PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS*

(Skripsi)

Oleh

DIPAMADYA KALINGGA

NPM 1715031059

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2023

ABSTRAK

PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS*

Oleh

DIPAMADYA KALINGGA

Internet of Things (IoT) adalah struktur dimana objek atau orang diberikan identitas eksklusif dan kemampuan untuk berbagi data melalui jaringan (internet) tanpa memerlukan interaksi langsung antara manusia dengan manusia atau interaksi manusia ke komputer. Salah satu tantangan yang harus diatasi untuk mendorong meluasnya implementasi IoT adalah faktor keamanan. Salah satu metode untuk mengamankan Jaringa IoT yaitu dengan *metode Two Factor Authentication (2FA). Metode 2FA yaitu suatu metode login yang memerlukan dua faktor autentikasi. Two Factor Authentication* itu menggabungkan dua metode autentikasi yaitu *Something You Know* (*password* statis atau *password* milik pengguna pribadi) dengan *Something You Have* (token atau kode acak yang berubah-ubah). Pada penelitian ini akan dibangun suatu sistem keamanan jaringan IoT dua autentikasi yaitu berupa *password* dan OTP (*One time password)* yang harus di*input* oleh *client* atau perangkat IoT untuk dapat mengirim data sensor suhu dan kelembapan ke dalam *server*. Hasil pengujian sistem menunjukkan sistem yang memenuhi parameter keamanan jaringan data *Confidentiality Integrity A*vailabili*ty* (CIA) dimana untuk parameter *confidentiality*, OTP berfungsi sebagai *key* untuk mengamankan sistem dari *client* yang tidak berhak mengakses *server*, dan juga dilakukan perbandingan proses enkripsi data pada saat proses pengiriman data dengan layanan IoT *thingspeak.* Pada pengujian parameter *integrity*, tidak terdapat perubahan besar data pada saat pengiriman dan saat data sensor diterima di *database* dimana besar data yang dikirim dan diterima konstan yaitu 88 bytes. Pengujian parameter *availability* dilakukan dengan pengambilan data selama 24 jam, dimana selama 24 jam tersebut ESP8266 dapat mengirim data suhu dan kelembapan secara terus menerus dengan interval waktu 5 menit. Data yang diterima dari ESP8266 berjumlah 288 buah data dengan nilai berupa suhu dan kelembapan dan tidak ada satupun data yang *error*. Nilai suhu memiliki nilai rata-rata 25,78 dimana nilai tertinggi adalah 30,7 dan nilai terendah adalah 24,1. Nilai kelembapan memiliki nilai rata-rata 85,14 dimana nilai tertinggi adalah 95 dan nilai terendah adalah 60.

Kata Kunci: *Internet of Things, Security IoT, Two Factor Authentication, One Time Password, Confidentiality Integrity Availability.*

ABSTRACT

DESIGN OF TWO FACTOR AUTHENTICATION ALGORITHM FOR INTERNET OF THINGS SECURITY

By

DIPAMADYA KALINGGA

The Internet of Things (IoT) *is a structure where objects or people are given exclusive identities and the ability to share data over a network* (internet) *without requiring direct human-to-human interaction or human-to-computer interaction. One of the challenges that must be overcome to encourage the widespread implementation of IoT is the security factor. One method for securing the IoT Network is the Two Factor Authentication* (2FA) *method. The 2FA method is a login method that requires two authentication factors. Two Factor Authentication combines two authentication methods, namely Something You Know (a static password or password belonging to a personal user) with Something You Have* (a random token or code that changes). *In this research, a two-authentication IoT network security system will be built, namely in the form of a password and OTP* (One time password) *which must be input by the client or IoT device to be able to send temperature and humidity sensor data to the server. The results of system testing show that the system meets the parameters of data network security Confidentiality Integrity Availability* (CIA) *where for the confidentiality parameter, OTP functions as a key to secure the system from clients who are not entitled to access the server, and also compares the data encryption process during the data transmission process with thingspeak IoT services. In testing the integrity parameter, there is no change in data size when sending and when sensor data is received in the database where the amount of data sent and received is constant, namely 88 bytes. Availability parameter testing is carried out by collecting data for 24 hours, during which 24 hours the ESP8266 can send temperature and humidity data continuously at 5 minute intervals. The data received from the ESP8266 totals 288 pieces of data with values in the form of temperature and humidity and none of the data has an error. The temperature value has an average value of 25.78 where the highest value is 30.7 and the lowest value is 24.1. The humidity value has an average value of 85.14 where the highest value is 95 and the lowest value is 60.*

Key Words: Internet of Things, Security IoT, Two Factor Authentication, One Time Password , Confidentiality Integrity Availability.

PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS*

Oleh

DIPAMADYA KALINGGA

Skripsi

Sebagai Salah Satu Syarat Untuk Mencapai Gelar

SARJANA TEKNIK

Pada

Program Studi Teknik Elektro

Jurusan Teknik Elektro

Fakultas Teknik Universitas Lampung

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2023

Judul Skripsi	: **PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS***
Nama Mahasiswa	: Dipamadya Kalingga
Nomor Pokok Mahasiswa	: 1715031059
Jurusan	: Teknik Elektro
Fakultas	: Teknik

MENYETUJUI

1. Komisi Pembimbing

Dr. Ing. Melvi, S.T., M.T.	**Aryanto, S.T., M.T.**
NIP 19730118 200003 2 001	NIP 19900621 201903 1 001

2. Mengetahui

Ketua Jurusan Teknik Elektro	Ketua Program Studi Teknik Elektro
Herlinawati, S.T., M.T.	**Dr. Eng. Nining Purwasih, S.T., M.T.**
NIP 19710314 199903 2 001	NIP 19740422 200012 2 001

MENGESAHKAN

1. Tim Penguji

Ketua : **Dr. Ing. Melvi, S.T., M.T.** .....

Sekretaris : **Aryanto, S.T., M.T.** .....

Penguji
Bukan Pembimbing : **Dr. Ing. Ardian Ulvan, S.T., M.Sc.** .....

2. Dekan Fakultas Teknik

Dr. Eng. Ir. Helmy Fitriawan, S.T., M.Sc.
NIP 19750928 200112 1 002

Tanggal Lulus Ujian Skripsi : **01 Februari 2023**

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **"PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS*"** merupakan hasil karya sendiri dan bukan hasil karya orang lain. Semua hasil yang tertuang dalam skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti skripsi ini merupakan salinan atau dibuat oleh orang lain. Maka saya bersedia menerima sanksi sesuai dengan ketentuan akademik yang berlaku.

Bandar Lampung, 08 Februari 2023

Dipamadya Kalingga

NPM. 1715031059

RIWAYAT HIDUP

Penulis dilahirkan di Bekasi pada tanggal 05 April 1999. Penulis merupakan anak pertama dari tiga bersaudara dari pasangan Bapak Timo Tinarko dan Ibu Irene Ratu Mustika yang diberi nama Dipamadya Kalingga.

Mengenai riwayat pendidikan, penulis lulus Sekolah Dasar (SD) di Mutiara 17 Agustus 2 pada tahun 2011, lulus Sekolah Menengah Pertama (SMP) di SMPN 05 Kota Bekasi pada tahun 2014, lulus Sekolah Menengah Atas (SMA) di SMAN 04 Kota Bekasi pada tahun 2017, dan pada tahun 2017 melalui jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN) diterima di Jurusan Teknik Elektro Universitas Lampung (UNILA).

Penulis aktif di Organisasi Himpunan Mahasiswa Teknik Elektro (HIMATRO) Fakultas Teknik sebagai Anggota Divisi Kewirausahaan Departemen Sosial dan Kewirausahaan pada periode 2017-2019 selama menjadi mahasiswa. Selain mengikuti organisasi, penulis juga berkesempatan menjadi Asisten Laboratorium Pengukuran Besaran Listrik dengan beberapa praktikum yaitu, Praktikum Fisika Dasar, Praktikum Instrumen dan Pengukuran, dan Praktikum Rangkaian Listrik. Selain itu itu penulis juga pernah menjadi Asisten Laboratorium Teknik Telekomunikasi dan menjadi asisten beberapa praktikum yaitu, Praktikum Dasar Telekomunikasi, Praktikum Sistem Komunikasi, dan Praktikum Jaringan Telekomunikasi. Penulis juga pernah menjadi *Assistant Chair-room* pada *International Conference on Sustainable and Biomass (ICSB)* pada bulan Oktober 2019. Selain itu, penulis pernah melakukan Kerja Praktek (KP) selama 40 hari di Laboratorium Telemetri Pusat Teknologi Elektronika (PTE), Badan Pengkajian dan Penerapan Teknologi (BPPT), Banten pada tahun 2020.

PERSEMBAHAN

Skripsi ini kupersembahkan untuk
“ Kedua Orang Tua’
Yang selalu mendoakan penulis di setiap saat .
Senantiasa memberikan dukungan moril maupun materil
dalam menyelesaikan Skripsi.

-TERIMA KASIH-

Motto

“If I don’t have to do it, I won’t. If I have to do it, I’ll make it quick.”

“Peace, Love, Empathy”

(Kurt Cobain)

SANWACANA

Alhamdulillahi rabbil alamin, penulis sampaikan puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penelitian Tugas Akhir ini.

Tugas Akhir dengan judul **"PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS* "** ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Jurusan Teknik Elektro Fakultas Teknik Universitas Lampung.

Dalam masa perkuliahan dan penelitian, penulis mendapatkan banyak hal baik berupa dukungan, semangat, motivasi, dan banyak hal yang lainnya. Untuk itu penulis mengucapkan terimakasih kepada:

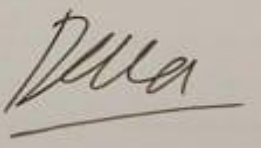
1. Allah SWT atas semua karunia, rahmat serta hidayah-Nya.
2. Orang tua dan saudara yang selalu memberikan doa dan semangat dari awal pelaksanaan skripsi hingga terselesaikan.
3. Ibu Dr. Ing. Melvi, S.T., M.T selaku pembimbing utama skripsi yang telah dengan sabar dan memberikan begitu banyak waktu untuk membimbing, memberikan ilmu, semangat, motivasi, dan juga arahan.
4. Bapak Aryanto, S.T., M.T selaku pembimbing pendamping yang telah memberikan saran, memberi ilmu motivasi selama masa pendidikan sampai pengujian skripsi.

