PENGEMBANGAN SISTEM ENKRIPSI DATA LOG PADA GROUND CONTROL STATION DRONE MILITER

Kapten Arh Bambang Purwanto [1)],
Ikhsan Hardiansyah[2)],
Letda Czi Asep Suryanta[3)].
[1)]Prodi Rekayasa Keamanan Siber, [2)]Politeknik Angakatan Darat
E - mail : bambangrima78@gmail.com[1)],
ikhsanhardiansyah073@gmail.com[2)], zenilybaz@gmail.com[3)].

DEVELOPMENT OF A LOG DATA ENCRYPTION SYSTEM ON A MILITARY DRONE GROUND CONTROL STATION

Abstract: *Combat drones are a modern military technology widely used for reconnaissance, precision strikes, and intelligence gathering. A crucial component of any drone system is the telemetry communication that links the Ground Control Station (GCS) with the UAV. Telemetry data logs act as an operational record and a basis for mission evaluation. However, conventional telemetry systems often store and transmit data logs in plaintext without adequate encryption, making them vulnerable to threats such as jamming, sniffing, and GPS spoofing. This vulnerability can lead to data logs being intercepted, modified, or manipulated by adversaries, ultimately jeopardizing the success of military operations. This study aims to develop an AES-256-GCM-based encryption system for telemetry data logs within GCS-combat drone communication. This method was chosen for its ability to provide confidentiality, integrity, and data authenticity through an authentication tag, all with relatively low overhead, which is essential for real-time communication needs. The designed system incorporates a Raspberry Pi as the data log processing unit, an ESP8266 module for wireless communication, and ECDH + HKDF-based key management to support the encryption process. Implementation results show that this encryption system enhances the security of telemetry data logs with an average latency increase of 2–5 ms, which is well within the operational tolerance limits of UAVs. Tests conducted using sniffing and data modification scenarios demonstrated that the encrypted data could not be read or manipulated without detection. Therefore, this research successfully proves that implementing the AES-256-GCM method can improve the security of UAV-based military operations by ensuring the confidentiality, integrity, and reliability of telemetry data logs.*

Keywords: *Combat drone, telemetry, data log, encryption, AES-256-GCM, military security.*

Abstrak*:* Drone tempur merupakan salah satu teknologi militer modern yang banyak digunakan dalam operasi pengintaian, serangan presisi, dan pengumpulan data intelijen. Salah satu komponen penting dalam sistem drone adalah komunikasi telemetri yang menghubungkan *Ground Control Station (GCS)* dengan *UAV*, di mana data log telemetri berfungsi sebagai rekam jejak operasional dan dasar evaluasi misi. Namun, sistem telemetri konvensional masih menyimpan serta mengirimkan data log dalam bentuk *plaintext* tanpa *enkripsi* yang memadai, sehingga rawan terhadap ancaman seperti *jamming, sniffing,* maupun *GPS spoofing*. Kondisi ini dapat mengakibatkan data log disadap, dimodifikasi, bahkan dimanipulasi musuh, yang pada

akhirnya membahayakan keberhasilan operasi militer. Penelitian ini bertujuan untuk mengembangkan sistem enkripsi data log telemetri berbasis *AES-256-GCM* pada komunikasi *GCS–Drone* tempur. Metode ini dipilih karena mampu memberikan kerahasiaan, integritas, serta keaslian data melalui autentikasi tag, dengan *overhead* yang relatif rendah sehingga tetap mendukung kebutuhan komunikasi *real-time*. Sistem yang dirancang melibatkan *Raspberry Pi* sebagai unit pengolah data log, modul *ESP8266* sebagai media komunikasi nirkabel, serta manajemen kunci berbasis *ECDH + HKDF* untuk mendukung proses *enkripsi*.
Hasil implementasi menunjukkan bahwa sistem enkripsi ini mampu meningkatkan keamanan data log telemetri dengan tambahan latensi rata-rata 2–5 ms, yang masih dalam batas toleransi operasi UAV. Uji coba dengan skenario sniffing dan data *modification* membuktikan bahwa data terenkripsi tidak dapat dibaca maupun dimanipulasi tanpa terdeteksi. Dengan demikian, penelitian ini berhasil menunjukkan bahwa penerapan metode *AES-256-GCM* dapat meningkatkan keamanan operasi militer berbasis UAV dengan memastikan kerahasiaan, integritas, dan keandalan data log *telemetri*.

