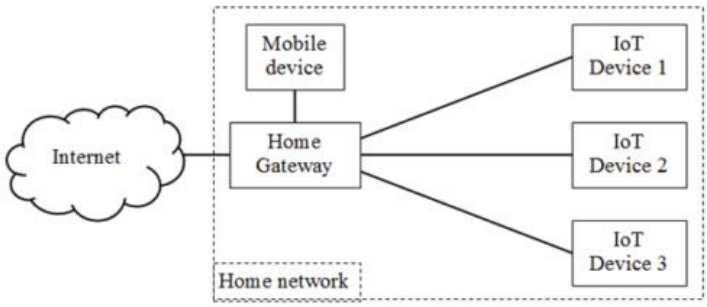
BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada abad ke-21 ini, teknologi informasi semakin berkembang untuk mempermudah pekerjaan manusia setiap hari. Semakin banyaknya kebutuhan manusia di masa yang akan datang membuat peran komputer mampu mendominasi pekerjaan manusia seperti mengendalikan alat elektronik dari jarak jauh menggunakan internet. Manusia menginginkan semua hal dapat terhubung dengan internet sehingga dapat melayani segala kebutuhannya. Seiring majunya teknologi internet dan perangkatnya, semua perangkat elektronik dapat dikendalikan melalui internet. Era dimana seluruh benda elektronik di sekitar kita akan terhubung dengan internet dan dapat saling berkomunikasi antar alat elektronik tersebut. Hal ini dikenal dengan *Internet of Things* (IoT).

Internet of Things merupakan suatu pengembangan internet yang sedang berjalan dimana benda-benda elektronik mampu berkomunikasi dan mampu memberikan informasi data yang *real time*. Saat ini *Internet of Things* banyak digunakan di beberapa bidang seperti pabrik mobil, pertanian, kesehatan, *security surveillance*, pengelolaan gedung dan *Smart Home* (Aamir & Sedky 2015). *Internet of Things* (IoT) ini menggunakan *embedded devices* atau sebuah perangkat yang sudah tertanam. Ada beberapa tantangan yang harus di hadapi pada IoT ini diantaranya *privacy*, *authentication* dan *secure end-to-end connection* (Koein & Abomhara 2014).

Salah satu sistem yang menggunakan perangkat IoT yaitu Sistem *Smart Home* yang saat ini digunakan di masyarakat untuk mempermudah mengawasi rumah dimana pun kita berada. *Smart Home* merupakan implementasi teknologi IoT pada perangkat – perangkat yang ada di rumah seperti kulkas, lampu, pintu, jendela, suhu ruangan dan sebagainya. Dengan menggunakan teknologi *Smart Home* kita dapat mengendalikan dan mengetahui informasi yang dikirimkan oleh perangkat IoT yang terhubung melalui internet.



Gambar 1.1 Sistem *Smart Home* (Santoso & Vun, 2015)

Pada gambar 1.1 menjelaskan skema sistem *Smart Home*, terdiri dari beberapa perangkat IoT yang terdiri dari sensor – sensor untuk mengambil data mentah terhadap lingkungan lalu dikirimkannya ke *Home Gateway* atau dalam beberapa penelitian *gateway* ini memiliki fungsi sebagai *Home Energy Management System* (HEMS) yang berfungsi untuk mengumpulkan informasi konsumsi pengguna dan juga informasi sensor yang akan di teruskan ke internet. Dalam penelitian ini, fungsi *gateway* hanya sebagai untuk mengumpulkan informasi dari sensor yang diteruskan ke internet. Informasi yang dikirimkan oleh perangkat IoT ke *home gateway* dan ke internet berbentuk *string* yang terdiri dari otentikasi dan informasi sensor yang sangat sensitif. Sehingga dibutuhkan pengamanan informasi menggunakan sistem enkripsi agar terhindar dari beberapa penyerangan yang dapat menyebabkan kerugian bagi pemilik sistem *Smart Home*, Salah satu contoh kasusnya yaitu *Attacks on The Energy Usage Data*, dalam sistem *Smart Home* terdapat *smart meter* yang berfungsi untuk mengumpulkan informasi konsumsi pengguna, informasi ini diteruskan ke HEMS yang memproses data meteran dan menerapkan informasi tagihan. *Attacks on Energy Consumption Reporting Devices*, dalam sistem *Smart Home* terdapat *smart meters* yang dapat menyediakan data konsumsi kepada konsumen selama 24 jam sehari. Dalam sistem *Smart Home* data konsumsi di simpan dan mengirimnya antara lingkungan *internal* dan *external*. *Eavesdropping attacks* dapat terjadi saat transmisi data dari peralatan rumah ke *Home Energy Management System* (HEMS). Penyerang dapat mengakses data konsumsi para konsumen dan memprosesnya untuk mengambil kesimpulan gaya hidup konsumen. Memodifikasi pesan juga menjadi ancaman dalam kasus ini. (Ali, Dustgeer, Awais, & Shah, 2017). Dari beberapa kasus tersebut dapat disimpulkan bahwa dengan mengimplementasikan sistem enkripsi pada *Home Gateway* dapat mengamankan informasi dari penyerang dari jaringan luar, tetapi tidak melindungi penyerang yang berada pada jaringan lokal. Sehingga pada penelitian ini akan

