Implementasi Algoritma PRESENT sebagai Pengamanan Data Autentikasi RFID pada UAV Berbasis Arduino

Dedy Septono Catur Putranto[1], Taufik Hidayatullah[2]
Jurusan Teknik Persandian
Sekolah Tinggi Sandi Negara
Bogor, Indonesia
[1]dedy.septono@stsn-nci.ac.id, [2]taufik.dayat21@gmail.com

***Abstrak*— RFID merupakan suatu metode identifikasi objek yang menggunakan gelombang radio. Aplikasi RFID banyak dikembangkan dewasa ini, salah satunya sebagai media transmisi pada *quadcopter*. *Quadcopter* yang digunakan dalam operasi khusus bidang siber dan sandi memerlukan pengamanan tinggi agar tidak mudah disadap data transmisi RFID yang digunakan sehingga tidak dapat di *Cloning* dan *Jamming* media transmisinya. Pada penelitian ini dilakukan penerapan skema autentikasi dan enkripsi pada media RFID berbasis Arduino dan nRF24L01. Skema autentikasi dan enkripsi diimplementasikan algoritma PRESENT guna meningkatkan efiiensi kinerja perangkat dan untuk mengatasi permasalahan *remote cloning*, *remote jamming* dan *eavesdropping*. Hasil yang didapatkan adalah transmisi *quadcopter* dan kontroler dapat berjalan dengan aman dan tidak mempengaruhi kinerja kontroler.**

Kata kunci—RFID, quadcopter, autentikasi, enkripsi, remote cloning, eavesdropping, arduino, nRF24L0;

I. PENDAHULUAN

Teknologi *Radio Frekuensi Identification* (RFID) dapat digunakan pada *Unmanned Aerial Vehicle* (UAV) dengan jenis *quadcopter* sebagai media transmisi antara *quadcopter* dengan perangkat kendali atau *remote* [1]. UAV dapat digunakan untuk berbagai macam kebutuhan seperti operasi militer [2], pengontrol lalulintas [3], hingga pengawas perbatasan [4]. Luasnya penggunaan UAV mengakibatkan semakin banyaknya pihak yang berusaha untuk melakukan serangan terhadap UAV [5] [6]. Berdasarkan luasnya kegunaan UAV jenis *quadcopter*, maka sisi keamanan pada transmisi *quadcopter* harus diperhatikan.

Pentingnya sisi keamanan pada transmisi *quadcopter* berbasis RFID disebabkan oleh adanya berbagai serangan yang dapat terjadi pada RFID seperti *tag cloning* [7], dan *eavesdropping* [8]. Serangan *tag cloning* dapat ditangani dengan meggunakan autentikasi dua arah pada RFID [7] [9]. Autentikasi dua arah dapat digunakan untuk menjamin keaslian *tag* RFID yang digunakan [10]. Enkripsi data dapat digunakan untuk menangani serangan *eavesdropping* pada RFID. Sehingga apabila terjadi *eavesdropping*, penyerang tidak dapat mengetahui pesan atau informasi sesungguhnya [8].

Skema keamanan yang diajukan Hsu [9] menggunakan autentikasi dua arah dan algoritma *Advanced Encryption Standard* (AES) untuk enkripsi data. Berdasarkan penelitian yang telah dilakukan, diketahui bahwa algoritma AES tidak cocok apabila digunakan untuk perangkat *tag* RFID dan jaringan sensor. Algoritma AES memiliki ukuran *gate equivalent* (GE) yang cukup besar. Algoritma AES juga memiiki ukuran *substitution box* (s-box) dengan ukuran yang besar. Ukuran GE dan ukuran s-box sangat berpengaruh pada penggunaan memori dan proses kinerja perangkat yang digunakan. Hal yang dapat dilakukan untuk mengatasi permasalahan pada implementasi adalah dengan menggunakan algoritma enkripsi *lightweight* seperti PRESENT [11]. Algoritma PRESENT dipilih karena memiliki ukuran GE yang lebih kecil yakni 1570 dibandingkan berapa algoritma lain yang dapat digunakan untuk efisiensi kinerja perangkat seperti *Data Encryption Standard* (DES) dengan 3000 GE, DESX dengan 2168 GE, dan *Tiny Encryption Algorith* (TEA) dengan 2100 GE.

Penggunaan autentikasi dua arah ditujukan agar *quadcopter* dapat memastikan keaslian *remote* serta untuk menangani permasalahan *tag cloning* atau *remote cloning* dalam lingkup *quadcopter* dan *remote jamming* [12]. Enkripsi digunakan dengan tujuan untuk mengatasi serangan *eavesdropping* [8] pada transmisi selama proses autentikasi. Perangkat Arduino dipilih karena merupakan perangkat yang mudah digunakan, murah dan memiliki kemampuan komputasi yang baik [13].

Berdasarkan latar berlakang yang telah disebutkan, penelitian ini ditujukan untuk memberikan ketersediaan suatu *prototype quadcopter* berbasis RFID dan Arduino dengan implementasi skema authentikasi dan enkripsi yang diajukan Hsu [9] dan modifikasi algoritma enkripsi yang digunakan sebagai pengamanan pada transmisi antara *quadcopter* dengan *remote*. Modifikasi yang dilakukan adalah merubah algoritma enkripsi yang digunakan yaitu AES menjadi algoritma PRESENT. Penggantian algoritma dilakukan dengan tujuan untuk mengoptimalkan kinerja antara perangkat Arduino yang digunakan sebagai *remote* dengan *quadcopter*. Selain implementasi algoritma enkripsi dan skema keamanan, dilakukan juga pengujian terhadap serangan *tag cloning* [7], dan *eavesdropping*, [8].

