# IMPLEMENTASI ALGORITMA *BLOWFISH* DAN AUTENTIKASI HMAC PADA SISTEM MONITORING KELEMBABAN TANAH BERBASIS IOT UNTUK MITIGASI SERANGAN *MAN-IN-THE-MIDDLE*

**MICHAEL MIDO RETA PRATAMA**
**H1051221037**

**SKRIPSI**

**PROGRAM STUDI REKAYASA SISTEM KOMPUTER**
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**
**UNIVERSITAS TANJUNGPURA**
**PONTIANAK**
**2026**

# IMPLEMENTASI ALGORITMA *BLOWFISH* DAN AUTENTIKASI HMAC PADA SISTEM MONITORING KELEMBABAN TANAH BERBASIS IOT UNTUK MITIGASI SERANGAN *MAN-IN-THE-MIDDLE*

**MICHAEL MIDO RETA PRATAMA**
**H1051221037**

Skripsi
Sebagai alah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer

**PROGRAM STUDI REKAYASA SISTEM KOMPUTER**
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**
**UNIVERSITAS TANJUNGPURA**
**PONTIANAK**
**2026**

# LEMBAR PENGESAHAN

| | | |
|---|---|---|
| Judul Tugas Akhir | : | Implementasi Algoritma *Blowfish* Dan Autentikasi Hmac Pada Sistem Monitoring Kelembaban Tanah Berbasis IoT Untuk Mitigasi Serangan *Man-In-The-Middle* |
| Nama Mahasiswa | : | Michael Mido Reta Pratama |
| NIM | : | H1051221037 |
| Jurusan/Program Studi | : | Rekayasa Sistem Komputer |
| Tanggal Lulus | : | 28 Juli 2026 |
| SK Pembimbing | : | No.623/DST/UN22.8/DT.00.09/2026 20 Febuari 2026 |
| SK Penguji | : | No.4533/DST/UN22.8/DT.00.09/2026 21 Juli 2026 |

Dosen Pembimbing

| Pembimbing I | Pembimbing II |
|---|---|
| Kasliono, S.Mat., M.Cs. | Syamsul Bahri, S.Kom., M.Cs |
| NIP. 199306202022031005 | NIP. 198802272015041001 |

Dosen Penguji

| Ketua Penguji | Anggota Penguji |
|---|---|
| Uray Ristian, S.Kom., M.Kom. | Hafiz Muhardi, S.T., M.Kom |
| NIP. 199012012019031017 | NIP. 199007232023211017 |

| Pimpinan Sidang (merangkap anggota penguji) | Sekretaris Sidang (merangkap anggota penguji) |
|---|---|
| Kasliono, S.Mat., M.Cs. | Syamsul Bahri, S.Kom., M.Cs |
| NIP. 199306202022031005 | NIP. 198802272015041001 |

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si., M.Si.
NIP. 197108022000031001



Dipindai dengan CamScanner

## PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Michael Mido Reta Pratama |
| NIM | : H1051221037 |
| Program Studi/ Jurusan | : Rekayasa Sistem Komputer |
| Fakultas | : Matematika dan Ilmu Pengetahuan Alam |

Dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyataan ini untuk digunakan sebagaimana mestinya.

Pontianak, 28 Juli 2026




Michael Mido Reta Pratama

H1051221037



Dipindai dengan CamScanner

**Implementasi Algoritma *Blowfish* Dan Autentikasi HMAC Pada Sistem Monitoring Kelembaban Tanah Berbasis IoT Untuk Mitigasi Serangan *Man-In-The-Middle***


