Implementasi Enkripsi *Advanced Encryption Standard* (AES-128) Mode *Cipher Block Chaining* (CBC) sebagai Keamanan Komunikasi Pergerakan Robot *Humanoid* KRSBI

Achmad Sudrajat[1], Yoyok Heru P.[2], Mila Kusumawardani[3]

[1,2] Program Studi Jaringan Telekomunikasi Digital,
Jurusan Teknik Elektro, Politeknik Negeri Malang, Indonesia
[3] Program Studi Teknik Telekomunikasi,
Jurusan Teknik Elektro, Politeknik Negeri Malang, Indonesia

[1]madsudra@gmail.com, [2]yoyok.heru@polinema.ac.id, [3]mila.kusumawardani@polinema.ac.id

Abstract— **A humanoid robot is a robot that has a human-like shape, which has a body and head, two arms and two legs that allow it to move and interact with the environment created by humans [1]. The humanoid soccer robot system currently used still uses the Robot Operating System (ROS) system, which is basically in the system without any encryption or data security every time communication is made by sending and requesting or what is commonly called Publish and Subscribe. In order to develop the humanoid soccer robot, this research is designed for "Implementation of Advanced Encryption Standard (AES-128) Cipher Block Chaining (CBC) Mode as Communication Security for Humanoid Robot Movement KRSBI". Which is designed to operate in low quality connectivity, with network bandwidth that secures every node running on the ROS which includes features for subscribing to topics and also publishing topics. Then with the addition of cryptography can keep data or messages safe when sent, from sender to receiver without experiencing interference from third parties. According to Bruce Scheiner in his book "Applied Cryptography", cryptography is the science and art of keeping messages secure [2]. So all communications are encrypted using Secure Sockets Layer (SSL), or more specifically Transport Layer Security (TLS).**

Keywords— **Robot Operating System (ROS), Humanoid Robot, Communication, Network, Wireless, Encryption, Decryption, Cryptography, Secure ROS.**

Abstrak— **Robot *humanoid* adalah robot yang memiliki bentuk seperti manusia yaitu memiliki tubuh dan kepala, dua tangan dan dua kaki yang memungkinkan dapat bergerak dan berinteraksi dengan lingkungan yang dibuat oleh manusia [1]. Pada sistem robot sepak bola *humanoid* yang digunakan saat ini masih menggunakan sistem *Robot Operating System* (ROS) saja, yang pada dasarnya di dalam sistem tersebut tanpa ada enkripsi atau pengaman data setiap kali komunikasi dilakukan dengan pengiriman dan permintaan atau yang biasa disebut *Publish* dan *Subscribe*. Dalam rangka pengembangan robot sepak bola *humanoid*, penelitian ini dirancang untuk "Implementasi Enkripsi *Advanced Encryption Standard* (AES-128) Mode *Cipher Block Chaining* (CBC) Sebagai Keamanan Komunikasi Pergerakan Robot Humanoid KRSBI". Yang didesain untuk beroperasi pada konektivitas dengan kualitas yang rendah, dengan network bandwidth yang mengamankan setiap *node* yang berjalan di dalam ROS yang didalamnya terdapat fitur untuk *subscribe* topik dan juga *publish* topik. Kemudian dengan tambahan kriptografi dapat menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "*Applied Cryptography*", kriptografi adalah ilmu pengetahuan dan seni menjaga *message- message* agar tetap aman (*secure*) [2]. Maka semua komunikasi dienkripsi dengan menggunakan *Secure Sockets Layer* (SSL), atau lebih spesifiknya *Transport Layer Security* (TLS).**

Kata Kunci— ***Robot Operating System* (ROS), Robot *Humanoid*, Komunikasi, Jaringan, *Wireless*, Enkripsi, Dekripsi, Kriptografi, *Secure* ROS.**

I. PENDAHULUAN

Perkembangan robot saat ini tidak hanya digunakan untuk keperluan industri dan pabrik, namun sudah menjadi bahan pelajaran penting baik di sekolah maupun perguruan tinggi. Maraknya perlombaan dan kontes robot menjadi bukti bahwa dunia robot sudah tidak asing lagi di mata masyarakat serta sudah menjadi ajang untuk mengadu bakat di bidang robotika.[3] Robot humanoid adalah robot yang memiliki bentuk seperti manusia yaitu memiliki tubuh dan kepala, dua tangan dan dua kaki yang memungkinkan dapat bergerak dan berinteraksi dengan lingkungan yang dibuat oleh manusia [1].