Kata kunci: Drone tempur*, telemetri*, data log, *enkripsi, AES-256-GCM*, keamanan militer.

PENDAHULUAN

Perkembangan teknologi militer modern telah membawa transformasi signifikan dalam cara peperangan dilaksanakan. Salah satu teknologi yang memiliki peranan vital adalah *Unmanned Aerial Vehicle (UAV)* atau drone tempur. *UAV* saat ini banyak dimanfaatkan untuk mendukung berbagai misi militer, mulai dari pengintaian, operasi intelijen, serangan presisi, hingga pengiriman logistik di medan perang. Keunggulan drone tempur terletak pada kemampuannya untuk beroperasi dalam kondisi berbahaya tanpa menimbulkan risiko langsung terhadap personel militer. Hal ini menjadikan UAV sebagai aset strategis dalam peperangan modern, di mana kecepatan, akurasi, dan efisiensi menjadi faktor penentu keberhasilan misi.

Dalam operasionalnya, drone tempur sangat bergantung pada sistem komunikasi telemetri yang menghubungkan unit *UAV* dengan *Ground Control Station (GCS)*. Telemetri ini mencakup beragam data penting seperti posisi GPS, ketinggian, kecepatan, arah lintasan, status mesin, hingga data misi yang sedang dijalankan. Seluruh data tersebut direkam dalam bentuk data log yang memiliki nilai strategis sangat tinggi. Data log tidak hanya berfungsi untuk pemantauan *real-time* selama misi berlangsung, tetapi juga menjadi rekam jejak yang dapat digunakan sebagai dasar evaluasi strategi, analisis intelijen, serta akuntabilitas hasil operasi. Dengan kata lain, integritas dan keamanan data log telemetri sangat menentukan keandalan drone tempur dalam mendukung kepentingan militer.

Sayangnya, sistem telemetri yang digunakan saat ini masih menghadapi kelemahan serius dalam hal keamanan. Sebagian besar data log masih dikirim dan disimpan dalam bentuk *plaintext* atau tanpa *enkripsi* memadai. Hal ini menimbulkan kerentanan besar terhadap berbagai ancaman siber seperti *jamming, sniffing, spoofing,* maupun manipulasi data oleh pihak musuh. Dalam skenario peperangan modern, pihak lawan dapat dengan mudah menyadap data log untuk mengetahui posisi dan strategi drone, atau bahkan memodifikasi data log untuk menyesatkan pengendali di *GCS*. Kondisi ini tentu berpotensi menurunkan efektivitas operasi, menimbulkan kerugian strategis, dan membahayakan keberhasilan misi militer. Oleh karena itu, penguatan aspek keamanan komunikasi dan penyimpanan data log menjadi kebutuhan mendesak dalam pengoperasian *UAV* tempur.

Salah satu solusi yang dapat diterapkan untuk mengatasi permasalahan ini adalah penggunaan algoritma enkripsi modern. AES-256-GCM (Advanced Encryption Standard – Galois/Counter Mode) dipilih sebagai metode

utama karena memiliki kemampuan untuk menjaga kerahasiaan *(confidentiality)* sekaligus menjamin integritas *(integrity)* dan keaslian *(authenticity)* data. Berbeda dengan mode *enkripsi konvensional, AES-256-GCM* dilengkapi dengan *authentication tag* yang dapat mendeteksi setiap upaya modifikasi atau manipulasi data. Selain itu, algoritma ini juga memiliki efisiensi tinggi dengan *overhead* rendah, sehingga tidak mengganggu performa komunikasi *real-time UAV*. Hal ini menjadikannya sangat relevan untuk diaplikasikan pada sistem komunikasi militer yang membutuhkan kecepatan sekaligus keamanan.