## Abstrak

Perkembangan *Internet of Things* (IoT) telah mendorong penerapan sistem monitoring kelembaban tanah secara otomatis dalam bidang pertanian. Namun, proses transmisi data pada sistem IoT masih rentan terhadap serangan Man-in-The-Middle (MITM) yang berpotensi menyebabkan penyadapan maupun manipulasi data. Oleh karena itu, penelitian ini dilakukan untuk meningkatkan keamanan transmisi data pada sistem monitoring kelembaban tanah berbasis IoT melalui penerapan algoritma Blowfish dan autentikasi HMAC. Kerahasiaan data dijaga menggunakan algoritma Blowfish, sedangkan integritas dan keaslian data dijamin melalui autentikasi HMAC. Sistem diimplementasikan menggunakan mikrokontroler ESP32, sensor soil moisture, relay, pompa air, dan Application Programming Interface (API) berbasis Laravel. Pengujian dilakukan melalui simulasi serangan sniffing dan ARP Poisoning serta pengukuran waktu pemrosesan sebelum dan sesudah penerapan algoritma. Hasil pengujian menunjukkan bahwa data yang ditransmisikan berhasil diamankan dari proses penyadapan karena telah diubah menjadi *ciphertext*. Selain itu, data yang dimanipulasi selama transmisi berhasil dideteksi melalui mekanisme verifikasi HMAC sehingga tidak dapat diproses oleh aktuator. Penerapan algoritma Blowfish dan HMAC menyebabkan peningkatan waktu pemrosesan pada kedua perangkat ESP32, namun seluruh proses sistem tetap dapat dijalankan dalam waktu kurang dari satu detik. Dengan demikian, algoritma Blowfish dan autentikasi HMAC dapat diterapkan secara efektif untuk meningkatkan keamanan transmisi data pada sistem monitoring kelembaban tanah berbasis IoT tanpa memberikan dampak yang signifikan terhadap performa sistem.



**Kata kunci:** *Internet of Things*, Blowfish, HMAC, *Man-in-The-Middle*

**Implementasi Algoritma *Blowfish* Dan Autentikasi HMAC Pada Sistem Monitoring Kelembaban Tanah Berbasis IoT Untuk Mitigasi Serangan *Man-In-The-Middle***


## Abstract

*The development of the Internet of Things (IoT) has encouraged the implementation of automated soil moisture monitoring systems in agriculture. However, data transmission processes in IoT systems remain vulnerable to Man-in-The-Middle (MITM) attacks that may lead to data interception and manipulation. Therefore, this study was conducted to enhance data transmission security in an IoT-based soil moisture monitoring system through the implementation of the Blowfish algorithm and HMAC authentication. Data confidentiality was maintained using the Blowfish algorithm, while data integrity and authenticity were ensured through HMAC authentication. The system was implemented using ESP32 microcontrollers, a soil moisture sensor, a relay module, a water pump, and a Laravel-based Application Programming Interface (API). Testing was carried out through sniffing and ARP Poisoning attack simulations as well as processing-time measurements before and after the implementation of the proposed algorithms. The results showed that transmitted data were successfully protected from interception by being transformed into ciphertext. Furthermore, manipulated data were successfully detected through the HMAC verification mechanism, preventing them from being processed by the actuator. The implementation of Blowfish and HMAC increased the processing time on both ESP32 devices; however, all system operations were still completed in less than one second. Therefore, the Blowfish algorithm and HMAC authentication can be effectively applied to improve data transmission security in IoT-based soil moisture monitoring systems without significantly affecting system performance.*



**Keywords:** *Internet of Things*, Blowfish, HMAC, *Man-in-The-Middle,*

# PRAKATA

Segala puji dan syukur penulis panjatkan ke hadirat Yesus Kristus atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Implementasi Algoritma *Blowfish* Dan Autentikasi HMAC Pada Sistem Monitoring Kelembaban Tanah Berbasis IoT Untuk Mitigasi Serangan *Man-In-The-Middle* "**. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Jurusan Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura Pontianak.

Penyusunan skripsi ini tidak terlepas dari dukungan, bantuan, dan bimbingan dari berbagai pihak yang telah memberikan motivasi serta arahan kepada penulis selama proses perkuliahan hingga penyelesaian skripsi ini. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura Pontianak.
2. Ibu Rahmi Hidayati , S.Kom., M.Cs. selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
3. Bapak Kasliono, S.Mat., M.Cs., selaku Dosen Pembimbing Pertama yang telah meluangkan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.
4. Bapak Syamsul Bahri, S.Kom., M.Cs., selaku Dosen Pembimbing Kedua yang telah memberikan bimbingan, saran, dan masukan selama proses penyusunan skripsi ini.
5. Bapak Uray Ristiyan, S.Kom., M.Kom., selaku Dosen Penguji Pertama yang telah memberikan kritik dan saran untuk penyempurnaan skripsi ini.
6. Bapak Hafiz Muhardi, S.T., M.Kom., selaku Dosen Penguji Kedua yang telah memberikan masukan dan saran yang membangun.
7. Kepada seluruh dosen prodi Rekayasa Sistem Komputer yang telah memberikan ilmu selama masa perkuliahan.
8. Kepada seluruh tenaga pendidik FMIPA Untan yang sudah membantu administratif selama masa perkuliahan penulis.