II. LANDASAN TEORI

A. Radio Frequency Identification

Radio Frequency Identification (RFID) merupakan salah satu jenis dari teknologi nirkabel yang menggunakan frekuensi radio untuk melakukan transmisi data [9]. RFID dapat digunakan pada berbagai bidang, seperti kesehatan, dan kendali akses [8]. Sistem RFID terdiri dari gabungan beberapa komponen seperti, *tag*, *reader*, protokol komunikasi, dan *database*. RFID *tag* secara umum dapat dikategorikan menjadi 3 kategori yakni *passive tag*, *semi-passive tag*, dan *active tag*.

Luasnya bidang yang dapat didukung dengan penggunaan RFID, menyebabkan semakin banyak timbulnya serangan pada RFID. Serangan tersebut antara lain *eavesdropping, man in the middle, jamming transmitter, cloning, dan unauthorized read/write* [8].

B. Quadcopter

Quadcopter merupakan salah satu jenis dari *Unmanned Aerial Vehicle* (UAV) yang beroperasi dengan menggunakan empat motor penggerak [14]. *Quadcopter* memiliki fungsi mendasar dari UAV yakni menggantikan peranan pilot manusia pada kendaraan [1]. *Quadcopter* diciptakan dengan desain yang dapat digunakan untuk melakukan penerbangan secara vertikal atau langsung keatas dari suatu tempat menuju tempat spesifik yang dituju [15]. *Quadcopter* dapat digunakan pada berbagai bidang seperti, militer [2], pada bidang arkeologi [16], hingga pengawas perbatasan [4]. *Quadcopter* dioperasikan melalui media transmisi nirkabel. Salah satu media nirkabel yang digunakan untuk mengoperasikan *quadcopter* adalah dengan menggunakan frekuensi radio [1].

C. Autentikasi

Autentikasi merupakan tindakan pengecekan terhadap identitas suatu entitas dengan menggunakan suatu objek yang spesifik [17]. Autentikasi dapat dilakukan dengan berbagai metode, dan dikategorikan menjadi 3 kategori. kategori tersebut adalah *something you know*, *something you have*, dan *something you are*.

- *Something You Know*

  Kategori autentikasi yang menggunakan *secret shared* antar entitas dalam autentikasi [17]. Contoh dari kategori ini adalah *password*, PIN [18].

- *Something You Have*

  Kategori autentikasi yang menggunakan suatu media untuk setiap sesi autentikasi [17] (Todorov, 2007). Contoh dari kategori ini adalah, *smart card*, dan token [18].

- *Something You Are*

  Kategori autentikasi yang menggunakan keunikan fisik suatu manusia atau biasa disebut *biometric* [17]. Contoh dari kategori ini adalah *fingerprint*, *face*, retina, dan *voice* [18].

D. Skema Autentikasi dan Enkripsi

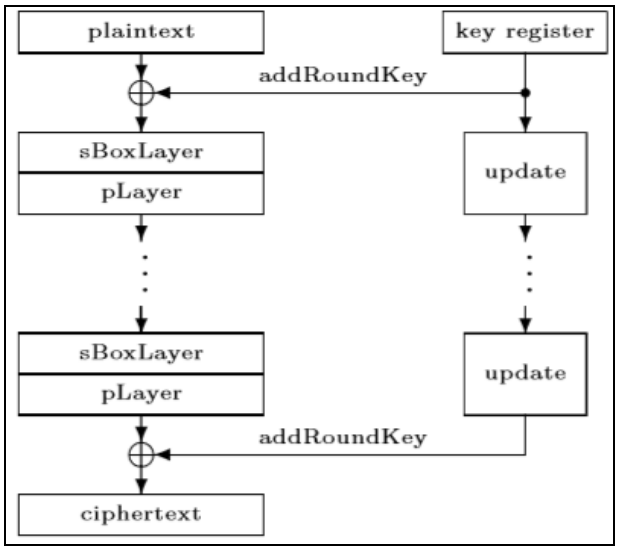
Pada skema autentikasi dan enkripsi yang diajukan Hsu [9] merupakan skema keamanan RFID dengan menggunakan autentikasi dua arah dan enkripsi data. Algoritma enkripsi yang digunakan pada skema autentikasi dan enkripsi ini adalah menggunakan algoritma AES. Skema yang diajukan Hsu [9] memiliki berbagai parameter seperti SID, K, TIDi, Ki, PRNG, dan R.

Pada proses autentikasi dua arah, dilakukan pertukaran identitas dan pengecekan identitas antara kedua entitas yang dilakukan secara terenkripsi. Kemudian juga dilakukan pembangkitan kunci. Setelah proses autentikasi berhasil, dilakukan pembaruan terhadap parameter-parameter yang digunakan untuk proses autentikasi sesi berikutnya. Pembaruan nilai parameter keamanan pada skema Hsu [9] ditujukan untuk menyediakan perangkat yang selalu berganti identitas dan kunci untuk mencegah terjadinya serangan.

E. PRESENT

PRESENT merupakan algoritma *lightweight* jenis *block cipher* yang diajukan oleh Bogdanov [11]. Algoritma PRESENT merupakan algoritma yang berorientasi pada perangkat keras. PRESENT dapat digunakan untuk *tag* RFID dan jaringan sensor. PRESENT memiliki *Gate Equivalent* (GE) yang lebih rendah dari algoritma lain seperti AES dan DES. Hal ini menunjukkan bahwa PRESENT akan bekerja optimal apabila digunakan pada perangkat keras [11].