5. Bapak Dr. Ing. Ardian Ulvan, S.T., M.Sc. selaku dosen penguji skripsi yang telah memberikan saran, kritikan yang sangat membangun dalam penyusunan skripsi.
6. Bapak Ibu dosen dan pegawai di Jurusan Teknik Elektro yang telah memberikan ilmu, arahan, dan wawasan yang tak terlupakan oleh penulis.
7. Teman-teman HIRO 2017 yang sudah menjadi seperti keluarga sendiri, terimakasih segala kebaikan yang sudah diberikan.

Penulis meminta maaf atas segala kesalahan dan ketidaksempurnaan dalam penyusunan tugas akhir ini. Saran dan kritik membangun sangat diharapkan penulis dalam kebaikan di masa yang akan datang, Terimakasih.

Bandar Lampung, 8 Februari 2023

Penulis,



Dipamadya Kalingga

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) adalah struktur dimana objek atau orang diberikan identitas eksklusif dan kemampuan untuk berbagi data melalui jaringan (internet) tanpa memerlukan interaksi langsung antara manusia dengan manusia atau interaksi manusia ke komputer. IoT muncul dari perkembangan teknologi nirkabel dimana IoT mengembangkan konektivitas perangkat elektronik dapat terhubung dengan *embedded tools* (alat tertanam) untuk berkomunikasi dan saling berhubungan dengan lingkungan eksternal melalui internet [1]. Menurut [2], *Internet of Things* (IoT) terdiri dari tiga lapisan yaitu *perception layer*, *network layer*, dan *application layer*, setiap lapisan ditentukan oleh fungsinya dan perangkat yang digunakan di dalamnya.

Salah satu tantangan yang harus diatasi untuk mendorong meluasnya implementasi IoT adalah faktor keamanan. Banyaknya entitas dan data yang terlibat berarti IoT menghadapi risiko keamanan yang dapat mengancam konsumen. Ancaman ini dapat terdiri dari akses oleh orang yang tidak berwenang untuk mengakses data dan menyalahgunakan informasi pribadi, memfasilitasi serangan terhadap sistem lain dan mengancam keamanan pribadi penggunanya [3].

Ada tiga elemen keamanan informasi, yaitu *confidentiality*, *integrity*, dan *availability*. Salah satu isu serangan yang sering terjadi di dunia IoT yaitu *Data & Identity Theft*, yang artinya seseorang mencuri atau mengambil data yang sedang dikirim dari perangkat menuju ke *server* data dan sebaliknya [4]. Beberapa solusi sistem keamanan jaringan IoT yaitu dengan menggunakan metode *authentication (password)* untuk mendapatkan akses ke sistem atau dengan menggunakan metode kriptografi untuk merahasiakan data yang dikirim pada *network layer*.

Kelebihan dalam pemanfaatan sistem dengan *authentication (password)* yaitu adanya kemudahan dalam penggunaan dan banyak *user* sudah terbiasa dengan sistem ini sehingga waktu penyesuaian dapat diminimalkan. Sistem autentikasi berbasis *password* ini memiliki kelemahan ketika *password* dilacak atau dicuri menggunakan perangkat lunak untuk mendapatkan informasi *login* jarak jauh seperti nama pengguna dan kata sandi [5].

Kriptografi adalah teknik menyampaikan pesan menggunakan metode enkripsi, sehingga data sebelum dikirim dienkripsi terlebih dahulu. Data dienkripsi menjadi *chipertext* sehingga sulit dimengerti dan juga hanya penerima (*user)* saja yang dapat membaca data aslinya karena memiliki *private key*. Kriptografi juga memiliki kelemahan, yaitu jika kunci hilang atau sulit ditebak, sistem kriptografi tidak lagi aman.

Selain dua metode di atas terdapat metode *Two Factor Authentication* (2FA), yaitu suatu metode *login* yang memerlukan dua faktor autentikasi. *Two Factor*

Authentication itu menggabungkan dua metode autentikasi yaitu *Something You Know* (*password* statis atau *password* milik pengguna pribadi) dengan *Something You Have* (token atau kode acak yang berubah-ubah) [5].

Dengan metode 2FA ini, sistem keamanan yang dibangun pada penelitian ini akan menggunakan dua autentikasi yaitu berupa *password* dan OTP (*One time password)* yang harus di*input* untuk mengakses jaringan *internet of things*, sehingga penelitian ini bertujuan untuk membuat sistem keamanan pada *Internet of Things* menggunakan algoritma *Two Factor Authentication (2FA).*

1.2 Tujuan Penelitian

Tujuan dari perancangan algoritma *two factor authentication* adalah sebagai berikut:

1. Meningkatkan keamanan jaringan *internet of things* (IoT) dengan menambahkan lapisan autentikasi tambahan selain dari *password id* saja. Ini memastikan bahwa individu yang memiliki akses ke-2 faktor autentikasi yang dapat mengakses jaringan IoT.
2. Membuat sistem keamanan untuk jaringan IoT yang dapat diimplementasikan ke *platform* IoT yang bersifat *independent.*

1.3 Rumusan Masalah

Permasalahan yang dibahas pada penelitian ini adalah sebagai berikut:

1. Bagaimana mengatasi *sniffing* pada masalah keamanan jaringan IoT?

2. Bagaimana cara membangun sistem keamanan IoT menggunakan algoritma *Two Factor Authentication (2FA)* dengan lapisan *password* dan OTP?

1.4 Batasan Masalah

Batasan masalah pada penulisan skripsi ini adalah :

1. *Two Factor Authentication (2FA)* yang dibangun menggunakan *password* dan *One time password* (OTP).
2. Pengujian sistem dilakukan saat enkripsi data dan pengiriman data sensor ke *database.*
3. Sistem yang dibangun dapat diimplementasikan pada *platform* IoT yang *independent.*

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Sebagai upaya melindungi jaringan IoT dari bahaya serangan *cyber.*
2. Sebagai sistem keamanan yang dapat digunakan pada *platform* IoT yang *independent.*

1.6 Sistematika Penulisan

Adapun sistematika Penulisan dari skripsi ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab ini berisi latar belakang penulisan, tujuan penelitian, rumusan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini memuat teori-teori dari beberapa hasil penelitian terdahulu yang berkaitan dengan topik pada skripsi ini antara lain: kajian pustaka yang berasal dari penelitian sebelumnya, *Internet of Things* (IoT), *security IoT, Confidentiality Integrity A*vailabili*ty* (CIA), *Authentication, Two Factor Authentication (2FA),* NodeMCU ESP8266, Sensor DHT11, *Visual Studio Code,* dan Algoritma *Advanced Encryption Standard (*AES).

BAB III. METODOLOGI PENELITIAN

Bab ini memuat tentang langkah-langkah penelitian yang dilakukan, seperti waktu dan tempat penelitian, alat dan bahan, alur penelitian dan pembuatan sistem keamanan IoT menggunakan 2FA.

BAB IV. HASIL DAN PEMBAHASAN

Bab ini memaparkan hasil yang diperoleh dari pengujian sistem keamanan dari penelitian yang dilakukan dan pembahasan hasil penelitian tersebut.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari keseluruhan penelitian yang telah dilakukan serta saran untuk penelitian kedepannya.

BAB II

TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Penelitian untuk skripsi ini mengacu pada beberapa penelitian sebelumnya dalam beberapa tahun terakhir. Penelitian-penelitian tersebut membahas tentang konsep IoT dan sistem keamanan pada perangkat IoT.

Penelitian [5] dengan judul "Implementasi Metode *One time password* pada Sistem Pemesanan *Online"* menghasilkan suatu sistem keamanan pada pemesanan *online* menggunakan *Two Factor Authentication.* Sistem *two factor authentication* yang dibuat menggunakan *username* dan *password* kemudian divalidasi menggunakan *One time password* (OTP). Metode yang digunakan untuk membangkitkan OTP adalah *Time-based One Time Password* (TOTP), yaitu dengan *password* dinamis yang berubah mengikuti waktu tertentu. *Password* tersebut dibangkitkan dengan melalui proses enkripsi *Secure Hash Algorithm 256 (*SHA-256) dengan bantuan *pseudo random number generator* yang menghasilkan enam digit nilai heksadesimal. Pada alur mekanisme pada penelitian ini, *user* melakukan *login* kemudian *server* akan mengirim OTP ke *email user* dan *user* harus memasukkan OTP yang dikirim untuk melakukan pemesanan *online.* OTP yang digunakan pada penelitian ini memiliki masa berlaku tertentu dan apabila melewati batas waktu

tersebut serta diganti dengan kode OTP yang baru atau deret angka berikutnya. OTP juga hanya berlaku untuk satu kali pemesanan saja.

Penelitian [6] dengan judul "*Threat model for securing internet of things (IoT) network at device-level"* membahas kerentanan perangkat IoT, ancaman serta rekomendasi kontrol keamanan untuk jaringan IoT yang mencangkup tiga bidang yaitu perawatan kesehatan, perdagangan, dan rumah. Pada penelitian ini penulis melakukan penghitungan skor kerentanan untuk perangkat IoT menggunakan *National Institute of Standards and Technology Common Vulnerability Scoring System* (NIST-CVSS). Beberapa ancaman pada domain kesehatan yaitu lemahnya enkripsi data, tidak adanya autentikasi, dan interferensi. Pada domain perdagangan yaitu serangan *software,* DoS, dan akses yang tidak sah, sedangkan pada domain rumah yaitu *backdoor, data transfer* yang tidak aman. Beberapa *security control* yang ditawarkan pada penelitian ini antara lain *traffic delay detection, PPD access control, password management, multi factor authentication, time divison multiplexing,* dll.

