IMPLEMENTASI KRIPTOGRAFI AES-128 PADA UNMANNED AERIAL VECHILE DAN GROUND CONTROL SYSTEM

Farhan Syafaat[1], Alif Finandhita[2]

[1,2] Teknik Informatika – Universitas Komputer Indonesia
Jalan Dipatiukur 112-116 Bandung
E-mail : farhan.syafaat@email.unikom.ac.id[1], alif.finandhita@email.unikom.ac.id[2]

ABSTRAK

Unmanned Aerial Vehicle (UAV) merupakan sistem tanpa awak (*Unmanned System*), yaitu sistem berbasis elektro-mekanik yang dapat melakukan misi-misi terprogram. UAV membutuhkan *Ground Control System* (GCS). Dalam operasional UAV tugas GCS adalah sebagai stasiun monitoring dan komando dimana operator di darat dapat mengirimkan perintah misi dan mengawasi jalannya misi tersebut dan kondisi UAV selama di udara. Berdasarkan hasil dari penelitian memebuktikan bahwa UAV profesional sekalipun masih bisa dilakukan serangan berupa *Man-in-the-Middle*. Sehingga data yang dikirimkan dapat terbaca oleh penyerang, maka dari itu diperlukan enkripsi *Advanced Encryption Standard* (AES-128) pada data yang dikirimkan UAV dan diterima oleh GCS. AES-128 dipilih karena memiliki tingkat pemrosesan kecepatan lebih cepat dibanding kriptografi AES lainya dan belum adanya *cryptanalysis* yang berhasil meretas AES-128. Enkripsi lapisan aplikasi dipilih karena lebih mudah digunakan dan lebih hemat biaya daripada enkripsi perangkat keras dalam berbagai kasus. Hasil dan kesimpulan bahwa dapat diterapkanya kriptografi AES-128bit pada komunikasi antara UAV dan GCS sehingga penyerangan yang dilakukan tidak dapat membaca data yang dikirimkan.

Kata kunci : *Unmanned Aerial Vehicle* (UAV), *Ground Control System* (GCS), Kriptografi, *Advanced Encryption Standard* (AES), *Man-in-the-Middle*.

1. PENDAHULUAN

Dalam empat tahun terakhir, berbagai jenis piranti tanpa awak telah digunakan oleh kalangan sipil dan ilmiah. Piranti tersebut dilengkapi dengan berbagai macam peralatan untuk memberikan data dalam berbagai aplikasi[1]. Pesawat tanpa awak atau *Unmanned Aerial Vehicle* (UAV) yang berkembang pesat untuk aplikasi penginderaan penglihatan jarak jauh, UAV merupakan sistem tanpa awak (*Unmanned System*), yaitu sistem berbasis elektro-mekanik yang dapat melakukan misi-misi terprogram[2]. Pada dasarnya meskipun mempunyai kemampuan *autonomous*, UAV tetap membutuhkan *Ground Control System* (GCS). Dalam operasional UAV tugas GCS adalah sebagai stasiun monitoring dan komando dimana operator di darat dapat mengirimkan perintah misi dan mengawasi jalannya misi tersebut dan kondisi UAV selama di udara [3].

UAV dengan GCS dapat berkomunikasi 2 arah dan saling mengirimkan data melalui telemetri. Berdasarkan hasil dari penelitian memebuktikan bahwa UAV profesional sekalipun masih bisa dilakukan serangan berupa *Man-in-the-Middle* (MitM), penulis memberikan dua solusi dapat digunakan: (1) enkripsi *on-board* XBee 868LP, adalah satu-satunya solusi yang juga mengurangi risiko *Remote AT Commands*, dan (2) enkripsi lapisan aplikasi. Sehingga diperlukan enkripsi pada data yang dikrimkan dan diterima oleh GCS[4].

Sulitnya mendapatkan *hardware* yang menanamkan enkripsi yang dijual bebas dipasaran dan dengan berbagai pertimbangan maka enkripsi ditingkat lapisan aplikasi dipilih. Enkripsi lapisan aplikasi lebih mudah digunakan dan lebih hemat biaya daripada enkripsi perangkat keras dalam berbagai kasus. Secara khusus, ketika layanan enkripsi baru diperlukan untuk lingkungan komputasi yang sudah digunakan, enkripsi lapisan aplikasi lebih cocok daripada perangkat keras[5].

Penelitian sebelumnya terkait keamanan UAV dan GCS adalah pengamanan data antara UAV dan GCS pernah dilakukan dengan berbasis *One Time Pad*[6]. Otentikasi komunikasi UAV menggunakan *Caesar Cipher Cryptography* telah dirancang dan disimulasikan. Sistem telah menjalani tes awal, simulasi dan hasilnya memuaskan[7]. Kombinasi keamanan UAV dilakukan dengan pembangkit kunci ChaCha sebagai stream chipper dan menggunakan otentikasi algoritma Poly1305[8]. Pengamanan antara *Micro Air Vehicle* (MAV) dan GCS menerapkan skema Advanced Encryption Standard (AES) pada mode CTR untuk enkripsi, SHA-256 untuk hashing kunci dan *Diffie Hellman* untuk pertukaran kunci pengiriman data dengan menggunakan MAVLink protocol[9]. Dalam penelitian yang dilakukan penulis tentang penerapan kriptografi AES pada UAV dan GCS berkontribusi untuk membuat algoritma kunci yang hanya diketahui oleh pihak terkait dengan pengiriman data menggunakan radio frekuensi.

Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Saat ini, AES merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh *National Institute of Standard and Technology* (NIST). Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, mengetahui bahwa mode CBC jauh lebih baik dari mode ECB dalam hal perlindungan[10]. Hasil penelitian untuk mengenkripsi dan dekripsi semua jenis file dengan algoritma AES-256, hasil dari penelitian menunjukkan bahwa algoritma AES dengan panjang kunci 256 bit dapat menyandikan isi suatu file sehingga dapat mengamankan file tersebut[11], enkripsi AES dapat mengamankan file multimedia, gambar bitmap, maupun file lainya[12][13][14]. Penelitian selanjutnya dijelaskan bahwa penggunaan MD5 pada enkripsi SSO masih bisa dapat diretas, sedangkan jika diterapkan menggunakan AES dengan kata kunci dinamis, maka SSO tidak dapat diretas[15], penelitian berikutnya dapat mengamankan E-diploma dengan menggunakan *digital signature autentication*[16]. Dengan demikian dapat disimpulkan bawah algoritma AES dapat mengamankan semua jenis file.

AES dengan panjang kunci 128 bit (AES-128) memiliki beberapa kelebihan dibandingkan dengan variasi kunci 192 bit dan 256 bit. Salah satunya adalah memiliki waktu proses yang paling cepat yaitu 110.78 ns[17]. Untuk melakukan *cracking* dengan menggunakan *brute force attack* pada AES-128 dibutuhkan waktu 〖1,02 x 10〗^18 Tahun[18]. Enkripsi AES dengan panjang kunci 128 bit cukup baik untuk dilakukan sebagai mana belum adanya *cryptanalysis* yang berhasil meretas AES[19].

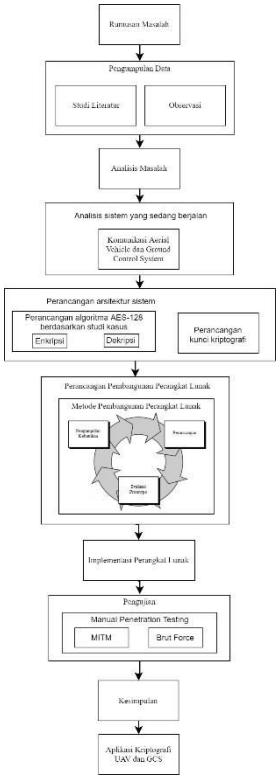
Berdasarkan pemaparan latar belakang penelitian di atas bahwa UAV profesional sekalipun jika tanpa penerapan kriptografi maka dapat dilakukan penyerangan dan dari penelitian sebelumnya mengenai penerapan algoritma kriptografi yang diterapkan pada UAV dan GCS belum pernah diterapka kriptografi AES-128. Penulis mengambil tema tentang keamanan sistem pada *Unmanned Aerial Vehicle* (UAV) dan *Ground Control System* (GCS) dengan judul "Implementasi Kriptografi AES pada *Unmanned Aerial Vehicle* dan *Ground Control System*" sebagai aplikasi yang akan melakukan enkripsi dan dekripsi pada pengiriman data antara UAV dan GCS.

1.1 Maksud dan Tujuan Penelitian

Maksud dari penulisan penelitian ini adalah untuk membangun aplikasi enkripsi dan dekripsi data antara UAV dan GCS menggunakan algoritma AES-128. Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah membuat data yang dikirimkan *Unmanned Aerial Vehicle* ke *Ground Control System* tidak dapat terbaca oleh penyerang.

1.2 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penilitian ini terbagi menjadi beberapa tahapan. Seperti yang ditampilkan pada gambar 1, yaitu sebagai berikut.



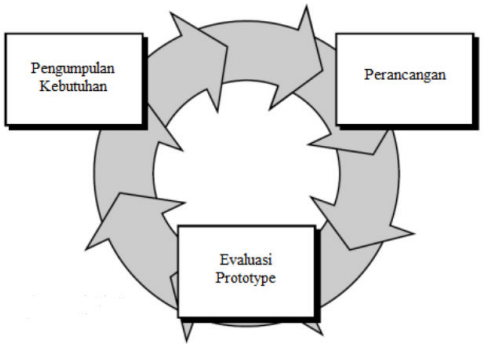
Gambar Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**1.** Metodologi Penelitian

Keterangan langkah-langkah dari metodologi penelitian yang terdapat pada gambar 1 adalah sebagai berikut:

1. Rumusan Masalah: Rumusan masalah adalah kalimat singkat berupa pertanyaan terhadap keberadaan variabel mandiri baik hanya satu variabel maupun lebih, rumusan masalah digunakan untuk menjelaskan masalah atau isu yang sedang diteliti.
2. Pengumpulan Data: Metode pengumpulan data yang dilakukan pada penelitian ini dilakukan dengan studi literatur dan observasi.
3. Analisis Masalah: Hasil dari rumusan masalah dan pengumpulan data menghasilkan analisis masalah, masalah dapat tervalidasi untuk dilakukan penelitian.
4. Analisis Sistem yang Sedang Berjalan: Pada tahapan ini, sistem yang berjalan perlu di analisis untuk evaluasi dari sistem baru yang akan dibuat.
5. Perancangan Arsitektur Sistem: Pada tahapan ini sudah terlihat arsitektur sistem yang baru, yang

akan diterapkan pada UAV dan GCS. Arsitektur sistem akan membahas proses bisnis yang baru.

6. Perancangan Perangkat Lunak: Perancangan perangkat lunak adalah suatu proses bertahap dimana semua kebutuhan atau persyaratan yang ada pada dokumen diterjemahkan menjadi suatu cetak blue (blue print) yang akan digunakan untuk membangun perangkat lunak dan memenuhi kebutuhan yang sesuai.
7. Metode Pembangunan Perangkat Lunak: Metode pembangunan perangkat lunak menggunakan paradigma perangkat lunak secara *prototype*. Alur dari metode *prototype* bisa di lihat pada Gambar 2 untuk penjelasan dari setiap alur metode *prototype* adalah sebagai berikut[20]:



Gambar 2. Model Prototype

Pengumpulan Kebutuhan - Pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper* dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

Perancangan - Perancangan dilakukan cepat dan rancangan mewakili semua aspek *software* yang diketahui. Rancangan ini akan menjadi dasar pembuatan *prototype*.

