IMPLEMENTASI PROTOKOL HTTPS DENGAN KRIPTOGRAFI *ELLIPTIC-CURVE* PADA PROSES PENGIRIMAN DATA KELEMBABAN TANAH DENGAN IoT

SKRIPSI

Disusun oleh:
Youngky
H1051191102

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

2024

IMPLEMENTASI PROTOKOL HTTPS DENGAN KRIPTOGRAFI *ELLIPTIC-CURVE* PADA PROSES PENGIRIMAN DATA KELEMBABAN TANAH DENGAN IoT

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer

Disusun oleh:
Youngky
H1051191102

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

2024

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Implementasi Protokol HTTPS Dengan Kriptografi *Elliptic-Curve* Pada Proses Pengiriman Data Kelembaban Tanah Dengan IoT
Nama Mahasiswa	: Youngky
NIM	: H1051191102
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 24 Januari 2025
SK Pembimbing	: No. 2713/UN22.8/TD.06/2024 / 10 / September
SK Penguji	: No. 216/UN22.8/TD.06/2025 / 23 / Januari

Dosen Pembimbing

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

Dosen Penguji

Ketua Penguji	Anggota Penguji
Ikhwan Ruslianto, S.Kom., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
198607012014041001	199007232023211017

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

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusnizal, S.Si., M.Si.
197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan dibawah ini:

Nama	: Youngky
NIM	: H1051191102
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



Youngky

H1051191102

Implementasi Protokol HTTPS Dengan Kriptografi *Elliptic-Curve* Pada Proses Pengiriman Data Kelembaban Tanah Dengan IoT

ABSTRAK

Dalam sistem penyiraman tanaman otomatis, data sensor kelembaban tanah memegang peran penting misalnya untuk menentukan kapan tanaman memerlukan air atau tidak. Permasalahan yang muncul dengan penerapan IoT adalah aspek keamanan yang sering terlewatkan. Setiap perangkat IoT seharusnya mengantisipasi bahwa perangkat tersebut mungkin akan diserang selama masa pemakaiannya. Penelitian yang akan dilaksanakan berfokus pada penerapan protokol HTTPS dengan algoritma enkripsi *Elliptic-Curve Cryptography* (ECC), dalam proses transmisi data kelembaban tanah dengan perangkat IoT melalui internet. Tujuan dari penelitian ini adalah untuk mengamankan pengiriman data kelembaban tanah selama proses transmisi dari perangkat IoT menuju *web server*. Hal yang perlu diperhatikan dalam aspek keamanan pada proses transmisi data adalah bentuk data yang dikirimkan harus berupa *ciphertext*. *Ciphertext* sendiri merupakan bentuk data yang tidak dapat dibaca baik oleh manusia ataupun mesin, sehingga tidak dapat diperoleh informasi dari data tersebut kecuali data tersebut berhasil di dekripsi. Dengan menggunakan pendekatan *bruteforce*, hal ini akan menghabiskan waktu yang sangat lama. Dari pengujian yang dilaksanakan, dapat diperoleh hasil bahwa data kelembaban tanah yang dikirimkan ketika dibandingkan dengan data yang disimpan pada *server*, telah bernilai sama. Kemudian data dikirimkan dalam bentuk *ciphertext* sehingga informasi berupa tingkat kelembaban tanah dari data yang dikirimkan tidak dapat diperoleh ataupun diubah.

Kata kunci: HTTPS, Kelembaban Tanah, Penyiraman Otomatis, *Internet of Things*, *Elliptic-Curve Cryptography*, *Ciphertext*.

HTTPS Protocol With Elliptic-Curve Algorithm Implementation on Soil Moisture Transmission Process Using IoT

ABSTRACT

Soil moisture data is essential on automatic plant watering systems, since it can help determine when a plant needs water or not. The security aspect of IoT implementation is often overlooked. Every IoT device should be prepared for potential cyber attacks throughout its lifespan. The main subject of this study is to implement HTTPS protocol with Elliptic-Curve Algorithm during the soil moisture transmission process using IoT over the internet. Securing the transmission of soil moisture data from IoT to the web server is the main goal of this study. Making sure the data is being transferred in the form of ciphertext is crucial on data transmission security. Ciphertext is a form of data that looks gibberish unless the data can be decrypted since neither humans nor computers can read the information. Brute-Force is one of many ways to crack the ciphertext, but this process was very time consuming. According to the test results, the soil moisture data that was sent by the IoT device and kept on the server was accurate. Additionally the data was sent in the form of ciphertext, which made sure that the information about the soil moisture level could not be obtained nor altered.