9. Kepada kedua orang tua yang telah memberikan dukungan, semangat, dan doa sepanjang perjalanan penulisan tugas akhir ini.
10. Kepada rekan kerja Himaster periode 2024/2025 yang telah memberikan pengalaman organisasi dan membantu pengembangan diri penulis agar menjadi lebih baik
11. Kepada angkatan Cytigon 2022 yang telah mendukung dan menemani penulis selama masa pekuliahan hingga penyelesaian skripsi ini.
12. Kepada saudara Hamdi yang telah memberikan masukan, kritik dan sumber daya yang mendukung proses penyelesaian skripsi ini.
13. Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.
14. Kepada penulis yang telah berjuang menyelesaikan masa studi, dengan berbagai penerimaan, penyesalan dan pembelajaran.

Pontianak, 28 Juli 2026

Michael Mido Reta Pratama

# DAFTAR ISI

LEMBAR PENGESAHAN ..... ii
PERNYATAAN INTEGRITAS AKADEMIK ..... iii
Abstrak ..... iv
Abstract ..... v
PRAKATA ..... vi
DAFTAR ISI ..... viii
DAFTAR GAMBAR ..... xii
DAFTAR TABEL ..... xiv
DAFTAR KODE PROGRAM ..... xv
BAB 1 PENDAHULUAN ..... 1
1.1 Latar Belakang ..... 1
1.2 Rumusan Masalah ..... 4
1.3 Batasan Masalah ..... 4
1.4 Tujuan Penelitian ..... 5
1.5 Manfaat Penelitian ..... 5
1.6 Sistematika Penulisan ..... 6
BAB 2 LANDASAN TEORI ..... 8
2.1 Perbandingan dengan Penelitian Terdahulu ..... 8
2.2 Blowfish ..... 9
2.2.1 Ekspansi Kunci ..... 10
2.2.3 Fungsi *F* ..... 11
2.2.4 Dekripsi Data ..... 12
2.3 HMAC ..... 12
2.3.1 Tahap Inner Padding ..... 13
2.3.2 Tahapan Outer Padding ..... 13
2.4 Wireshark ..... 14
2.5 Serangan MiTM (*Man-in-The-Middle*) ..... 14
2.5.1 ARP Poisoning ..... 14
2.5.2 Sniffing ..... 15
2.6 ESP32 ..... 15

2.7 Modul Soil Moisture ..... 16
2.8 Arduino IDE ..... 16
2.9 PHP ..... 17
2.10 *Application Programming Interface (*API) ..... 17
2.11 Laravel ..... 17
2.12 Laragon ..... 18
2.13 Modul Relay ..... 18
2.14 Pompa DC ..... 19
2.15 Visual Studio Code ..... 19
2.16 Burp Suite ..... 19
2.17 MySQL ..... 20
BAB 3 METODE PENELITIAN ..... 21
3.1 Studi Literatur ..... 22
3.2 Analisis Kebutuhan ..... 22
3.2.1 Kebutuhan Perangkat Keras ..... 22
3.2.2 Kebutuhan Perangkat Lunak ..... 22
3.3 Perancangan Sistem ..... 23
3.4 Implementasi ..... 23
3.5 Pengujian Sistem ..... 24
3.6 Pengumpulan Data ..... 24
3.7 Kesimpulan dan Saran ..... 24
BAB 4 PERANCANGAN ..... 25
4.1 Deskripsi Sistem ..... 25
4.2 Perancangan Arsitektur Sistem ..... 26
4.3 Perancangan Perangkat Keras ..... 27
4.3.1 Perancangan ESP32 A dan Modul Soil Moisture ..... 27
4.3.2 Perancangan ESP32 B dan Aktuator ..... 28
4.3.3 Perancangan Keseluruhan Alur Kendali Pompa ..... 29
4.4 Perancangan Perangkat Lunak ..... 30
4.5 Perancangan Implementasi Algoritma Blowfish dan HMAC ..... 30
4.5.1 Perancangan S-Box pada Blowfish ..... 30