Evaluasi Prototype -Pengujian terhadap software yang dibuat dan digunakan untuk memperjelas kebutuhan *software*.

8. Implementasi Perangkat Lunak: Suatu proses pengubahan spesifikasi sistem menjadi sistem yang dapat dijalankan untuk dapat dilakukan pengujian.
9. Pengujian: Pengujian yang digunakan adalah *Manual penetration testing* yaitu pengujian penetrasi yang dilakukan oleh manusia. Dalam jenis pengujian ini, kerentanan dan resiko suatu mesin diuji oleh seorang ahli di bidangnya[21].

   Secara umum, teknisi pengujian melakukan metode berikut :

   Data Collection − *Data collection* memiliki peran penting untuk pengujian. Seseorang dapat mengumpulkan data secara manual atau dapat menggunakan layanan alat / *software* (seperti teknik analisis kode sumber halaman web, *man-in-the-middle attack,* dll.).

   Vulnerability Assessment −Setelah data dikumpulkan,selanjutnya penguji untuk mengidentifikasi kelemahan keamanan dan mengambil langkah-langkah pencegahan yang sesuai.

   Actual Exploit − adalah metode khas yang digunakan oleh penguji ahli untuk melakukan serangan pada sistem target dan juga, mengurangi risiko serangan. Dalam penelitian ini menggunakan *brute force attack*.

   Report Preparation − Setelah penetrasi dilakukan, tenaga ahli menyiapkan laporan akhir yang menjelaskan segala sesuatu tentang sistem. Akhirnya laporan dianalisis untuk mengambil langkah korektif untuk melindungi sistem target.
10. Kesimpulan: Kesimpulan adalah pernyataan singkat tentang hasil analisis deskripsi dan pembahasan tentang isi dari penelitian, kesimpulan berisikan fakta-fakta jawaban dari pertanyaan yang ada di rumusan masalah pernelitian.

2. ISI PENELITIAN

2.1 Unmanned Aerial Vehicle (UAV)

UAV adalah kependekan dari Unmanned Aerial Vehicle, yang merupakan pesawat tanpa pilot. UAV dapat berupa pesawat yang dikendalikan dari jarak jauh misal diterbangkan oleh pilot di stasiun pengendali darat(GCS) atau dapat terbang secara mandiri berdasarkan rencana penerbangan yang diprogram sebelumnya atau sistem otomasi dinamis yang lebih kompleks[22].

2.2 Ground Control System (GCS)

Gorund Control System dibuat untuk mengntrol dan memantau penerbangan, serta menerima visualisasi dan perekaman gambar selama penerbangan secara realtime. Gorund control system kompatibel dengan berbagai jenis UAV[23].

2.3 Communication System (CS)

Sistem Komunikasi atau Communication System (CS) terdiri dari sistem modul radio dengan antena pada gain yang diinginkan (2 dBi, 10 dBi, 30 dBi) dan frekuensi (900-922MHz, 2,4 GHz, 1,3 GHz) melalui komunikasi serial. Radio Receiver adalah bagian dasar terdapat pada ground. Sistem bisa berupa komunikasi satu arah atau dua arah yang menerima sinyal dari pesawat(UAV) ke darat(GCS)[24].

2.4 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi, dan autentifikasi data[25].

Kriptografi hanya memenuhi empat aspek dalam keamanan informasi yang merupakan tujuan dari kriptografi yaitu kerahasiaan (*confidentiality*), integritas data (*integrity*), otentikasi data (*authentication*), dan *non-repudiation*[26].

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun

kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi. Kriptografi memenuhi aspek kerahasiaan karena informasi tidak dapat secara langsung diketahui.

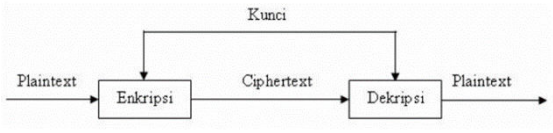
2. Integritas data adalah layanan yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan mensubstitusi data lain ke dalam data yang sebenarnya.
3. Otentikasi adalah layanan yang berhubungan dengan identifikasi/ pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui jaringan harus diotentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Untuk alasan ini aspek kriptografi biasanya dibagi menjadi dua kelas utama yaitu otentikasi entitas dan otentikasi data asal.
4. Non-repudiation adalah layanan yang mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan ataumembuat. Sebagai contoh, satu entitas dapat mengijinkan pembelian properti oleh entitas lain dan kemudian berusaha menyangkal otorisasi tersebut diberikan. Sebuah prosedur yang melibatkan pihak ketiga yang terpercaya diperlukan untuk menyelesaikan sengketa tersebut.

2.5 Algoritma Kriptografi

Algoritma kriptografi yang handal adalah algoritma kriptografi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. Berdasarkan jenis kuncinya, algoritma kriptografi dibagi menjadi dua jenis yaitu algoritma simetris dan algoritma asimetris[26].

2.5.1 Algoritma Kunci Simetris

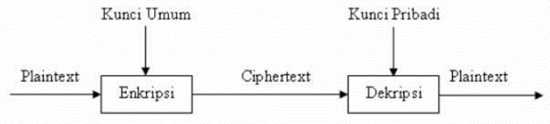
Algoritma Kunci simetris (*symmetric key algorithm*) adalah suatu algoritma di mana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*[26].



Gambar 3. Ilustrasi Kriptografi Dengan Kunci Simetris.

2.5.2 Algoritma Kunci Asimetris

Algoritma kunci asimetris (*asymmetric key algorithm*) adalah suatu algoritma di mana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi[26].



Gambar 4. Ilustrasi Kriptografi Dengan Kunci Asimetris.

