - Pembangkitan Kunci AES-128.....	31
Gambar 2.23 <i>Flowchart</i> Proses Cara Kerja Enkripsi AES-128.....	32
Gambar 2.24 Proses <i>Initial Round (AddRoundKey)</i> - Enkripsi AES-128.....	33
Gambar 2.25 Proses <i>SubBytes</i> - Enkripsi AES-128.....	34
Gambar 2.26 Proses <i>ShiftRows</i> - Enkripsi AES-128.....	34
Gambar 2.27 Proses <i>MixColumn</i> - Enkripsi AES-128.....	35
Gambar 2.28 Pengoperasian Polinomial Galois versi 1 pada <i>MixColumn</i>	35
Gambar 2.29 Pengoperasian Polinomial Galois versi 2 pada <i>MixColumn</i>	36
Gambar 2.30 Proses <i>AddRoundKey</i> - Enkripsi AES-128.....	36

Gambar 2.31 <i>Flowchart</i> Proses Cara Kerja Dekripsi AES-128.....	37
Gambar 2.32 Ilustrasi Proses <i>InvShiftRows</i> - Dekripsi AES-128	38
Gambar 2.33 Tabel Inversi <i>S-box</i> - Dekripsi AES-128.....	38
Gambar 2.34 Matriks tertentu pada <i>InvMixColumn</i> - Dekripsi AES-128.....	39
Gambar 3.1 Desain Penelitian menggunakan DRM	43
Gambar 3.2 Metode Pengembangan Sistem <i>Agile</i>	46
Gambar 3.3 Ilustrasi Cara Kerja <i>Black-box Testing</i>	50
Gambar 4.1 <i>Block Diagram</i> Pengembangan Sistem.....	51
Gambar 4.2 <i>Wiring Diagram</i> Pengembangan Sistem.....	52
Gambar 4.3 <i>Architecture Diagram</i> Pengembangan Sistem	53
Gambar 4.4 Desain PCB Pengembangan Sistem.....	53
Gambar 4.5 Tampilan Samping Hasil Akhir Sistem Perangkat Keras	54
Gambar 4.6 Tampilan Depan Hasil Akhir Sistem Perangkat Keras	55
Gambar 4.7 Tampilan Belakang Hasil Akhir Sistem Perangkat Keras	55
Gambar 4.8 Tampilan Pemasangan <i>Doorlock</i> Solenoid pada Pintu	56
Gambar 4.9 Akrilik LCD pada Alat Sistem	56
Gambar 4.10 Skenario Protokol Komunikasi MQTT	57
Gambar 4.11 <i>Flowchart</i> secara General pada <i>Microcontroller</i>	59
Gambar 4.12 <i>Flowchart</i> Sistem dengan <i>Mode LogHistory (Tap IN)</i>	60
Gambar 4.13 <i>Flowchart</i> Sistem dengan <i>Mode LogHistory (Tap OUT)</i>	61
Gambar 4.14 <i>Flowchart</i> Sistem dengan <i>Mode Enrollment</i>	62
Gambar 4.15 <i>Flowchart MQTTHandler</i> pada <i>Laravel Console</i>	63
Gambar 4.16 <i>Flowchart Subscribe Microcontroller</i> untuk Respons <i>Payload</i>	64
Gambar 4.17 <i>Use Case Diagram</i> pada Sistem Pengamanan Pintu RFID.....	65
Gambar 4.18 ERD pada Sistem Pengamanan Pintu RFID	66
Gambar 4.19 <i>Sequence Diagram</i> untuk <i>Mode LogHistory (Tap IN)</i>	67
Gambar 4.20 <i>Sequence Diagram</i> untuk <i>Mode Enrollment</i>	67
Gambar 4.21 <i>Activity Diagram</i> pada Sistem Pengamanan Pintu RFID.....	68
Gambar 4.22 Cara Penghitungan dan Hasil <i>sample</i> Korelasi untuk AES-128	76
Gambar 4.23 Pengujian <i>Network Sniffing</i> sebelum Implementasi AES-128.....	79
Gambar 4.24 Skenario Penetrasi untuk melihat Pengaruh AES-128.....	80
Gambar 4.25 Eksploitasi MiTM dengan teknik <i>ARP Spoofing (Ettercap)</i>	80