4.5.2 Perancangan Impelemntasi Algoritma *Blowfish* Dan Algoritma HMAC Pada Proses Enkripsi ..... 31
4.5.3 Perancangan Implementasi *Blowfish* Dan Penambahan HMAC Pada Proses Dekripsi ..... 34
4.6 Perancangan Database ..... 36
4.7 Perancangan Pengujian ..... 37
4.7.1 Pengujian Waktu Sebelum Dan Sesudah Implementasi Algoritma *Blowfish* Dan Algoritma HMAC ..... 37
4.7.2 Pengujian *Sniffing* ..... 37
4.7.3 Pengujian ARP Poisoning ..... 38
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN ..... 39
5.1 Implementasi Perangkat Keras ..... 39
5.1.1 Implementasi Sensor *Soil Moisture* ..... 39
5.1.2 Implementasi Aktuator ..... 40
5.2 Implementasi Perangkat Lunak ..... 40
5.2.1 Implementasi Server Laragon dan API ..... 40
5.2.2 Implementasi S-Box Blowfish ..... 41
5.2.3 Implementasi Fungsi F ..... 42
5.2.4 Implementasi P-Array Blowfish ..... 42
5.2.5 Implementasi Inisialisasi Kunci Blowfish ..... 43
5.2.6 Implementasi Proses Enkripsi Blowfish ..... 43
5.2.7 Implementasi Proses Dekripsi Blowfish ..... 44
5.2.8 Implementasi SHA-256 ..... 45
5.2.9 Implementasi Proses HMAC ..... 46
5.2.10 Implementasi Perhitungan Waktu Proses ESP32 A ..... 47
5.2.11 Implementasi Perhitungan Waktu ESP32 B ..... 48
5.3 Algoritma Blowfish ..... 49
5.3.1 Proses Enkripsi ..... 49
5.3.2 Proses Dekripsi ..... 50
5.3.3 Proses HMAC ..... 51
5.4 Pengujian Sistem ..... 53

5.4.1 Pengujian *Sniffing* Data Sebelum Implementasi Blowfish dan HMAC ..... 53
5.4.2 Pengujian *Sniffing* Data Setelah Implementasi Blowfish dan HMAC ..... 55
5.4.3 Pengujian ARP Poisoning Sebelum Implementasi Blowfish dan HMAC ..... 58
5.4.4 Pengujian ARP Poisoning Sesudah Implementasi Blowfish dan HMAC ..... 61
5.4.5 Pengujian Waktu Sebelum Dan Sesudah Penerapan Algoritma Blowfish Dan HMAC ..... 65
5.4.6 Pembahasan ..... 68
BAB 6 PENUTUP ..... 71
6.1 Kesimpulan ..... 71
6.2 Saran ..... 71
DAFTAR PUSTAKA ..... 73
LAMPIRAN ..... 76

# DAFTAR GAMBAR

Gambar 2.1 ESP32 ..... 16
Gambar 2.2 Modul Soil Moisture ..... 16
Gambar 2.3 Modul Relay ..... 18
Gambar 2.4 Pompa DC ..... 19
Gambar 3.1 Diagram Alir Penelitian ..... 21
Gambar 4.1 Alur Sistem Keseluruhan ..... 25
Gambar 4.2 ESP32 A ke Modul Soil Moisture ..... 27
Gambar 4.3 ESP32 B ke Pompa ..... 28
Gambar 4.4 Alur Kendali Pompa ..... 29
Gambar 4.5 Proses Enkripsi pada Blowfish ..... 32
Gambar 4.6 Proses Penambahan HMAC pada ESP32 A ..... 33
Gambar 4.7 Proses Dekripsi Blowfish ..... 34
Gambar 4.8 Keseluruhan Alur Blowfish dan HMAC ..... 36
Gambar 5.1 Implementasi Sensor Soil Moisture ..... 39
Gambar 5.2 Implementasi Aktuator ..... 40
Gambar 5.3 Implementasi Server Laragon dan API ..... 41
Gambar 5.4 Hasil Enkripsi pada Arduino IDE ..... 50
Gambar 5.5 Hasil Dekripsi pada Arduino IDE ..... 51
Gambar 5.6 Hasil Perhitungan HMAC pada Arduino IDE ..... 52
Gambar 5.7 *Sniffing* dari ESP32 A ke Database API Laravel ..... 55
Gambar 5.8 *Sniffing* dari Database API Laravel ke ESP32 B ..... 55
Gambar 5.9 *Sniffing* setelah implementasi Blowfish dan HMAC dari ESP32 A ke Database API Laravel ..... 58
Gambar 5.10 *Sniffing* setelah implementasi Blowfish dan HMAC dari Database API Laravel ke ESP32 B ..... 58
Gambar 5.11 Proses Perubahan Data Pada Burp Suite ..... 60
Gambar 5.12 Eksekusi Data Pada Aktuator Setelah Data Diubah ..... 61
Gambar 5.13 Hasil Perubahan Data Pada Database API Laravel ..... 61
Gambar 5.14 Perubahan Data Pada Burp Suite ..... 64