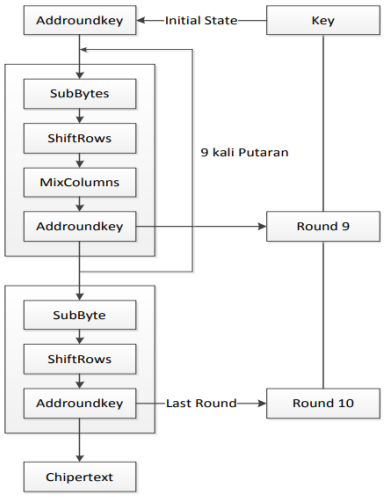
2.6 Advanced Encryption Standard (AES)

Advanced Encryption Standard adalah cipher blok simetris yang bisa memproses blok data 128 bit, menggunakan kunci sandi dengan panjang 128, 192, dan 256 bit. Algoritma AES dapat digunakan dengan tiga panjang kunci yang berbeda yang ditunjukkan di atas, dan oleh karena itu "kunci" yang berbeda ini dapat disebut sebagai "AES-128", "AES-192", dan "AES-256".

Setiap state akan mengalami proses yang terdiri dari empat tahap yaitu, *Add Round Key, Sub Bytes, Shift Rows, dan Mix Columns*. Kecuali pada tahap *Mix Columns*, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap *Mix Columns* tidak akan dilakukan pada tahap terakhir[27].

2.6.1 Proses Enkripsi Algoritma AES

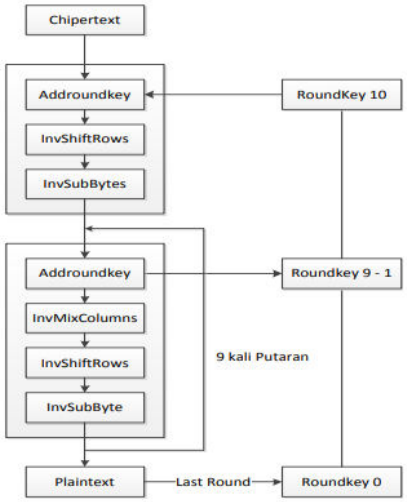
Proses enkripsi algoritma AES terdiri atas empat jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah dikopikan ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Selanjutnya, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses tersebut dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir berbeda dengan *round* sebelumnya di mana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns*[28]. Gambar 2.3 merupakan langkah-langkah proses enkripsi AES.



Gambar 5. Proses enkripsi algoritma AES.

2.6.2 Proses Dekripsi Algoritma AES

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*[28]. Gambar 6 merupakan langkah-langkah proses dekripsi AES.



Gambar 6. Proses dekripsi algoritma AES.

2.7 Sensor pada UAV

1. *Gyroscope* adalah perangkat untuk mengukur atau mempertahankan orientasi, dengan prinsip ketetapan momentum sudut, alat ini bekerja sama dengan accelerometer. Mekanismenya adalah sebuah roda berputar dengan piringan didalamya yang tetap stabil. Alat ini sering digunakan pada robot atau drone serta alat-alat canggih lainnya.
2. *Magnetometer* adalah sensor yang bekerja atas dasar pendeteksian gaya magnet bumi.Salah satu kegunaan dari magnetometer adalah untuk menentukan arah mata angin.Sensor magnetik mengukur medan magnet. Dengan menghitung sudut medan magnet bumi yang terdeteksi, dan membandingkan sudut pengukuran dengan gravitasi yang diukur dengan accelerometer, dapat memungkinkan untuk mengukur arah perangkat berkenaan dengan Utara dengan tingkat akurasi yang tinggi.
3. *Accelerometer* mengukur akselerasi, yang meliputi komponen akselerasi dengan gerak perangkat dan akselerasi akibat gravitasi. Accelerometer juga tersedia dengan sumbu tunggal, ganda atau tiga, yang didefinisikan dalam sistem koordinat X, Y, Z. Periode gerakan kompleks perangkat dapat menyebabkan perhitungan orientasi menjadi sulit, terutama selama gerak cepat dan kompleks, di mana sinyal mencakup penjumlahan percepatan linear, percepatan sentripetal, dan gravitasi.

2.8 Analisis Masalah

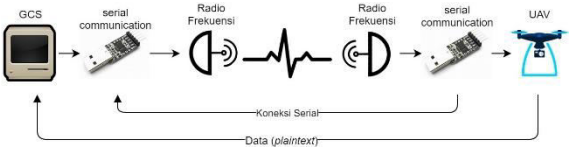
Analisis Masalah merupakan langkah pertama dari analisis sistem. Langkah ini diperlukan untuk mengetahui permasalahan yang sedang terjadi di sistem yang sedang berjalan. Berikut adalah titik dari permasalahan dalam penelitian ini, yaitu data yang dikirmkan UAV ketika belum diterapkannya kriptografi data dapat terbaca oleh penyerang karena masih berbentuk *plaintext,* maka perlunya diterapkan kriptografi untuk mengamankan data dari pembacaan penyerangan.

2.9 Analisis Sistem yang Sedang Berjalan

Analisa sistem yang sedang berjalan antara UAV dan GCS, bertujuan untuk mengetahui lebih jelas bagaimana cara kerja sistem tersebut. Dari urutan kejadian tersebut dapat dibuat ilustrasi.

2.9.1 Analisis Pengiriman Data Unmanned Aerial Vehicle dan Ground Control System

Dalam pengiriman data tidak memiliki protokol dikarenakan media komunikasi menggunakan radio frekuensi untuk mengirimkan data secara *realtime*.



Gambar 7. Proses dekripsi algoritma AES.

