BAB I
PENDAHULUAN

1.1 Latar Belakang

Menurut [1] *Unmanned Aerial Vehicle* atau dikenal juga dengan singkatan UAV, merupakan salah satu wahana tanpa awak di udara yang dapat terbang menggunakan gaya aerodinamik untuk menghasilkan gaya angkat (*lift*), serta dapat terbang secara *autonomous* atau dioperasikan dengan radio kontrol merupakan definisi dari *Unmanned Aerial Vehicle* (UAV). Pada awalnya UAV difungsikan sebagai pengawasan militer. Beberapa tahun terakhir UAV memberikan banyak manfaat di sektor-sektor tertentu seperti industri kreatif, pertanian, medis, pemasaran dan tren ini akan berlanjut sampai beberapa dekade mendatang [2]. Selain itu, UAV juga dipakai untuk *High Altitude Platforms* (HAPs) [3], [4]. Meskipun begitu, UAV hanya mampu terbang dengan jarak ± 5 km jika menggunakan *flight controller* yang ditambahkan dengan telemetri 433 MHz dan antena yagi pada *Ground Control Station* [5]. Sedangkan *flight controller* dengan telemetri 2,4 GHz dan antena *cloverleaf* hanya mampu terbang dengan jarak $\pm 1{,}66$ km [6]. Hal ini karena jarak terbang UAV dipengaruhi oleh besar penguatan dan jenis antena yang digunakan. Sebenarnya, UAV lebih baik menggunakan internet dalam pengoperasiannya, mengingat internet pada masa ini menjadi *trend* karena kemudahan untuk mengaksesnya. Dengan membuat UAV berbasis *Internet of Things* (IoT), memungkinkan UAV memiliki cakupam area yang luas sehingga *user* dapat mengoperasikannya tanpa terikat jarak yang terbatas [7].

Suatu konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara kontinyu serta dapat menghubungkan mesin, peralatan dan benda fisik lainnya sehingga memungkinkan untuk berkolaborasi sesuai informasi baru yang diperoleh secara independen adalah pengertian dari IoT [8]. Dengan memanfaatkan kode program, dimana setiap perintah argumen menghasilkan interaksi antar mesin yang terhubung secara otomatis tanpa campur tangan manusia dan dalam jarak berapapun. Pada dasarnya internet yang menjadi penghubung diantara interaksi mesin dan manusia hanya bertugas sebagai pengatur serta

pengawas beroperasinya alat tersebut [9]. Seiring dengan berkembangnya kebutuhan layanan data, IoT juga masuk ke *massive machine-type communication* (mMTC) dari implementasi teknologi generasi kelima (5G) [10], [11].

Dengan terkoneksinya alat pada internet, peluang terjadinya ancaman terhadap pengubahan dan pencurian data semakin besar. Karena sebuah aplikasi yang melintas pada jaringan publik seperti internet diasumsikan dapat diakses oleh siapapun, termasuk oknum-oknum yang berniat mengubah atau mencuri data tersebut [12]. UAV juga dianggap rentan terkait dengan masalah keamanan, terutama pada berbagai jenis serangan *cyber*. Seperti pada kasus [13], yang mengarah pada intersepsi lalu lintas data yang terhubung ke *Wireless Fidelity* (Wi-Fi). Dengan demikian, penyerang dapat menangkap informasi sensitif pengguna. Pembajakan UAV lain dengan menghubungkan perangkat Raspberry Pi ke *drone* dan memprogramnya untuk mencegat dan membajak UAV terdekat [14]. Faktanya, serangan UAV bisa mengubah input sensor UAV yang dapat ditargetkan dan dieksploitasi oleh penyerang [15]. Oleh karena itu, untuk melindungi data perlu adanya proteksi yang berguna untuk mengubah data menjadi karakter acak dan hanya ditujukan kepada orang yang memiliki sebuah kunci untuk mengubahnya kembali, sehingga data pada saat transmisi terlindung dari aktivitas pengubahan atau pencurian oleh pihak yang tidak berwenang [16].

Oleh karena itu, kami membuat proyek tugas akhir [17]-[19], *Control and monitoring unmanned aerial vehicle using internet of things web based* (TRUSTED) dimana UAV dapat dikendalikan dan dipantau secara bersamaan dari jarak jauh, yang dilengkapi dengan sensor dan transduser. Produk TRUSTED mempunyai 3 subsistem yaitu kendali [18], pengamanan data dan *website* [19]. Kemudian metode pengendalian dan pemantauan juga dapat dilakukan secara praktis menggunakan *mobile web* [19]. Buku Tugas Akhir (TA) ini adalah bagian dari subsistem pengamanan data, bertujuan untuk merancang dan mengimplementasikan sistem keamanan berbasis IoT pada produk TRUSTED dengan menggunakan metode algoritma keamanan yang handal yaitu algoritma *Advanced Encryption Standard* panjang kunci 128 bit dengan *Cipher Block Chaining* (AES-128-CBC).