Gambar 5.15 Data Yang Dirubah Ditolak Oleh Aktuator ..... 65

# DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu ..... 8
Tabel 4.1 Konfigurasi Pin pada ESP32 dan Modul Soil Moisture..... 27
Tabel 4.2 Konfigurasi Pin pada ESP32 dan Modul Relay ..... 28
Tabel 5.1 Hasil Enkripsi Blowfish ..... 50
Tabel 5.2 Hasil Dekripsi Blowfish ..... 51
Tabel 5.3 Hasil HMAC ..... 52
Tabel 5.4 Pengujian Sniffing Sebelum Implementasi Blowfish dan HMAC..... 53
Tabel 5.5 Hasil pengujian sniffing setelah implementasi algoritma Blowfish dan HMAC ..... 55
Tabel 5.6 Perubahan Data antara ESP32 A ke Database API Laravel ..... 59
Tabel 5.7 Pengubahan Data Sesudah Implementasi Blowfish Dan HMAC ..... 61
Tabel 5.8 Pengujian Delay Algoritma Blowfish dan HMAC..... 65

# DAFTAR KODE PROGRAM

Kode Program 5.1 S-Box Blowfish ..... 41
Kode Program 5.2 Implementasi Fungsi F ..... 42
Kode Program 5.3 Implementasi P-Array Blowfish ..... 42
Kode Program 5.4 Implementasi inisialisasi kunci Blowfish ..... 43
Kode Program 5.5 Implementasi Proses Enkripsi Blowfish ..... 44
Kode Program 5.6 Implementasi Proses Dekripsi Blowfish ..... 44
Kode Program 5.7 Implementasi SHA-256 ..... 45
Kode Program 5.8 Implementasi HMAC ..... 46
Kode Program 5.9 Implementasi Perhitungan Waktu Proses ESP32 A ..... 47
Kode Program 5.10 Implementasi Perhitungan Waktu ESP32 B ..... 48

# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang

Pesatnya perkembangan mikrokontroler dan internet, penggunaan *Internet of Things* (IoT) menjadi masif diterapkan dalam kehidupan sehari-hari. IoT merupakan perangkat keras yang menggunakan mikrokontroler sebagai pengendali dengan melakukan otomatisasi dalam pengambilan, pengiriman dan pengolahan data dari internet (Youngky, 2025). Perkembangan IoT ini mengakibatkan masifnya penerapan IoT di beberapa sektor seperti sektor industri, pertanian, kesehatan dan lainnya. Dalam bidang pertanian, otomatisasi berbasis IoT mampu merubah praktik bertani konvensional menjadi sistem pertanian cerdas atau *smart farming*, seperti melalui pengembangan sistem monitoring kelembaban tanah yang membantu petani dalam mengelola lahan menjadi lebih efisien. Pada penelitian sistem irigasi berbasis IoT, parameter kelembaban tanah merupakan salah satu indikator utama dalam menentukan kebutuhan air tanaman. Berdasarkan penelitian yang dilakukan oleh Aisyah et al. (2025),Ketika nilai kelembaban tanah turun dibawah 30%, tanah mendekati kondisi bernama *Permanent Wilting Point* (PWP), yaitu titik di mana air di dalam tanah tidak lagi dapat diserap oleh akar tanaman. Pada kondisi ini, tanaman mulai mengalami stres air yang ditandai dengan gejala seperti layu dan penurunan aktivitas fotosintesis. Sebaliknya, ketika kelembaban tanah melebihi 50%, kondisi tanah mendekati *Field Capacity* (FC), yaitu kapasitas maksimum tanah dalam menahan air setelah proses drainase gravitasi. Pada kondisi ini, penambahan air tidak lagi memberikan manfaat bagi tanaman, bahkan berpotensi menyebabkan kelebihan air.