Salah satu implementasi robot humanoid adalah dijadikan sebagai robot sepakbola pada ajang Kontes Robot Indonesia (KRI) adalah ajang kompetisi rancang bangun dan rekayasa dalam bidang teknologi robotika yang diselenggarakan oleh Direktorat Kemahasiswaan, Direktorat Jenderal Pembelajaran dan Kemahasiswaan,

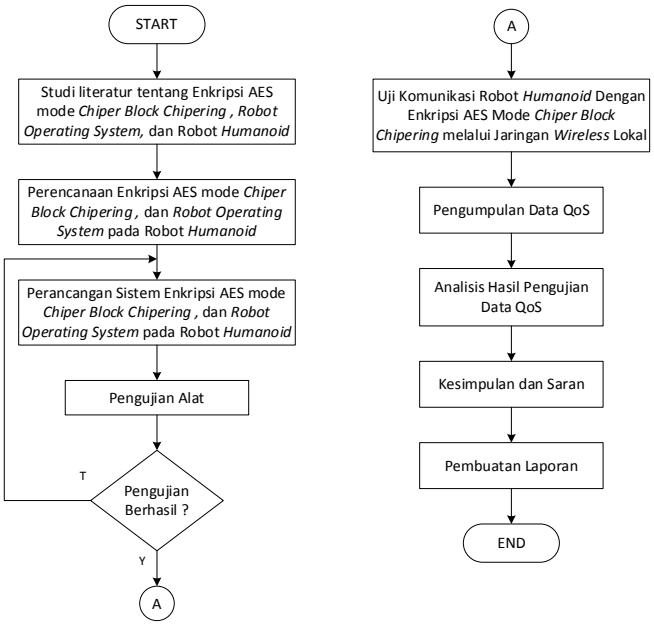
Kementrian Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia. Kontes ini dapat diikuti oleh tim mahasiswa pada Perguruan Tinggi yang tercatat di Kemenristekdikti. KRI tersebut terdapat berbagai divisi, salah satunya adalah Kontes Robot Sepak Bola Indonesia (KRSBI), divisi ini merupakan salah satu ajang kompetisi yang disertai dengan unsur-unsur sepak bola. Dan juga untuk dapat menjadi salah satu unggulan sarana edukasi dan ajang latih kreatifitas mahasiswa di bidang rekayasa robotika di tingkat dunia. Kontes ini juga menjadi ajang kualifikasi nasional untuk mewakili Indonesia dalam RoboCup yang merupakan kompetisi robot sepakbola resmi tingkat dunia di bawah organisasi RoboCup, seperti organisasi FIFA dalam kejuaraan dunia sepak bola manusia [4].

Sistem operasi yang biasa digunakan pada robot sepak bola humanoid adalah *Robot Operating System (ROS)*, yang pada dasarnya di dalam sistem tersebut tanpa ada enkripsi atau pengaman data setiap kali komunikasi dilakukan dengan pengiriman dan permintaan atau yang biasa disebut Publish dan Subscribe.

Dalam rangka pengembangan sistem ROS pada robot sepak bola humanoid, penelitian ini dirancang untuk memenuhi sebagai persyaratan memperoleh gelar Sarjana Terapan Teknik maka diusulkan judul "Implementasi Enkripsi Advanced Encryption Standard (AES-128) Mode Cipher Block Chaining (CBC) Sebagai Keamanan Komunikasi Pergerakan Robot Humanoid KRSBI" yang didesain untuk beroperasi pada konektivitas dengan kualitas yang rendah, dengan network bandwidth yang mengamankan setiap node yang berjalan di dalam ROS yang didalamnya terdapat fitur untuk subscribe topik dan juga publish topik. Kemudian dengan tambahan kriptografi dapat menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga message- message agar tetap aman (secure) [2]. Maka semua komunikasi dienkripsi dengan menggunakan Secure Sockets Layer (SSL), atau lebih spesifiknya Transport Layer Security (TLS). Setelah itu selesai menuju ke penggunaan Public Key Infrastructure (PKI), yang dimana setiap node ROS itu akan disediakan X.509 Certificate, yang setara dengan asymmetric key pair, yang telah diverifikasi oleh Certificate Authority (CA).