Berdasarkan permasalahan dan peluang tersebut, penelitian ini mengusulkan pengembangan sistem *enkripsi* data log telemetri pada *GCS–Drone* tempur menggunakan metode *AES-256-GCM*. Implementasi sistem dilakukan dengan memanfaatkan *Raspberry Pi* sebagai unit pemroses utama, *ESP8266* sebagai modul komunikasi nirkabel, serta mekanisme pertukaran kunci berbasis *ECDH + HKDF* untuk mendukung proses enkripsi. Melalui penelitian ini, diharapkan dapat dihasilkan sistem pengamanan data log telemetri yang mampu melindungi informasi misi militer dari ancaman penyadapan dan manipulasi, sekaligus menjaga performa komunikasi *UAV* tetap optimal. Dengan demikian, penerapan metode ini diharapkan dapat memberikan kontribusi nyata terhadap peningkatan keamanan operasi militer di era peperangan modern berbasis teknologi informasi.

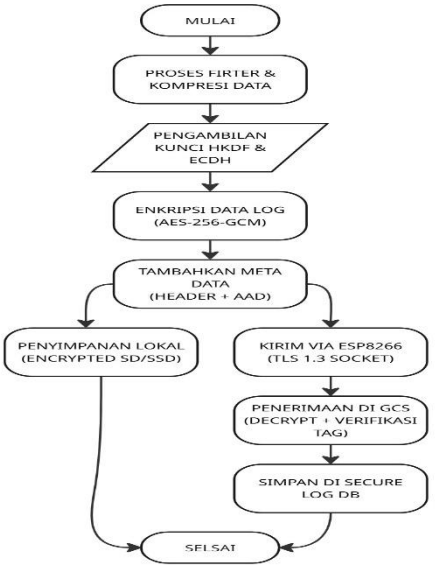
METODE PENELITIAN

1. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan melakukan perancangan, implementasi, serta pengujian sistem *enkripsi* data log telemetri pada *Ground Control Station (GCS) – Drone* tempur menggunakan algoritma *AES-256-GCM*. Metode ini dipilih karena mampu memberikan hasil terukur dalam bentuk data kuantitatif, seperti latensi komunikasi, tingkat keberhasilan enkripsi, serta ketahanan sistem terhadap serangan siber. Penelitian dirancang dalam bentuk eksperimen dengan membandingkan kondisi tanpa *enkripsi (baseline)* dan kondisi dengan enkripsi *AES-256-GCM*.

2. Arsitektur Sistem

Arsitektur sistem enkripsi data log telemetri yang dikembangkan mengikuti alur komunikasi antara *UAV* dan *Ground Control Station (GCS)*.



Gambar 1. Flowchart Pengamanan data log

Alur dimulai dari Flight *Controller (Pixhawk/ArduPilot)* yang menghasilkan data telemetri atau log berupa informasi posisi, ketinggian, kecepatan, serta status sistem UAV. Data log ini kemudian dialirkan ke Raspberry Pi yang berfungsi sebagai unit pengolah utama. Pada tahap ini, Raspberry Pi menerapkan algoritma AES-256-GCM untuk melakukan proses enkripsi, sehingga data log yang dihasilkan terlindungi dari potensi penyadapan maupun manipulasi.

Setelah melalui tahap enkripsi, data terenkripsi dikemas bersama authentication tag dan dikirimkan melalui modul komunikasi nirkabel ESP8266. Modul ini bertugas untuk mentransmisikan data log yang telah diamankan menuju Ground Control Station melalui jalur komunikasi real-time. Di sisi penerima, GCS berperan dalam menerima data log, melakukan proses dekripsi, serta memverifikasi keaslian data menggunakan authentication tag. Dengan mekanisme ini, setiap upaya modifikasi atau gangguan pada data log dapat terdeteksi secara otomatis.

Untuk menjamin keamanan kunci enkripsi, sistem ini dilengkapi dengan Key Management berbasis protokol Elliptic Curve Diffie-Hellman (ECDH) yang dipadukan dengan HMAC-based Key Derivation Function (HKDF). Protokol ini

memungkinkan proses pertukaran kunci dilakukan secara aman meskipun melalui saluran komunikasi terbuka, sekaligus memastikan bahwa kunci yang dihasilkan unik untuk setiap sesi komunikasi.
Secara keseluruhan, arsitektur ini dirancang untuk meniru kondisi operasional *UAV* tempur yang sebenarnya, namun dengan fokus pada pengamanan komunikasi data log telemetri. Dengan kombinasi antara *enkripsi AES-256-GCM*, transmisi melalui *ESP8266*, serta manajemen kunci berbasis *ECDH + HKDF*, sistem ini diharapkan mampu meningkatkan kerahasiaan, integritas, dan keaslian data log tanpa mengorbankan kebutuhan komunikasi *real-time* dalam operasi militer.