Keywords: *Internet of Things, Elliptic-Curve Cryptography, HTTPS, Ciphertext, Soil Moisture, Automatic Watering.*

PRAKATA

Puji syukur kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga penulisan karya ilmiah dengan judul "Implementasi Protokol HTTPS Dengan Kriptografi Elliptic-Curve Pada Proses Pengiriman Data Kelembaban Tanah Dengan IoT" dapat diselesaikan. Karya ilmiah ini disusun untuk memenuhi salah satu persyaratan untuk kelulusan gelar kesarjanaan pada program studi Rekayasa Sistem Komputer Jenjang Pendidikan Strata-1 di Universitas Tanjungpura.

Karya Ilmiah ini ditulis oleh mahasiswa dari Universitas Tanjungpura dengan program studi Rekayasa Sistem Komputer. Penulis karya ilmiah ini telah mengikuti setiap mata kuliah yang diwajibkan di Universitas Tanjungpura dari tahun 2019 sehingga dapat menyusun karya ilmiah ini dengan baik.

Pada kesempatan ini, atas segala bantuan, dukungan dan bimbingan yang diberikan dari berbagai pihak, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Tedy Rismawan, S.Kom., M.Cs., selaku Ketua Jurusan Program Studi Rekayasa Sistem Komputer.
3. Bapak Syamsul Bahri, S.Kom., M.Cs., selaku Dosen Pembimbing Utama yang telah memberikan bimbingan serta waktu dan tenaga dalam penyusunan skripsi ini.
4. Bapak Kasliono, S.Mat., M.Cs., selaku Dosen Pembimbing Pendamping yang telah memberikan bimbingan serta waktu dan tenaga dalam penyusunan skripsi ini.
5. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., selaku Dosen Penguji Pertama yang telah memberikan saran dan masukan dalam penulisan skripsi ini.

6. Bapak Hafiz Muhardi, S.T., M.Kom., selaku Dosen Penguji Kedua yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
7. Ibu Dwi Marisa Midyanti, S.T., M.Cs., selaku Dosen Pembimbing Akademik yang telah memberikan saran dan dukungan dari awal perkuliahan hingga saat ini.
8. Bapak dan Ibu Dosen serta Staf Administrasi Jurusan/Program Studi Rekayasa Sistem Komputer yang telah memberikan arahan dari awal perkuliahan sampai saat ini.
9. Kepada kedua Orang Tua beserta keluarga yang selalu mendoakan, memberikan dukungan sehingga dapat menyelesaikan tugas akhir.
10. Pihak-pihak yang tidak dapat disebutkan, yang turut membantu dalam penyusunan skripsi ini.

Akhir kata, penulis karya ilmiah ini juga mengucapkan terima kasih kepada semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu penyusunan karya ilmiah ini. Penulis menyadari bahwa penulisan karya ilmiah ini masih terdapat kekurangan yang diakibatkan oleh keterbatasan pengetahuan dan pengalaman. Oleh karena itu penulis mengharapkan adanya kritik dan saran yang bersifat membangun. Semoga karya ilmiah ini dapat bermanfaat dan memberikan semangat serta motivasi agar dapat menyusun laporan untuk kepentingan serta perkembangan ilmu pengetahuan bagi pembaca.

Pontianak, Desember 2024

Youngky

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
ABSTRAK iv
ABSTRACT v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
DAFTAR KODE PROGRAM xiv
DAFTAR LAMPIRAN xv

BAB 1 PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 3
1.3. Batasan Masalah 3
1.4. Tujuan Penelitian 4
1.5. Manfaat Penelitian 4
1.6. Sistematika Penulisan 5

BAB 2 LANDASAN TEORI 7
2.1. Perbandingan Dengan Penelitian Terdahulu 7
2.2. HTTPS 8
2.3. REST API 13
2.4. *Let's Encrypt* 14
2.5. *Certbot* 15
2.6. *Elliptic-Curve Cryptography* 15
2.7. Pengujian *White Box* 19
2.8. *Docker* 20
2.9. ESP32 20
2.10. *Capacitive Soil Moisture Sensor* 21

BAB 3 METODE PENELITIAN 22
3.1. Studi Literatur 23
3.2. Analisis Kebutuhan 23
3.2.1. Kebutuhan Perangkat Keras 23
3.2.2. Kebutuhan Perangkat Lunak 24

