SEMINAR NASIONAL 2026 Universitas Ma Chung

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026

ISSN: 2808-2826 online

Algoritma Enkripsi AES 256 dan Verifikasi OTP Komunikasi Client-Server pada Python

Clint Joy Perez Melody Mokosandi[1], Bita Parga Zen[2], Hendry Setiawan[3]

[1,2,3] Teknik Informatika, Universitas Ma Chung, Malang, Indonesia

Correspondence: Bita Parga Zen (bita.parga@machung.ac.id)

Received: 27 05 2026 – Revised: 29 07 2026 - Accepted: 04 08 2026 - Published: 05 08 2026

Abstrak. Dalam sistem berbasis jaringan komunikasi kendali beberapa tahapan yang dilakukan terutama untuk menjaga keamanan data. Komunikasi client-server menjadi hal yang penting dalam melakukan komunikasi, banyak nya tantangan dalam keamanan menjadi perioritas utama untuk menjaaga integritas data, penelitian ini menyarankan penggunaan AES sebagai enkripsi data dalam hal komunikasi nya, sistem AES menggunakan kunci yang sama untuk enkripsi dan dekripsi AES.generate_key, pada sistem ini menggunakan standar AES dalam CBC mode dengan kunci 128-bit untuk enkripsi, selanjutnya menggunakan PKCS7 padding, HMAC digunakan SHA256untuk autentikasi dan menggunakan token = f.encrypt(b"Secret message!") dalam pengiriman pesan pada proses enkripsi hasil enkripsi (byte): b'\x80\x01\x02...' (64+ byte). Hasil dari encode base64: gAAAAABkO. dekripsi dengan token Base64 gAAAAABkO didecode ke byte asli., sistem ini dibuat untuk dapat mengenkripsi pesan di sisi klien sebelum dikirimkan ke server melalui koneksi TCP. Dengan menggunakan metode enkripsi AES dalam komunikasi client server, sistem dapat melindungi privasi data dengan mengenkripsinya dan menjamin kualitas komunikasi yang aman, pada penelitian ini terbukti dapat dijalankan dengan baik

Kata kunci: AES, Client-Server, Enkripsi, Programming, Python

PENDAHULUAN

Dalam era digital yang berkembang pesat, keamanan informasi menjadi aspek krusial, terutama dalam institusi yang menangani data dengan sensitivitas tinggi seperti militer. Komunikasi yang aman dan rahasia antar unit-unit militer merupakan fondasi utama untuk menjaga stabilitas dan kedaulatan negara. Tanpa mekanisme enkripsi yang handal, risiko kebocoran informasi strategis dan taktis meningkat secara signifikan, yang pada gilirannya dapat membahayakan operasi militer dan keamanan nasional Luo et al. (2020) (Doukas et al., 2020; Kencana et al., 2024) Marpaung et al. (2024).

Berbagai upaya telah dilakukan untuk mengatasi tantangan keamanan komunikasi, mulai dari adopsi protokol enkripsi standar hingga pengembangan algoritma kriptografi yang lebih kompleks. Namun, penerapan yang efektif dan sederhana namun tetap kuat untuk lingkungan militer masih menjadi area eksplorasi yang memerlukan penelitian lebih lanjut Mistri et al. (2023), Mumtaz et al. (2019)

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

Penelitian ini mengusulkan pengembangan sistem komunikasi client–server menggunakan bahasa pemrograman Python, dirancang khusus untuk memenuhi kebutuhan komunikasi rahasia di lingkungan militer. Sistem ini melibatkan tiga entitas klien—TNI AD, TNI AL, dan TNI AU—yang berkomunikasi dengan satu server pusat (MABES TNI). Untuk menjamin kerahasiaan pesan, sistem menggunakan algoritma enkripsi **AES** dari pustaka *Cryptography*, yang mengandalkan AES-128-CBC untuk enkripsi dan HMAC-SHA256 untuk otentikasi Zen BP et al. (2024) Nurrobi et al. (2020)