II. METODE

A. Tahapan Penelitian



Gambar 1. Diagram alir perancangan penelitian

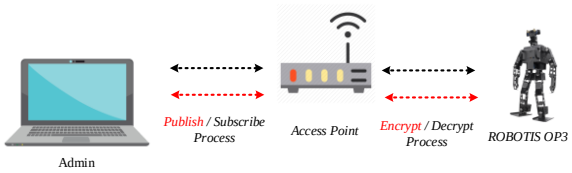
Gambar 1 merupakan perancangan penelitian yang akan dilakukan dalam pembuatan sistem, dengan penjelasan sebagai berikut:

1. Tahap pertama merupakan studi literatur untuk mencari berbagai referensi mengenai Enkripsi AES mode *Chiper Block Chipering*, *Robot Operating System*, dan Robot *Humanoid*. Pada tahap ini mempelajari penggunaan dan karakteristik mengenai Enkripsi AES mode *Chiper Block Chipering*, *Robot Operating System* dan Robot *Humanoid* serta bahasa pemrograman yang dibutuhkan untuk pengimplementasian sistem.
2. Tahap kedua yaitu perencanaan sistem mengenai permasalahan keamanan pergerakan robot dan parameter pengujian yang akan diperoleh dari Robot *Humanoid*.
3. Tahap ketiga yaitu perancangan Enkripsi AES mode *Chiper Block Chipering*, *Robot Operating System*, pada Robot *Humanoid* yang akan diuji.
4. Tahap keempat yaitu pengujian sistem dengan melakukan pengamanan data pergerakan robot dengan Enkripsi AES mode *Chiper Block Chipering* untuk mengetahui hasil pengujian sistem yang telah direncanakan. Jika hasil pengujian tidak sesuai dengan perencanaan maka kembali pada tahap perancangan sistem.
5. Tahap kelima yaitu pembuatan perintah dengan menggunakan bahasa pemrograman yang akan digunakan pada robot *humanoid* untuk uji komunikasi dengan laptop admin.
6. Tahap keenam yaitu uji komunikasi dengan robot *humanoid* yang sudah sesuai dengan perencanaan melalui jaringan *wireless* lokal.

7. Tahap ketujuh yaitu tahap pengumpulan data QoS yang meliputi data Bandwidth, Delay, Packet Loss, dan Throughput yang diperoleh dari pengujian sistem.
8. Tahap kedelapan yaitu tahap penarikan kesimpulan dan saran dari hasil pengujian.
9. Tahap kesembilan yaitu tahap akhir yaitu pembuatan laporan akhir hasil dari pengujian.

B. Perancangan Sistem

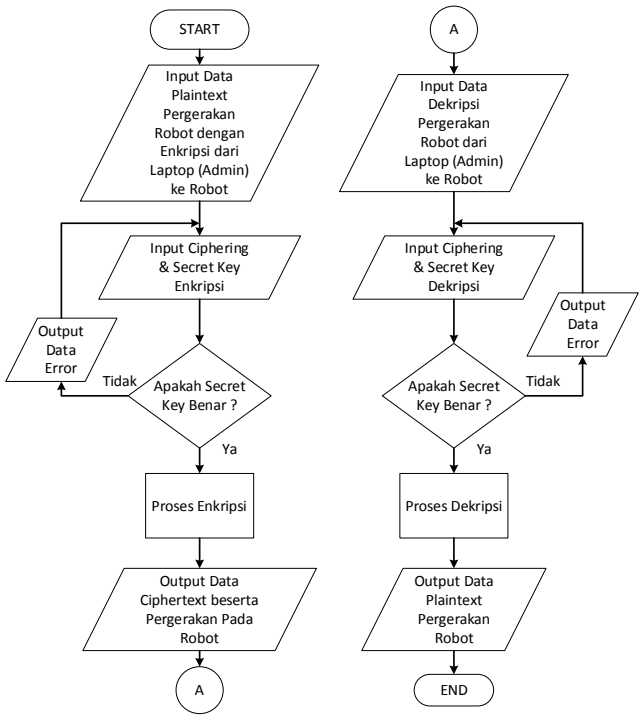
Untuk memberikan perintah pada robot *humanoid* dengan *script* yang menggunakan bahasa pemrograman python atau C++ yang di operasikan menggunakan Laptop Ubuntu 16.04 dengan tambahan berupa Enkripsi pada robot yang terkoneksi pada Access Point agar dapat memberi perintah pada robot sekaligus memantau keberadaan dan posisi robot berada.