Gambar 4.26 Pengujian <i>Network Sniffing</i> setelah Implementasi AES-128	81
Gambar 4.27 <i>Ciphertext</i> Data UID Kartu RFID AES-128 pada <i>Database</i>	81

DAFTAR LAMPIRAN

Lampiran 1. Jadwal Penelitian	92
Lampiran 2. Dokumentasi Instrumen Sebelum Penelitian.....	92
Lampiran 3. <i>Repository</i> Gitlab untuk Kode Program Pengembangan Sistem.....	93
Lampiran 4. Alat Penghitung Korelasi Antar 2 Variabel Koefisien Pearson	93
Lampiran 5. Dokumentasi pengujian MiTM dengan teknik ARP <i>Spoofing</i>	94
Lampiran 6. Dokumentasi Hasil <i>Network Sniffing</i> pada Wireshark	94
Lampiran 7. Pengujian Fitur <i>Export Data History</i> Masuk & Keluar Pintu.....	95
Lampiran 8. Dokumentasi Pengujian Kecepatan Proses Enkripsi AES-128	95
Lampiran 9. Dokumentasi Pengujian Kecepatan Pengiriman Data <i>Ciphertext</i>	96
Lampiran 10. Dokumentasi Pengembangan dan Pengujian Sistem oleh Penulis .	96
Lampiran 11. <i>Topic</i> MQTT di Broker Adafruit IO.....	97
Lampiran 12. Dokumentasi Tampilan Halaman Dari Web <i>Dashboard</i> Sistem ...	98
Lampiran 13. <i>Library & Function</i> penting pada kode program C++ di ESP32.	100
Lampiran 14. Kode Program <i>MQTTHandler</i> pada Laravel PHP.....	102

DAFTAR PERSAMAAN

Persamaan 4.1 Rumus Perhitungan Koefisien Korelasi Pearson.....	76
---	----

DAFTAR PUSTAKA

- Abdullah, D., David, N., Veronika, M., Arlis, N., & Ningsih, A. (2020). *Rancang Bangun Rumah Cerdas Menggunakan RFID*. 2(5), 2655–7541. <https://jurnal.ikhafi.or.id/index.php/jusibi/570>
- Al-Mashhadani, M., & Shujaa, M. (2022). IoT Security Using AES Encryption Technology based ESP32 Platform. *International Arab Journal of Information Technology*, 19(2), 214–223. <https://doi.org/10.34028/iajit/19/2/8>
- Amos, B. (2020). *Hands-On RTOS with Microcontrollers: Building real-time embedded systems using FreeRTOS, STM32 MCUs, and SEGGER debug tools*. Packt Publishing Ltd.
- Annaba, I. A., Faisal, S., Arum, S., & Lestari, P. (2021). *Keamanan Pintu Rumah Dengan RFID dan Magentic Switch Berbasis Internet Of Things*. II(1), 57. <http://journal.ubpkarawang.ac.id/mahasiswa/index.php/ssj/article/view/225>
- Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *JTSI*, 4(2), 394–405. <https://doi.org/10.35957/jtsi.v4i2.6077>
- Armada-IT. (2024). *BF-870 Web Based RFID Multi Door Controller*. <http://armada-it.com/product/bf-870-web-based-rfid-multi-door-controller.html> (Diakses pada 18 April 2024)
- Arora, M. (2012). *How Secure is AES 128 and 256 Encryption Against Brute Force Attacks?* EETimes. <https://www.eetimes-com.translate.goog/how-secure-is-aes-against-brute-force-attacks/> (Diakses pada 25 April 2024)
- Arpaia, P., Bonavolontá, F., & Cioffi, A. (2020). Problems of the advanced encryption standard in protecting Internet of Things sensor networks. *Measurement: Journal of the International Measurement Confederation*, 161. <https://doi.org/10.1016/j.measurement.2020.107853>
- Athallah Aditya, R., & Setia Budi, A. (2023). *Prototipe Sistem Keamanan Parkir berbasis RFID dengan Protokol MQTT*. 7(7), 3287–3295. <http://j-ptiik.ub.ac.id>
- Bader, K. C. (2016, September 24). *Unveiling PINs with Thermal Imaging on Number Pads*. <https://www.kaibader.de/thermal-imaging-of-fingerprints-how-to-get-your-pin-from-a-number-pad/> (Diakses pada 11 April 2024)
- Bell, C. (2024). MQTT with Adafruit IO. Dalam *MicroPython for the Internet of Things* (hlm. 465–496). Apress. https://doi.org/10.1007/978-1-4842-9861-9_14