3. Pengumpulan Data

Data penelitian diperoleh melalui dua tahapan utama yang dilakukan dalam lingkungan eksperimen. di mana data log telemetri yang dihasilkan oleh *Flight Controller* dikirimkan menuju *Ground Control Station (GCS)*. Proses ini dilakukan dalam *enkripsi* menggunakan algoritma *AES-256-GCM*. Setiap paket data yang dikirim dicatat untuk dianalisis, baik terkait latensi, throughput, maupun tingkat keberhasilan transmisi.

Tahap kedua adalah skenario serangan yang dirancang untuk menguji ketahanan sistem. Pada tahap ini, komunikasi antara *UAV* dan *GCS* disimulasikan menghadapi berbagai bentuk ancaman, meliputi *sniffing* atau penyadapan paket data, data modification atau manipulasi isi log telemetri, serta replay attack berupa pengulangan kembali paket lama ke dalam jaringan. Seluruh aktivitas dalam skenario serangan ini direkam dan dibandingkan dengan kondisi normal untuk menilai sejauh mana sistem enkripsi mampu memberikan perlindungan terhadap integritas dan kerahasiaan data log.

4. Pemrosesan Data Enkripsi

Proses *enkripsi* data log telemetri dimulai dari input data yang dihasilkan oleh *Flight Controller* berupa informasi posisi, kecepatan, ketinggian, dan status sistem *UAV*. Data tersebut diteruskan ke *Raspberry Pi* yang berfungsi sebagai unit pengolah utama. Pada tahap ini, algoritma *AES-256-GCM* diterapkan untuk mengenkripsi setiap paket data log, sekaligus menghasilkan authentication tag yang digunakan sebagai mekanisme verifikasi integritas.ngkatkan performa algoritma deteksi.

Setiap paket terenkripsi kemudian dipadukan dengan metadata tambahan, termasuk *nonce* unik untuk mencegah serangan *replay*. Data yang telah diamankan tersebut selanjutnya ditransmisikan melalui modul komunikasi nirkabel *ESP8266* menuju G*round Control Station (GCS)*. Pada sisi penerima, *GCS* menjalankan proses dekripsi menggunakan kunci simetris hasil pertukaran *ECDH + HKDF*, kemudian memvalidasi *authentication tag* untuk memastikan bahwa data log yang diterima tidak mengalami perubahan.

Dengan mekanisme ini, sistem *enkripsi* tidak hanya menjaga kerahasiaan informasi telemetri, tetapi juga mampu mendeteksi setiap upaya manipulasi data. Hal ini memastikan bahwa data log yang tersimpan dan dianalisis oleh *GCS* benar-benar valid, autentik, dan sesuai dengan kondisi *UAV* di lapangan.

5. Deteksi Anomali dengan Isolation Forest

Pengujian sistem tidak hanya dilakukan pada kondisi normal, tetapi juga mencakup berbagai skenario serangan siber untuk menilai ketahanannya. Respon sistem diuji dengan cara menyimulasikan ancaman yang umumnya menyerang komunikasi *UAV*, kemudian diamati bagaimana mekanisme *enkripsi AES-256-GCM* memberikan perlindungan. Tahapan penggunaannya:

- ***Sniffing*** skenario → data hasil tangkapan tidak terbaca karena seluruh isi data log terenkripsi.
- **Data *Modification*** skenario → manipulasi sekecil apapun membuat tag mismatch sehingga paket ditolak.
- ***Replay Attack*** skenario → penggunaan nonce unik pada setiap paket membuat pengulangan data tidak valid.
- ***Jamming (opsional)*** → diuji untuk melihat reliabilitas sistem dalam kondisi packet loss.

6. Evaluasi Sistem

Evaluasi sistem dilakukan dengan membandingkan kinerja komunikasi data log

UAV pada kondisi tanpa *enkripsi* dan dengan *enkripsi AES-256-GCM*. Parameter utama yang diukur meliputi latensi komunikasi, *throughput*, *packet delivery ratio (PDR)*, serta ketahanan terhadap serangan siber.