Gambar 2. Blok diagram sistem

Gambar 2 menjelaskan bahwa perangkat penelitian terdiri dari *Script* Perintah Robot, Laptop OS Ubuntu 16.04, Access Point, ROS (*Robot Operating System*), dan Robot *Humanoid*.

C. Diagram Alir Cara Kerja Sistem



Gambar 3. Diagram alir cara kerja sistem

Pada Gambar 3 dijelaskan tentang alir sistem implementasi enkripsi aes sebagai keamanan komunikasi pergerakan robot *humanoid* krsbi. Langkah awal yaitu adanya input data plaintext pergerakan robot dengan enkripsi dari Laptop (Admin) menuju ke robot humanoid. Data pergerakan robot yang masuk akan di enkripsi dan dijalankan jika menginputkan secret key dengan benar. Output data yang akan dikeluarkan ialah hasil dari enkripsi data yang dinamakan ciphertext dan juga pergerakan robot. Untuk melihat isi data yang telah dienkripsi, Admin harus memasukkan secret key dengan benar. Kemudian data berupa ciphertext inilah yang akan di dekripsi kembali menjadi data informasi sebenarnya yang dinamakan plaintext. Output yang akan dikeluarkan ialah plaintext data dari pergerakan robot.

D. Algoritma Enkripsi AES Mode CBC

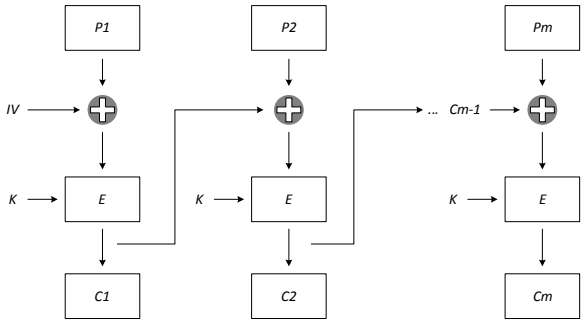
Algoritma Cipher Block Chaining (CBC) merupakan penerapan mekanisme umpan balik pada sebuah blok bit dimana hasil enkripsi blok sebelumnya diumpan balikkan ke dalam proses enkripsi blok current. Caranya, blok plaintext yang current di-XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma CBC, setiap blok ciphertext tidak hanya bergantung pada blok plaintextnya tetapi juga pada seluruh blok plaintext sebelumnya. Dekripsi dilakukan dengan memasukkan blok ciphertext yang current ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok ciphertext sebelumnya. Blok ciphertext sebelumnya berfungsi sebagai umpan maju (feedforward) pada akhir proses dekripsi [5].

Secara matematis, enkripsi dan dekripsi dengan algoritma CBC dinyatakan sebagai:

$$Ci = Ek\,(\oplus\, Ci - 1) \qquad (1)$$

$$Pi = Dk(Ci \oplus Ci - 1) \qquad (2)$$

Dimana $i = 1, 2, \ldots, m$



Gambar 4. Cara kerja sistem enkripsi AES mode CBC

Enkripsi blok pertama, *C0 = IV* (*Initialization Vector*). *IV* dapat diberikan kepada pengguna atau dibangkitkan secara acak oleh program jadi, untuk menghasilkan blok ciphertext pertama (*C1*), *IV* digunakan untuk menggantikan blok ciphertext sebelumnya. Sebaliknya pada dekripsi blok plaintext pertama diperoleh dengan cara meng-XOR-kan *IV*

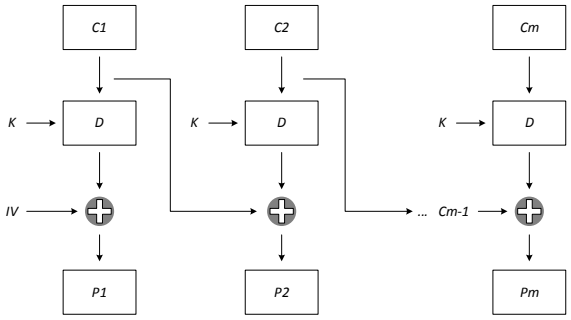
dengan hasil dekripsi terhadap blok ciphertext pertama. *IV* tidak perlu rahasia, jadi untuk m buah blok plaintext, enkripsi nya adalah [5]:

$$C1 = Ek\ (P1 \oplus IV) \quad (3)$$

$$C2 = Ek\ (P2 \oplus C1) \quad (4)$$

$$C3 = Ek(P3 \oplus C2) \quad (5)$$

$$Cm = Ek\ (Pm \oplus Cm\text{-}1) \quad (6)$$



Gambar 5. Cara kerja sistem dekripsi AES Mode CBC

Sebaliknya pada dekripsi, blok plainteks diperoleh dengan cara meng-XOR-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama [6].