PRESENT merupakan algoritma yang dibangun dengan struktur *Substitution Permutation Network* (SPN) dengan jumlah *round* adalah 31 dan memiliki Panjang blok 64 bit. PRESENT menyediakan layanan kunci 80 bit dan 128 bit



Gambar 1. Algoritma PRESENT

Gambar 1 menunjukkan tahapan pada algoritma PRESENT. Algoritma PRESENT memiliki 4 tahapan yakni, *addRoundKey*, *SBoxlayer*, *pLayer*, dan *Key Schedule* [11]. Berikut merupakan penjelasan 4 tahapan PRESENT

- *AddRoundKey*,

  Pada tahap ini, setiap bit pada plaintext dari setiap *round* akan di xor dengan bit sub kunci yang merupakan hasil dari *key schedule*.

- *SBoxlayer*

  Pada tahap ini, hasil dari *AddRoundKey* diproses dengan menggunakan s-box. S-box yang digunakan memiliki ukuran 4x4

- *PLayer*

  Pada tahap ini, hasil dari *SBoxlayer* diproses dengan tabel permutasi. Proses yang terjadi adalah perpindahan posisi bit pada algoritma

- *Key Schedule*

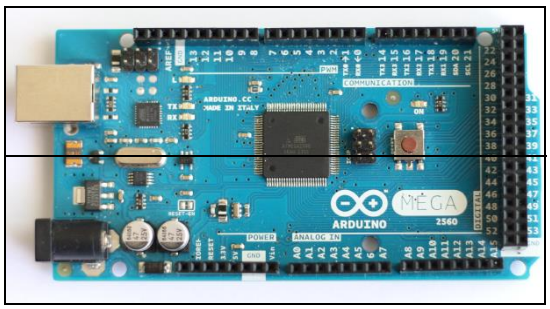
  Pada tahap ini, kunci yang diinput sepanjang 80 bit akan diproses sehingga menghasilkan kunci sepanjang 64 bit yang akan diperbarui setiap pada *round*. Inputan kunci sepanjang 128 bit akan diproses sehingga menghasilkan kunci sepanjang 64 bit.

F. Arduino

Arduino merupakan perangkat *microcontroller* yang dapat digunakan untuk melakukan pemrograman dan untuk menjalankan perintah. Arduino memiliki berbagai kelebihan, antara lain murahnya perangkat, populer digunakan atau banyak dimanfaatkan dalam bidang penelitian maupun pendidikan, dan *open source* yang membuat berbagai kalangan dapat melakukan eksplorasi dengan menggunakan perangkat arduino [19]. Arduino memiliki beberapa jenis, berikut merupaan beberapa jenis Arduino

- Arduino Mega 2560

Arduino Mega 2560 merupakan perangkat *microcontroller* yang menggunakan ATmega2560 sebagai basis pemrosesan. Pada Arduino Mega 2560 terdapat 54 pin digital untuk masukan maupun keluaran. Dari 54 pin yang ada, terdapat 15 pin dapat digunakan untuk keluaran *Pulse With Modulation* (PWM). Kemudian terdapat juga pin lain, yakni 16 pin untuk masukan analog, dan 4 pin untuk UART.

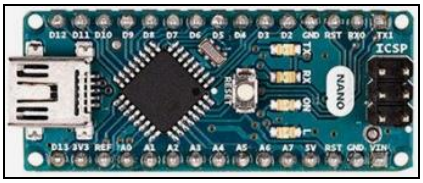


Gambar 2. Arduino Mega 2560

Gambar 2 menunjukkan gambar Arduino Mega 2560 dengan pin-pin yang tersedia.

- Arduino Nano

Arduino Nano, merupakan Arduino yang didesin dengan ukuran kecil, lengkap, dan mudah digunakan. Arduino Nano dibangun dengan menggunakan ATmega328P.

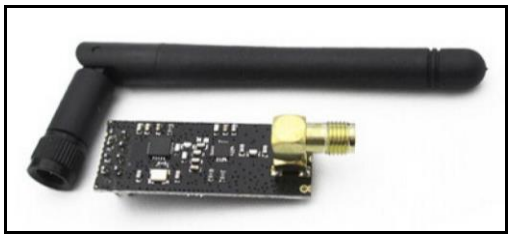


Gambar 3. Arduino Nano

Gambar 3 menunjukkan gambar Arduino Nano dengan pin-pin yang tersedia

G. nRF24L01

nRF24L01 merupakan sebuah *transreceiver single chip* radio yang beroperasi pada frekuensi 2,4 sampai 2,5 GHz. Perangkat nRF24L01 terdiri dari *frequency synthesizer, power amplifier*, osilator kristal, *demodulator, modulator, Enhanced ShockBurst*™, dan *protocol engine*.



Gambar 4. nRF24L01

Gambar 4 menunjukkan gambar perangkat nRF24L01. Perangkat *transreceiver* nRF24L01 dapat digunakan pada berbagai bidang, seperti *Wireless data communication, Alarm and security systems, Home automation*.

H. Electronic Speed Controller

Electronic Speed Controller (ESC) merupakan perangkat yang digunakan untuk mengatur kecepatan motor pada *quadcopter*.

Gambar 5. ESC SimonK 30 A

Gambar 5 menunjukkan gambar ESC dengan jenis SimonK 30 A.

I. Motor Brushless

Motor *brushless* merupakan motor yang memiliki tiga buah *coil*. *Coil yang* terdapat pada motor *brushless* masing-masing memiliki kabel yang akan digunakan untuk terhubung dengan

ESC dan baterai, sehingga secara fisik motor *brushless* memiliki 3 kabel yang digunakkan untuk koneksi.