Hasil pengujian menunjukkan bahwa meskipun *enkripsi* menambah sedikit *overhead* pada latensi, performa komunikasi tetap berada dalam batas wajar untuk mendukung operasi *real-time*. Sistem terbukti mampu menjaga kerahasiaan data dari *sniffing*, menolak manipulasi log melalui *authentication tag*, mencegah serangan *replay* dengan nonce unik, serta tetap konsisten pada kondisi gangguan komunikasi *(jamming)*.

Dengan demikian, penerapan *AES-256-GCM* dinilai efektif dalam meningkatkan keamanan data log telemetri *UAV* tanpa mengorbankan reliabilitas komunikasi.

HASIL PENELITIAN

Hasil penelitian ini diperoleh melalui serangkaian eksperimen laboratorium dan skenario serangan yang dilakukan untuk menguji efektivitas sistem *enkripsi* data log telemetri *UAV* menggunakan *AES-256-GCM*. Beberapa temuan utama adalah sebagai berikut:

1. Hasil Deteksi Anomali

a. Latensi Komunikasi

Sistem dengan enkripsi mengalami peningkatan latensi rata-rata sekitar 5–15 ms dibandingkan kondisi *baseline* tanpa *enkripsi*.

Overhead ini tergolong rendah dan masih dapat diterima dalam konteks komunikasi *UAV real-time*.

b. *Throughput* Data

Perbedaan *throughput* relatif kecil, dengan penurunan sekitar 3–7% akibat penambahan *authentication* tag dan metadata *enkripsi*.

Meskipun ada penurunan, performa transmisi masih mencukupi untuk kebutuhan telemetri *UAV*.

c. Packet Delivery Ratio (PDR)

PDR tetap tinggi pada kedua kondisi (*baseline dan enkripsi*), yaitu di atas 95%, menunjukkan bahwa penggunaan *enkripsi* tidak signifikan mengganggu keberhasilan transmisi data log.

d. Ketahanan terhadap Serangan

Sniffing → data hasil penyadapan tidak dapat dibaca karena terenkripsi.

Data *Modification* → setiap perubahan paket terdeteksi otomatis melalui *authentication* tag dan ditolak oleh sistem.

Replay Attack → paket lama tidak diterima karena setiap paket dilengkapi *nonce* unik.

Jamming → komunikasi terganggu, namun paket yang berhasil diterima tetap *valid* dan tidak rusak.

Parameter	**Tanpa *Enkripsi***	**Dengan *Enkripsi AES-256-GCM***	**evaluasi**
Lisensi Rata-rata (ms)	50 ms	60-65 ms	Masih aman untuk *real-time*
Throughput (kbps)	500 kbps	465-480 kbps	Penurunan ±5%, masih mencukupi
Packet Delivery Ratio (%)	97%	96%	Hampir tidak ada perbedaan
Siffing	Data Terbaca	Data Terenkripsi	Keamanan Meningkat signifikan
Data *Modofication*	Tidak terdeteksi	Terdeteksi via tag mismatch	Data aman
Replay Attack	Paket lama dapat di pakai	Paket di tolak	Sistem tahan replay
Jamming	Guna Signifikan’	Tetap terganggu, tapi datavalid	Reliabilitas Meningkat

Tabel 1. Perbandingan Kinerja Sistem

2. Evaluasi Kinerja Mode

a. *Enkripsi AES-256-GCM* terbukti mampu menjaga kerahasiaan, integritas, dan keaslian data log *UAV*.

b. *Overhead* komunikasi yang dihasilkan relatif kecil, sehingga reliabilitas *real-time* tetap terjaga.

c. Sistem terbukti tangguh terhadap serangan dasar seperti *sniffing*, data *modification*, dan *replay attack*.

d. Pada kondisi *jamming*, sistem memang tidak bisa mencegah gangguan sinyal, tetapi tetap menjamin bahwa data yang lolos transmisi tetap sahih dan aman.