Server MABES TNI akan menerima pesan terenkripsi, menampilkannya, dan mendekripsinya sehingga pesan asli dapat dibaca. Sistem juga memastikan ketiga klien dapat berkomunikasi secara bergantian atau simultan, dengan contoh pesan "latihan gabungan militer," menyerupai kondisi komunikasi taktis. Tujuan penelitian ini adalah membangun dan mendemonstrasikan prototipe sistem komunikasi client–server yang aman dan terenkripsi menggunakan Python dan algoritma AES, sebagai acuan awal sistem komunikasi rahasia di lingkungan militer. Padhiary et al. (2025), Shim et al. (2025), Sulistiya et al. (2023)

MASALAH

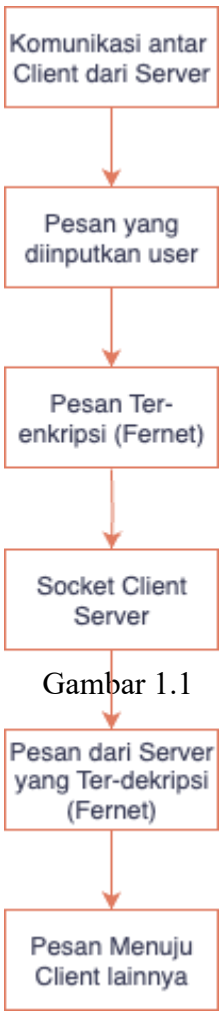
Dalam komunikasi militer TNI, menjaga kerahasiaan dan integritas informasi sangat vital karena berkaitan langsung dengan keselamatan personel TNI dan keberhasilan operasi pada pertahanan siber. Yang menjadi tantangan utama yang dihadapi adalah risiko penyadapan dan intersepsi pesan oleh musuh yang bersifat massive dan sulit diketahui.

Militer TNI di Indonesia memerlukan sistem komunikasi yang aman namun tetap ringan, mudah digunakan, dan cepat diterapkan di berbagai kondisi medan, untuk membantu koordinasi antar matra TNI (AD, AL, AU) dalam menghadapi kendala sistem komunikasi yang bersifat realtime

Komunikasi client-server menggunakan enkripsi AES secara khusus untuk skenario komunikasi antar matra TNI demi menjaga keamanan data. Dimana terintegrasi socket Python dengan cryptography.AES. Suryani et al. (2018)

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

METODE PELAKSANAAN



Gambar 1.1

Pada bagian ini menguraikan pendekatan dan tahapan yang akan digunakan untuk mengembangkan serta menganalisis sistem komunikasi client-server terenkripsi menggunakan algoritma AES dalam lingkungan Python, khususnya untuk skenario komunikasi militer antar klien TNI. Metode yang diterapkan adalah Difusi dan Penerapan Ipteks karena kegiatan ini menghasilkan prototipe sistem komunikasi yang aman dan fungsional sebagai solusi atas kebutuhan spesifik pengguna (TNI).

1. Desain Sistem Komunikasi Client-Server

Pada tahap ini, akan dilakukan perancangan arsitektur sistem komunikasi client-server yang melibatkan satu server pusat (MABES TNI) dan tiga klien (TNI AD, TNI AL, TNI AU). Desain ini akan mencakup:

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

- Arsitektur Jaringan: Penggunaan model komunikasi TCP/IP berbasis soket Python untuk memastikan koneksi yang andal dan berorientasi koneksi.
- Peran Server (MABES TNI):
  - Mendengarkan koneksi dari ketiga klien secara simultan atau bergantian.
  - Menerima pesan terenkripsi dari klien.
  - Menampilkan pesan terenkripsi dalam server.
  - Mengirimkan balasan/konfirmasi terenkripsi ke klien yang bersangkutan.

- Peran Klien (TNI AD, TNI AL, TNI AU):
  - Membangun koneksi ke server MABES TNI.
  - Menghasilkan atau menggunakan kunci AES yang sama dengan server.
  - Mengenkripsi pesan menggunakan kunci AES sebelum pengiriman.
  - Mengirimkan pesan terenkripsi ke server.
  - Menerima dan mendekripsi balasan dari server.
- Manajemen Kunci AES: Untuk kebutuhan prototipe, kunci AES akan dihasilkan oleh server dan dibagikan ke semua klien secara *out-of-band* atau melalui mekanisme sederhana yang aman sebelum komunikasi terenkripsi dimulai. Dalam implementasi riil, mekanisme pertukaran kunci yang lebih robust akan diperlukan.