Penelitian [7] dengan judul "*Advance Encryption Standard* (AES) 128 bit untuk Keamanan Data *Internet of Things* (IoT) Tanaman Hidroponik" menggunakan algoritma AES karena mempunyai hasil enkripsi lebih aman dibanding algoritma simetris sejenis misalnya *blowfish, caesar cipher* serta lebih cepat dibandingkan dengan *Data Encryption Standard (DES),* hal ini diperoleh dari 10 putaran kunci sebelum proses enkripsi. Pada penenelitian ini juga disimpulkan AES cocok untuk diterapkan dalam mengamankan data yang terdapat pada sistem/*database.* Pada

penelitian ini didapat Hasil percobaan untuk membuktikan keamanan data dalam sistem IoT telah dilakukan dengan menganalisis teks dan *cipher-text*, menghitung nilai *Avalanche Effect (AE),* entropi *dan Bit Error Ratio (BER).*

Penelitian [8] dengan judul "Implementasi *Two Factor Authentication* Dan *Protokol Zero Knowledge Proof* Pada Sistem Login" menghasilkan sistem login dimana *Zero Knowledge Proof* digunakan untuk menjaga kerahasiaan kata sandi dan *Two Factor Authentication* digunakan untuk mengamankan proses *login* pada perangkat yang tidak dipercaya. Penelitian ini melakukan lima skenario pengujian yang berbeda, setiap pengujian akan dilakukan pada 5 pengguna yang berbeda dan pada masing-masing pengguna dilakukan sebanyak 20 iterasi. Sistem yang diusulkan telah diuji dan hasil awal menunjukkan bahwa sistem tersebut mampu mengamankan proses *login* tanpa membocorkan *password* pengguna.

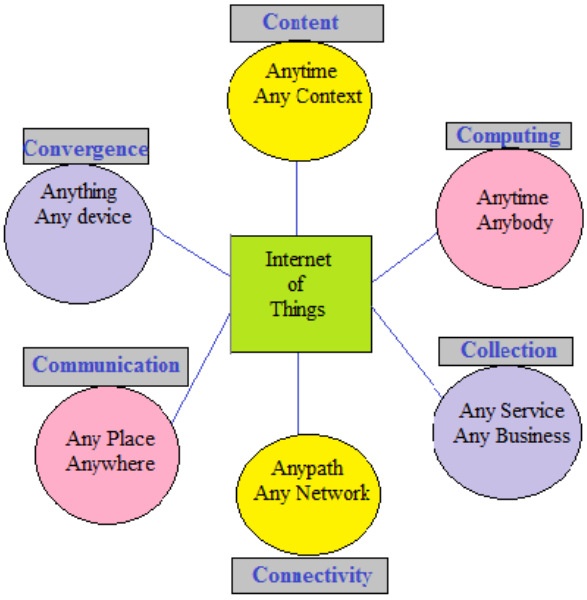
Penelitian [9] dengan judul "*Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application*", mengusulkan kerangka kerja autentikasi dua faktor berdasarkan *blockchain ethereum* dengan *dApp* sebagai sistem pembuatan token dan membuat sistem autentikasi dua faktor tanpa menggunakan pihak ketiga. Token yang dibangkitkan menggunakan algoritma SHA-256 dan akan disimpan sementara pada *session struct. Session struct* berisi berisi email, alamat *Ethereum* pengguna, peran, token, dan verifikasi token. Untuk melakukan autentikasi dua faktor, pengguna harus mengklik tombol autentikasi, kemudian *token hash* dikirim ke *blockchain* menggunakan alamat *Ethereum* pengguna untuk disimpan. *Server web*

akan membandingkan apakah alamat *Ethereum* yang melakukan transaksi atau menyimpan token ke dalam *blockchain* memiliki alamat yang sama dengan alamat yang disimpan sementara dalam *session struct*. Jika alamat *Ethereum* pengguna cocok, maka nilai verifikasi token akan disetel ke *true* dan akses ke situs *web* diberikan. Sehingga sistem pada penelitian ini tidak perlu mengirimkan token kepada pengguna terlebih dahulu, tetapi akan dicek secara otomatis oleh sistem. Metode keamaan ini melindungi token dari serangan MITM (*Man in The Middle)* karena semua pemeriksaan dilakukan oleh autentikasi pengguna *dApp.*

Perbedaan antara penelitian terdahulu dengan penelitian yang dilakukan penulis adalah penulis menggunakan algoritma *two factor authentication* untuk mengamankan jaringan IoT dimana metoda 2FA yang dibangun menggunakan *password* dan OTP. Sistem keamanan yang dibangun penulis dapat digunakan untuk *platform* IoT yang bersifat *independent.*

2.2 *Internet of Things* (IoT)

Internet of Things (IoT) adalah struktur dimana objek dan orang diberikan identitas unik dan kemampuan untuk berbagi data melalui jaringan (internet) tanpa memerlukan interaksi langsung antara manusia dengan manusia.



Gambar 2.1 *Internet of Things*

IoT muncul dari perkembangan teknologi nirkabel dimana IoT mengembangkan konektivitas perangkat elektronik yang dapat dihubungkan dengan alat terintegrasi untuk berkomunikasi dan berinteraksi dengan lingkungan *eksternal* melalui internet.

Beberapa tantangan penelitian pada teknologi IoT ini antara lain [10]:

1. Privasi dan Keamanan
2. Pengolahan, Analisis dan Manajemen Data
3. Monitoring dan *Sensing*
4. M2M (*Machine to Machine*) *Communication* dan Protokol Komunikasi
5. *Blockchain of Things* (BCoT): Perpaduan *Blockchain* dan *Internet of Things*
6. Interoperabilitas

2.2.1 *Security IoT*

Banyaknya komponen seperti sensor, perangkat pintar, dan peralatan rumah tangga yang terlibat dalam IoT menjadikan IoT suatu sistem yang kompleks. Namun,

pengintegrasian komponen-komponen ini ke dalam jaringan internet memunculkan berbagai tantangan keamanan. Salah satu ancaman keamanan pada IoT adalah ancaman pada layer jaringan. Ancaman ini yaitu penyerang mencuri data pada saat pertukaran data yang terjadi pada kanal komunikasi. Jika data tidak dienkripsi, penyerang dapat membaca dan mengumpulkan data penting seperti *username* dan *password*, serta data lain seperti informasi *access control*, konfigurasi *node*, *share network password*, dan identitas *node*, jika si penyerang dapat mengekstrak informasi yang diperlukan untuk menambahkan sebuah *node* yang sah, penyerang akan dengan mudah menambahkan *node* palsu di dalam sistem [3].

2.3 *Confidentiality Integrity A*vailabili*ty* (CIA) Triad

CIA *Triad* adalah suatu model yang dirancang dengan tujuan memandu kebijakan yang terkait keamanan informasi pada suatu organisasi. CIA itu sendiri terdiri dari tiga aspek yaitu *confidentiality*, *integrity dan availability*. Unsur-unsur tersebut dianggap sebagai tiga komponen *cyber security* yang paling penting di seluruh *platform* terutama pada *web app.*

Gambar 2.2 CIA *Triad*

1. *Confidentiality* (kerahasiaan), *confidentiality* ini merupakan serangkaian tindakan yang harus diambil untuk mencegah pengungkapan informasi sensitif kepada orang yang tidak berwenang dan juga untuk memastikan bahwa orang yang tepat memperoleh data yang dibutuhkan.
2. *Integrit*y (keakuratan data), terkait dengan integritas aset suatu sistem informasi dimana proses penyimpanan, pemrosesan dan transmisi data tidak terekspos dan memungkinkan terjadinya campur tangan pihak lain yang dapat merusak atau merubah keaslian data.
3. *Availability* adalah ketersediaan informasi dalam format tertentu tanpa adanya halangan kepada pihak yang telah diberi hak untuk mengaksesnya.

2.4 *Authentication*

Authentication adalah proses verifikasi identitas pengguna sistem komunikasi saat masuk ke sistem, pengguna yang telah lulus verifikasi identitas adalah pengguna resmi sistem, pemilik sistem, atau mungkin aplikasi yang berjalan di sistem.

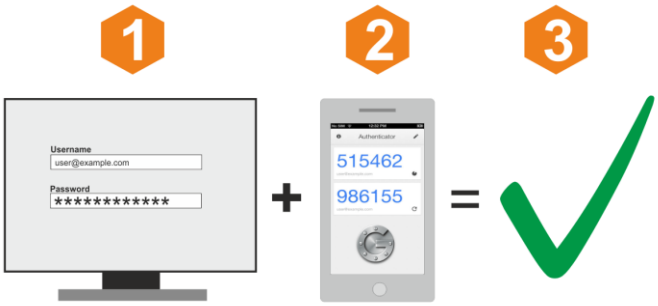
Cara paling sederhana adalah autentikasi login, dimana pengguna memasukkan nama pengguna dan kata sandi (kredensial), yang kemudian diverifikasi oleh sistem untuk menentukan apakah kredensial itu valid atau tidak valid. Jika kredensial valid, pengguna dapat mengakses sistem [11]. Jika tidak valid, pengguna tidak akan memiliki akses ke sistem. Autentikasi berbasis kata sandi memungkinkan kita untuk menambahkan lapisan keamanan dan menggabungkan autentikasi dua faktor yang dikenal sebagai *Two Factor Authentication* (2FA).

2.4.1 *Two Factor Authentication* (2FA)

Two-Factor Authentication adalah sebuah metode autentikasi *client* dimana terdapat dua faktor yang digunakan dalam membuktikan adanya klaim bahwa sebuah entitas atau identitas itu asli. Penggunaan *Two Factor Authentication* dapat mengurangi resiko seorang *adversary* dapat masuk ke sebuah sistem dengan menggunakan identitas pribadi individu karena selain harus mengetahui *password* yang kita gunakan, *adversary* juga harus mendapatkan informasi kedua yang bisa dihasilkan dari sumber yang berbeda [5]. Pada kebanyakan sistem yang ada saat ini digunakan kombinasi antara *username*/*password* dan juga kode *OTP* (*One Time Password*) yang dikirimkan melalui SMS ke perangkat digital (*smartphone* /*tablet*) atau dihasilkan melalui aplikasi pihak ketiga, misalnya Google Authenticator atau Authy [8].