Algoritma dengan metode ini dipilih karena memiliki tingkat pengamanan yang tinggi dan belum adanya *cryptanalysis* yang berhasil meretasnya [20]. AES sulit untuk dipecahkan oleh komputer kuantum yang dianggap *quantum-safe*, terutama AES-256 karena *cipher*-nya bisa beradaptasi untuk serangan kuantum dengan meningkatkan ukuran kuncinya untuk memperbaiki kerentanan yang diperkenalkan oleh komputasi kuantum [21]. Supremasi kuantum yang dilakukan oleh google dengan komputer kuantum menyelesaikan tugas dalam 200 detik, sedangkan jika dibandingkan super komputer dibutuhkan waktu 10.000 tahun untuk melakukan perhitungan sama [22]. Walaupun begitu tetap saja berdasarkan analisa bahwa komputer kuantum sulit untuk membobol AES [21]. Namun tidak menutup kemungkinan di masa yang akan datang, algoritma ini akan bisa diretas oleh komputer kuantum [23], tapi sejauh yang kami tahu belum ada yang berhasil meretasnya.

1.2 *Related Work*

[24] pada tahun 2019 telah melakukan penelitian implementasi kriptografi *Advanced Encryption Standard* bit 128 (AES-128) pada UAV dan *Ground Control System* (GCS). Pengujian dilakukan menggunakan dua metode, yaitu dengan menggunakan metode *man-in-the-middle attack* dan metode *brute-force attack.* Pada pengujian menggunakan metode *man-in-the-middle attack*, data berhasil didapatkan oleh penyerang akan tetapi tidak dapat terbaca karena data berupa *ciphertext*. Sedangkan pada pengujian menggunakan *brute-force attack*, sangat tidak memungkinkan untuk melakukan *cracking* sebuah kunci AES-128 sampai ditemukan super komputer yang lebih cepat dari 10.51×10^{15} *flops*. Dengan demikian, dapat disimpulkan bahwa AES-128 dapat diterapkan pada komunikasi antara UAV dan GCS yang menjadi proteksi saat pengiriman data berlangsung.

Oktario pada tahun 2020 [25] telah melakukan penelitian terkait kriptografi portable yang dapat mengamankan data pada jaringan komunikasi Wi-Fi dari perilaku *sniffing*. Penelitian ini mengamankan data dalam komunikasi Wi-Fi dengan menggunakan metode kriptografi AES. Pengujian sistem konfigurasi telah berhasil mengirimkan data konfigurasi ke perangkat dan menyimpannya pada *electrically erasable programmable read-only memory* (EEPROM) perangkat

sistem. Hasil penelitian menunjukkan bahwa penggunaan sistem pada jarak 4 m, 10 m dan 20 m, dapat menerima pesan berupa *ciphertext* dari perangkat pemancar dengan waktu pengiriman data masing-masing sebesar 118.067 μs, 119.467 μs dan 123.533 μs.

Dari pemaparan diatas, dapat dikatakan bahwa AES-128 memiliki beberapa kelebihan dibandingkan dengan AES-192 dan AES-256. Algoritma AES-128 mempunyai ukuran data yang lebih kecil sehingga kecepatan waktu pada saat transmisi yang lebih tinggi. AES-128 juga cukup baik sebagai proteksi saat melakukan transmisi data karena belum adanya *cryptanalysis* yang berhasil meretas AES [20]. Pada penelitian ini penulis mengimplementasikan sistem pengaman data pada UAV dengan menggunakan metode kriptografi AES-128. Komunikasi melibatkan *flight controller* dan *website* yang dilakukan secara dua arah, yaitu data pemantauan yang dikirim dari *flight controller* menuju *website* dan data kendali yang dikirim dari *website* menuju *flight controller*. Selain itu, keberhasilan pada alat kami yaitu sistem yang bekerja dengan baik mengirimkan data dan mempunyai tingkat keberhasilan yang tinggi namun memerlukan perbaikan peningkatan terhadap waktu ketika transmisi berlangsung di penelitian mendatang agar lebih cepat. Tambahan lagi, untuk implementasi dipenelitian mendatang, mikrokontroler yang digunakan modul nirkabel ESP NodeMCU karena dapat secara langsung menggantikan Arduino dan mendukung koneksi Wi-Fi sekaligus agar dapat mempercepat waktu transmisi. Demikian, kami harapkan penelitian ini dapat memberikan kontribusi untuk masyarakat dan ilmu pengetahuan dalam pengembangan teknologi UAV secara mandiri di Sumatra, Indonesia dan dunia.

1.3 Tujuan Perancangan

Dalam penyusunan tugas akhir ini, penulis mempunyai tujuan utama yaitu merancang dan mengimplementasikan sistem keamanan berbasis IoT pada pengendalian serta pemantauan UAV. Kemudian penulis melakukan pengujian terhadap performa alat seperti menghitung waktu proses enkripsi dan dekripsi, mengambil data pada saat pengiriman berlangsung dengan bantuan *Network Analyzer Software*, lalu melihat validitas data yang ditransmisikan.

1.4 Ruang Lingkup

Tugas akhir ini melingkupi spesifikasi sebagai berikut:

a) Aplikasi ini dibangun pada sisi *software* berbasis *website*.

b) Data masukan dikirimkan dari data simulasi UAV.

c) Implementasi pada jaringan Wi-Fi 2,4 GHz [26].

Implementasi enkripsi AES-128-CBC menggunakan *library* yang telah ada pada Arduino *Integrated Development Environment* (IDE).