3.3. Perancangan Sistem..... 24
3.3.1. Perancangan Perangkat Keras..... 24
3.3.2. Perancangan Perangkat Lunak..... 25
3.4. Implementasi Sistem..... 25
3.4.1. Implementasi Perangkat Keras..... 25
3.4.2. Implementasi Perangkat Lunak..... 25
3.5. Pengujian Sistem..... 26
3.6. Pengumpulan Data..... 26
3.7. Kesimpulan dan Saran..... 27

BAB 4 PERANCANGAN..... 28
4.1. Deskripsi Sistem..... 28
4.2. Perancangan Arsitektur Sistem..... 28
4.2.1. Proses Enkripsi Data pada ESP32..... 30
4.2.2. Pengiriman Data oleh ESP32..... 31
4.2.3. Pengambilan Data oleh ESP32..... 32
4.2.4. Pengiriman Data oleh Pengguna..... 33
4.2.5. Pengambilan Data oleh Pengguna..... 34
4.3. Perancangan perangkat Keras..... 34
4.4. Perancangan Perangkat Lunak..... 35
4.4.1. Perancangan pada ESP32..... 36
4.4.2. Perancangan pada *Web Server*..... 36
4.5. Perancangan Basis Data..... 37
4.6. Perancangan Antarmuka..... 38
4.7. Perancangan Pengujian *Black Box*..... 40
4.8. Perancangan Pengujian *White Box*..... 40

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN..... 41
5.1. Implementasi Perangkat Keras..... 41
5.2. Implementasi Perangkat Lunak..... 42
5.2.1. Implementasi pada ESP32..... 42
5.2.2. Implementasi pada *Web Server*..... 44
5.3. Implementasi Kode Program..... 49
5.3.1. *Void Loop* pada ESP32..... 49
5.3.2. *Send Data* pada ESP32..... 50
5.3.3. *Get Data* pada ESP32..... 50
5.3.4. Jenis Algoritma yang Didukung *Certbot*..... 51
5.4. Perhitungan Dengan Metode *Elliptic-Curve Cryptography*..... 52

5.5. Pengujian Sistem.....54
5.5.1. Pengujian *Black Box*..... 54
5.5.2. Pengujian *White Box*..... 57
5.6. Analisis dan Pembahasan.....67

BAB 6 PENUTUP.....68
6.1. Kesimpulan..... 68
6.2. Saran.....68

DAFTAR PUSTAKA.....69
LAMPIRAN.....73

DAFTAR GAMBAR

Gambar 2.1. HTTP dan HTTPS....9
Gambar 2.2. Proses TLS *Handshake* 1.2....10
Gambar 2.3. Proses TLS *Handshake* 1.3....12
Gambar 2.4. TLS pada model OSI....13
Gambar 2.5. *Elliptic-Curve*....15
Gambar 2.6. ESP32....21
Gambar 2.7. *Capacitive Soil Moisture Sensor* V2.0....21
Gambar 3.1. Diagram Alir Penelitian....22
Gambar 4.1. Perancangan Sistem....29
Gambar 4.2. Proses Enkripsi Data pada ESP32....30
Gambar 4.3. *Flowchart* Pengiriman Data oleh ESP32....31
Gambar 4.4. *Flowchart* Pengambilan Data oleh ESP32....32
Gambar 4.5. *Flowchart* Mengubah Data Konfigurasi oleh Pengguna....33
Gambar 4.6. *Flowchart* Pengambilan Data oleh Pengguna....34
Gambar 4.7. *Wiring Diagram* Perangkat Keras....35
Gambar 4.8. *Flowchart* Validasi JWT pada *Web Server*....37
Gambar 4.9. ERD Basis Data Sistem....38
Gambar 4.10. Antarmuka Halaman *Login*....39
Gambar 4.11. Antarmuka Halaman *Dashboard*....39
Gambar 5.1. Implementasi Perangkat Keras....41
Gambar 5.2. Sensor pada Tanah....42
Gambar 5.3. Langkah Setup pada ESP32....43
Gambar 5.4. Pembacaan Data Kelembaban Tanah....43
Gambar 5.5. Pengiriman Data oleh ESP32....44
Gambar 5.6. Pengambilan Data Persentase oleh ESP32....44
Gambar 5.7. Arsitektur pada *Backend*....45
Gambar 5.8. Daftar API pada *Backend*....46
Gambar 5.9. Tampilan Halaman *Home*....46
Gambar 5.10. Tampilan Halaman *Login*....47
Gambar 5.11. Tampilan Halaman *Dashboard*....47
Gambar 5.12. Alur Kerja *Web Server*....48
Gambar 5.13. Tampilan *Web Server*....48
Gambar 5.14. Data pada ESP32 Tanpa Enkripsi....58
Gambar 5.15. Data dari ESP32 pada Database Tanpa Enkripsi....58
Gambar 5.16. Data pada *Wireshark* Tanpa Enkripsi....59
Gambar 5.17. Data pada ESP32 Dengan Enkripsi....59
Gambar 5.18. Data dari ESP32 pada Database Dengan Enkripsi....60