Meskipun terdapat berbagai keandalan pada IoT, terdapat kelemahan dalam aspek keamanan yang menjadi perhatian dengan meningkatnya jumlah perangkat yang terhubung (Sari, 2024). Perangkat IoT yang melibatkan begitu banyak komponen dan data yang terus-menerus berpindah di internet, membuat IoT menghadapi risiko keamanan yang membahayakan (Suryono & Chandra, 2022). Hal ini membuat perangkat IoT rentan terhadap serangan *cyber* seperti *Man-in-the-*

*Middle* (MITM) yang menyusup ke dalam transmisi data. Dalam serangan MITM, penyerang bisa secara diam-diam mengintip, mengubah dan mencuri data (H. Putri et al., 2025). Serangan ini sangat berisiko terhadap IoT terutama dalam sistem pendeteksi kelembaban tanah. Dalam skenario penyerangan sistem pemantauan kelembaban tanah, data yang menunjukkan bahwa tanah sedang basah lalu diubah oleh penyerang menjadi data yang mengatakan bahwa tanah masih kering, maka tindakan ini dapat menyebabkan *trigger* seperti pompa air akan menyiram terus menerus yang dapat menyebabkan kerusakan pada tumbuhan dan kerugian material bagi petani. Dengan rentannya sistem IoT terhadap serangan *cyber,* diperlukan sistem keamanan yang mampu dalam menjaga integritas data. Di sinilah kriptografi hadir sebagai solusi dalam menjaga integritas data selama proses pengiriman data (Febrianto & Zulianto, 2024).

Kriptografi merupakan ilmu yang mempelajari teknik matematis terkait dengan aspek keamanan informasi seperti integritas data, autentikasi entitas dan autentikasi keaslian data. Teknik ini memungkinkan data asli yang dapat dibaca atau *plaintext* diubah menjadi data yang disamarkan atau *ciphertext* melalui proses enkripsi. Kriptografi memastikan tiga hal penting: Kerahasiaan, agar hanya pihak yang berhak yang dapat mengakses, Integritas, agar data tidak diubah selama proses pengiriman data dan Keaslian, agar data yang dapat diolah menjadi sebuah tindakan tidak palsu (Asih & Rizki, 2025).

Penelitian ini menggunakan teknik kriptografi simetris, yaitu algoritma yang memakai satu kunci rahasia yang sama untuk mengunci (enkripsi) dan membuka (dekripsi) data. Algoritma yang akan digunakan adalah Blowfish. Blowfish dipilih karena algoritma ini memiliki kelebihan penggunaan memori yang kecil sehingga dapat diterapkan ke sistem IoT yang memiliki memori yang terbatas. *Blowfish* dikenal karena dapat dijalankan pada memori kurang dari 5KB yang memungkinkan untuk diterapkan pada sistem bermemori kecil seperti mikrokontroler pada IoT dan menggunakan operasi logika XOR untuk proses pengubahan data. Selain itu, Blowfish fleksibel karena panjang kunci yang dapat diatur, dari 32-bit sampai dengan 448-bit membuat algoritma tersebut dapat diatur sesuai dengan penggunaan sumber daya yang digunakan (Sitinjak et al., 2024a).

Selain menggunakan algoritma kriptografi simetris Blowfish untuk kerahasiaan, penelitian ini juga menggunakan algoritma autentikasi sebagai lapisam keamanan tambahan dalam proses pengamanan komunikasi data. Penelitian oleh Yahya et al., 2025 autentikasi merupakan suatu proses yang digunakan untuk memverifikasi dan memastikan keaslian identitas suatu entitas, baik berupa pengguna, perangkat hingga sistem yang berkomunikasi dalam suatu jaringan. Proses ini bertujuan dalam memastikan bahwa pihak yang melakukan komunikasi atau pertukaran data benar benar merupakan entitas yang sah dan memiliki hak akses yang telah disetujui. Dengan adanya mekanisme autentikasi, sistem dapat mencegah akses dari pihak yang tidak berwenang yang memililki potensi dalam melakukan penyadapan, manipulasi data dan serangan lainnya terhadap komunikasi data.

Pada penelitian ini algoritma autentikasi yang digunakan adalah autentikasi HMAC (Hash-based Messeage Authentication Code). HMAC dipakai dalam menutupi kelemahan dari algoritma Blowfish yang hanya menjaga kerahasiaan dari data yang dikirimkan dan masih beresiko untuk diubah saat proses pengiriman data sedang berlangsung. HMAC menggunakan fungsi hash kriptografi seperti SHA-256 dengan kunci rahasia bersama yang menghasilkan tag autentikasi yang akan diverifikasi oleh penerima sebelum data akhirnya akan diproses lebih lanjut. Autentikasi ini dipakai dalam memitigasi jenis serangan MiTM yang dapat mengubah dan memodifikasi data selama alur pengiriman data agar sisi penerima seperti database mengenali data tesebut berasal dari sumber yang terpercaya atau tidak (Anwar & Sriani, 2024).