Gambar 7 diatas menjelaskan bagaimana proses komunkasi data dapat berlangsung antara UAV dan GCS. Dimana UAV dan GCS menggunakan radio frekuensi yang memiliki frekuensi yang sama. Terlebih dahulu GCS membuka koneksi serial setelah itu UAV melakukan *booting* secara otomatis akan membuka koneksi serial, setalah terkoneksi maka secara otomatis UAV dapat mengirimkan data-data kepada GCS.

2.9.2 Analisis Data Sensor yang Dikirimkan

Data yang didapatkan oleh sensor yang berada pada UAV akan ditransmisikan dan diterima oleh GCS. Berikut adalah tabel 1 hasil dari pengamatan data yang dikirimkan UAV ke GCS.

Tabel 1. Tabel data sensor

No.	*Gyroscope*			*Magnetometer*			*Accelerometer*		
	xgyro	ygyro	zgyro	roll	pitch	yaw	xacc	yacc	zacc
1.	-1	0	0	-0.006028093	-0.003806141	0.1218428	-2	20	-1001
2.	0	1	0	-0.00604068	-0.003788484	0.1216723	-4	20	-997
3.	0	0	-1	-0.00609304	-0.003684698	0.1214509	-3	22	-998
4.	0	1	0	-0.00606191	-0.003721761	0.121368	0	21	-1001
5.	-2	0	0	-0.005961491	-0.003736289	0.1212841	-2	23	-997

2.10 Analisis Plain Text

Dari tabel data sensor, maka dapat menganalisis *plaintext* yang akan digunakan sebagai masukan untuk sistem. Berikut adalah data *plaintext*:

Tabel 2. Tabel data plaintext

Iterasi	*Plaintext*
1.	-1|0|0|-0.006028093|-0.003806141|0.1218428|-2|20|-1001
2.	0|1|0|-0.00604068|-0.003788484|0.1216723|-4|20|-997
3.	0|0|-1|-0.00609304|-0.003684698|0.1214509|-3|22|-998
4.	0|1|0|-0.00606191|-0.003721761|0.121368|0|21|-1001
5.	-2|0|0|-0.005961491|-0.003736289|0.1212841|-2|23|-997

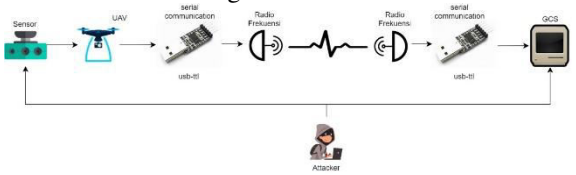
2.11 Analisis Drone

Jenis UAV yang digunakan pada saat pengamatan adalah berupa drone *quadcopter, drone* tersebut memiliki fungsi untuk pengujian sistem, latihan terbang, ataupun melakukan simulasi, *drone* ini disebut sebagai *drone* latih.

Gambar 8. *Drone Quadcopter*

2.12 Analisis Metode Serangan

Salah satu metode penyerangan pada pengiriman data antara UAV dan GCS yaitu *Man-in-the-Middle* (MitM). MitM adalah salah satu teknik dalam keamanan jaringan dimana penyusup menempatkan dirinya berada di tengah-tengah dua perangkat atau lebih yang saling berkomunikasi. Pada gambar 9 adalah ilustrasi serangan *Man-in-the-Middle*.



Gambar 9. Proses *Man-in-the-Middle*

Attacker dapat masuk ke dalam sistem dan mengambil data yang sedang dikirimkan[29].

2.13 Analisis Algoritma AES

2.13.1 Proses Enkripsi

sebagai contoh kasus berikut *plaintext* berupa data dari sensor *magnetometer*(*roll*) dan key menggunakan tanggal ditambah tanggal terbalik :

Plaintext : -0.006028093
Dalam HEX : 2d 30 2e 30 30 36 30 32 38 30 39 33 30 30 30 30
Key : 3004201991024003
Dalam HEX : 33 30 30 34 32 30 31 39 39 31 30 32 34 30 30 33