2. Implementasi Sistem

Tahap implementasi akan fokus pada pengembangan kode program menggunakan Python, dengan memanfaatkan pustaka-pustaka utama sebagai berikut:

- Library socket: Digunakan untuk membangun koneksi TCP/IP antara client dan server, serta untuk mengirim dan menerima data.
- Library cryptography (AES): Digunakan untuk implementasi algoritma enkripsi dan dekripsi AES.
  - Pembangkitan Kunci: AES.generate_key() akan digunakan untuk menghasilkan kunci simetris yang aman.
  - Enkripsi: Objek AES akan diinisialisasi dengan kunci yang dihasilkan, dan metode encrypt() akan digunakan untuk mengenkripsi pesan (dalam format byte).
  - Dekripsi: Metode decrypt() akan digunakan untuk mengubah pesan terenkripsi kembali ke bentuk asli (plainteks).
- Struktur Data Pesan: Pesan akan dienkripsi dalam bentuk *byte*. Struktur pesan dapat mencakup informasi pengirim (klien AD, AL, AU) dan isi pesan itu sendiri.

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

3. Skenario Uji dan Pengumpulan Data

Pengujian sistem akan dilakukan dengan mengimplementasikan skenario komunikasi taktis yang mirip dengan kondisi militer.

- Skenario Komunikasi:

o Setiap klien (TNI AD, TNI AL, TNI AU) akan mengirimkan pesan contoh "latihan gabungan militer" ke server MABES TNI.

o Pengiriman pesan dapat dilakukan secara bergantian maupun simultan untuk menguji kapabilitas server dalam menangani beberapa koneksi.

o Server akan menerima pesan terenkripsi, mendekripsinya, dan menampilkannya di konsol server.

- Teknik Pengumpulan Data:

o Observasi Langsung: Memantau fungsionalitas sistem secara langsung selama pengiriman dan penerimaan pesan terenkripsi dan terdekripsi.

o Pencatatan Log: Merekam *output* konsol dari sisi client dan server untuk memverifikasi proses enkripsi, transmisi, dan dekripsi pesan.

4. Teknik Analisis Data

Analisis data akan berfokus pada validasi fungsionalitas dan demonstrasi keamanan sistem.

- Analisis Kualitatif:

o Verifikasi Fungsionalitas: Memastikan bahwa pesan yang dikirimkan oleh klien berhasil dienkripsi, ditransmisikan, dan diterima oleh server lalu dikirimkan kepada client dan didekripsikan sehingga membentuk pesan asli (plainteks).

o Validasi Keamanan: Menganalisis pesan dari server yang melalui command prompt, melihat apakah pesan tersebut sudah terenkripsi dengan baik dan ditampilkan pada layar server sebagai acuan agar mengetahui bahwa pesan tersebut sudah terenkripsi dengan benar.

o Kemudahan Implementasi: Mengevaluasi kemudahan dan efisiensi penggunaan library cryptography.AES dalam pengembangan sistem ini.

- Evaluasi Relevansi Militer: Mengevaluasi bagaimana prototipe ini dapat menjadi acuan awal dan memenuhi kebutuhan komunikasi rahasia di lingkungan militer, khususnya dalam menjaga kerahasiaan dan integritas informasi antar TNI.

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

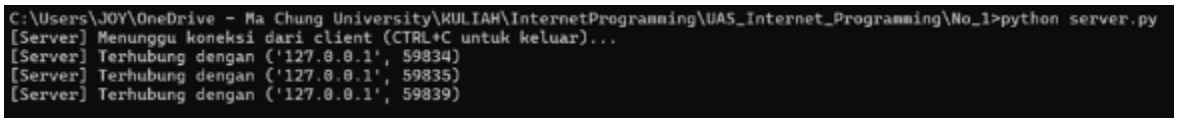
5. Lokasi dan Waktu Kegiatan

- Lokasi: Implementasi dan pengujian sistem akan dilakukan di lingkungan laboratorium pada Universitas Ma Chung, menggunakan dua atau lebih command prompt yang terhubung dalam satu komputer pada jaringan lokal.
- Waktu dan Durasi: Proyek ini direncanakan berlangsung selama 2 minggu, dimulai dari perancangan (2 hari), implementasi (10 hari), serta pengujian secara berkala dan analisis hasil pengujian (2 hari).