Gambar 5.19. Data pada *Wireshark* Dengan Enkripsi.....60
Gambar 5.20. Hasil *Capture Pktmon* pada Transmisi Tanpa Enkripsi.....61
Gambar 5.21. Hasil *Capture Pktmon* pada Transmisi Dengan Enkripsi.....62
Gambar 5.22. Sertifikat pada *Web Server*..... 64
Gambar 5.23. Implementasi Sertifikat *Web Server* pada ESP32.....64
Gambar 5.24. Pengujian Sertifikat yang Tidak Valid.....65

DAFTAR TABEL

Tabel 2.1. Persamaan dan Perbedaan Penelitian Terdahulu..... 7
Tabel 2.2. NIST *Recommended Security Strength*..... 16
Tabel 4.1. Hubungan *Pin* Pada Perangkat Keras.....35
Tabel 5.1. Hasil Pengujian API pada *Web Server*..... 55
Tabel 5.2. Hasil Pengujian Aplikasi *Frontend*..... 56
Tabel 5.3. Hasil Pengujian Sistem Enkripsi Secara Keseluruhan..... 62
Tabel 5.4. Hasil Pengujian Validasi Sertifikat *Web Server*.....65

DAFTAR KODE PROGRAM

Kode Program 5.1. *Void Loop* pada ESP32.....49
Kode Program 5.2. *Send Data* pada ESP32.....50
Kode Program 5.3. *Get Data* pada ESP32.....51
Kode Program 5.4. CLI *helper* pada *Certbot*.....51

DAFTAR LAMPIRAN

Lampiran 1. Hasil *Sniffing*.....73

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Seiring dengan perkembangan mikrokontroler dan internet yang semakin pesat, *Internet of Things* (IoT) menjadi banyak diterapkan dalam kehidupan sehari-hari manusia. IoT merupakan sebuah perangkat yang memanfaatkan mikrokontroler untuk melakukan otomatisasi dengan mengambil, mengirim dan mengolah data melalui internet. Perkembangan IoT ini mengakibatkan luasnya penerapan IoT di masa sekarang, hal ini dikarenakan IoT dianggap mampu membantu manusia menyelesaikan masalah dengan solusi otomatisasi yang ditawarkan.

Sistem penyiraman tanaman otomatis merupakan salah satu hasil dari penerapan IoT pada bidang pertanian. Dalam sistem penyiraman tanaman otomatis, data sensor kelembaban tanah memegang peran penting misalnya untuk menentukan kapan tanaman memerlukan air atau tidak, sehingga tanaman dapat disiram secara otomatis dan tidak layu karena kelebihan air ataupun kekurangan air. Selain itu, data kelembaban tanah juga digunakan pada sistem monitoring tanaman. Informasi tingkat kelembaban tanah pada tanaman dapat dipantau secara *online*. Oleh karena itu data kelembaban tanah merupakan data yang bersifat sensitif dalam sistem penyiraman tanaman otomatis.

Permasalahan yang muncul dengan penerapan IoT adalah aspek keamanan yang sering terlewatkan. Perangkat IoT yang terjual pada umumnya tidak mampu menawarkan solusi keamanan yang baik. Hal ini dapat dilihat dari perangkat smart home seperti lampu, TV dan lainnya (Kleinhans, 2017). Hal ini mengakibatkan perangkat IoT sering dianggap sebagai perangkat yang tidak aman. Salah satu hal penting yang membuat IoT menjadi teknologi yang rentan terhadap serangan *cyber* adalah kurangnya mekanisme keamanan yang disediakan (Vahdati *et al*., 2019). Setiap perangkat IoT seharusnya mengantisipasi bahwa perangkat tersebut mungkin akan diserang selama masa pemakaiannya.

Dalam proses transmisi data, terdapat berbagai macam protokol yang dapat digunakan, salah satunya *Hypertext Transfer Protocol Secure* (HTTPS).