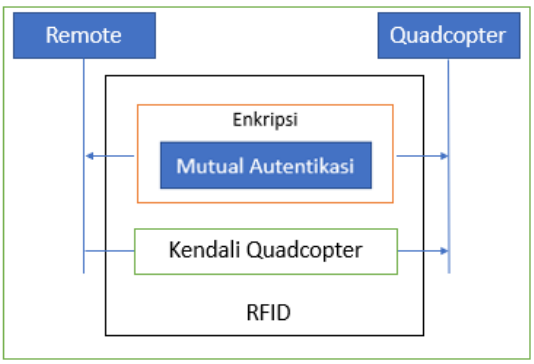
Gambar 6. Motor *brushless*

Gambar 6 menunjukkan gambar motor *brushless* dengan jenis *brushless* RCX 2212.

III. IMPLEMENTASI PENGAMANAN PADA RFID UNTUK TRANSMISI *QUADCOPTER* BERBASIS ARDUINO

A. *Gambaran Umum Sistem*

Pada penelitian ini, dilakukan implementasi skema autentikasi dan enkripsi yang diajukan oleh Hsu [9] untuk pengamanan pada transmisi antara *remote* dengan *quadopter*.



Gambar 7. Gambaran umum sistem

Gambar 7 menunjukkan gambaran umum sistem pada penelitian ini. Mutual autentikasi atau autentikasi dua arah dilakukan antara *remote* dengan *quadcopter* pada bagian *receiver* secara terenkripsi. Enkripsi digunakkan untuk menjamin keamanan data pada proses autentikasi. Algoritma enkripsi yang digunakan adalah algoritma PRESENT. Apabia autentikasi antara *remote* dengan *receiver quadcopter* berhasil, maka *remote* baru dapat mengirimkan data kontrol terhadap *quadcopter*, sehingga *remote* mampu digunakan untuk mengontrol *quadcopter*. Apabila autentikasi gagal, maka *remote* tidak dapat digunakan untuk mengontrol *quadcopter*.

B. *Gambaran Arsitektur*

Pada penelitian ini, skema keamanan yang diajukan Hsu [9] diimplementasikan sebagai pengamanan pada RFID untuk transmisi *quadcopter* berbasis Arduino. Pada penelitian ini dibangun dua perangkat yakni, *remote* dan *quadcopter*. Membangun *Remote* dan *quadcopter* dapat dilakukan dengan menggunakan berbagai perangkat. Berikut merupakan gambaran arsitektur dari perangkat *remote* dan *quadcopter*

- Arsitektur *remote*

Remote dibangun dengan menggunakan berbagai kombinasi perangkat. Berikut merupakan gambar arsitektur dari *remote*

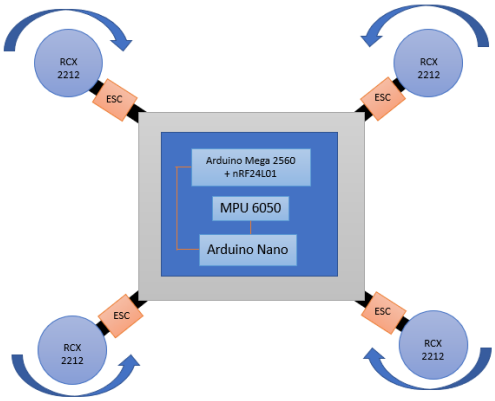
Gambar 8. Arsitektur *Remote*

Gambar 8 menunjukkan gambar arsitektur *remote*. Dapat diihat pada gambar 7, *remote* dibangun dengan menggunakan Arduino Mega 2560, nRF24L01, modul analog, dan *switch*.

Analog *module* atau modul analog digunakan untuk mengatur pergerakan dari *quadcopter*, dan *switch flight mode* digunakan untuk menentukan *flight mode* yang akan diplih. Perangkat Arduino Mega 2560 digunakan sebagai inti pemrosesan pada remote, dan perangkat nRF24L01 digunakan sebagai *transreceiver*.

- Arsitektur *quadcopter*

Pada penelitian ini, *quadcopter* dibangun dengan menggunakan berbagai perangkat yang disatukan menjadi suatu kesatuan. Berikut merupakan gambar arsitektur dari *quadcopter*



Gambar 9. Arsitektur *quadcopter*

Gambar 9 menunjukkan gambar arsitektur *quadcopter*. Dapat diihat pada gambar 9, *remote* dibangun dengan menggunakan Arduino Mega 2560, nRF24L01, Arduino Nano, MPU 6050, ESC, dan motor *brushless* RCX2212.

Perangkat Arduino Mega 2560 digunakan sebagai *receiver* untuk *quadcopter* dan perangkat yang akan melakukan autentikasi secara terenkripsi dengan *remote*. Perangkat nRF24L01 digunakan sebagai *transreceiver*. Arduino Nano digunakan sebagai perangkat untuk *flight controller*. MPU

6050 digunakan sebagai sensor *gyroscope* dan *accelerometer*. perangkat ESC digunakan untuk mengatur kecepatan motor *brushless*, dan motor *brushless* RCX2212 digunakan untuk memutar propeller sehingga *quadopter* dapat terbang.

C. Implementasi

Implementasi skema autentikasi dan enkripsi Hsu [9] dilakuan dengan menggunakan bahasa Arduino yang berbasis dengan bahasa pemrograman C. Implementasi dilakukan pada dua sisi yakni, *remote* dan *quadcopter*.