Secara umum, cara kerja 2FA adalah sebagai berikut:

1. *User* masuk ke aplikasi atau situs *web* dengan nama pengguna dan *passwor*d.
2. *Server* akan mengecek apabila *username* dan *password* tersebut benar (cocok dengan *database* di *server* mereka).
3. Apabila benar, maka pengguna diharuskan memasukkan faktor autentikasi kedua. Faktor autentikasi ini bisa berupa PIN, kode, OTP, dan lain-lain.
4. Jika pengguna berhasil memasukkan faktor autentikasi kedua, aplikasi/ *website* akan memperbolehkan pengguna untuk *login*.



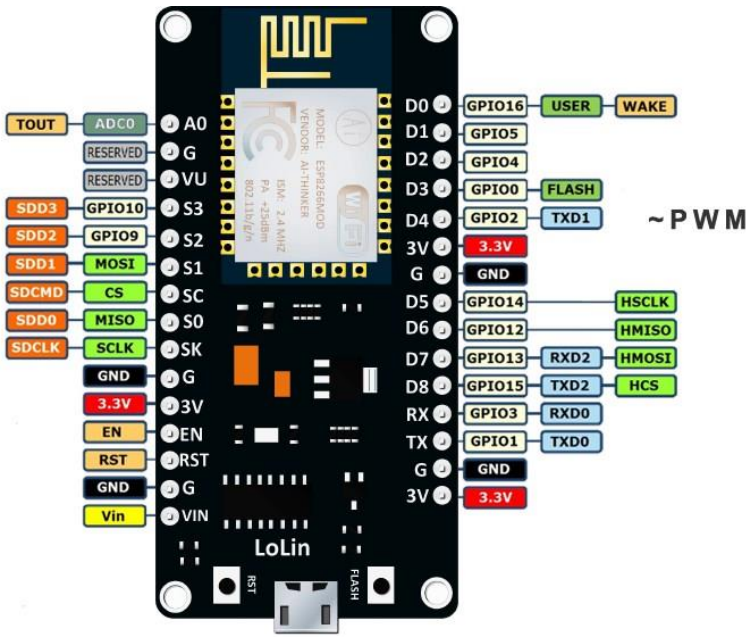
Gambar 2.3 Proses *Authentication*

Namun kode atau token yang masih menggunakan pihak ketiga untuk mengirim kode tidak aman untuk sistem 2FA karena token dapat dicuri oleh penyerang melalui metode *Man-In-The-Middle* (MITM). Model 2FA ini dapat dimodifikasi sedikit dengan membuat sistem yaitu dengan menghasilkan kode autentikasi sendiri dan pengguna tidak perlu menginput kode secara manual karena pengecekan akan dilakukan secara otomatis oleh sistem. Sistem ini akan mengubah sistem terpusat menjadi sistem terdistribusi dengan kemampuan pemrograman dan dapat melawan serangan MITM dan 2FA dari pihak ketiga [9].

2.5 NodeMCU ESP8266

NodeMCU adalah sebuah papan elektronik yang berbasis chip ESP8266, yang dapat menjalankan fungsi mikrokontroler dan juga koneksi internet *(WiFi)*. Proyek IoT ESP9266 NodeMCU memiliki banyak pin I/O untuk mengembangkan aplikasi pemantauan dan kontrol. NodeMCU ESP8266 dapat diprogram dengan kompiler arduino menggunakan *arduino* IDE. NodeMCU ESP8266 adalah modul hasil pengembangan dari modul platform IoT tipe ESP-12. Secara fungsional, modul ini

hampir mirip dengan platform modul arduino, tetapi perbedaannya adalah secara khusus untuk "*Connected to Internet*" [12]. NodeMCU ESP8266 v0.9 memiliki 4MB *flash*, 11 pin GPIO dimana 10 diantaranya dapat digunakan untuk PWM, 1 pin ADC, 2 pasang UART, WiFi 2,4GHz serta mendukung WPA/ WPA2 [13].



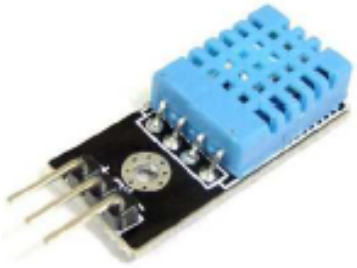
Gambar 2.4 *Pinout* NodeMCU ESP8266

2.6 Sensor DHT-11

DHT11 adalah satu jenis modul sensor suhu dan kelembapan. DHT11 memiliki *output* sinyal digital terkalibrasi dengan sensor suhu dan kelembapan yang kompleks. Teknologi ini memastikan keandalan yang tinggi dan stabilitas jangka panjang yang sangat baik dari mikrokontroler yang dikaitkan dengan kinerja 8-bit yang tinggi. Sensor DHT11 ini mengandung elemen resistansi dan *resistor* dengan tipe NTC (*Negative Temperature Coefficient*) [14]. DHT11 ini memiliki 4 kaki pin, dan terdapat juga sensor DHT11 dengan *breakout* PCB yang terdapat hanya memiliki 3 kaki pin yaitu pin tegangan, data, dan *ground.*

Spesifikasi dari DHT11 adalah sebagai berikut:

1. Tegangan Input 3-5V
2. Arus 0.3mA, *Iddle* 60uA
3. Periode sampling 2 detik
4. *Output* data serial
5. Resolusi 16 bit
6. Temperatur antara 0°C sampai 50°C (akurasi 1°C)
7. Kelembapan antara 20% sampai 90% (akurasi 5%)



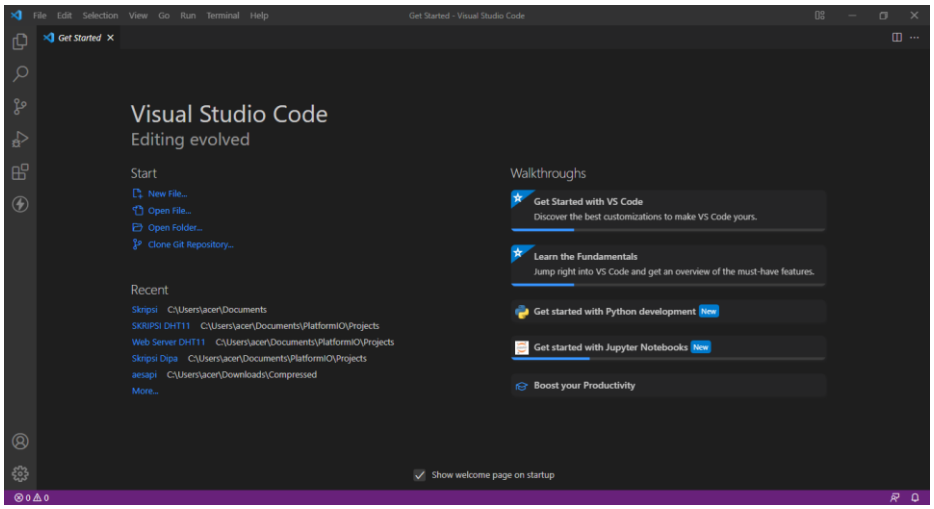
Gambar 2.5 Sensor DHT-11

2.7 *Visual Studio Code*

Visual Studio Code merupakan editor kode yang dibuat oleh *Microsoft* untuk Windows, Linux, dan macOS. Fitur ini mencakup dukungan untuk penyorotan sintaks, *debugging*, penyelesaian kode cerdas, cuplikan, pemfaktoran ulang kode, dan Git yang disematkan. *Visual Studio Code* adalah editor kode yang menggunakan beberapa bahasa pemrograman, yaitu Javascript, Go, Java, Python, Nodejs, dan C++. Kelebihan *visual studio code* antara lain:

1. Mudah untuk mengelola *extention*
2. Memiliki *extention* yang banyak
3. Kontribusi tampilan

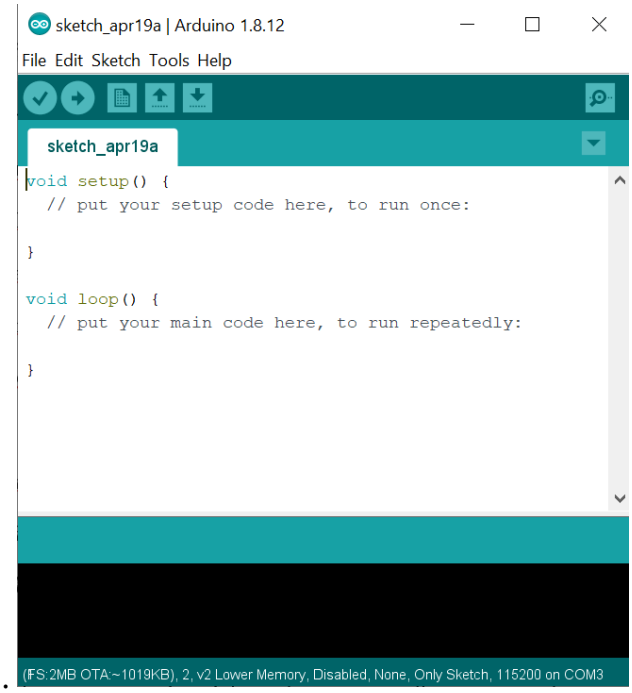
4. Dukungan bahasa
5. *Text editor* gratis
6. Dapat membuat *snippet* sendiri
7. Mudah dalam memahami dan mempelajari *coding*



Gambar 2.6 Tampilan awal *Visual Studio Code*

2.8 *Arduino Integrated Development Enviroment* (IDE)

Arduino IDE adalah *software* untuk membuat program. *Software* ini digunakan untuk membuat, meng*edit*, dan meng*upload sketch* pada *board arduino*. Arduino IDE dilengkapi dengan *library* C/C++ yang biasa disebut *wiring* yang membuat operasi *input* dan *output* menjadi lebih mudah. Program yang ditulis dengan menggunakan Arduino IDE disebut *script*. *Script* dimasukkan dalam suatu teks editor dan disimpan dalam file dengan ekstensi '*.ino'*. tampilan awal dari *software Arduino* IDE dapat dilihat pada Gambar 2.8.