III. HASIL DAN PEMBAHASAN

A. Pengaruh Enkripsi AES (Advanced Encryption Standard) Terhadap Keamanan Data Pergerakan Robot

Pengujian dilakukan di lapangan sepakbola robot yang berada di Gedung Sipil Lt.8 dengan menggunakan 1 Laptop sebagai Admin, 1 Robot humanoid dan 1 Access Point sebagai pemancar koneksi Wireless. Seperti pada gambar berikut:

Gambar 6. Set-up pengujian enkripsi AES terhadap keamanan data pergerakan robot

1. Menjalankan program yang bernama "ball_ballan.launch" untuk mengaktifkan robot pada mode sepakbola, dengan perintah "roslaunch krsbi ball_ballan.launch". Seperti gambar di bawah ini:

```
$ roslaunch krsbi ball_ballan.launch
```

Gambar 7. Menjalan Program ball_ballan.launch

Maka robot akan aktif pada mode sepakbola, seperti gambar di bawah ini:

Gambar 8. Robot Aktif Pada Mode Sepakbola

2. Menjalankan program yang bernama "kembaliKePosisiSiapCiphered.launch" yang telah dienkripsi dengan AES-128 mode CBC namun tanpa memasukkan kunci rahasia / secret_key dengan perintah "roslaunch simple_talker_listener kembaliKePosisiSiapCiphered.launch". Seperti pada gambar di bawah ini:

```
$ roslaunch simple_talker_listener
kembaliKePosisiSiapCiphered.launch
```

Gambar 9. Menjalankan program kembalikeposisisiapciphered.launch tanpa key

Maka akan muncul notifikasi error pada log program yang dijalankan yaitu seperti pada gambar di bawah ini:

```
[ERROR] [1591097445.566094]:
Key yang anda masukkan salah
```

Gambar 10. Notifikasi error pada log program

Gambar di atas menampilkan log:
"[ERROR] [1591091060.598761]: Invalid encryption method >: "
Dengan penjelasan sebagai berikut:

- [ERROR] = Respon info gagal dari program yang dijalankan
- [1591097445.566094] = Timestamp (urutan karakter yang dikodekan kapan peristiwa terjadi)
- Key yang anda masukkan salah = Key yang dimasukkan salah / tidak memasukkan key

Maka yang terjadi robot tetap bergerak pada mode sepakbola dant tidak kembali ke posisi siap, seperti gambar di bawah ini:

Gambar 11. Robot tetap pada mode sepakbola

3. Menjalankan program yang bernama "kembaliKePosisiSiapCiphered.launch" yang telah dienkripsi dengan AES-128 mode CBC namun dengan memasukkan kunci rahasia / secret_key dengan perintah "roslaunch simple_talker_listener kembaliKePosisiSiapCiphered.launch ciphering:=AES secret_key:= polinemajayaokay". Seperti pada gambar di bawah ini:

```
roslaunch simple_talker_listener
kembaliKePosisiSiapCiphered.launch
ciphering:=AES secret_key:=polinemajayaokay
```

Gambar 12. Menjalankan program kembalikeposisisiapciphered.launch dengan key

Maka yang terjadi robot yang awalnya pada mode sepakbola akan berubah menjadi mode kembali ke posisi siap, seperti gambar di bawah ini:

Gambar 13. Robot kembali ke posisi siap

4. Hasil pesan yang dienkripsi:

```
---
data: !!binary |
  3nYlVhkU0C+DYYYZLWBCSSqL9/+bYIbQiEVQUy+BvGRBl0LiX7mEuancgEf
e7UHhGo32dAH8sREs
  fM2DXx+/5RR89keSCn/vIlBTgARxbXYOnynQ74H8MSQFo8p7OKEV
---
data: !!binary |
  UAEF0LMcHPZryTULHYZ9lRx8ew8drHwiCGktn6l6ICmwqkO5U6l2P04yWcV
m6bo5gcyv95OQVhUl
  fmJafZy8UjKzWsL2lk6+AvrZfSNuwU9OM7TjRVASJiXE/MrPVWIP
```

Gambar 14. Hasil pesan yang dienkripsi

Dari gambar 14 menampilkan hasil data berupa ciphertext / pesan yang telah dienkripsi, maka dari itu hasil data tersebut tidak dapat dibaca atau sulit untuk dipecahkan, dikarenakan hasil dari ciphertext secara acak dan terus menerus, hingga kita dapat mendekripsikan pesan tersebut dengan program.