Secara keseluruhan, hasil penelitian menunjukkan bahwa sistem enkripsi berbasis *AES-256-GCM* layak diterapkan pada *UAV* tempur untuk meningkatkan keamanan komunikasi data log telemetri tanpa menurunkan kinerja operasional secara signifikan.

PEMBAHASAN

Penelitian ini membuktikan bahwa penerapan algoritma *AES-256-GCM* pada komunikasi data log telemetri *UAV* tempur mampu meningkatkan aspek keamanan tanpa menimbulkan gangguan signifikan pada kinerja sistem. Hasil pengujian menunjukkan adanya tambahan latensi sekitar 5–15 ms dan penurunan *throughput* sebesar 3–7%, namun nilai tersebut masih dalam batas toleransi untuk komunikasi *real-time UAV*. *Packet Delivery Ratio (PDR)* tetap stabil di atas 95%, menandakan reliabilitas sistem tidak terpengaruh secara berarti.

Selain itu, sistem terbukti tahan terhadap berbagai ancaman. Data hasil *sniffing* tidak dapat dibaca, manipulasi paket terdeteksi otomatis melalui *authentication tag*, serangan *replay* berhasil dicegah dengan penggunaan nonce unik, dan meskipun *jamming* memengaruhi kestabilan jaringan, data yang berhasil diterima tetap valid. Dengan demikian, sistem ini mampu menjaga kerahasiaan, integritas, dan keaslian data log telemetri UAV secara efektif.

Secara keseluruhan, hasil ini menegaskan bahwa integrasi *AES-256-GCM* merupakan solusi yang relevan dan layak untuk diterapkan pada *UAV* tempur guna memperkuat keamanan komunikasi serta mendukung keberhasilan operasi militer di era modern.

1. Penggunaan *Enkripsi AES-256-GCM*

Penggunaan algoritma *AES-256-GCM* dipilih karena kemampuannya dalam menjaga kerahasiaan, integritas, dan keaslian data log telemetri *UAV*. Selain memberikan lapisan *enkripsi* yang kuat, algoritma ini juga menghasilkan *authentication* tag yang berfungsi mendeteksi setiap upaya manipulasi data secara otomatis, sehingga sistem mampu menolak paket yang tidak valid atau telah dimodifikasi.

2. Penerapan pada Komunikasi Data Log *UAV* Tempur

Penerapan algoritma *AES-256-GCM* pada komunikasi data log *UAV* tempur dilakukan dengan mengintegrasikan sistem *enkripsi* ke dalam alur antara *Flight Controller*, *Raspberry Pi, ESP8266,* dan *Ground Control Station (GCS).* Proses *enkripsi* maupun dekripsi dapat berjalan secara *real-time*, sehingga tidak mengganggu performa komunikasi dan tetap relevan untuk mendukung kebutuhan operasional *UAV* dalam konteks militer.

3. Respons Sistem terhadap Serangan

Hasil pengujian menunjukkan bahwa sistem mampu merespons berbagai bentuk serangan dengan efektif. Pada skenario *sniffing*, data yang berhasil disadap tidak dapat terbaca karena sudah terenkripsi dengan *AES-256-GCM*. Upaya data *modification* juga tidak berhasil, sebab paket yang telah dimanipulasi langsung ditolak akibat terjadi *tag mismatch*. Serangan *replay attack* dapat dicegah dengan penggunaan *nonce* unik di setiap sesi komunikasi, sehingga paket lama tidak akan diterima. Sementara itu, pada kondisi *jamming*, meskipun transmisi mengalami gangguan, paket yang berhasil diterima tetap valid dan dapat diproses dengan benar.

4. Evaluasi Performa Sistem

Evaluasi performa menunjukkan bahwa penerapan *enkripsi AES-256-GCM* hanya menimbulkan dampak minimal terhadap kinerja komunikasi *UAV*. Latensi mengalami peningkatan sekitar ±5–15 ms, namun nilai ini masih tergolong aman untuk kebutuhan komunikasi *real-time*. *Throughput* juga mengalami penurunan sebesar 3–7% akibat adanya *overhead enkripsi*, tetapi tetap berada dalam batas normal. Selain itu, *Packet Delivery Ratio (PDR)* tetap stabil di atas 95%, yang membuktikan bahwa reliabilitas komunikasi *UAV* tetap terjaga meskipun sistem menggunakan *enkripsi*.