- Binar Academy. (2023). *Metode Agile: Pengertian, Tujuan, dan Prinsipnya*. <https://www.binaracademy.com/blog/metode-agile-adalah> (Diakses pada 8 Mei 2024)
- Biswal, U., Paul, R., Pattnaik, S., & Pattanayak, B. K. (2022). AES Based End-to-End Encryption Scheme for Secure Communication on Internet of Things (IoT). *SPECIALUSIS UGDYMAS / SPECIAL EDUCATION*, 1(43), 5600–5616.
- Blessing, L., & Chakrabarti, A. (2009). DRM: A Design Research Methodology. Dalam *DRM, a Design Research Methodology* (hlm. 13–42). Springer London. https://doi.org/10.1007/978-1-84882-587-1_2
- Çelik, S., Yalçın, N., & Çakır, S. (2023). MitM Attacks and IoT Security: A Case Study on MQTT 1. *Journal of Artificial Intelligence and Data Science (JAIDA)*, 3(2), 99–106. <https://dergipark.org.tr/pub/jaida>
- Chen, F., Huo, Y., Zhu, J., & Fan, D. (2020). A Review on the Study on MQTT Security Challenge. *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, 128–133. <https://doi.org/10.1109/SmartCloud49737.2020.00032>
- Ciesla, R. (2020). Creating Extremely Secure Encrypted Systems. Dalam *Encryption for Organizations and Individuals* (hlm. 103–148). Apress. https://doi.org/10.1007/978-1-4842-6056-2_6
- Das, R., & Chang, Y.-H. (2023). *RFID Forecasts, Players and Opportunities 2023-2033*. <https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2023-2033/927> (Diakses pada 14 Mei 2024)
- Erwin, Datya, A. I., Nurohim, Sepriano, Waryono, Adhicandra, I., Budihartono, E., & Purnawati, N. W. (2023). *Pengantar & Penerapan Internet Of Things: Konsep Dasar & Penerapan IoT di berbagai Sektor* (Efitra, Ed.). PT. Sonpedia Publishing Indonesia.
- Espressif. (2024). *ESP32 Series Datasheet 2.4 GHz Wi-Fi + Bluetooth® + Bluetooth LE SoC Including*. https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (Diakses pada 14 Mei 2024)
- Fakri Husni, M., & Elfizon. (2022). Rancang Bangun Pengaman Brankas menggunakan RFID (Radio Frequency Identification), Pin dan GPS Berbasis Arduino Mega dan Internet Of Things (IoT). *R2J*, 4(2). <https://doi.org/10.38035/rrj.v4i2>
- Ferrara, P., Mandal, A. K., Cortesi, A., & Spoto, F. (2021). Static analysis for discovering IoT vulnerabilities. *International Journal on Software Tools for Technology Transfer*, 23(1), 71–88. <https://doi.org/10.1007/s10009-020-00592-x>