HTTPS merupakan pengembangan dari HTTP, protokol ini menyediakan keamanan kriptografi, dengan membawa pesan HTTP melalui *Transport Layer Security* (TLS), daripada langsung (tanpa kriptografi) melalui *Transmission Control Protocol* (TCP) (Felt *et al*., 2017). Selain digunakan untuk mengamankan jalur komunikasi antara *client* dengan *web server*, protokol ini juga dimaksudkan untuk memastikan bahwa *client* dapat mempercayai bahwa *web server* yang sedang diakses adalah tujuan yang dimaksud oleh *client*, dikarenakan *web server* yang sedang diakses, telah terautentikasi dengan sertifikat digital yang valid (Cooper *et al*., 2008).

Salah satu penelitian dengan kasus serupa pernah dilaksanakan oleh Ramadan *et al*. (2021), dengan judul "Implementasi Kriptografi AES untuk Keamanan Pengiriman Data *Internet of Things* Menggunakan *Web Service* REST pada NodeMCU". Penelitian tersebut menerapkan algoritma AES (*Advanced Encryption Standard*) dalam melakukan enkripsi terhadap data suhu dan kelembaban udara. Data hasil enkripsi berupa *ciphertext*, kemudian di dekripsi kembali menjadi *plaintext* pada *web server*.

Penelitian lainnya yang menerapkan algoritma *Elliptic-Curve Cryptography* (ECC) pernah dilakukan oleh Khan *et al*. (2020), dengan judul penelitian "*A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data*". Penelitian tersebut menerapkan *Substitution-Caesar*, dan *Improved* ECC dalam melakukan enkripsi data pada perangkat IoT di bidang medis, dimana data tersebut berupa informasi *biometric* pasien pada sebuah rumah sakit. Penelitian tersebut menawarkan sebuah metode terapan dari ECC yang dikembangkan sendiri yang disebut sebagai *Improved* ECC.

Adapun terdapat penelitian yang melakukan perbandingan terhadap algoritma kriptografi RSA dan ECC, yang dilakukan oleh Vahdati *et al*. (2019), dengan judul penelitian "*Comparison of ECC and RSA algorithms in IoT devices*". Penelitian tersebut berfokus pada perbandingan RSA dan ECC, dengan mengumpulkan data seperti waktu enkripsi, waktu dekripsi, ukuran *key* yang digunakan, penggunaan daya dan lainnya khususnya pada perangkat IoT. Hasil dari penelitian ini menunjukkan bahwa algoritma ECC lebih unggul dibandingkan

RSA dalam hal efisiensi komputasi khususnya dalam kasus penggunaan pada perangkat IoT.

Penelitian yang akan dilaksanakan berfokus pada penerapan protokol HTTPS dengan algoritma kriptografi *Elliptic-Curve* (ECC), dalam proses transmisi data perangkat IoT penyiraman tanaman otomatis melalui internet. Algoritma ini memungkinkan dua pihak untuk bertukar *public key* dengan ukuran *key* yang kecil, sehingga cocok untuk kondisi lingkungan dengan kekuatan komputasi yang terbatas (Mahto & Yadav, 2017). Pada penelitian ini, data kelembaban tanah akan dienkripsi sebelum dikirimkan oleh ESP32 melalui internet ke *web server* yang menerapkan standar REST API. Data tersebut kemudian akan disimpan pada *database* MySQL untuk kebutuhan monitoring. Data pada *database* dapat diakses dengan *dashboard* pada aplikasi berbasis *web* yang dibuat dengan bahasa pemrograman *JavaScript*. Selain itu *dashboard* juga dapat digunakan untuk mengubah pengaturan otomatisasi penyiraman pada perangkat ESP32.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, dapat dirumuskan rincian permasalahan pada penelitian ini sebagai berikut:

1. Bagaimana cara memastikan data kelembaban tanah, ditransmisikan dari perangkat IoT ke *web server* melalui protokol HTTPS yang menerapkan algoritma kriptografi ECC telah terenkripsi?
2. Bagaimana protokol HTTPS yang menerapkan algoritma kriptografi ECC dapat melindungi perangkat IoT dari akses tidak sah?