Maka didapatkan hasil *rounkey*-1 sampai *roundkey*-10

36	04	3D	09
34	04	35	05
F3	C2	F2	C2
2C	15	27	14

RoundKey 2

5F	5B	66	6F
11	15	20	25
09	CB	39	FB
2D	38	1F	0B

RoundKey 3

64	3F	59	36
1E	0B	2B	0E
22	E9	D0	2B
85	BD	A2	A9

RoundKey 4

C7	F8	A1	97
EF	E4	CF	C1
F1	18	C8	E3
80	3D	9F	36

RoundKey 5

AF	57	F6	61
FE	1A	D5	14
F4	EC	24	C7
08	35	AA	9C

RoundKey 6

75	22	D4	B5
38	22	F7	E3
2A	C6	E2	25
E7	D2	78	E4

RoundKey 7

24	06	D2	67
07	25	D2	31
43	85	67	42
32	E0	98	7C

RoundKey 8

63	65	B7	D0
2B	0E	DC	ED
53	D6	B1	F3
B7	57	CF	B3

RoundKey 9

2D	48	FF	2F
26	28	F4	19
3E	E8	59	AA
C7	90	5F	EC

RoundKey 10

CF	87	78	57
8A	A2	56	4F
F0	18	41	ED
D2	42	1D	F1

Gambar 10. Hasil *Roundkey*

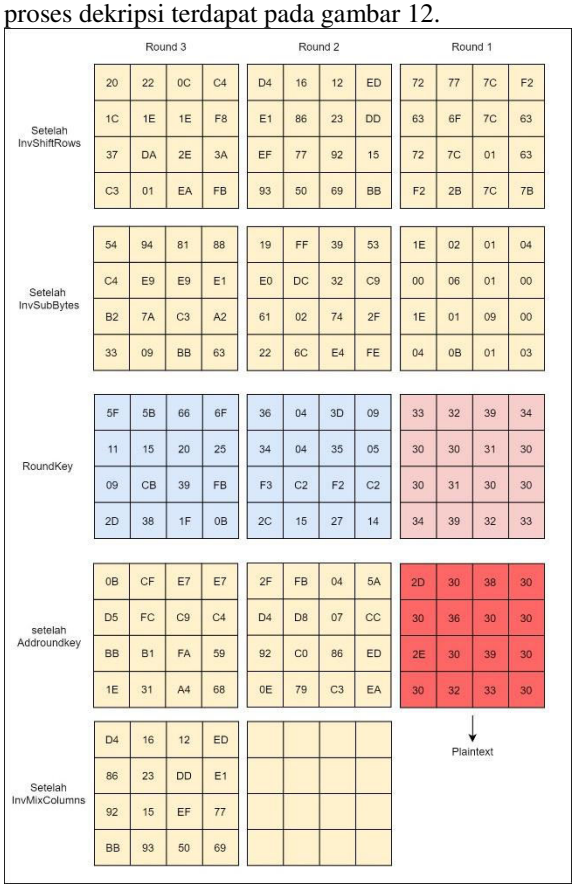
Setelah melalui beberapa tahapan didalam proses enkripsi maka plaintext berubah menjadi chippertext, hasil dari proses enkripsi dapat dilihat pada gambar 11.

	Round 8				Round 9				Round 10			
Setelah SubByte	BF	50	C0	97	0F	A6	0A	7A	84	9C	E2	52
	80	6C	0C	B5	1D	3E	8F	2F	71	22	8B	2C
	A7	76	E0	CC	EA	DA	AE	4B	11	67	9F	70
	D8	EC	B5	A9	C2	4B	6E	90	FF	80	C9	B6
Setelah ShiftRows	BF	50	C0	97	0F	A6	0A	7A	84	9C	E2	52
	80	6C	0C	B5	1D	3E	8F	2F	22	8B	2C	71
	EC	CC	A7	76	EA	DA	AE	4B	9F	70	11	67
	A9	D8	EC	B5	C2	4B	6E	90	B6	FF	80	C9
Setelah MixColumns	98	A0	14	6D	62	54	C4	67				
	F5	DF	AF	A3	0A	BC	3A	5B				
	E8	AC	0F	EF	DD	E2	37	7A				
	1F	9B	8A	25	BA	AA	4D	95				
RoundKey	63	65	B7	D0	2D	48	FF	2F	CF	87	78	57
	2B	0E	DC	ED	26	28	F4	19	8A	A2	56	4F
	53	D6	B1	F3	3E	E8	59	AA	F0	18	41	ED
	B7	57	CF	B3	C7	90	5F	EC	D2	42	1D	F1
Setelah AddRoundKey	FB	C5	A3	BD	4F	1C	3B	48	4B	1B	9A	05
	DE	D1	73	4E	2C	94	CE	42	A8	29	7A	3E
	BB	7A	BE	CC	E3	0A	6E	D0	6F	68	50	8C
	A8	CC	45	96	7D	3A	12	79	64	BD	9D	38

Gambar 11. Hasil akhir enkripsi

2.13.2 Proses Dekripsi

Proses dekripsi adalah mengubah chippertext kembali kedalam bentuk plaintext, hasil akhir dari proses dekripsi terdapat pada gambar 12.



Gambar 11. Hasil akhir dekripsi

2.14 Analisis Pembangkitan Kunci

Untuk inisialisasi kunci awal yaitu dengan tanggal ditambah tanggal terbalik ***Key = "date" + "reverse(date)"***, sebagai contoh:

Key = "30042019" + "91024003" (1)

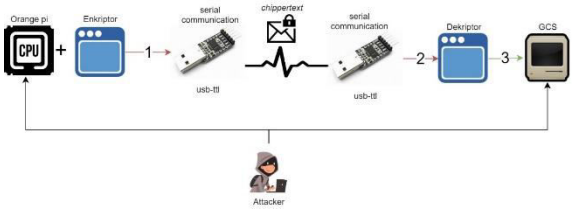
Key = "3004201991024003". (2)

Tabel 3. Contoh tabel kunci

Iterasi	Kunci
1.	3004201991024003
2.	3004201991024004
3.	3004201991024005
4.	3004201991024006
5.	3004201991024007

2.15 Analisis Arsitektur Sistem Yang Akan Dibangun

Pada sistem komunikasi antara UAV dan GCS yang akan diterapkan terdapat dua fungsi utama yakni enkripsi dan dekripsi. Arsitektur sistem pada kriptografi UAV dan GCS dilihat pada gambar 12.

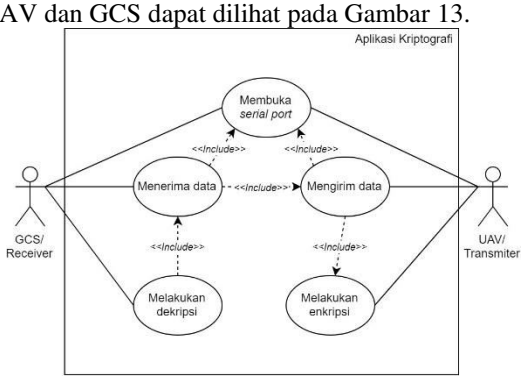


Gambar 12. Arsitektur kriptografi UAV dan GCS

2.16 Analisis Kebutuhan Fungsional

2.16.1 Use Case Diagram

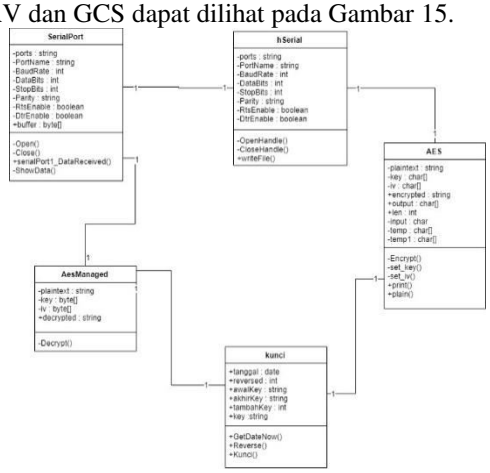
Berikut ini *use case* dari aplikasi kriptografi UAV dan GCS dapat dilihat pada Gambar 13.