- Figueroa, S., Carías, J. F., Añorga, J., Arrizabalaga, S., & Hernantes, J. (2018). A RFID-based IoT Cybersecurity Lab in Telecommunications Engineering. *IEEE XIII Technologies Applied to Electronics Teaching Conference (TAE)*. <https://doi.org/10.1109/TAE.2018.8475973>
- Fragaria Audika, R. (2021). *Smart Laboratory Menggunakan Radio Frequency Identification (RFID) Berbasis Internet Of Things*. [Universitas Siliwangi]. <http://repositori.unsil.ac.id/3129/>
- Gothwal, R., Dharmani, G., Reen, R. S., & Abdallah, E. G. (2023). Evaluation of Man-in-the-Middle Attacks and Countermeasures on Autonomous Vehicles. *Proceedings - 2023 10th International Conference on Dependable Systems and Their Applications, DSA 2023*, 502–509. <https://doi.org/10.1109/DSA59317.2023.00070>
- Gunawan, I. (2023). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *Jurnal Media Informatika (JUMIN)*, 4(2), 102–109. <https://doi.org/10.55338/jumin.v4i2.496>
- Guseti, J. H. (2021). *Pencatatan Kehadiran Mahasiswa Menggunakan Teknologi RFID Berbasis Mobile Studi Kasus Universitas Siliwangi*. [Universitas Siliwangi]. <http://repositori.unsil.ac.id/5966/>
- Hadi Prayitno, R., Sudiro, S. A., Madenda, S., & Harmanto, S. (2022). Hardware Implementation Of Galois Field Multiplication For Mixcolumn And Inversemixcolumn Process In Encryption-Decryption Algorithms. *Journal of Theoretical and Applied Information Technology*, 31(14). www.jatit.org
- Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent security trends in internet of things: A comprehensive survey. *IEEE Access*, 9, 113292–113314. <https://doi.org/10.1109/ACCESS.2021.3103725>
- Hintaw, A. J., Manickam, S., Aboalmaaly, M. F., & Karuppayah, S. (2023). MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT). *IETE Journal of Research*, 69(6), 3368–3397. <https://doi.org/10.1080/03772063.2021.1912651>
- Hutasuhut, D. I. G., Aldizar, M. R., Nasution, I. F., & Nasution, M. F. (2023). Perbandingan Algoritma Kriptografi Simetris dan Asimetris. *UNES Journal of Information System*, 8(1), 42–47. <https://fe.ekasakti.org/index.php/UJIS>
- Imperva. (2020). *ARP Spoofing*. <https://www.imperva.com/learn/application-security/arp-spoofing/> (Diakses pada 14 Mei 2024)
- Irawan, B. (2020). *Pengembangan Alarm Keamanan Balita di Lingkungan Rumah Berbasis Raspberry Pi dan Radio Frequency Identification (RFID) Menggunakan Metode Fuzzy Mamdani*. [Universitas Islam Riau]. <https://repository.uir.ac.id/9881/>

- Kaindl, S. (2021). *Balancing performance, energy consumption and security in resource constrained environments* [Institut für Information Systems Engineering]. <https://doi.org/10.34726/hss.2021.92781>
- Khursheed, F., Sami-Ud-Din, M., Sumra, I. A., & Safder, M. (2020). A Review of Security Mechanism in internet of Things(IoT). *IEEE 3rd International Conference on Advancements in Computational Sciences, ICACS 2020*. <https://doi.org/10.1109/ICACS47775.2020.9055949>
- Kietzmann, P., Boeckmann, L., Lanzieri, L., Schmidt, T. C., & Ahlisch, M. W. (2021). *A Performance Study of Crypto-Hardware in the Low-end IoT*.
- Kurniawan, A. B. (2019, Januari 3). *3 Cara Algoritma Konversi Biner Ke ASCII Dengan Javascript*. KopiCoding. <https://www.kopicoding.com/3-cara-algoritma-konversi-biner-ke-ascii/> (Diakses pada 21 Mei 2024)
- LastMinuteEngineers. (2024). *What is RFID? How It Works? Interface RC522 RFID Module with Arduino*. <https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/> (Diakses pada 21 Mei 2024)
- Light, R. (2022, Oktober 6). *Understanding MQTT Quality of Service or also known as MQTT QoS*. Cedalo. <https://cedalo.com/blog/understanding-mqtt-qos/> (Diakses pada 20 Mei 2024)
- Lounis, K., & Zulkernine, M. (2020). Attacks and Defenses in Short-Range Wireless Technologies for IoT. *IEEE Access*, 8, 88892–88932. <https://doi.org/10.1109/ACCESS.2020.2993553>
- Majidha Fathima, K. M., & Santhiyakumari, N. (2021). A Survey on Network Packet Inspection and ARP Poisoning Using Wireshark and Ettercap. *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, 1136–1141. <https://doi.org/10.1109/ICAIS50930.2021.9395852>
- Mubarok, F. H. A., & Subali, M. (2020). Sistem Keamanan Pintu Portal Pada Perumahan Dengan Rfid Menggunakan Nodemcu Berbasis Website. *Seminar Nasional Teknologi Informasi dan Komunikasi STI&K (SeNTIK)*, 4(1).
- Munir, R. (2004). *Advanced Encryption Standard (AES)*. [https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Advanced%20Encryption%20Standard%20\(AES\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Advanced%20Encryption%20Standard%20(AES).pdf) (Diakses pada 8 Mei 2024)
- Munir, R. (2020). *Kripto 20: Advanced Encryption Standard (AES)*. Youtube. <https://youtu.be/4q3bA0W7UHg?si=0LYyzdmIu2fniv3U> (Diakses pada 8 Mei 2024)
- Muthohir, M., Rakasiwi, S., & Ubaidillah, L. (2023). *Warehouse Management System Berbasis Radio Frequency Identification*. 3(1), 2827–9379.