1.3. Batasan Masalah

Batasan permasalahan dalam penelitian yang dilakukan dapat dijabarkan sebagai berikut:

1. Sistem yang dibuat akan berada pada tahap *prototype*, yang mensimulasikan penggunaan sebenarnya.

2. Penelitian ini berfokus pada penerapan protokol HTTPS dengan algoritma kriptografi ECC, pada proses transmisi data antara perangkat IoT dengan *web server*.
3. Penelitian ini tidak bertujuan untuk menguji tingkat keamanan, ataupun mencoba untuk meretas sistem keamanan pada kriptografi ECC.
4. Penelitian ini hanya berfokus pada mengamankan transmisi data kelembaban tanah tanpa memperhatikan parameter lain seperti kelembaban udara.
5. Penelitian ini menerapkan bahasa pemrograman *JavaScript* pada pembuatan *dashboard* sederhana.
6. Penelitian ini berfokus pada keamanan pada proses transmisi, sehingga hal seperti keamanan pada *database* ataupun *web server* tidak akan dibahas dalam penelitian ini.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini diharapkan dapat menjawab permasalahan yang telah dirumuskan, dengan rincian tujuan sebagai berikut:

1. Menerapkan protokol HTTPS dengan algoritma kriptografi ECC, untuk mengamankan proses transmisi data kelembaban tanah dari perangkat IoT penyiraman tanaman otomatis ke *web server*.
2. Menerapkan sistem keamanan dimana perangkat IoT akan melakukan validasi terhadap *web server* yang dihubungi untuk mencegah akses yang tidak sah ke perangkat IoT penyiraman tanaman otomatis.
3. Melakukan enkripsi terhadap data yang dikirimkan oleh perangkat IoT penyiraman tanaman otomatis ke *web server* untuk menjaga integritas data kelembaban tanah.

1.5. Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat mencapai manfaat seperti pada penjabaran berikut:

1. Mengamankan data kelembaban tanah dari perangkat IoT untuk menjaga integritas data, sehingga data yang diperoleh dari perangkat IoT dapat

dipercaya kebenarannya untuk memantau kondisi dari tanaman yang dibudidayakan.

2. Memungkinkan perangkat IoT untuk berkomunikasi dengan *web server* secara aman melalui protokol HTTPS yang menerapkan algoritma kriptografi ECC.
3. Mengendalikan perangkat IoT dengan integrasi *web server* untuk memastikan keamanan pada perangkat IoT dari akses yang tidak sah.
4. Memberikan alternatif solusi keamanan terhadap implementasi dengan perangkat IoT.

1.6. Sistematika Penulisan

Pembahasan pada penelitian ini akan dibagi menjadi beberapa bagian sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan berisi latar belakang yang menjadi alasan kenapa penelitian ini dilaksanakan. Kemudian untuk memperkuat alasan tersebut bab pendahuluan juga akan berisi rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian. Selain itu bab pendahuluan juga akan berisi sistematika penulisan yang menjelaskan pembagian pembahasan pada setiap bab.

BAB II LANDASAN TEORI

Bab landasan teori berisi pembahasan terkait dengan dasar teori yang mendukung penelitian ini. Pembahasan ini meliputi metode yang akan digunakan yaitu HTTPS, *Elliptic-Curve Cryptography* dan REST API, *tools* berupa perangkat lunak yang akan digunakan yaitu *Let's Encrypt* dan *Certbot* kemudian perangkat keras yang digunakan yaitu *ESP32* dan *Capacitive Soil Moisture Sensor*.

BAB III METODOLOGI PENELITIAN

Bab metodologi penelitian berisi pembahasan terkait bagaimana prosedur penelitian ini dilaksanakan sehingga penelitian ini dapat berjalan secara

sistematis. Adapun bagian yang terdapat pada bab ini adalah studi literatur, metode pengumpulan data, analisis kebutuhan perangkat lunak maupun perangkat keras, perancangan sistem, implementasi dan pengujian sistem. Adapun bab ini juga berisi integrasi terkait sistem yang akan dibangun.

BAB IV PERANCANGAN

Bab perancangan berisi pembahasan terkait bagaimana sistem dirancang baik itu dari segi perangkat lunak dan perangkat keras. Selain itu bab ini juga berisi pembahasan terkait perancangan bagaimana proses pengujian dengan metode *black box* dan *white box*.

BAB V IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian dan pembahasan berisi pembahasan terkait implementasi dan pengujian terhadap sistem yang sudah dirancang kemudian analisis dan pembahasan mengenai bagaimana hasil dari implementasi dan pengujian dari sistem yang sudah dibuat.

BAB VI PENUTUP

Bab penutup berisi pembahasan terkait kesimpulan dari penelitian yang telah dilaksanakan beserta saran terkait pengembangan selanjutnya yang dapat dilakukan dari penelitian ini.