HASIL DAN PEMBAHASAN (CLINT)

Pada bagian ini menyajikan hasil yang diperoleh dari pengujian serta pembahasan penggunaan algoritma enkripsi AES secara mendalam. Pengujian dilakukan dengan membuat sistem komunikasi client dan server menggunakan bahasa pemrograman python menggunakan algoritma enkripsi AES.

Langkah awal dimulai dengan membuat key dari enkripsi AES yang akan dibuat dan disimpan didalam file key.key, serta menyertakan key tadi kedalam program server dan client agar nantinya pesan yang dikirim dapat di dekripsi.



Gambar 1.2

Kemudian, program server dijalankan, server akan berada dalam kondisi **siaga** untuk menerima koneksi dari client. Hal ini ditunjukkan oleh pesan pada terminal: [Server] Menunggu koneksi dari client (CTRL+C untuk keluar)... Selanjutnya, ketika terdapat client yang mencoba terhubung, server akan mencatat alamat IP dan nomor port dari masing-masing client yang berhasil terkoneksi. Sebagai contoh, pada Gambar 1.2 ditunjukkan bahwa beberapa client berhasil terhubung ke server dengan alamat IP lokal '127.0.0.1' dan port yang berbeda-beda, yaitu 59834, 59835, 59839, dan 59839. Alamat '127.0.0.1' merupakan alamat **localhost**, yang menandakan bahwa client dijalankan di komputer yang sama dengan server. Setiap koneksi menggunakan port yang unik untuk membedakan komunikasi antar client. Proses ini menjadi tahap awal sebelum server menerima pesan dari client, yang kemudian akan ditampilkan bersama dengan informasi identitas pengirim, hasil enkripsi, serta pesan yang telah berhasil didekripsi.

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

```
C:\Users\JOY\OneDrive - Ma Chung University\KULIAH\InternetProgramming\UAS_Internet_Programming\No_1>python client.py
Pilih identitas client:
1. TNI AD
2. TNI AL
3. TNI AU
Masukkan pilihan (1/2/3): 1

Terhubung ke server. Ketik 'exit' untuk keluar.

Masukkan pesan untuk dikirim ke MABES TNI: Siap latihan gabungan
[CLIENT] Pesan terenkripsi berhasil dikirim.
Masukkan pesan untuk dikirim ke MABES TNI: exit
[CLIENT] Keluar dari aplikasi.
```

Gambar 1.3

```
C:\Users\JOY\OneDrive - Ma Chung University\KULIAH\InternetProgramming\UAS_Internet_Programming\No_1>python client.py
Pilih identitas client:
1. TNI AD
2. TNI AL
3. TNI AU
Masukkan pilihan (1/2/3): 2

Terhubung ke server. Ketik 'exit' untuk keluar.

Masukkan pesan untuk dikirim ke MABES TNI: Kami siap latihan gabungan
[CLIENT] Pesan terenkripsi berhasil dikirim.
Masukkan pesan untuk dikirim ke MABES TNI: exit
[CLIENT] Keluar dari aplikasi.
```

Gambar 1.4

```
C:\Users\JOY\OneDrive - Ma Chung University\KULIAH\InternetProgramming\UAS_Internet_Programming\No_1>python client.py
Pilih identitas client:
1. TNI AD
2. TNI AL
3. TNI AU
Masukkan pilihan (1/2/3): 3

Terhubung ke server. Ketik 'exit' untuk keluar.

Masukkan pesan untuk dikirim ke MABES TNI: Menunggu perintah latihan gabungan
[CLIENT] Pesan terenkripsi berhasil dikirim.
Masukkan pesan untuk dikirim ke MABES TNI: exit
[CLIENT] Keluar dari aplikasi.
```