- Nandy, T., Idris, M. Y. I. Bin, Md Noor, R., Mat Kiah, M. L., Lun, L. S., Annuar Juma'At, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. *IEEE Access*, 7, 151054–151089. <https://doi.org/10.1109/ACCESS.2019.2947723>
- Nas, M., Harfina, & Armila, N. (2019). *Sistem Pengontrolan Pintu Gerbang Berbasis IoT*. 42. <https://jurnal.poliupg.ac.id/index.php/snp2m/article/viewFile/1774/1618>
- Nurwijaksana, T., & Candra, R. (2021). Access Server Room Using RFID Implemented for Security. *Techno.Com: Jurnal Teknologi Informasi*, 20(3), 411–419.
- Osawa, Y., & Katsura Seiichiro. (2019). Rendering Thermal Sensation of Fingertip by Using Spatial Information of Heat Sources. *IEEE/SICE International Symposium on System Integration (SII)*.
- Othman Sharif, H., Hama Ali Faraj, K., Hassan Ahmed, K., Nawzad Ahmed Al Attar, T., Mustafa Hameed, W., & Baker Kanbar, A. (2002). Response Time analysis for XAMPP Server based on Different Versions of Linux Operating System. *The Scientific Journal of Cihan University-Sulaimaniya*, 4, 102–114. <https://doi.org/10.25098/4.2.23>
- Pearson, B., Zou, C., Zhang, Y., Ling, Z., & Fu, X. (2020). SIC2: Securing Microcontroller Based IoT Devices with Low-cost Crypto Coprocessors. *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, 2020-December*, 372–381. <https://doi.org/10.1109/ICPADS51040.2020.00057>
- Prasetyo, D. B. (2020). *Protokol Jaringan Dalam Internet of Things*. LPPM UPN “Veteran” Yogyakarta. <http://eprints.upnyk.ac.id/27440/1/buku-protokol-jaringan-dalam-iot-dan-sertifikat-haki.pdf>
- Pratiwi, A., Fauzi, A., & Sulistya Kusumaningrum, D. (2022). Sistem Pengamanan Pintu Otomatis Berbasis RFID Menggunakan Metode AES. *Scientific Student Journal for Information, Technology and Science*, III(2), 202.
- Putra, J., Hd, M. A., & Pamungkas, W. (2022). *Sistem Pengaman Pintu Rumah Menggunakan Sensor RFID RC522 dan Fingerprint Berbasis Internet Of Things*. 8(2), 14–21. <https://ejournal.borobudur.ac.id/index.php/08/article/download/1148/942>
- Rampalemba, & Febrian, P. (2016). *Analisis Iterated Cipher Berdasarkan Avalanche Effect pada Rancangan Skema Transposisi (P-Box) dan S-box Crypton: Suatu Tinjauan Optimasi Putaran pada Block Cipher* [Universitas Kristen Satya Wacana]. <http://repository.uksw.edu/handle/123456789/13569>