Gambar 2.7 Tampilan awal *Arduino* IDE

2.9 Algoritma *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang digunakan untuk mengamankan suatu data. Algoritma AES adalah *cipher* blok simetris yang dapat mengenkripsi dan mendekripsi informasi. Enkripsi mengubah data yang tidak dapat dibaca lagi, disebut *ciphertext*; sebaliknya dekripsi adalah mengubah data *ciphertext* ke bentuk aslinya yang kita kenal sebagai *plaintext*. Satu atau lebih kunci enkripsi digunakan dalam proses enkripsi dan dekripsi. Dalam algoritma enkripsi AES 128, 1 blok *plainteks* berukuran 128 bit pertama-tama diubah menjadi matriks heksadesimal berukuran 4x4 yang disebut *state*. Setiap elemen *state* berukuran 1 *byte*. Proses enkripsi pada AES merupakan transformasi terhadap *state* berulang kali selama 10 putaran [15]. Pada penelitian ini menggunakan algoritma AES karena AES berdasarkan jurnal [7] AES cocok untuk diterapkan dalam

mengamankan data yang terdapat pada sistem/*database* sesuai dengan sistem IoT yang dibangun pada penelitian ini.

BAB III

METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian

Adapun waktu dan tempat penelitian skripsi ini adalah sebagai berikut:

Waktu : Juli 2022 ─ Januari 2023

Tempat : Laboratorium Teknik Telekomunikasi, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung.

3.2 Alat dan Bahan

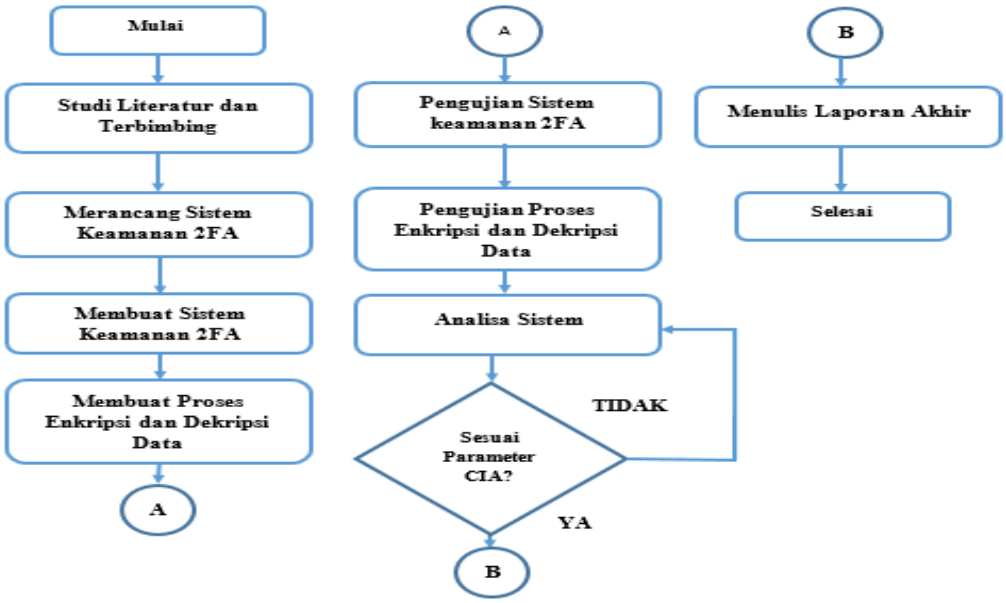
Peralatan dan bahan-bahan yang digunakan pada penelitian penelitian ini dapat dilihat pada Tabel 3.1.

Tabel 3.1 Alat dan Bahan

No	Alat dan bahan	Justifikasi Penggunaan
1	Laptop	Sebagai alat memprogram sistem dan ESP8266.
2	*WiFi* atau *hotspot*	Sebagai akses jaringan internet.
3	NodeMCU ESP8266	Sebagai mikrokontroler bagi sensor DHT11.
4	DHT-11	Sensor untuk mendeteksi suhu dan kelembapan.
5	Kabel USB	Menghubungkan ESP8266 ke komputer.
6	Kabel *Jumper*	Menghubungkan sensor DHT11 ke ESP8266.
7	*Software Visual Studio Code*	*Software text editor* untuk menuliskan *source code.*
8	*Software Arduino* IDE	*Software* yang berguna untuk mengoperasikan mikrokontroler.

3.3 Metode Penelitian

Metode penelitian yang digunakan untuk mencapai tujuan penelitian dari skripsi ini. Metode yang digunakan dalam penelitian ini yaitu *experimental*. Adapun tahapan metode penelitian yang akan dilakukan dalam melaksanakan penelitian ini adalah sebagai berikut.



Gambar 3.1 Blok Diagram Penelitian

3.3.1 Studi Literatur

Studi literatur dilakukan dengan pencarian informasi terkait dengan skripsi yang dikerjakan yang bersumber dari buku, jurnal, skripsi, internet serta sumber-sumber lain yang berkaitan dengan skripsi ini, yaitu:

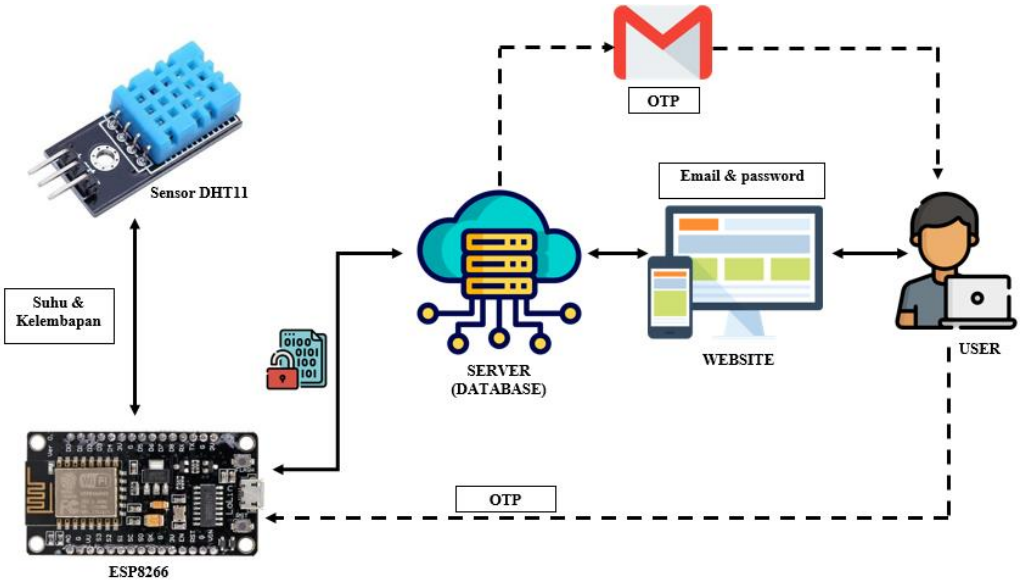
1. Konsep jaringan dan keamanan IoT.
2. Mempelajari sistem *two factor authentication.*
3. Mempelajari modul NodeMCU ESP8266.
4. Mempelajari sensor suhu dan kelembapan DHT11.
5. Mempelajari metode enkripsi AES 128.

3.3.2 Studi Bimbingan

Studi bimbingan dilakukan dengan cara berdiskusi berkala dengan dosen pembimbing baik dalam pembuatan laporan maupun dalam perancangan sistem algoritma *two factor authentication* untuk keamanan jaringan IoT sehingga didapatkan sistem keamanan jaringan IoT yang baik.

3.3.3 Perancangan Sistem

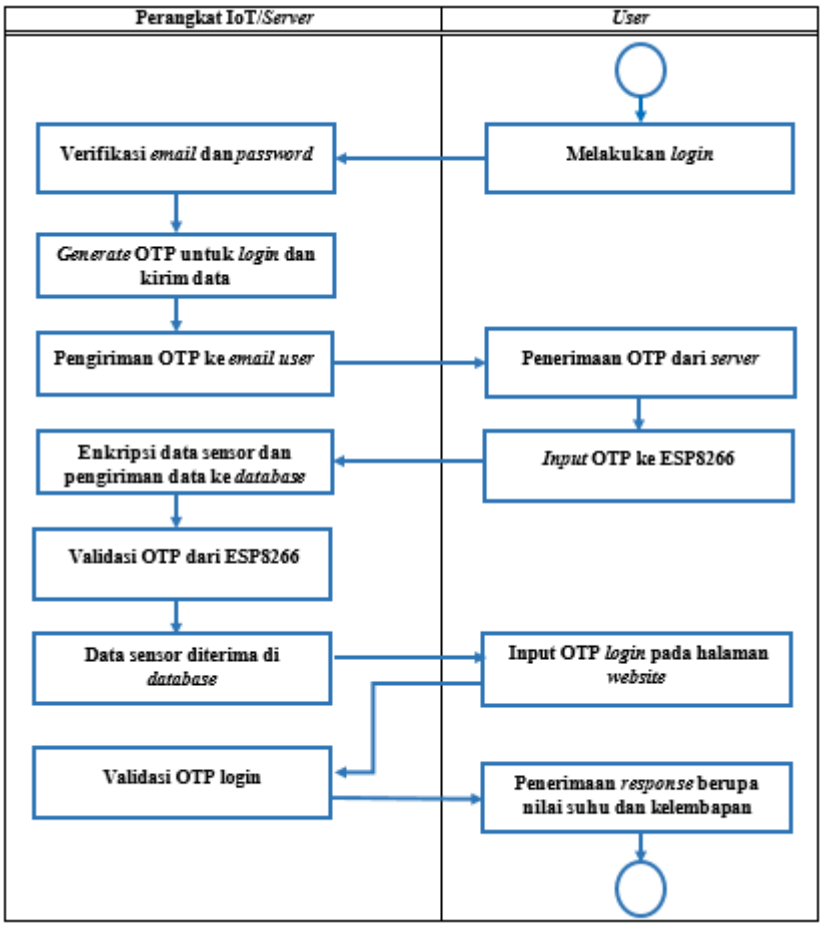
Rancangan sistem yang akan dibuat ditunjukkan seperti gambar berikut:



Gambar 3.2 Rancangan Sistem

Sistem keamanan jaringan IoT yang dibangun terdiri sensor suhu DHT11 dan NodeMCU ESP8266. Sensor suhu DHT11 dihubungkan ke modul ESP8266, untuk mendapatkan akses masuk ke sistem IoT, pertama *user* melakukan *login* ke *server* dengan memasukkan *email* dan *password* yang telah terdaftar di *database.* Setelah berhasil *login, server* akan mengirimkan OTP (*One time password)* sebagai *key 2* kepada *user* melalui *email.* OTP yang dikirim terdiri dari 2 jenis OTP yaitu OTP

untuk *login* ke *website* dan OTP untuk mengirim data sensor ke *database*. OTP *login* dimasukkan agar *user* dapat melihat data sensor yang ditampilkan, sedangkan OTP untuk ESP8266 di*input* ke ESP8266. Jika OTP sesuai maka data dari ESP8266 dapat di*input* ke *database*. Pada saat pengiriman data sensor akan dilakukan enkripsi data terlebih dahulu kemudian didekripsi saat diterima di *server*. Hal ini bertujuan untuk mengamankan data sensor dan OTP yang dikirim dari ESP8266.