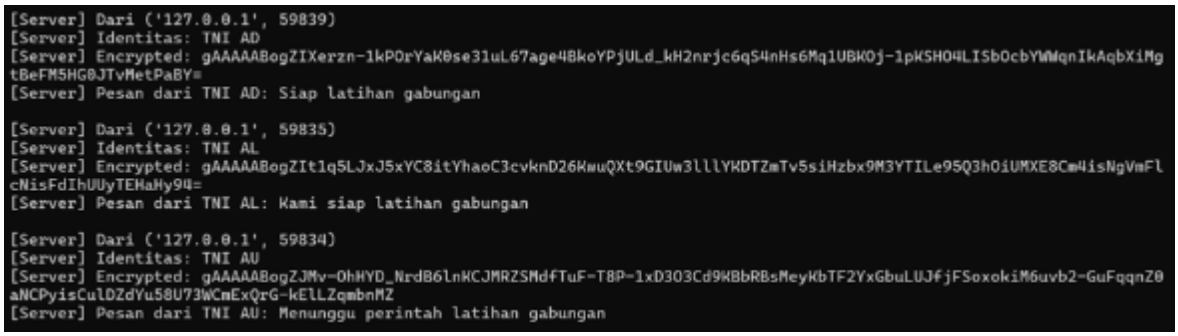
Gambar 1.5

Setelah server aktif, langkah selanjutnya adalah menjalankan program client. Aplikasi client dijalankan sebanyak tiga instance untuk merepresentasikan tiga satuan TNI, yaitu TNI AD, TNI AL, dan TNI AU. Pada saat eksekusi, pengguna diminta memilih identitas client dengan memasukkan angka 1 hingga 3. Pemilihan ini digunakan untuk membedakan setiap client yang terhubung ke server pusat (MABES TNI). Setelah koneksi dengan server berhasil, pengguna dapat mulai mengirimkan pesan.

Pengiriman pesan dari client ke server dilakukan dalam bentuk terenkripsi. Sistem menggunakan algoritma enkripsi simetris **AES** dari pustaka cryptography, yang memastikan pesan tidak dapat dibaca oleh pihak yang tidak memiliki kunci enkripsi yang sama. Ketika pengguna mengetikkan sebuah pesan, sistem akan mengenkripsi pesan tersebut terlebih dahulu, kemudian mengirimkannya ke server. Setelah pesan berhasil dikirim, client menampilkan notifikasi bahwa pesan telah terenkripsi dan dikirimkan ke MABES TNI. Proses ini berjalan hingga pengguna mengetikkan perintah exit, yang akan menutup koneksi dan keluar dari aplikasi. Contoh hasil eksekusi dapat dilihat pada Gambar 1.6, di mana client

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

dengan identitas TNI AU berhasil mengirimkan pesan “Menunggu perintah latihan gabungan” yang telah terenkripsi, sebelum akhirnya keluar dari aplikasi setelah perintah exit.



Gambar 1.6

Pada gambar tersebut ditampilkan hasil implementasi komunikasi antara client dan server menggunakan enkripsi simetris *AES* pada socket di Python. Ketika client mengirimkan sebuah pesan, server akan menerima data dalam format gabungan antara identitas pengirim dan pesan yang telah dienkripsi.

Pada prosesnya, server akan memisahkan identitas pengirim dan pesan terenkripsi berdasarkan delimiter ||. Selanjutnya, server akan menampilkan tiga informasi penting, yaitu:

1. **Identitas Pengirim:** Identitas client yang mengirimkan pesan, seperti "TNI AD", "TNI AL", atau "TNI AU", ditentukan pada saat client melakukan koneksi.
2. **Pesan Terenkripsi:** Merupakan hasil enkripsi menggunakan algoritma *AES*, yang menunjukkan bahwa pesan telah diamankan sebelum dikirim melalui jaringan.
3. **Pesan Terdekripsi:** Merupakan hasil dekripsi dari server menggunakan kunci simetris yang sama dengan client. Ini menunjukkan bahwa sistem berhasil melakukan proses dekripsi dan mendapatkan kembali pesan asli, misalnya "halo".

Tampilan tersebut mengonfirmasi bahwa proses pengiriman pesan antar client dan server berjalan dengan aman dan sesuai skema, di mana data yang dikirim melalui jaringan tidak dalam bentuk teks biasa (*plaintext*) tetapi terenkripsi, sehingga menjaga kerahasiaan isi pesan.