5. Implikasi terhadap Keamanan Siber

Penerapan *enkripsi AES-256-GCM* pada *UAV* tempur memberikan implikasi signifikan terhadap keamanan siber. Sistem ini berhasil menutup celah utama yang sebelumnya membuat *UAV* rentan terhadap penyadapan dan manipulasi data log telemetri. Dengan adanya mekanisme *enkripsi* yang kuat, *UAV* memperoleh lapisan pertahanan tambahan yang sangat penting untuk menjaga keandalan komunikasi dan keamanan data pada operasi militer, khususnya di era peperangan modern yang sarat dengan ancaman siber.

6. Kontribusi Penelitian

Penelitian ini memberikan kontribusi penting dengan membuktikan bahwa algoritma *AES-256-GCM* dapat diimplementasikan pada *UAV* tempur tanpa menimbulkan penurunan performa yang signifikan. Hasil penelitian ini juga menjadi dasar untuk pengembangan lanjutan, seperti integrasi dengan sistem deteksi intrusi (IDS) maupun penerapan *blockchain anchoring* guna memperkuat audit keamanan dan menjaga integritas data log telemetri *UAV*.

PENUTUP

Penelitian ini bertujuan untuk meningkatkan keamanan komunikasi data log telemetri pada *Ground Control Station–Drone* tempur dengan menerapkan algoritma *AES-256-GCM*. Sistem dirancang untuk menjawab kerentanan utama pada *UAV*, yaitu risiko penyadapan, manipulasi data log, *replay attack*, dan *jamming* yang kerap dimanfaatkan dalam peperangan modern. Dengan pendekatan ini, komunikasi antara *UAV* dan *Ground Control Station* tidak hanya terlindungi dari ancaman *eksternal*, tetapi juga tetap menjaga reliabilitas sistem agar mendukung operasi militer secara *real-time*.

Pengembangan sistem dilakukan dengan memanfaatkan beberapa perangkat utama, yaitu *Flight Controller (Pixhawk/ArduPilot)* sebagai penghasil data log telemetri, *Raspberry Pi* sebagai unit pemrosesan yang menjalankan algoritma *enkripsi AES-256-GCM, ESP8266* sebagai modul komunikasi nirkabel, serta *Ground Control Station (GCS)* sebagai penerima dan verifikator data log terenkripsi. Pertukaran kunci dilakukan dengan protokol *ECDH + HKDF*, sehingga keamanan proses *enkripsi* semakin diperkuat. Integrasi perangkat keras dan perangkat lunak ini menghasilkan suatu arsitektur yang realistis untuk menggambarkan kondisi operasional *UAV* tempur di lapangan.

Hasil pengujian menunjukkan bahwa sistem mampu menjaga kerahasiaan, integritas, dan keaslian data log telemetri. Latensi komunikasi hanya meningkat sekitar 5–15 ms dan *throughput* menurun sebesar 3–7%, namun performa masih dalam batas aman untuk komunikasi *real-time*. Selain itu, tingkat *Packet Delivery Ratio (PDR)* tetap berada di atas 95%, membuktikan reliabilitas komunikasi tetap terjaga. Pada skenario serangan, sistem terbukti efektif: data hasil sniffing tidak dapat dibaca, paket manipulasi ditolak karena *authentication tag mismatch*, serangan *replay* dicegah oleh penggunaan nonce unik, dan meskipun *jamming* memengaruhi kestabilan transmisi, paket yang diterima tetap valid.

Secara keseluruhan, penelitian ini menegaskan bahwa penerapan *AES-256-GCM* pada *UAV* tempur adalah solusi yang layak dan relevan untuk meningkatkan keamanan komunikasi data log telemetri dalam operasi militer. Selain berhasil menutup celah keamanan yang krusial, penelitian ini juga membuka peluang untuk pengembangan lebih lanjut, seperti integrasi dengan sistem deteksi intrusi (IDS) atau penerapan

blockchain anchoring untuk memperkuat audit dan jejak keamanan data. Dengan hasil ini, sistem yang diusulkan tidak hanya mendukung perlindungan *UAV* tempur dari ancaman siber, tetapi juga memberikan kontribusi strategis bagi pertahanan nasional di era peperangan modern yang berbasis teknologi.