Pada konteks keamanan sistem monitoring kelembaban tanah, Blowfish dan HMAC menjadi pilihan yang relevan dalam masalah keamanan data mengingat algoritma tersebut fleksibel dan ringan dan tidak menggunakan banyak memori dalam komputasinya. Penelitian Gunawan & Rahmi (2025) mencatat bahwa *Blowfish* memiliki fleksibilitas kunci yang dapat digunakan pada perangkat bermemori kecil dan penelitian oleh Gunawan & Rahmi (2025) yang menyatakan bahwa algoritma HMAC memiliki *Avalanche effect* sebesar 68.24% yang dimana perubahan kecil pada bit data dapat menyebabkan hasil yang sangat berbeda pada output hash.

Berdasarkan penelitian sebelumnya, maka diangkat sebuah penelitian berjudul "Implementasi Algoritma *Blowfish* Dan Autentikasi HMAC Pada Sistem Monitoring Kelembaban Tanah Berbasis Iot Untuk Mitigasi Serangan *Man-In The Middle"*. Penelitian ini bertujuan dalam mengevaluasi kinerja Blowfish dan HMAC dalam mengamankan data selama transmisi dan menganalisis waktu kinerja dari implementasi algoritma tersebut pada sistem monitoring kelembaban tanah.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka didapatlah rumusan permasalahan sebagai berikut:

1. Bagaimana tingkat keamanan transmisi data setelah diterapkannya algoritma Blowfish dan autentikasi HMAC dalam menghadapi serangan *Man-in-the-Middle* (MITM) seperti *sniffing* dan ARP Poisoning yang dapat melihat dan memodifikasi data?.
2. Bagaimana performa waktu pemrosesan untuk proses enkripsi, dekripsi, dan penambahan tag autentikasi menggunakan algoritma Blowfish dan HMAC pada perangkat mikrokontroler ESP32 yang memiliki keterbatasan sumber daya?

## 1.3 Batasan Masalah

Dalam penelitian ini diterapkan ruang lingkup sebagai berikut:

1. Penelitian ini berfokus pada implementasi algoritma kriptografi *Blowfish* dan autentikasi HMAC untuk keamanan transmisi data.
2. Fokus pengamanan data yang diterapkan terbatas pada transmisi nilai kelembaban tanah antar Mikrokontroler dan Mikrokontroler ke *Database*.
3. Masalah keamanan yang disasar untuk diatasi adalah kerentanan terhadap serangan *Sniffing* dan ARP Poisoning pada jalur transmisi data.
4. Penelitian ini berfokus pada pengukuran waktu pengiriman data sebelum dan sesudah menggunakan kriptografi *Blowfish* dan autentikasi HMAC
5. Penelitian ini tidak berfokus pada keamanan *web server.*

6. Penelitian ini hanya menggunakan jaringan lokal seperti pada pengujian serangan yang dimana perangkat terhubung ke satu jaringan yang sama.
7. Perangkat keras yang digunakan adalah ESP32, sensor *soil moisture,* pompa air dan relay.
8. Perangkat lunak yang digunakan untuk melakukan pemrograman sistem adalah Arduino IDE dan Visual Studio Code.
9. Penyimpanan data menggunakan MySQL.

## 1.4 Tujuan Penelitian

Berdasarkan rumusan permasalahan, penelitian ini memiliki tujuan sebagai berikut:

1. Menganalisis keamanan transmisi data kelembaban tanah setelah diimplementasikannya algoritma *Blowfish* dan autentikasi HMAC, khususnya dalam hal ketahanan sistem terhadap upaya serangan *Man-in-the-Middle* (MITM).
2. Menganalisis waktu pemrosesan data sebelum dan setelah di implementasikannya algoritma *Blowfish* serta Algoritma HMAC pada perangkat mikrokontroler IoT dengan keterbatasan sumber daya.

## 1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Menyediakan keamanan berupa kriptografi *Blowfish* dan autentikasi HMAC untuk menjaga kerahasiaan data kelembaban tanah yang dikirimkan melalui jaringan.
2. Memberikan model keamanan yang dapat diterapkan ke perangkat IoT.
3. Mendorong penerapan kriptografi sebagai keamanan data terutama pada perangkat IoT.
4. Menjadi referensi penelitian berikutnya tentang penggunaan kriptografi pada IoT.