5. Hasil pesan yang didekripsi:

```
[INFO] [1591097556.123661]: /listenerCiphererPosisiSiap - I h
eard: Robot humanoid dalam keadaan siap with cipher 159109755
6.02
[INFO] [1591097556.323954]: /listenerCiphererPosisiSiap - I h
eard: Robot humanoid dalam keadaan siap with cipher 159109755
6.22
```

Gambar 15. Hasil pesan yang didekripsi

Dari gambar di atas menampilkan log:

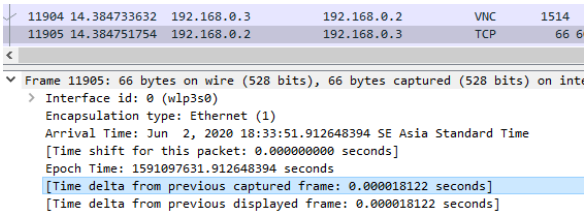
- "[INFO] [1591097556.123661]: /listenerCipherer PosisiSiap – I heard: Robot humanoid dalam keadaan siap with cipher 1591097556.02"

Dengan penjelasan sebagai berikut:

- [INFO] = Respon info berhasil dari program yang dijalankan
- [1591097556.123661] = Timestamp (urutan karakter yang dikodekan kapan peristiwa terjadi)
- /listenerCiphererPosisiSiap = Nama node pada sebuah topik
- I heard: Robot humanoid dalam keadaan siap with cipher = Isi data sebenarnya yang dienkripsi

B. Pengkuruan Waktu Delay Berdasarkan Perubahan Waktu Terhadap Keamanan Data Pergerakan Robot

Melihat hasil capture data seperti pada gambar di bawah ini:



Gambar 16. Hasil pengkuruan waktu delay

Dari gambar di atas terdapat "Time delta from previous captured frame: " yang artinya selisih waktu dengan paket sebelumnya atau bisa disebut sebagai delay yakni selama: 0.000018122 seconds atau sama halnya dengan 0.018122 miliseconds.

Kemudian dilakukan pengukuran selama 15 detik, 30 detik, dan 60 detik. Dan didapatkan hasil pada tabel berikut ini:

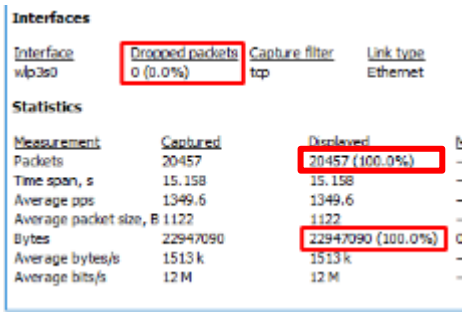
TABEL 1
HASIL PENGUKURAN WAKTU DELAY

No.	Waktu (s)	Delay (s)	Delay (ms)
1.	15	0.000018122	0,018122
2.	30	0,000026423	0,026423
3.	60	0,000032117	0,032117

Berdasarkan hasil data tabel di atas menunjukan bahwa delay yang didapatkan pada saat komunikasi antara robot humanoid dengan Admin(laptop) tidak menyentuh angka 1 Second (detik) yang artinya delay yang didapatkan tidaklah besar sehingga data yang dikirim dan diterima dapat sampai dengan cepat dan aman. Delay tertinggi diperoleh pada percobaan selama 60 detik yaitu sebesar 0,032117 ms dan delay terendah diperoleh pada percobaan selama 15 detik yaitu 0,018122 ms.