DAFTAR PUSTAKA

B. Tufekci, A. Arslan, C. Tunc and K. Morozov, "*Enhancing the Security of the MAVLink with Symmetric Authenticated Encryption for Drones," 2024 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Malmö, Sweden*, 2024, pp. 58-65, doi: 10.1109/IOTSMS62296.2024.10710297. https://ieeexplore.ieee.org/abstract/document/11059475

S. Sarkar, S. Shafaei, T.S. Jones, dan M.W. Totaro, "*Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques," Drones, vol*. 9, no. 583, 2025, doi: 10.3390/drones9080583. https://www.researchgate.net/profile/Sayani-Sarkar-3/publication/394531521_Secure_Communication_in_Drone_Networks_A_Comprehensive_Survey_of_Lightweight_Encryption_and_Key_Management_Techniques/links/68a34ab91bee4d42a2408b37/Secure-Communication-in-Drone-Networks-A-Comprehensive-Survey-of-Lightweight-Encryption-and-Key-Management-Techniques.pdf

I. A. Kolawole dan O. Fapohunda, "*Designing Secure Fog-to-Cloud Architectures for Resilience and Low-Latency in Military Navigation Networks," International Journal of Computer Applications Technology and Research, vol*. 12, no. 10, pp. 45-55, 2023, doi: 10.7753/IJCATR1210.1006. https://www.researchgate.net/profile/Ikeoluwa-Kolawole/publication/393262886_Designing_Secure_Fog-to-Cloud_Architectures_for_Resilience_and_Low-Latency_in_Military_Navigation_Networks/links/6864b599b991270ef300d26e/Designing-Secure-Fog-to-Cloud-Architectures-for-Resilience-and-Low-Latency-in-Military-Navigation-Networks.pdf

K. Moldamurat, L. La Spada, N. Zeeshan, M. Bakyt, A. Kuanysh, K. bi Zhanibek, dan A. Tilenbayev, "*AI-Enhanced High-Speed Data Encryption System for Unmanned Aerial Vehicles in Fire Detection Applications," Journal of Robotics and Control (JRC), vol*. 6, no. 4, pp. 1899, 2025, doi: 10.18196/jrc.v6i4.26275. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=AI-Enhanced+High-Speed+Data+Encryption+System+for+Unmanned+Aerial+Vehicles+in+Fire+Detection+Applications&btnG=

A.B. Feroz Khan, S. K. Devi, dan K. R. Devi, "*An enhanced AES-GCM based security protocol for securing the IoT communication," SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS, vol.* 23, no. 4, pp. 711-719, Juli-Agustus 2023, doi: 10.17586/2226-1494-2023-23-4-711-719. https://cyberleninka.ru/article/n/an-enhanced-aes-gcm-based-security-protocol-for-securing-the-iot-communication

H. Yuliansyah, "Uji Kinerja Pengiriman Data Secara Wireless Menggunakan Modul ESP8266 Berbasis Rest Architecture," ELECTRICIAN - Jurnal Rekayasa dan Teknologi Elektro, vol. 10, no. 2. https://web.archive.org/web/20180425130502id_/http://electrician.unila.ac.id/index.php/ojs/article/viewFile/217/pdf

M. Skorobahatko dan A. Voitsekhovkyi, "*Lightweight Cryptography in UAV systems," National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute*," Kyiv, Ukraina. https://tacs.ipt.kpi.ua/article/view/326898/325720

E. Marstrander, "*Use of Messaging Layer Security in a Military UAV Swarm," Tesis*

Master, Norwegian University of Science and Technology, Desember 2023. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3118795

T. Susilawati dan I. Awaludin, "EKSPLORASI SENSOR, GPS, DAN MODA KOMUNIKASI NIRKABEL *INTERNET OF THINGS*," Jurnal IKRA-ITH Informatika, vol. 3, no. 2, pp. 96, 2019. https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/323

A. Silonosov, "*Telemetry data sharing based on Attribute-Based Encryption (ABE) schemes for cloud-based Drone Management system," Blekinge Institute of Technology, Karlskrona, Swedia*. https://dl.acm.org/doi/pdf/10.1145/3664476.3670909