## 1.6 Sistematika Penulisan

Dalam penelitian ini, penulisan dibagi menjadi enam bab sehingga permasalahan yang dibahas dapat disesuaikan secara urut dan sistematis. Adapun pembagian bab dalam penelitian ini sebagai berikut

BAB 1 PENDAHULUAN

Bab pendahuluan adalah bagian yang menjelaskan dasar dan gambaran awal tentang penelitian yang akan dilakukan. Pada bab ini akan dibahas berbagai hal yang menjadi dasar dari penelitian, seperti latar belakang yang menjelaskan tentang alasan mengapa penelitian dilakukan, rumusan masalah yang menjelaskan permasalahan utama yang akan diteliti dan tujuan penelitian yang menunjukan apa yang ingin dicapai melalui penelitian tersebut. Ruang lingkup penelitian dijelaskan dalam batasan masalah agar penelitian tidak menyimpang ke lingkup yang tidak relevan dengan topik penelitian. Manfaat dari penelitian juga dijelaskan dalam bab ini, yang menunjukkan manfaat yang diharapkan dari hasil penelitian bagi pihak praktisi dan bidang ilmu pengetahuan. Sistematika penulisan dijelaskan untuk memberi gambaran tentang struktur bab-bab yang akan dibahas dalam penelitian ini.

BAB 2 LANDASAN TEORI

Bab landasan teori membahas terkait dasar teori yang akan digunakan selama penelitian berlangsung. Adapun landasan teori pada bab ini berupa algoritma Blowfish, Autentikasi HMAC, Wireshark, Serangan MiTM, ESP32, Modul Soil Moisture V1.2, Driver Relay, Arduino IDE, PHP dan MySQL. Dasar teori ini diperoleh dari artikel penelitian yang dapat mendukung pembahasan pada penelitian ini.

BAB 3 METODE PENELITIAN

Bab metode penelitian menjelaskan secara rinci tahapan-tahapan yang dilakukan dalam pelaksanaan penelitian untuk menjawab rumusan masalah yang telah ditetapkan. Metode penelitian digunakan sebagai pedoman agar proses penelitian dapat dilakukan secara sistematis, terstruktur, dan terarah sehingga tujuan penelitian dapat tercapai dengan baik. Tahapan yang dibahas dalam bab ini

meliputi studi literatur, analisis kebutuhan, perancangan sistem, implementasi, pengujian sistem, pengumpulan data, serta kesimpulan dan saran.

BAB 4 PERANCANGAN

Bab perancangan berisi tentang arsitektur sistem, perangkat keras, perangkaat lunak basis data dan antarmuka *website*. Perancangan arsitektur sistem dimulai dari proses pembacaan modul, implementasi algoritma *Blowfish* dan HMAC, pengiriman data dan data diterima lalu dieksekusi sebagai tindakan. Pada perancangan perangkat keras, perangkat keras terdiri dari 2 buah ESP32, modul soil moisture, modul relay dan pompa air. Sedangkan untuk perangkat lunak terdiri dari perancangan antarmuka *website*, perancangan database dan algoritma *Blowfish* dan HMAC yang akan diimplementasikan ke perangkat keras sebagai keamanan pengiriman data.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Pada bab implementasi, pengujian dan pembahasan akan membahas terakit analisis dan implementasi sistem yang sudah dirancang pada bab sebelumnya. Tahapan ini terdiri dari implementasi perangkat keras, implementasi perangkat lunak, pengujian dan pembahasan. Implementasi dilakukan dengan menerapkan rancangan dalam perangkat keras dan perangkat lunak secara nyata. Pengujian dilakukan dengan menguji hasil implementasi yang telah diterapkan baik ke perangkat keras maupun perangkat lunak. Setelah melewati pengujian, hasil akan dianalisis dan dibahas berdasarkan data yang didapat dari pengujian.

BAB 6 PENUTUP

Pada bab ini merupakan kesimpulan dari hasil penelitian yang telah dilakukan. Kesimpulan akan meliputi penjelasan bagaimana hasil dari penelitian yang telah dilakukan secara ringkas dan objektif. Bab ini juga terdapat saran yang memiliki tujuan sebagai panduan pengembangan dan referensi bagi penelitian selanjutnya.