Gambar 3.3 Alur Perancangan Sistem

3.3.4 Pembuatan Sistem

Pembuatan sistem terdiri dari proses konfigurasi perangkat dan proses kerja algoritma *two factor authentication.* Penelitian ini diawali dengan membuat sebuah

sistem yang akan dijalankan. Terdapat beberapa tahapan pada proses pembuatan sistem, antara lain: proses perangkaian alat, pembuatan halaman *website*, pembuatan *two factor authentication*, konfigurasi ESP8266, dan pembuatan enkripsi dan dekripsi data. Proses-proses tersebut dilakukan bertujuan agar setiap alat yang digunakan saling berkomunikasi dan dapat mengirim data berupa nilai suhu dan kelembapan dalam sistem keamanan yang menggunakan metode *two factor authentication.*

a. Proses Perangkaian Alat

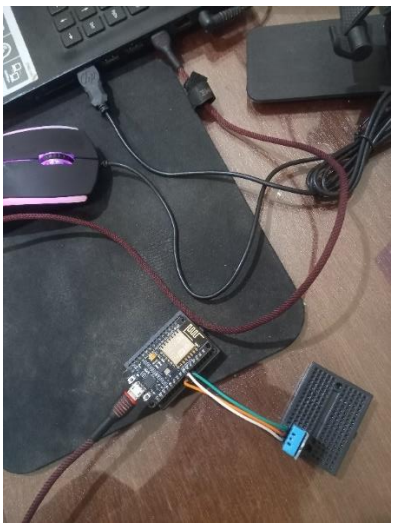
Alat-alat yang digunakan pada penelitian ini adalah ESP8266, sensor DHT11, kabel *jumper*, kabel USB dan 1 unit Laptop. ESP8266 sebagai mikrokontroler untuk menerima data dari sensor DHT11, DHT11 sebagai sensor yang akan melakukan *sensing* terhadap suhu dan kelembapan, kabel *jumper* digunakan untuk menghubungkan ESP8266 dengan DHT11, kabel USB digunakan untuk menghubungkan ESP8266 dengan laptop.

ESP32 dihubungkan dengan DHT11 pada pin-pin sebagai berikut: Pin VCC pada DHT11 dihubungkan dengan Pin 3v3 pada ESP8266

- Pin Data pada DHT11 dihubungkan dengan Pin D5 (Pin Data) pada ESP8266
- Pin *Ground* pada DHT11 dihubungkan dengan Pin *Ground* pada ESP8266

Gambar 3.4 Penyambungan ESP8266 dengan DHT11

Pada ESP8266 terdapat port USB sehingga dapat langsung dihubungkan ke laptop menggunakan kabel USB dan kemudian diprogram menggunakan Arduino IDE. ESP8266 akan menghidupkan *led*-nya apabila berhasil tersambung ke laptop. Apabila ESP8266 berhasil tersambung maka ESP8266 sudah bisa diprogram menggunakan *Arduino* IDE.



Gambar 3.5 Penyambungan ESP8266 ke Laptop

b. Pembuatan Halaman *Website*

Halaman *website* yang dibuat agar *user* dapat berinteraksi dengan *server* saat proses *register*, *login*, *input* OTP *login*, dan menampilkan data sensor suhu dan kelembapan yang dikirim ESP8266. Tampilan *web* dibuat menggunakan bahasa pemrograman html dan css.

- Halaman *register*

Halaman *register* dibuat agar *user* dapat registrasi menggunakan *email* dan *password* yang akan digunakan untuk proses *login.*

```
<style>
      body {
         background: #007bff;
         background: linear-gradient(to right, #0062E6, #33AEFF);
      }
      .btn-login {
         font-size: 0.9rem;
         letter-spacing: 0.05rem;
         padding: 0.75rem 1rem;
      }
      .btn-google {
         color: white !important;
         background-color: #ea4335;
      }

      .btn-facebook {
         color: white !important;
         background-color: #3b5998;
      }
   </style>
<form action="registerservice.php" method="post">
        <div class="form-floating mb-3">
                <input class="form-control" id="floatingInput" type="text"
                name="nama" required>
                <label for="floatingInput">Nama</label>
```

```
    </div>
        <div class="form-floating mb-3">
        <input class="form-control" id="floatingPassword" type="email"
name="email" required>
      <label for="floatingPassword">Email</label>
        </div>
        <div class="form-floating mb-3">
                <input class="form-control" id="floatingPassword"
        type="password" name="password" required>
                <label for="floatingPassword">Password</label>
        </div>
        <div class="d-grid">
                <button class="btn btn-primary btn-login text-uppercase fw-bold"
        type="submit">Register
                </button>
   </div>
</form>
```

Script di atas menunjukkan *codingan* untuk tampilan *interface* saat *user* melakukan proses *register*. Proses *register* ini *user* harus memasukkan nama, *email*, dan *password* .

- Halaman *login*

Halaman *login* dibuat agar *user* dapat meng*input email* dan *password* yang telah didaftarkan sebelumnya untuk proses *login*. Proses *login* harus dilakukan agar *user* mendapatkan OTP yang di*generate* oleh *server*.

```
<style>
      body {
        background: #007bff;
        background: linear-gradient(to right, #0062E6, #33AEFF);
      }
      .btn-login {
        font-size: 0.9rem;
```

```
        letter-spacing: 0.05rem;
        padding: 0.75rem 1rem;
      }
      .btn-google {
        color: white !important;
        background-color: #ea4335;
      }
      .btn-facebook {
        color: white !important;
        background-color: #3b5998;
      }
      .register {
        text-decoration: none ;
      }
    </style>

<form action="loginservice.php" method="post">
        <div class="form-floating mb-3">
                <input type="email" class="form-control" id="floatingInput"
                  name="email" required>
                <label for="floatingInput">Email address</label>
        <div class="form-floating mb-3">
                <input type="password" class="form-control"
                  id="floatingPassword" name="password" required>
                <label for="floatingPassword">Password</label>
        </div>
        <div class="d-grid">
                <p><a href="register.php" class="register">Register</a></p>
        </div>
        <div class="d-grid">
                <button class="btn btn-primary btn-login text-uppercase fw-bold"
                  type="submit">Login
                </button>
        </div>
</form>
```

Script di atas menunjukkan *codingan* untuk tampilan *interface* saat *user* melakukan proses *login.* Proses *login* ini *user* harus memasukkan *email*, dan *password* yang telah terdaftar di *database*

- Halaman OTP *login*

Pada halaman ini, *user* akan meng*input* OTP yang digunakan untuk melihat data sensor yang telah berhasil dikirim oleh ESP8266

```
<style>
      body {
         background: #007bff;
         background: linear-gradient(to right, #0062E6, #33AEFF);
      }

      .btn-login {
         font-size: 0.9rem;
         letter-spacing: 0.05rem;
         padding: 0.75rem 1rem;
      }

      .btn-google {
         color: white !important;
         background-color: #ea4335;
      }

      .btn-facebook {
         color: white !important;
         background-color: #3b5998;
      }
   </style>
<form action="otpservice.php" method="post">
         <div class="form-floating mb-3">
                  <input class="form-control" id="floatingInput" type="text"
                    name="otp" required>
                  <label for="floatingInput">OTP</label>
```

```
        </div>
                <input type="hidden" name="email" value="<?php echo
                 $_SESSION['email']; ?>">
        <div class="d-grid">
                <button class="btn btn-primary btn-login text-uppercase fw-bold"
                 type="submit">Input OTP
                </button>
         </div>
</form>
```

Script di atas menunjukkan *codingan* untuk tampilan *interface* saat *user* memasukkan OTP *login.*

- Halaman tampilan data sensor

Pada halaman ini akan menampilkan nilai data suhu dan kelembapan yang telah berhasil dikirim oleh ESP8266 ke *database.*