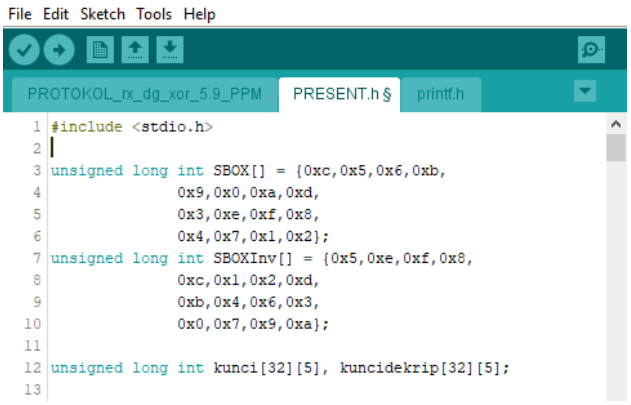
- Implementasi skema Autentikasi

Skema autentikasi dan enkripsi Hsu [9] diimplementasikan pada Arduino dengan menggunakan Arduino IDE. Skema Autentikasi dan enkripsi dibuat dengan menggunakan pemrograman bahasa C. Implementasi skema yang dilakukan, belum menggunakan algoritma enkripsi karena implementasi dilakukan secara bertahap.

- Implementasi Algoritma PRESENT

Setelah melakukan implementasi skema autentikasi, dilakukan implementasi algoritma enkripsi yang digunakan yakni PRESENT. Algoritma PRESENT digunakan sebagai algoritma pengamanan pada proses autentikasi secara terenkripsi sesuai dengan skema keamanan Hsu [9].

Algoritma PRESENT diimplementasikan dengan cara membuat program secara terpisah yang kemudian dijadikan sebagai file *hehader*. Penggunaan file header algoritma PRESENT dilakukan dengan cara memanggil fungsi enkripsi dan dekripsi. Hal ini dilakukan untuk efisiensi dan mempermudah pembuatan program *prototype* secara keseluruhan. Algoritma PRESENT dibuat dengan menggunakan pemrograman bahasa C.

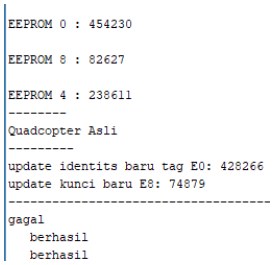


Gambar 10. Implementasi algoritma PRESENT

Gambar 10 menunjukkan implementasi algoritma PRESENT sebagai file *header* pada skema Autentikasi Hsu [9] sebagai pengganti algoritma enkripsi AES. Penggantian algoritma enkripsi dari AES menjadi PRESENT dilakukan dengan tujuan untuk efisiensi proses kinerja pada perangkat Arduino dan RFID.

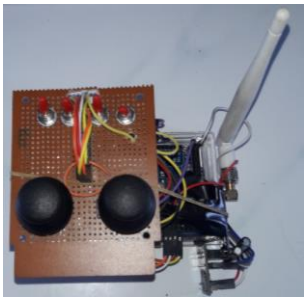
- Implementasi *remote*

Remote dibangun dengan menggunakan perangkat Arduino Mega 2560, nRF24L01, modul analog, *switch* dan akrilik. Skema autentikasi dan enkripsi Hsu [9] diimplementasikan pada *remote* dengan menggunakan Arduino IDE.



Gambar 11. Hasil implementasi skema keamanan RFID pada sisi *remote*.

Gambar 11 menunjukkan hasil implementasi skema keamanan RFID yang diajukan Hsu [9] pada sisi *remote*. Pada gambar 11 ditampilkan nilai parameter yang digunakan ketika sesi autentikasi, setelah sesi autentikasi berhasil, dilakukan pembaruan nilai parameter untuk sesi autentikasi berikutnya dan dilakukan pengiriman data untuk mengontrol pergerakan *quadcopter*.

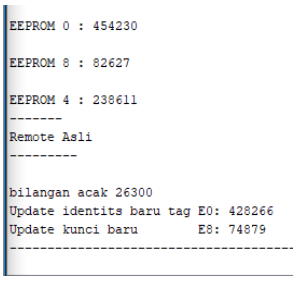


Gambar 12. Perangkat remote

Gambar 12 menunjukkan perangkat *remote* yang telah diimplementasikan skema keamanan RFID Hsu [9] dan dapat digunakan untuk mengendalikan *quadcopter*.

- Implementasi *quadcopter*

Implementasikan skema autentikasi dan enkripsi Hsu [9] pada perangkat *quadcopter* dilakukan pada bagian *receiver quadcopter* yang dibangun dengan menggunakan Arduino Mega 2560.



Gambar 13. Hasil implementasi skema keamanan RFID pada sisi *quadcopter*

Gambar 13 menunjukkan hasil implementasi skema keamanan RFID yang diajukan Hsu [9] pada sisi *quadcopter*.

Gambar 13 menampilkan nilai parameter yang digunakan pada sesi autentikasi. Setelah sesi autentikasi berhasil, dilakukan pembaruan nilai parameter untuk sesi autentikasi berikutnya dan dilakukan pengiriman data kontrol *quadcopter* untuk *flight controller*.