Gambar 13. Use Case Diagram

2.16.3 Class Diagram

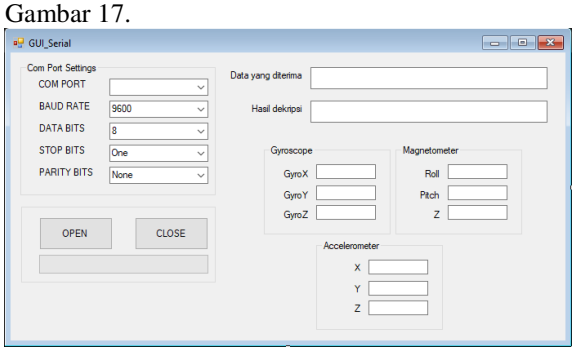
Berikut ini class diagram dari aplikasi kriptografi UAV dan GCS dapat dilihat pada Gambar 15.



Gambar 15. Class diagram

2.17 Implementasi Antarmuka

Berikut adalah implementasi antarmuka dari aplikasi kriptografi UAV dan GCS dapat dilihat pada Gambar 17.



Gambar 17. Implementasi Antarmuka

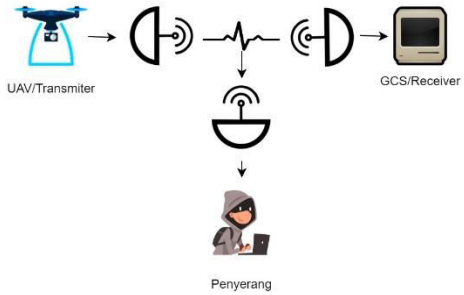
2.18 Pengujian

2.18.1 Manual Penetration Testing

Dalam tahap pengujian dilakukan *manual penetration testing*[21] dengan tahap yang dilakukan pada *data collection* adalah dengan *man-in-the-middle attack*, *vulnerability assessment* menganalisa data yang didapat untuk dicari kelemahan sedangkan pada tahap *actual exploit* adalah dengan metode *brute force attack,* dilanjutkan dengan *report preparation* yaitu mendeskripsikan hasil dari penetrasi yang dilakukan.

2.18.1.1 Man-in-the-Middle Attack

Tujuan dari pengujian ini adalah untuk mengetahui tingkat keamanan dari masing-masing sistem komunikasi antara UAV dan GCS. Arsitektur pengujian yang digunakan dapat dilihat pada gambar 18.



Gambar 18. Skema pengujian MitM[29]

2.18.1.2 Hasil dan Kesimpulan Man-in-the-Middle attack

Hasil pengujian *Man-in-the-Middle attack* diperoleh berdasarkan pengujian yang telah dilakukan.

Tabel 4. Hasil Pengujian Man-in-the-Middle attack

No.	Skenario pengujian	Percobaan Penyadapan	Hasil Data
1.	Tidak menggunakan kriptografi	Penaydapan berhasil	Dapat diketahui
2.	Menggunakan kriptografi	Penyadapan berhasil	Tidak dapat diketahui

2.18.2.1 Brute Force Attack

Setelah data didapatkan maka pada tahap *actual exploit* adalah penguji menggunakan metode *brute force* untuk meluncurkan serangan pada sistem. Penulis mengambil artikel mengenai "*How secure is AES against brute force attacks*?" dengan hasil sebagai berikut[18]:

Tabel 5. *Key Size* dan *Combinations Key*

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Ada juga argumen bahwa kunci simetris 128-bit secara komputasi aman terhadap serangan brute-force. Pertimbangan sebagai berikut ini:

1. Superkomputer lebih cepat: 10,51 Pentaflops = 10.51 Pentaflops = 10.51 x 1015 Flops [Flops = Floating point operations per second].(1)
2. Jumlah flops yang dibutuhkan kombinasi per cek: 1000. (2)
3. Jumlah cek kombinasi per detik = (10,51 x 1015) / 1000 = 10,51 x 1012. (3)
4. Jumlah detik dalam satu Tahun = 365 x 24 x 60 x 60 = 31536000 detik. (4)
5. Jumlah Tahun untuk memecahkan AES dengan Kunci 128-bit

= (3,4 x 1038) / [(10,51 x 1012) x 31536000](5)
= (0,323 x 1026) / 31536000 (6)
= 1,02 x 1018 Tahun (7)
= 1 miliar miliar Tahun (8)

2.18.2.1 Hasil dan Kesimpulan Brute Force Attack

Dengan perhitungan kombinasi yang telah dijabarkan maka akan sangat sulit untuk melakukan *cracking* sebuah kunci AES-128bit, dan dapat disimpulkan bahwa AES-128bit masih tetap aman digunakan meskipun diserang dengan serangan *brute forece* sekalipun.

3. PENUTUP

3.1 Kesimpulan

Kesimpulan dari suatu penelitian dapat diambil setelah melakukan proses implementasi dan pengujian. Berikut ini adalah beberapa point yang dapat disimpulkan dalam penelitian berdasarkan hasil dari pengujian yang telah yaitu data yang didapatkan penyerang dengan menggunakan metode *man-in-the-middle attack* berhasil didapatkan akan tetapi data tidak bisa terbaca oleh penyerang karena sudah menjadi *chippertext*, sedangkan pada pengujian *brute-force attack* untuk melakukan *cracking* pada sebuah kunci AES-128bit sangatlah tidak memungkinkan, sehingga pengamanan menggunakan kriptografi AES-128 masih tepat digunakan untuk saat ini, sampai di temukanya super komputer yang lebih cepat dari 10.51×10^{15} Flops

3.1 Saran

Saran pada penelitian ini berguna untuk pengembangan aplikasi yang dibuat. Adapun saran untuk pengembangan aplikasi adalah memilih kombinasi kunci pertama yang akan digunakan

dikarenakan akan berdampak pada kombinasi kunci pada perulangan ke-1, ke-2, dst. Maka dari itu perlunya kombinasi kunci yang sulit.