mengimplementasikan sistem enkripsi langsung pada perangkat IoT agar dapat melindungi informasi dari penyerang yang berada pada jaringan lokal. Terdapat beberapa algoritma enkripsi yang dapat digunakan pada perangkat IoT diantaranya yaitu, enkripsi menggunakan fungsi *hash* , RC4-based, AES256 dan *key exchange* Diffie-Hellman (Mantoro, Ayu, & Binti Mahmod, 2014) dan menggunakan skema *Lightweight lattice-based* (Abdallah & Shen, 2014).

Terdapat beberapa perangkat IoT pada *Smart Home*, diantaranya yaitu perangkat IoT berfungsi sebagai *Mobile Fire Alarm System Using Wireless Sensor Networks* (Muheden, Erdem, & Vancin, 2017). Perangkat IoT ini menggunakan sensor suhu dan kelembapan yang berfungsi untuk membaca kelembapan dan suhu lalu mengirimkannya nilainya ke *server* sehingga pihak ketiga seperti aplikasi android atau pusat pemadam kebakaran jika sensor tersebut mendeteksi perbandingan nilai yang berbeda dari pembacaan sebelumnya yang dapat menyebabkan kebakaran, pihak ketiga seperti pemilik rumah atau pemadam kebakaran akan mendapatkan notifikasi bahwa tempat di daerah perangkat IoT tersebut terjadi kebakaran sehingga pihak ketiga dapat langsung menuju tempat tersebut untuk memastikan dan melakukan prosedur keselamatan. Data suhu ini sangat penting untuk dirahasiakan dan diamankan agar tidak terjadi penyerangan dan manipulasi data oleh penyerang agar tidak terjadi kesalahan notifikasi kepada pihak ketiga. Maka dari itu, pada penelitian ini menggunakan algoritma ECC untuk melakukan pengamanan data yang dikirimkan oleh perangkat IoT untuk mencegah penyerangan dan manipulasi data tersebut.

Smart Home menggunakan perangkat yang membutuhkan daya yang kecil, sehingga beberapa algoritma tidak cocok di implementasikan pada *Smart Home*. Salah satu algoritma yang membutuhkan daya kecil adalah *Elliptic Curve Cryptography* (ECC). Beberapa penelitian yang menggunakan algoritma ECC pada perangkat IoT untuk menyelesaikan isu kemananan dan isu privasi, protocol otentikasi berbasis password untuk arsitektur *multi-server* menggunakan ECC (Kalra & Sood, 2013). Skema otentikasi yang aman berbasis ECC yang berintegrasi dengan *ID-verifier transfer protocol* (Liao & Hsiao, 2014). Implementasi *low-resource* 160-bit algoritma ECDSA *signature generation*. Mereka mempresentasikan implementasi perangkat keras menggunakan algoritma ECDSA melalui 160-bit-prime-field *curve*. (Workshop & Hutchison, 2014).