Gambar 14. Perangkat quadcopter dengan transmisi RFID berbasis arduino

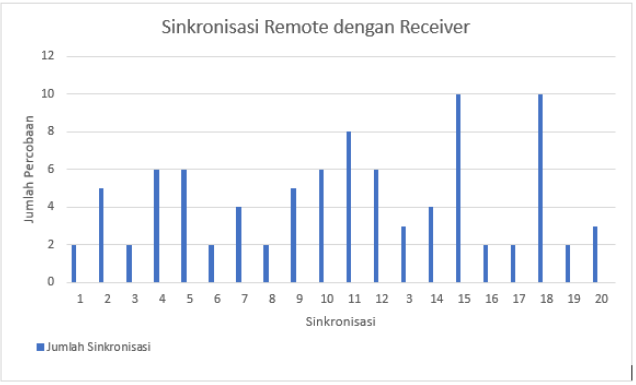
Gambar 14 menunjukkan perangkat *quadcopter* yang telah diimplementasikan skema keamanan RFID Hsu [9].

IV. ANALISIS

Pada bab ini, dibahas mengenai analisis terhadap imlementasi dan hasilnya. Analisis dilakukan terhadap sistem hasil implementasi, pengujian sistem, dan pengujian keamanan.

A. Analisis Hasil Implementasi

Implementasi modifikasi skema keamanan RFID Hsu [9] dapat dilakukan dengan baik pada *remote* dan *quadcopter*, namun terdapat kendala pada transmisi nirkabel yang dilakukan. Kendala yang dialami berupa sinkronisasi antara *remote* dengan *quadcopter*. Sinkronisasi yang dimaksud adalah dapat berjalannya komunikasi antara *remote* dengan *quadcopter* menggunakan media nirkabel RFID. Setelah dilakukan Analisa, didapatkan bahwa cara untuk menangani permasalahan ini adalah dilakukan dengan menekan tombol reset Arduino pada *remote* dan *quadcopter* secara bersamaan.

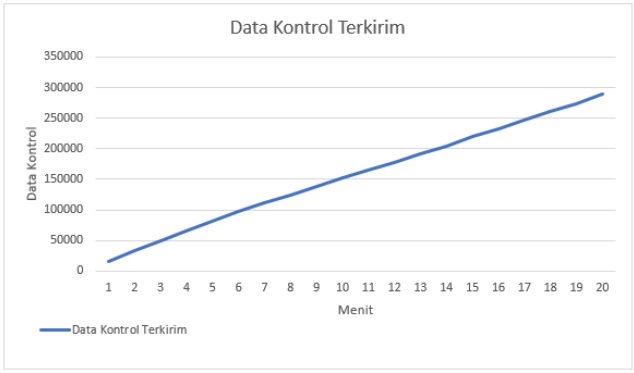


Gambar 15. Sinkronisasi *remote* dengan *quadcopter*

Gambar 15 menunjukkan percobaan sinkronisasi antara *remote* dan *quadcopter*. Dari gambar 15 dapat dilihat jumlah hasil percobaan sinkronisasi, percobaan dilakukan sebanyak 20 kali sesi sinkronisasi. Jumlah percobaan sinkronisasi terendah adalah dua kali sinkronisasi atau dua kali penekanan tombol reset dan jumlah percobaan sinkronisasi tertinggi adalah 10 kali sinkronisasi. Dari percobaan yang dilakukan sebanyak 20 kali, didapatkan rata-rata sinkronisasi adalah empat hingga lima kali sinkronisasi atau penekanan tombol reset.

Dari hasil yang ditunjukkan pada gambar 15, terdapat faktor-faktor yang dapat mempengaruhi intensitas penekanan tombol reset untuk sinkronisasi komunikasi Arduino secara nirkabel. Faktor tersebut adalah

1) Sumber tegangan Arduino
2) Sumber tegangan perangkat nRF24L01
3) Listrik statis pada perangkat Arduino dan nRF24L01
4) Banyaknya sinyal *wireless* lain seperti sinyal Wifi di lingkungan sekitar perangkat
5) Pemasangan kabel untuk perangkat Arduino dengan nRF24L01



Gambar 16. Data kontrol *quadcopter* yang berhasil dikirim *remote*

Gambar 16 menunjukkan percobaan pengiriman data kontrol dari *remote* untuk *quadcopter*. Data kontrol yang dikirim adalah data yang didapatkan dari *remote* untuk mengontrol pergerakan dari *quadcopter*. Dapat dilihat bahwa data kontrol yang dikirimkan dari *remote* untuk *quadcopter* berbanding lurus dengan waktu berjalannya transmisi. Semakin lama penggunaan *remote* maka semakin banyak pula data *kontrol* yang dikirimkan. Data kontrol ini dapat dikirimkan setelah proses autentikasi berhasil. Data kontrol dihitung dengan cara menampikan keberhasilan pengiriman dan jumlah keseluruhan keberhassilan melalui serial monitor Arduino IDE. Berdasarkan hasil percobaan didapatkan sebanyak 288658 data pada menit ke-20 *remote* dan *quadcopter* berkomunikasi.

B. Pengujian Sistem

Pengujian sistem dilakukan berdasarkan kebutuhan fungsional dan non-fungsional dari sistem. Berikut akan ditunjukkan tabel hasil pengujian berdasarkan kebutuhan fungsional, dan non-fungsional dari sistem

TABEL I. HASIL PENGUJIAN SISTEM BERDASARKAN KEBUTUHAN FUNGSIONAL

No	Kebutuhan Fungsional	Hasil
1	Media transmisi yang digunakan *remote* dan *quadcopter* berbasis RFID.	✓
2	*Remote* dapat digunakan untuk melakukan kontrol terhadap *quadcopter*	✓

No	Kebutuhan Fungsional	Hasil
3	Transmisi antara *quadcopter* dan *remote* berjalan secara aman	✓
4	Pengamanan yang digunakan adalah skema autentikasi dan enkripsi RFID Hsu [9]	✓
5	PRESENT digunakan sebagai algoritma enkripsi	✓