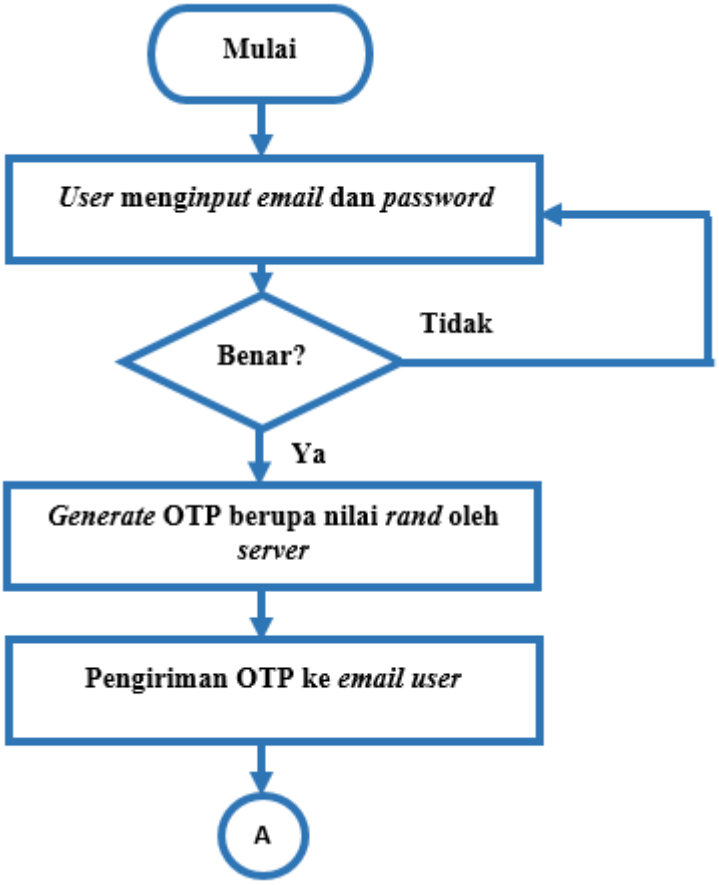
```
<div class="profile">
        <br>
        <h3><?php echo $nama; ?></h3>
        <p><a href=" logoutservice.php">Logout</a></p>
      </div>
      <div class="container">
        <div class="kotak">
          <h2 class="h2">Suhu</h2>
          <div class="nilai">
            <?php echo $data['suhu'] ?><font size="7">°C</font>
          </div>
        </div>
        <div class="kotak">
          <h2 class="h2">Kelembaban</h2>
          <div class="nilai">
            <?php echo $data['kelembaban'] ?><font size="7">%</font>
          </div>
        </div>
```

```
        </div>

body{
    background-color: #CFE8EF;
}

.container {
    text-align: center;
}

.kotak {
    width: 400px;
    height: 400px;

    margin-top: 40px;
    margin-bottom: 20px;

    margin-left: 20px;
    margin-right: 20px;

    padding-top: 20px;
    padding-bottom: 20px;

    padding-right: 20px;
    padding-left: 20px;

    border: 10px solid #333;

    display: inline-block;

    background-color: #FFFFF0;
}

.nilai{
    font-size: 150pt;
}
#reset:hover{
    cursor: pointer;
}
```

Script di atas menunjukkan *codingan* html dan css halaman data sensor untuk menampilkan nilai suhu dan kelembapan.

c. Pembuatan Algoritma *Two Factor Authentication*

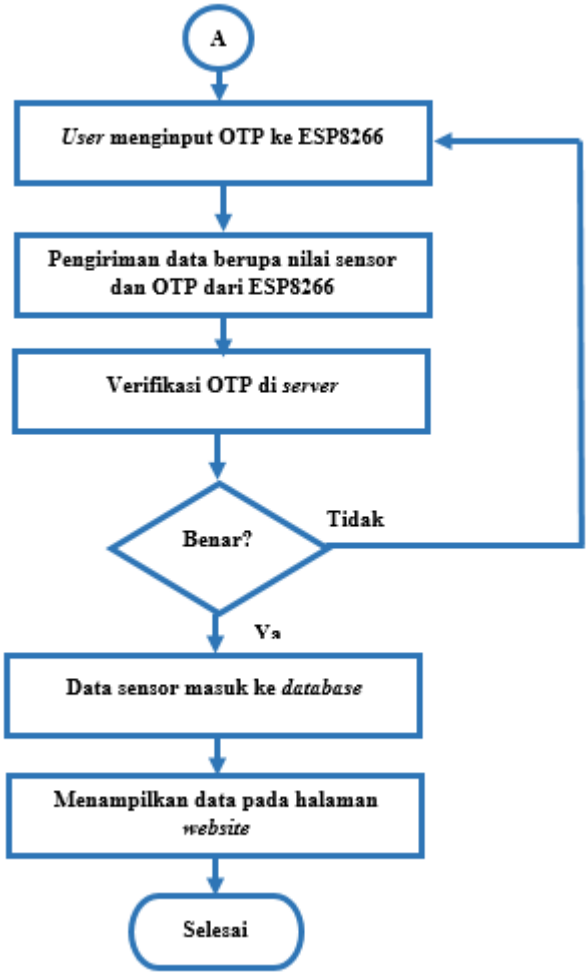
Proses algoritma *two factor authentication* berfungsi untuk mengamankan sistem IoT yang ada, algoritma tersebut berupa *email* dan *password* untuk melakukan *login* ke sistem dan juga OTP agar data dari ESP8266 dapat masuk ke *database* dan ditampilkan.



Gambar 3.6 Diagram Alir Sistem Bagian 1

Pada diagram alir sistem bagian 1, pertama *user* harus *login* ke sistem untuk mendapat akses, *user* harus memasukkan *email* dan *password* yang telah terdaftar

dengan benar. *Server* akan mengecek apakah *email* dan *password* yang dimasukkan sudah sesuai dengan data di *database*. *Server* akan melakukan proses *generate* OTP berupa nilai *rand* dan mengirimkan OTP tersebut ke *email user* yang melakukan *login* jika verifikasi *email* dan *password* sudah benar.



Gambar 3.7 Diagram Alir Sistem Bagian 2

Pada diagram alir sistem bagian 2, *user* harus memasukkan OTP yang diterima ke ESP8266 atau perangkat IoT yang digunakan agar mendapatkan akses masuk ke *database*. *Server* akan memverifikasi apakah OTP yang dimasukkan *user* benar atau tidak, jika sudah benar maka data sensor yang dikirimkan oleh perangkat IoT

dapat diterima *server* dan disimpan ke dalam *database*. Langkah-langkah pembuatan *two factor authentication* adalah sebagai berikut:

- *Login* dan *generate* OTP

User yang telah berhasil *login* menggunakkan *email* dan *password* pada halaman *website*, maka *server* akan melakukan proses *generate* OTP untuk perangkat IoT.

```
if ($total == 1 || $total == '1') {

    $myOTP = rand(10000, 99999);
    $myOTPESP = rand(10000, 99999);
    $date = date('Y-m-d H:i:s');
    $expiredOTP = strtotime($date) + (1440 * 60);
    $query = mysqli_query($koneksi, "UPDATE user SET otp = '" . $myOTP . "',
otpesp = '" . $myOTPESP . "', expired_otp = '" . $expiredOTP . "' WHERE id = " .
$data['id']);

    $_SESSION['email'] = $data['email'];

    $mail = new PHPMailer();

    try {
        $mail->isSMTP();                                    //Send using SMTP
        $mail->Host       = 'smtp.gmail.com';               //Set the SMTP server to
send through
        $mail->SMTPAuth   = true;
        $mail->SMTPSecure = 'ssl';                          //Enable SMTP
authentication
        $mail->Username   = 'smssk201222@gmail.com';        //SMTP
username
        $mail->Password   = 'wevrxkthzbmowoyh';         //Enable implicit TLS
encryption
        $mail->Port       = 465;                            //TCP port to connect to; use
587 if you have set `SMTPSecure = PHPMailer::ENCRYPTION_STARTTLS`
        $mail->addAddress($data['email']);
        //Content
        $mail->isHTML(true);                                //Set email format to HTML
```

```
        $mail->Subject = 'OTP Login';
        $mail->Body    = 'Berikut OTP untuk login Anda ke Sistem Monitoring
Sensor Suhu dan Kelembapan: <b>' . $myOTP . '</b> <br> Berikut OTP untuk
Microcontroller Anda: <b>' . $myOTPESP . '</b>';
        if ($mail->send()) {
            unset($_SESSION['message']);
            header("location:otp.php");
        } else {
            echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";
        }
    } catch (Exception $e) {
        echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";
        header("location:login.php");
    }

    // unset($_SESSION['message']);
    // header("location:otp.php"); // kembali ke tampil data
} else {
    $_SESSION['message'] = "Email atau password tidak sesuai!";
    header("location:login.php"); // kembali ke tampil data
}
```

Script di atas menunjukkan *codingan* saat *server generate* OTP. OTP yang di*generate* berupa 5 digit angka *rand* dan berlaku selama 24 jam. OTP yang di*generate* kemudian dikirim ke *email user* yang melakukan *login.*

- Verifikasi OTP

Perangkat IoT yang mengirim data ke *server* atau *database* akan diverifikasi terlebih dahulu. Jika OTP yang dikirim dari perangkat IoT sesuai dengan yang di*generate* oleh *server* maka data sensor dari perangkat IoT tersebut dapat diterima *server* dan masuk ke *database* untuk ditampilkan pada halaman *website.*

```
if ($otpesp != '') {
```

```
        $query = mysqli_query($koneksi, "SELECT * FROM user WHERE otpesp
= '" . $otpesp . "'");
        $total = mysqli_num_rows($query);
        $data = mysqli_fetch_array($query);

        if ($total == 1) {
            // $_SESSION['email'] = $data['email'];
            if (time() > $data['expired_otp']) {
                echo 'Expired OTP';
                // echo 'bener udah lewat';
            } else {
                // echo 'bener tapi masih dalam waktu';
                $kirim = mysqli_query($koneksi, "INSERT INTO tbsensor (tanggal,
suhu, kelembaban) VALUES (" . $tanggal . ", " . $suhu . ", " . $kelembaban . ")");

                if ($kirim) {
                    echo "Data berhasil diinput";
                } else {
                    echo "Gagal diinput";
                }
            }
        } else {
            echo 'OTP Salah, Silahkan Coba Lagi!';
            // header("location:login.php");
        }
    } else {
        echo 'Unauthorized!';
    }
```

Script di atas menunjukkan *codingan* untuk memverifikasi apakah OTP yang diterima dari perangkat IoT sesuai dengan yang di*generate* server atau tidak.

d. Konfigurasi ESP8266

Pada perangkat IoT yaitu ESP8266 perlu dilakukan konfigurasi agar dapat membaca sensor DHT11 dan juga mengirimkannya ke *server*.

```
#include <ESP8266WiFi.h>
#include <WiFiClient.h>
#include <ESP8266WebServer.h>
#include <ESP8266HTTPClient.h>
#include "DHT.h"

const char *ssid = "SamsungA31";
const char *password = "madara123";

#define DHTPIN D5
#define DHTTYPE DHT11
DHT dht(DHTPIN, DHTTYPE);
```