Tabel 1.1 Perbandingan Kunci Publik Algoritma ECC (Afreen & Mehrotra, 2011)

Symmetric-key	ECC	RSA/DLP
64 bit	128 bit	700 bit
80 bit	160 bit	1024 bit
128 bit	256 bit	2048-3072 bit

Pada Tabel 1.1, algoritma ECC dapat menyediakan tingkat keamanan yang sama dengan RSA hanya saja dengan kunci yang lebih kecil, sebagai contoh 1024 bit tingkat keamanan RSA dapat di tawarkan oleh ECC hanya dengan 160 bit untuk mendapatkan tingkat keamanan yang sama dengan RSA. Berdasarkan penjelasan yang sudah dipaparkan, dapat disimpulkan bahwa algoritma ECC sangat cocok untuk mengamankan data yang ada di sistem *Smart Home*, karena perangkat IoT yang akan digunakan dalam sistem tersebut memiliki sumber daya yang terbatas. Penelitian serupa juga pernah dilakukan oleh Freddy K Santoso dan Nicholas C H Vun pada tahun 2015, hanya saja penelitian ini mengimplementasikan sistem enkripsi pada bagian *gateway*. Semoga dalam penelitian ini, sistem keamanan pada *smart home* dapat lebih terlindungi dari ancaman penyerang pada jaringan lokal.

Secara umum algoritma kriptografi kurva eliptik terdiri dari 2 algoritma, yaitu *Elliptic Curve Diffie Hellman Key Exchange* (ECDH) dan *Elliptic Curve Digital Signature Algorithm* (ECDSA) (Dhillon, 2016). Semakin berkembangnya algoritma *Diffie-Hellman* beberapa peneliti banyak mengajukan skema enkripsi diantaranya yaitu skema enkripsi pada ECC. Terdapat beberapa skema sistem enkripsi pada ECC yaitu terdiri dari *Early Cryptosystems* dan *Hybrid Cryptosystems* (Martínez, Álvarez, & Encinas, n.d.). *Early Cryptosystems* pada ECC setara dengan sistem kripto pada ElGamal (Elgamal, 1985) dan Menezes-Vanstone sistem kripto (Menezes & Vanstone, 1993). Perbedaan dari kedua sistem kripto tersebut, yaitu pada ElGamal pesan terenkripsi harus di gambarkan sebagai titik *elliptic curve* sedangkan Menezes-Vanstone menggambarkan pesan sebagai pasangan $\mathbb{F}^* x\, \mathbb{F}^*$ dimana $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. Kedua sistem kripto tersebut memiliki kelemahan yaitu semakin besar pesan tersebut di enkripsi semakin lemah performa nya dibandingkan dengan algoritma enkripsi simetrik seperti AES (Martínez et al., n.d.). Sehingga pada tahun 1998 Klaus Kiefer menganggap sistem kripto tersebut tidak aman untuk digunakan (Kiefer, Saarlandes, & Informatik, n.d.).

Akibat dari kelemahan *early cryptosystems* pada ECC beberapa komunitas akademik melakukan riset bertahun-tahun sehingga lahir *hybrid cryptosystem* yang

memiliki karakteristik kedua kriptografi simetrik dan asimetrik. Skema *Hybrid* yang terpenting pada ECC yaitu *Elliptic Curve Integrated Encrpytion Scheme* (ECIES), *Provably Secure Elliptic Curve Encryption Scheme* (PSEC) dan *Advanced Cryptographic Engine* (ACE). Dari ketiga skema *hybrid*, ECIES tersedia dalam beberapa standar seperti ANSI X9.63, IEEE 1363rc, ISO/IEC 18033-2 dan SECG SEC 1 dan ECIES menawarkan serangkaian fitur terbaik, memberikan hasil yang aman dan fleksibel untuk enkripsi data (Martínez et al., n.d.)