TABEL II. HASIL PENGUJIAN SISTEM BERDASARKAN KEBUTUHAN NON FUNGSIONAL

No	Kebutuhan Non-Fungsional	Hasil
1	Perangkat *quadcopter* dapat beroperasi dengan daya jangkau lebih dari 20 meter.	✓
2	Quadcopter dapat beroperasi selama 20 menit.	✓
3	Frame quadcopter tidak mudah pecah	✓

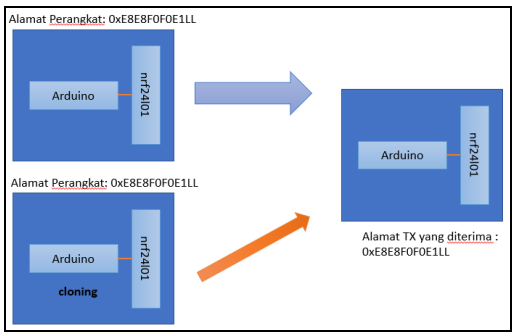
Dari pengujian yang dilakukan, didapatkan hasil bahwa seluruh persyaratan sistem dapat terpenuhi, hal ini menunjukkan bahwa telah terdapat kesesuaian dengan kebutuhan.

C. *Pengujian Keamanan*

Pengujian keamanan pada penelitian ini digunakan untuk membuktikan bahwa penerapan skema autentikasi dan enkripsi Hsu [9] dapat mengamankan transmisi antara *remote* dengan *quadcopter*. Pengujian keamanan akan dilakukan dengan dua metode yakni dengan *remote cloning* dan *eavesdropping*.

- *Remote Cloning*

Pengujian keamanan dengan metode *remote cloning* digunakan untuk menunjukkan penggunaan autentikasi dua arah dapat diterapkan untuk mengatasi permasalahan *remote cloning* pada *quadcopter* berbasis RFID.



Gambar 17. Skenario *remote cloning*

Gambar 17 menunjukkan skenario yang digunakan untuk melakukan pengujian keamanan dengan metode *remote cloning*. Dapat dilihat bahwa terdapat dua *remote* yang dibangun secara identik dan ditujukan untuk mengontrol *quadcopter*. Akan dilakukan dua uji coba yakni *remote cloning* tanpa penerapan skema Hsu [9] dan *remote cloning* dengan penerapan skema Hsu [9]

1) Remote cloning tanpa penerapan skema Hsu [9]

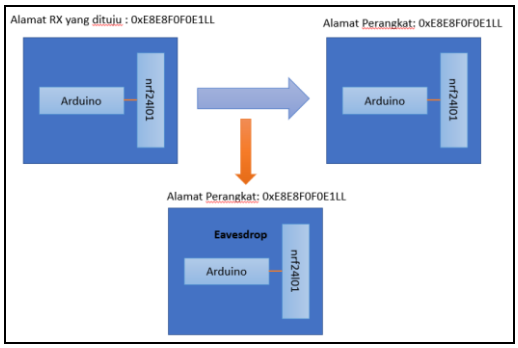
Uji keamanan telah dilakukan dan didapatkan hasil bahwa *remote cloning* sangat berpengaruh terhadap *quadcopter* dengan RFID berbasis Arduino. Dengan skenario ini, *quadcopter* dapat dikendalikan bahkan hingga diambil alih. Dicontohkan bahwa dengan skenario ini dan dengan *remote* tanpa penerapan skema keamanan RFID Hsu [9] *quadcopter* dapat dikendalikan dari *armed* menjadi *disarmed* atau bahkan sebaliknya.

2) Remote cloning dengan penerapan skema Hsu [9]

Uji keamanan telah dilakukan dan didapatkan hasil bahwa penerapan skema autentikasi dan enkripsi Hsu [9] sangat berpengaruh pada *remote cloning*. *Remote* lain tidak dapat mengendalikan *quadcopter* karena *remote* harus terautentikasi terlebih dahulu sebelum melakukan kontrol terhadap *quadcopter*. Skenario uji keamanan ini tidak mendapatkan hasil seperti pada uji *remote cloning* tanpa penerapan skema, hal ini disebabkan adanya penerapan skema autentikasi dan enkripsi Hsu [9].

- *Eavesdropping*

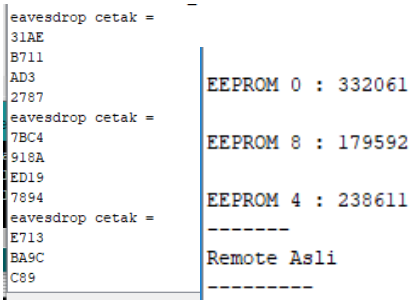
Pengujian keamanan dengan metode *eavesdropping* digunakan untuk menunjukkan penggunaan enkripsi untuk mengatasi *eavesdropping* pada *quadcopter* berbasis RFID.



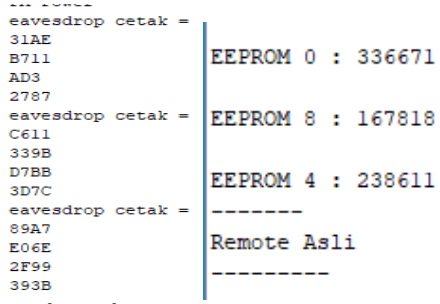
Gambar 18. Skenario *eavesdropping*

Gambar 18 menunjukkan skenario yang digunakan untuk melakukan pengujian keamanan dengan metode *eavesdropping*. Dari gambar 16 dapat dilihat bahwa terdapat dua perangkat yang saling berkomunikasi yakni *remote* dengan *quadcopter*. Kemudian terdapat satu perangkaat lagi yang melakukan *eavesdropping* untuk mengetahui data apa saja yang ada dalam komunikasi yang dilakukan, terlebih pada saat sesi autentikasi dilakukan.