DAFTAR PUSTAKA

[1] R. Shofiyanti, "Teknologi Pesawat Tanpa Awak Untuk Pemetaan Dan Pemantauan Tanaman Dan Lahan Pertanian," Inform. Pertan., vol. 20, no. 2, pp. 58–64, 2011.

[2] Wikantika. K. 2009. Unmanned Mapping Technology: Development and Applications. Workshop Sehari "Unmanned Mapping Technology: Development and Applications" (UnMapTech2008). Bandung, Indonesia. 9 Juni 2008.

[3] A. A. Farghani, R. Sumiharto, and S. B. Wibowo, "Purwarupa Ground Control System untuk Pengamatan dan Pengendalian Unmanned Aerial Vehicle Bersayap Tetap," Indones. J. Electron. Instrum. Syst., vol. 3, no. 1, pp. 1–10, 2013.

[4] N. Rodday, "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles," no. Noms, p. 95, 2015.

[5] D. H. B, J. Lee, D. Kim, D. Kwon, K. H. Ryu, and D. Lee, "LEA : A 128-Bit Block Cipher for Fast Encryption on Common Processors," vol. 1, pp. 3–27, 2014.

[6] I. Avdonin, M. Budko, M. Budko, V. Grozov, and A. Guirik, "A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on One-Time pads," Int. Congr. Ultra Mod. Telecommun. Control Syst. Work., vol. 2017–November, pp. 410–413, 2018.

[7] B. S. Rajatha, C. M. Ananda, and S. Nagaraj, "Authentication of MAV communication using Caesar Cipher cryptography," 2015 Int. Conf. Smart Technol. Manag. Comput. Commun. Control. Energy Mater. ICSTM 2015 - Proc., no. May, pp. 58–63, 2015.

[8] M. Podhradsky, C. Coopmans, and N. Hoffer, "Improving communication security of open source UAVs: Encrypting radio control link," 2017 Int. Conf. Unmanned Aircr. Syst. ICUAS 2017, pp. 1153–1159, 2017.

[9] N. Prapulla, S. Veena, and G. Srinivasalu, "Development of algorithms for MAV security," 2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc., pp. 799–802, 2017.

[10] J. Thakur and K. Nagesh, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," Int. J. Emerg. Technol. Adv. Eng., vol. 1, no. 2, pp. 6–12, 2011.

[11] V. Yuniati, G. Indriyata, and A. C Rachmat, "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256," J. Inform., vol. 5, no. 1, pp. 23–31, 2009.

[12] A. Rosyadi, "Implementasi Algortma Kriptografi AES Untuk Enkripsi dan Dekripsi Email," Transient, pp. 1–6, 2012.

[13] G. W. Bhaudhayana, I M. Widiartha, "Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi Lsb pada Gambar Bitmap" 16 Jurnal Ilmu Komputer Vol.VIII, No. 2, September 2015, hlm.15-25

[14] N. B. Tampubolon, R. R. Isnanto, and E. W. Sinuraya, "Implementasi Dan Analisis Algoritma Advanced Encryption Standard (Aes) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia," Transient, vol. 4, no. 4, 2015.

[15] Z. Musliyana, T. Y. Arif, and R. Munadi, "Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," J. Rekayasa Elektr., vol. 12, no. 1, p. 21, 2016.

[16] Finandhita, A., dan I. Afrianto "Development of E-Diploma System Model with Digital Signature Authentication Development of E-Diploma System Model with Digital Signature Authentication," pp. 0–6, 2018.

[17] M. Gupta, S. Mahto, and A. Patel, "Advanced Encryption Standard on Reconfigurable Logic," vol. 50, no. 6, pp. 305–309, 2017.

[18] How secure is AES against brute force attacks?, 10 Juni 2019 [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1279619

[19] Does Size Matter? AES 128-Bit Encryption is (Probably) Good Enough, 10 Juni 2019 [Online]. Available: https://security-architect.com/does-size-matter-aes-128-bit-encryption-is-probably-good-enough/

[20] R. S dan M. Shalahuddin. Rekayasa Perangkat Lunak. Informatika. 2013.

[21] tutorialspoint (2017, Jul.8) Penetration Testing - Manual & Automated [online]. Available : https://www.tutorialspoint.com/penetration_testing/penetr ation_testing_manual_automated.htm

[22] The UAV - Unmanned Aerial Vechile, 4 Maret 2019 [Online]. Available: https://www.theuav.com/

[23] Ground Control Station (GCS), 4 Maret 2019 [Online]. Available: http://a-techsyn.com/gcs/

[24] Communication System (CS), 4 Maret 2019 [Online]. Available: http://a-techsyn.com/gcs/cs/

[25] Kim, David, dan Michael G Solomon. 2012. Fundamentals of Information Systems Security. Jones & Bartlett Learning, United State of America.

[26] Munir, Rinaldi. Kriptografi. Informatika, Bandung. 2006.

[27] F. Information, “Announcing the ADVANCED ENCRYPTION STANDARD (AES),” 2001.
[28] Setyaningsih, Emy. Kriptografi & Implementasinya menggunakan MATLAB. Andi, Yogyakarta,2015.
[29] A. Setiyadi, “Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet,” vol. 2017, pp. 113–120, 2017.