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka yang menjadi rumusan masalah sebagai berikut:

1. Bagaimana cara kerja perangkat lunak sistem enkripsi pada perangkat *IoT* dengan menggunakan algoritma ECIES bekerja.
2. Bagaimana kompleksitas *randomness* ECIES sebagai sistem enkripsi pada perangkat IoT.
3. Bagaimana data *confidentiality* dan *integrity* setelah dilakukan proses enkripsi dengan metode ECIES

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Memberikan gambaran cara kerja sistem enkripsi dengan menggunakan algoritma ECIES bekerja mengamankan data pada perangkat *IoT*.
2. Menghitung kompleksitas *randomness* sistem enkripsi data dengan menggunakan algoritma ECIES pada perangkat *IoT*.
3. Memberikan hasil data *privacy* dan *integrity* setelah dilakukan proses enkripsi dengan menggunakan metode ECIES

1.4 Batasan Masalah

Batasan masalah yang akan dikaji pada penelitian ini adalah:

1. Pesan yang akan di enkripsi berbentuk blok teks.
2. Menggunakan metode *Elliptic Curve Integrated Encryption Scheme*.
3. Algoritma Enkripsi Simetrik yang digunakan AES-128-CBC.
4. Kurva Eliptik yang digunakan secp256k1.
5. Algoritma Hash yang digunakan SHA-256.

1.5 Manfaat Penelitian

Dari pembuatan skripsi ini diharapkan adanya manfaat agar penggunaan perangkat IoT pada *Smart Home* memiliki keamanan yang lebih baik dan lebih hemat energi.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan skripsi ini adalah sebagai berikut:

1.6.1 Metodologi Pengumpulan Data

Metode pengumpulan data yang digunakan adalah studi pustaka. Pengumpulan data dengan cara mengumpulkan beberapa literatur, *browsing* internet dan buku yang berkaitan dengan *Smart Home*, keamanan data, algoritma ECC dan *Internet of Things*.

1.6.2 Analisis dan Desain Sistem

Metode analisis dan desain sistem dimulai dengan menentukan keperluan dan batasan untuk sistem *Smart Home*, pengumpulan materi dari algoritma ECC, menentukan bahasa pemrograman pada perangkat IoT, membuat desain infrastruktur sistem *Smart Home* dan skema sistem enkripsi.

1.6.3 Metode Pembuatan Sistem Enkripsi *Smart Home*

Metode analisis data yang digunakan dalam pembuatan perangkat lunak adalah *waterfall*, dengan rincian sebagai berikut:

1. Penentuan Algoritma Sistem Enkripsi

   Penentuan algoritma sistem enkripsi dalam penelitian ini dimulai dengan mengumpulkan materi algoritma-algoritma yang memiliki karakteristik dan sesuai untuk perangkat IoT yang dipakai.

2. Coding

   Tahap melakukan penambahan kode pemrograman dalam hal ini Arduino, sehingga dapat menjalankan seluruh fungsi yang diharapkan dalam pembuatan perangkat lunak *Smart Home* sesuai dengan desain antarmuka yang telah dikerjakan dari tahap sebelumnya.

3. Testing

   Tahap melakukan pengujian terhadap perangkat lunak *Smart Home* yang telah dibuat agar dapat berjalan sesuai dengan yang diinginkan.

4. Kesimpulan

Tahap mengumpulkan data dari hasil testing sistem enkripsi *Smart Home* yang telah berjalan. Dan memberikan hasil akhir dari pengumpulan data tersebut berdasarkan pada rumusan masalah yang telah dibuat.

1.7 Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan. Dalam hal ini menguraikan tentang masalah yang muncul dari penggunaan Sistem *Smart Home* dan bagaimana cara mengamankan data yang ada pada *Smar Home*.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan beberapa teori yang mendukung dalam pembuatan sistem *Smart Home* seperti teori *Internet of Things, Smart Home,* Kriptografi, Kriptografi Kunci Publik, Sistem Enkripsi, Algoritma ECC, Platform Arduino dan Gambaran Aplikasi Sistem Enkripsi *Smart Home*.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari implementasi Algoritma ECC untuk Sistem Enkripsi *Smart Home*. Mencakup analisis, dan desain model sistem.

BAB IV IMPLEMENTASI

Pada bab ini akan dibahas secara mendalam hal-hal yang akan menjawab apa yang sudah dirumuskan dalam rumusan masalah. Dalam hal ini mengenai implementasi pembuatan perangkat lunak *Smart Home* yang telah dilengkapi sistem enkripsi secara detil termasuk tampilan antar muka dan pengujian perangkat lunak yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari BAB IV dan saran yang diajukan agar dapat menjadi bahan pertimbangan untuk rekomendasi penelitian selanjutnya.