- RandomNerdTutorials. (2018). *ESP32 DOIT DEVKIT V1 Board Pinout 30 GPIO*. <https://randomnerdtutorials.com/> (Diakses pada 29 Mei 2024)
- Ravida, R., & Santoso, H. A. (2020). Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Internet of Things (IoT) Tanaman Hidroponik. *JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(6), 1157–1164. <https://doi.org/10.29207/resti.v4i6.2478>
- Saiqul Umam, M., Adi Wibowo, S., & Agus Pranoto, Y. (2023). Implementasi Protokol MQTT Pada Aplikasi Smart Garden Berbasis IoT (Internet Of Things). Dalam *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Nomor 1).
- Saputra, B. B. (2024). *Pengembangan Website Dokumentasi Chart.js Dan Laravel Untuk Menampilkan Data IoT* [Universitas Muhammadiyah Yogyakarta]. <https://etd.umy.ac.id/id/eprint/44524/>
- Sarker, V. K., Gia, T. N., Tenhunen, H., & Westerlund, T. (2020, Juni). Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. *IEEE International Conference on Communications (ICC)*. <https://doi.org/10.1109/ICC40277.2020.9149359>
- Satria, D. (2022). Sistem Pengamanan Pintu Berbasis RFID (Radio Frekuensi Identification) Menggunakan Arduino Uno. *Journal Computer Science & Information System*, 3(2), 115–121. <https://doi.org/10.53514/jco.v3i2.430>
- Setiawan, D. (2020). Rancang Bangun Sistem Keamanan Kunci Pintu Lemari Berbasis Mikrokontroler. *Journal of Science and Social Research*, 1, 51–56. <http://jurnal.goretanpena.com/index.php/JSSR>
- Shaikh, E., Mohiuddin, I., & Manzoor, A. (2019). Internet of Things (IoT): Security and Privacy Threats. *IEEE 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. <https://doi.org/10.1109/CAIS.2019.8769539>
- Silveira, M. F., & Gradvohl, A. L. S. (2021). Security analysis of the message queuing telemetry transport protocol. *Revista Brasileira de Computação Aplicada*, 13(2), 83–95. <https://doi.org/10.5335/rbca.v13i2.12163>
- Simsek, M. M., & Atilgan, E. (2023). Attacks on Availability of IoT Middleware Protocols: A Case Study on MQTT. *Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi*, 4(2), 16–27. <https://doi.org/10.53608/estudambilisim.1297052>
- Stacey, L. (2023, Januari 4). *MQTT beginner's guide*. u-blox. <https://www.u-blox.com/en/blogs/insights/mqtt-beginners-guide> (Diakses pada 30 Mei 2024)
- Swathika, O. V. G., & Hemapala, K. T. M. U. (2019). IoT Based Energy Management System for Standalone PV Systems. *Journal of Electrical*

- Engineering and Technology*, 14(5), 1811–1821.
<https://doi.org/10.1007/s42835-019-00193-y>
- Syafaat, M., Ramadhan, A. N., Syafiun, R. B., & Haerunnisa, D. A. (2023). IoT-Based Smart Garden Using MQTT Protocol With Adafruit IO App. *Jurnal Teknik Informatika (Jutif)*, 4(4), 723–732.
<https://doi.org/10.52436/1.jutif.2023.4.4.636>
- Syms, R. R. A., Sydoruk, O., & Wiltshire, M. C. K. (2021). Magneto-Inductive HF RFID System. *IEEE Journal of Radio Frequency Identification*, 5(2), 148–153. <https://doi.org/10.1109/JRFID.2020.3042719>
- Tu, Y. J., Chi, H., Zhou, W., Kapoor, G., Eryarsoy, E., & Piramuthu, S. (2019). Critical evaluation of RFID applications in healthcare. *Communications in Computer and Information Science*, 1113 CCIS, 240–248.
https://doi.org/10.1007/978-3-030-34353-8_18
- Wicaksono, S. R. (2021). *Blackbox Testing Teori dan Studi Kasus* (1 ed.). CV. Seribu Bintang . <https://doi.org/10.5281/zenodo.7659674>
- Windryani, N. P., Bogi, N., & Mayasari, R. (2019). *Analisa Perbandingan Protokol MQTT dengan HTTP Pada IoT Platform Patriot Comparison Analysis Between MQTT and HTTP Protocol In Patriot IoT Platform*. 3192–3199.
<https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/issue/view/118>
- Yudinata, F. (2022). *Rancang Bangun Alat Pemindai E-Ktp Untuk Loker Penitipan Barang Menggunakan Teknologi RFID Berbasis Arduino* [Universitas Mercu Buana]. <https://repository.mercubuana.ac.id/69051/>
- Yulisman, Iman, N., Sabna, E., & Fonda, H. (2021). Sistem Pintu Otomatis Menggunakan E-KTP Berbasis Internet of Things (IoT) pada Kamar Hotel. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, 1(2), 85–91.
<https://doi.org/10.54259/satesi.v1i2.60>
- Zuo, J., Feng, J., Gameiro, M. G., Tian, Y., Liang, J., Wang, Y., Ding, J., & He, Q. (2022). RFID-based sensing in smart packaging for food applications: A review. *Future Foods*, 6. <https://doi.org/10.1016/j.fufo.2022.100198>