Dari skenario uji keamanan ini, didapatkan hasil bahwa *eavesdropping* dapat dilakukan, namun hasil yang didapat adalah data tidak dapat dimengerti. Hal ini disebabkan karena penggunaan enkripsi pada transmiisi nirkabel yakni dengan RFID.



Gambar 19. Hasil eavesdropping



Gambar 20. Hasil eavesdropping

Gambar 19 dan gambar 20 menunjukkan hasil dari *eavesdropping* . hasil yang didapatkan adalah berupa nilai heksa desimal, nilia ini adalah nilai dari *cipher* algoritma PRESENT pada transmisi RFID. Hasil *eavesdropping* menunjukkan bahwa nilai yang didapat tidak mudah untuk dipahami atau dengan kata lain nilai asli dari data yang ditransmisikan tidak dapat diketahui.

V. KESIMPULAN

Hasil dari penelitian ini didapatkan bahwa implementasi algoritma PRESENT pada skema keamanan Hsu [9] untuk pengamanan *quadcopter* dengan RFID berbasis Arduino membuat transmisi antara *remote* dengan *quadcopter* berjalan secara aman dan tidak mempengaruhi kinerja *remote* untuk melakukan kontrol terhadap *quadcopter*. Transmisi antara *remote* dan *quadcopter* dengan RFID berbasis Arduino dapat diamankan dengan menerapkan modifikasi skema autentikasi dan enkripsi Hsu [9]. Penerapan skema Hsu [9] pada *quadcopter* berbasis RFID terbukti dapat menangani permasalahan *remote cloning*, dan untuk mengatasi *eavesdropping*.

Permasalahan pada transmisi antara *remote* dengan *quadcopter* dengan RFID masih memiliki peluang untuk dapat terjadi. Hal ini disebabkan oleh perangkat Arduino dan nRF24L01 yang dipengaruhi oleh faktor-faktor yang telah disebutkan pada penelitian ini.

UCAPAN TERIMA KASIH

Terimakasih disampaikan oleh kepada Sekolah Tinggi Sandi Negara yang telah mendukung penelitian ini.

REFERENSI

[1] Gemilang et al., "Kendali Jarak Jauh UAV (Unmanned Aerial Vehicle) Tipe Quadcopter Menggunakan Transceiver NRF24L01+ Beserta Job Sheet Uji Coba," *Jurnal Pendidikan Teknik Elektro*, vol. 5, no. 03, pp. 861-866. 2016.

[2] E. B. Carr, "Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy, and Regulatory Issues of Integration into U.S.Airspace," *National Centre for Policy Analysis (NCPA)*, 2013.

[3] R. G. Holcombe, "Integrating Drones into the US Air Traffic Control System," *Mercatus Working Paper*, October 12, 2016.

[4] J. S. Gadda and R. D. Patil, "Quadcopter (UAVS) for Border Security With GUI System," *International Journal of Research in Engineering and Technology (IJRET)*, vol. 2, no. 12, pp. 620-624, 2013.

[5] E. Rivera, R. Baykov and G. Gu, "A Study On Unmanned Vehicles and Cyber Security," *Texas, USA*. 2016.

[6] K. Hartmann and C. Steup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference*, pp. 1-23, Jun 4, 2013.

[7] A. Yang et al, "A new unpredictability-based radio frequency identification f.orward privacy model and a provably secure construction," *Security and Communication Networks*, vol. 8, no. 16, pp. 2836-2849, 2015.

[8] Q. Xiao, T. Gibbons, and H. Lebrun, "RFID Technology, Security Vulnerabilities, and Countermeasures," *Supply Chain the Way to Flat Organisation*, InTech, 2009.

[9] CH. Hsu et al., "Efficient identity authentication and encryption technique for high throughput RFID system," *Security and Communication Network*, vol. 9, no. 16, pp. 2581-2591, 2016.

[10] RI. Paise and S. Vaudenay, "Mutual authentication in RFID: security and privacy," *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pp. 292-299, 2008.

[11] Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 450-466, 2007.

[12] K. Parlin, "*Jamming of Spread Spectrum Communications Used In UAV Remote Control System*," Tallinn Univerrsity of Technology, 2017.

[13] C. Silva, S. M. Vieira, and J. M. C. Sousa, "Arduino Implementation of Automatic Tuning in PID Control of Rotation in DC Motor," *Lect. Notes Electr. Eng.*, vol. 321, pp. 365–373, 2015.

[14] M. Q. Vechian, "Wireless Control Quadcopter With Stereo Camera and Balancing System," Doctoral dissertation, Universiti Tun Hussein Onn Malaysia, 2012.

[15] M. Parker, C. Robbiano, and G. Bottorff, "Quadcopter" *BS, Electrical and Computer Engineering Department, Colorado State Univ., Fort Collins*, 2011.

[16] S. Campana, "Drones in Archaeology. State-of-the-art and Future Prespective*" Archaeological Prospection*, vol. 24, no. 4, pp. 275-296 2017.

[17] D. Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Auerbach Publications, 2007.

[18] M. A. Alia, A. A. Tamimi, and O. N. AL-Allaf, "Cryptography Based Authentication Methods," *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, 2014.

[19] D. Artanto, *Interaksi Arduino dan LabView*. Jakarta: Elex Media Komputindo, 2012.