Gambar 3.8 Konfigurasi ESP8266 Bagian 1

```
void setup() {
  dht.begin();
  delay(1000);
  Serial.begin(115200);
  WiFi.mode(WIFI_OFF);
  delay(1000);
  WiFi.mode(WIFI_STA);
  WiFi.begin(ssid, password);
  Serial.println("");
  Serial.print("Connecting");

  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }

  Serial.println("");
  Serial.print("Connected to ");
  Serial.println(ssid);
  Serial.print("IP address: ");
  Serial.println(WiFi.localIP());
}
```

```
void loop() {
  HTTPClient http;

  String temperature, humidity, getData, Link;
  String baseURL, datasend, otpESP;

  temperature = dht.readTemperature();
  humidity = dht.readHumidity();

  Serial.println(temperature);
  Serial.println(humidity);

  baseURL = "http://192.168.252.218/skripsi_dipa/input.php?encrypted=";
  otpESP = "43043";

  datasend = "suhu=" + temperature + "&kelembaban=" + humidity + "&otpesp=" + otpESP;
```

Gambar 3.9 Konfigurasi ESP8266 Bagian 2

Gambar 3.8 dan 3.9 menunjukkan *codingan* pada *Arduino* IDE untuk konfigurasi ESP8266 agar dapat melakukan pembacaan nilai sensor DH11 dan mengirimkan data ke *server*.

e. Enkripsi dan Dekripsi Data

Sebelum ESP8266 mengirim data ke *server*, dilakukan enkripsi data terlebih dahulu menjadi *cipher text* di ESP8266. Proses enkripsi menggunakan metode *Advanced Encryption Standard* (AES) 128. Data yang dienkripsi yaitu nilai suhu dan kelembapan dan juga OTP untuk perangkat IoT (ESP8266).

```
AES aes;
byte cipher[1000];
char b64[1000];

// msg: message need to be encrypted.
// key_str: secrete key, 16 bytes
// iv_str:  initial vector, 16 bytes
String do_encrypt(String msg, String key_str, String iv_str) {

  byte iv[16];
  // copy the iv_str content to the array.
  memcpy(iv,(byte *) iv_str.c_str(), 16);

  // use base64 encoder to encode the message content. It is optional step.
  int blen=base64_encode(b64,(char *)msg.c_str(),msg.length());

  // calculate the output size:
  aes.calc_size_n_pad(blen);
  // custom padding, in this case, we use zero padding:
  int len=aes.get_size();
  byte plain_p[len];
  for(int i=0;i<blen;++i) plain_p[i]=b64[i];
  for(int i=blen;i<len;++i) plain_p[i]='\0';

  // do AES-128-CBC encryption:
  int blocks = len / 16;
  aes.set_key ((byte *)key_str.c_str(), 16) ;
  aes.cbc_encrypt (plain_p, cipher, blocks, iv);

  // use base64 encoder to encode the encrypted data:
  base64_encode(b64,(char *)cipher,len);
  //Serial.println("Encrypted Data output: "+String((char *)b64));
  return String((char *)b64);
}


   String msg= datasend;
   String key_str="aaaaaaaaaaaaaaaa";// 16 bytes
   String iv_str="aaaaaaaaaaaaaaaa"; //16 bytes
   String encrypted_data=do_encrypt(msg,key_str,iv_str);
```

Gambar 3.10 Enkripsi Data

Gambar 3.10 menunjukkan *codingan* untuk enkripsi data pada ESP8266 menggunakan *Advanced Encryption Standard* (AES) 128. Setelah dikirim ke *server* maka data yang terenkripsi akan didekripsi terlebih dahulu menjadi *plaintext* di *server*.

```
<?php
   include('koneksi.php');
```

```
// PHP code:
$method = "AES-128-CBC";
$key = "aaaaaaaaaaaaaaaa";
$iv = "aaaaaaaaaaaaaaaa"; // dont do this in real application!

// encode the message with base64 encoder (optional, make the same as we did with Arduino).

$result = base64_decode(str_replace(" ", "+", $_GET['encrypted']));
$result = openssl_decrypt($result, $method, $key, OPENSSL_NO_PADDING, $iv);
$decoded_msg = base64_decode($result);

$parse = explode('&', $decoded_msg);

$tanggal = time();
$suhu = explode('=', $parse[0])[1];
$kelembaban = explode('=', $parse[1])[1];
$otpesp = explode('=', $parse[2])[1];
```

Script di atas menunjukkan *codingan* untuk melakukan dekripsi data yang dikirim oleh ESP8266 dari *ciphertext* menjadi *plaintext* yang dilakukan di s*erver.*

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan dari skripsi ini adalah:

1. untuk meningkatkan tingkat keamanan jaringan dengan menambahkan lapisan autentikasi tambahan berupa *password* dan OTP (*One Time Password)*, sehingga hanya individu yang memiliki akses ke-2 faktor autentikasi yang dapat mengakses jaringan. Ini memastikan bahwa jaringan IoT lebih terlindungi dari serangan dan akses yang tidak sah, sesuai dengan parameter keamanan jaringan data CIA dengan pengujian yang telah dilakukan.
2. Berdasarkan hasil pengujian dan analisa, sistem yang dibangun memenuhi parameter CIA dimana pada parameter *confidentiality* terdapat OTP yang mengamankan jaringan IoT dan enkripsi data pada saat pengiriman dari ESP8266 ke *server*. Pada parameter *integrity*, berdasarkan data yang diterima oleh *server* dan juga hasil *sniffing* menggunakan *wireshark* tidak terdapat perubahan pada bentuk enkripsi data. Hal ini menunjukkan selama proses pengiriman data, tidak ada gangguan dan data suhu dan kelembapan yang diterima oleh *server* sesuai dengan yang dikirim oleh ESP8266. Pada parameter *availability* pengujian pengambilan data selama 24 jam dimana selama 24 jam

tersebut ESP8266 dapat mengirim data suhu dan kelembapan secara terus menerus dengan interval waktu 5 menit.

3. Sistem keamanan menggunakan *two factor authentication* yang dibangun dapat digunakan untuk *platform* IoT yang bersifat *independent.*

5.2 Saran

Saran dari penelitian ini untuk penelitian selanjutnya adalah mengembangkan *platform* IoT yang *independent* sehingga dapat menampilkan bentuk grafik dari data sensor yang dikirim sehingga lebih mudah untuk melakukan analisa data dan juga menambahkan beberapa sensor yang digunakan dalam sistem IoT.

DAFTAR PUSTAKA

[1] A. W. Burange, H. D. Misalkar. "Review of Internet of Things in Development of Smart Cities with Data Management & Privacy," *in Conf. Int. Advances in Computer Engineering and Application (ICACEA)*, Ghaziabad, India, 2015, pp. 189-195.

[2] I. Mashal, O. Alsaryrah, T. Y. Chung, C. Z. Yang, W. H. Kuo, D. P. Agrawal. “Choices for Interaction with Thing on Internet and Underlying Issues, *in Conf. Innovation Center for Big Data and Digital*, Taoyuan, Taiwan, 2015, pp.22.

[3] W. Najib, S. Sulistyo, dan Widyawan. "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 9, No. 4, pp. 375-384, Nov. 2020.

[4] M. S. Asang, dan I. Sembiring. "Keamanan Data Pada Perangkat Internet Of Things," *Jurnal Teknologi Informasi-Aiti*, vol. 14, pp. 80-87, 2017.

[5] N. S. Hapsari, Y. Fatman, dan Isbandi. “Implementasi Metode One time password pada Sistem Pemesanan Online*,” Jurnal Media Informatika Budidarma*, vol. 4, No. 4, pp. 930-939, Okt. 2020.

[6] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams. "Threat model for securing internet of things (IoT) network at device-level," *Journal of Information Sciences and Technology*, pp. 1-20, 2020.

[7] R. Ravida, H. A. Santoso" *Advance Encryption Standard* (AES) 128 bit untuk Keamanan Data *Internet of Things* (IoT) Tanaman Hidroponik," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi),* vol. 4, No. 6, pp.1157-1164, 2020.

[8] W. S. Raharjo, I. D. E. K. Ratri, dan H. Susilo. "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," *Jurnal Teknik Informatika dan Sistem Informasi,* vol. 3, No. 1, pp. 127-136, Apr. 2017.

[9] M. C. I. Putri, P. Sukarno, A. A. Wardana. "Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application", *Jurnal Ilmiah Teknologi Sistem Informasi,* vol. 6, No. 2, pp. 74-85, 2020.

[10] A. R. H. Hussein. "Internet of Things (IOT): Research Challenges and Future Applications," *International Journal of Advanced Computer Science and Applications,* vol. 10, No. 6, pp. 77-82, 2019.

[11] Guntoro, M. Fikri. "Perancangan Aplikasi Single Sign-On (SS0) Menggunakan Autentikasi Gambar," *Jurnal Teknologi Informasi & Komunikasi Digital Zone* , vol. 9, No. 1, pp. 12-21, Mei. 2018.

[12] Dewi, N. H. L., Rohmah, M. F., Zahara, S. "Prototype Smart Home dengan Modul NodeMCU ESP8266 Berbasis Internet of Things*",* pp. 1-9, 2018.

[13] Wicaksono, M. F. (2017). "Implementasi Modul Wifi NodeMCU ESP8266 untuk Smart Home*," Jurnal Teknik Komputer Unikom,* Volume 6, No. 1, pp. 1- 6, 2017.

[14] S. Rumalutur, dan A. Mappa. “Temperaure and Humidity Moisture Monitoring System With Arduino R3 and DHT 11,” *Jurnal Elektro Luceat*, vol. 5, No. 2, 2019.

[15] A. R. Tulloh, Y. Permanasari, E. Harahap. “Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen,” *Jurnal Matematika UNISBA*, vol. 15, No. 1, pp.7-14, 2016.