C. Pengkuruan Packet Loss dan Throughput Berdasarkan Perubahan Waktu Terhadap Keamanan Data Pergerakan Robot

Melihat hasil capture file properties untuk melihat secara keseluruhan kebutuhan data yang dikomunikasikan antara robot dengan admin(laptop). Seperti pada gambar di bawah ini:



Gambar 17. Hasil capture file properties

Dari gambar di atas didapatkan hasil pengukuran Packet Loss dan Throughput pada tabel 2 dan tabel 3 di bawah ini:

TABEL 2
HASIL PENGUKURAN PACKET LOSS

No.	Waktu (s)	Dropped Packets / Packet Loss
1.	15	0(0,0%)
2.	30	0(0,0%)
3.	60	0(0,0%)

Berdasarkan hasil data tabel di atas menunjukan bahwa Dropped Packets / Packet Loss yang didapatkan pada saat komunikasi antara robot humanoid dengan Admin(laptop) sebesar 0 (0,0%) yang artinya tidak ada paket yang hilang sehingga data yang dikirim dan diterima dapat tersampaikan dengan akurat dan aman.

Untuk hasil pengukuran Throughput terdapat pada tabel 3 di bawah ini:

TABEL 3
HASIL PENGUKURAN THROUGHPUT

No.	Waktu (s)	Packets	Bytes (B) / Throughput	Megabytes (MB) / Throughput
1.	15	11908	13979847 (100%)	13,97
2.	30	4954	4937262 (100%)	4,9
3.	60	10378	10274431 (100%)	10,27

Berdasarkan hasil data tabel di atas menunjukan bahwa nilai Throughput yang didapatkan mengalami kenaikan dan juga penurunan. Kenaikan dan penurunan tersebut dipengaruhi oleh besarnya Packets yang tercapture, semakin sedikit Packets yang tercapture maka nilai Throughput yang didapatkan semakin kecil, dan semakin besar Packets yang tercapture maka nilai Throughput yang didapatkan juga semakin besar. Nilai Throughput terkecil terdapat pada percobaan selama 30 detik, yaitu sebesar 4,9 MB (Megabytes) dan nilai Throughput terbesar terdapat pada percobaan selama 15 detik, yaitu sebesar 13,97 MB (Megabytes).

IV. KESIMPULAN

Dari hasil yang didapatkan pada percobaan dan hasil analisis sebelumnya, maka didapatkan beberapa poin kesimpulan berdasarkan rumusan masalah dari penelitian "Implementasi Enkripsi AES-128 Mode CBC Sebagai Keamanan Komunikasi Pergerakan Robot Humanoid KRSBI". Hasil kesimpulan tersebut ialah:

1. Hasil ciphertext yang diperoleh dari enkripsi dengan metode Cipher Block Chaining ialah sebanyak 128 bit dan dengan panjang kunci 16 bit.
2. Didapatkan hasil pengukuran packet loss sebesar 0,0% dan delay paling tinggi mencapai 0,023 ms pada percobaan enkripsi terhadap data String.
3. Didapatkan hasil pengukuran packet loss sebesar 0,0% dan delay paling tinggi mencapai 0,032 ms pada percobaan enkripsi terhadap data pergerakan robot.

REFERENSI

[1] A. Jalil, "Robot Operating System (Ros) Dan Gazebo Sebagai Media Pembelajaran Robot Interaktif," *Ilk. J. Ilm.*, vol. 10, no. 3, p. 284, 2018, doi: 10.33096/ilkom.v10i3.365.284-289.

[2] H. Ary, "PENGENALAN KRIPTOGRAFI DAN PEMAKAIANYA SEHARI-HARI," *J. Pengenalan Kriptografi*, no. May, 2016.

[3] S. H. SINAGA, "PERANCANGAN DAN IMPLEMENTASI ROBOT TARI HUMANOID DENGAN 24 DERAJAT KEBEBASAN PERANCANGAN DAN IMPLEMENTASI ROBOT TARI," *Dok. TUGAS AKHIR Inst. Teknol. DEL*, no. 1, 2019.

[4] Kemenristekdikti, "ATURAN PERTANDINGAN (LAWS OF GAME) KONTES ROBOT SEPAK BOLA INDONESIA (KRSBI) Humanoid 2019," *Buku Pandu. KRSBI Humanoid*, 2019.

[5] D. Andriani, "Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining," *J. Tek. Inform. Unika St. Thomas*, vol. 02, no. 338, pp. 14–23, 2017.

[6] B. Kuliah, "Tipe dan Mode Algoritma Simetri Departemen Teknik Informatika Institut Teknologi Bandung," no. Bagian 2, pp. 1–18, 2004.