Prosiding Seminar Teknologi Informasi
pp. 165-174, 2026
ISSN: 2808-2826 online

KESIMPULAN

Kegiatan ini berhasil mencapai seluruh target yang telah direncanakan, yaitu membangun sistem komunikasi client-server berbasis socket Python yang dilengkapi dengan fitur enkripsi menggunakan algoritma AES dari pustaka cryptography. Implementasi algoritma AES terbukti berhasil menjaga kerahasiaan pesan dengan mengenkripsi dan mendekripsi data secara simetris menggunakan kunci rahasia yang sama. Sistem dapat menangani komunikasi antar beberapa client secara paralel setelah dilakukan modifikasi multi-threading, serta mampu menjamin keamanan data yang ditransmisikan. Dampak dari kegiatan ini adalah meningkatnya pemahaman peserta terhadap konsep enkripsi simetris dan penerapannya dalam komunikasi jaringan nyata. Ke depan, sistem ini direkomendasikan untuk dikembangkan lebih lanjut dengan menambahkan otentikasi pengguna dan penggunaan protokol yang lebih aman seperti TLS guna meningkatkan keamanan dan skalabilitas aplikasi.

DAFTAR PUSTAKA

Luo, S., Zhang, Z., Wang, S., Zhang, S., Dai, J., Bu, X., & An, J. (2020). Network for hypersonic UCAV swarms. *Science China Information Sciences*, *63*(4), 1–28. https://doi.org/10.1007/s11432-019-2765-7

Marpaung, N. L., Amri, R., Febrianzio, S., Ervianto, E., & Ali, N. D. (2024). Identification of internet network based on quality of service using TIPHON. *AIP Conference Proceedings*, *3026*(1), 50002. https://doi.org/10.1063/5.0199879

Mistri, R. K., Mahto, S. K., Singh, A. K., Sinha, R., Al-Gburi, A. J. A., Alghamdi, T. A. H., & Alathbah, M. (2023). Quad Element MIMO Antenna for C, X, Ku, and Ka-Band Applications. *Sensors (Basel, Switzerland)*, *23*(20). https://doi.org/10.3390/s23208563

Mumtaz, N., Perdana, D., & Bisono, G. (2019). Performance Evaluation of VoIP Traffic in 5G Millimeter Wave Network. *International Journal of Simulation: Systems, Science & Technology*, *18*(1), 6. https://doi.org/10.5013/ijssst.a.20.02.18

Zen, B. P., Abdurahman, Zafia, A., Utami, A., Putro, I. N. Y., & Aditama, F. D. (2024). Multi Socket Transmission System Application with Advanced Encryption Standard Algorithm to Support Confidential Medical Data Security. *Proceedings of the 4th International Conference on Electronics, Biomedical Engineering, and Health Informatics. ICEBEHI 2023. Lecture Notes in Electrical Engineering, vol 1182*. Springer, Singapore. https://doi.org/10.1007/978-981-97-1463-6_1

Nurrobi, I., Kusnadi, K., & Adam, R. (2020). Penerapan Metode QoS (Quality of Service) untuk Menganalisa Kualitas Kinerja Jaringan Wireless. *Jurnal Digit*, *10*(1), 47. https://doi.org/10.51920/jd.v10i1.155

Padhiary, M., Roy, P., & Kumar, K. (2025). Simulation Software in the Design and AI-Driven Automation of All-Terrain Farm Vehicles and Implements for Precision Agriculture. *Recent Progress in Science and Engineering*, *01*(02), 6. https://doi.org/10.21926/rpse.2502006

Shim, H., Kang, B., Im, H., Jeon, D., & Kim, S. (2025). TrustNet Virtual Private Network (VPN): Enhancing Security in the Quantum Era. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3530985

 Sulistiya, Kusuma, Y. F., Yohanes, F. A., Daryanto, Y., Risnawan, N., & Baehaqi, F. A. (2023). Validation of the turbulence model in predicting aerodynamic characteristics of PUNA MALE using OpenFOAM software. *AIP Conference Proceedings*, *2941*(1), 20009. https://doi.org/10.1063/5.0181456

 Suryani, I., Lindawati, L., & Salamah, I. (2018). Analisa QOS (Quality Of Service) Jaringan Internet Di Teknik Elektro Politeknik Negeri Sriwijaya. *It Journal Research and Development*, *3*(1), 32–42. https://doi.org/10.25299/itjrd.2018.vol3(1).1846