Pengembangan Sistem Keamanan Terintegrasi untuk Pengiriman Paket Bernilai Tinggi pada Jaringan Logistik

Development of an Integrated Security System for High-Value Package Delivery in Logistics Networks

Haykal Nabil Nurdiana
Computer Engineering
Telkom University
Bandung, Indonesia
haykalnabil@student.telkomuniversity.ac.id

Reza Rendian Septiawan
Computer Engineering Telkom University
Bandung, Indonesia
rezaseptiawan@telkomuniversity.ac.id

Purba Daru Kusuma
Computer Engineering Telkom University
Bandung, Indonesia
purbodaru@telkomuniversity.ac.id

***Abstrak* — Pengiriman paket bernilai tinggi (*Valuable Goods*/VG) pada lingkungan operasional PT Pos Indonesia, khususnya Kantor Pos Pusat Cimahi, masih mengandalkan sistem pelacakan berbasis *barcode* konvensional tanpa dukungan sensor *Internet of Things* (IoT) maupun *GPS tracker*, sehingga pengawasan bersifat manual dan reaktif dengan kerugian rata-rata Rp200.000–Rp1.000.000 per kasus. Penelitian ini mengembangkan sistem keamanan logistik terintegrasi berbasis IoT berupa perangkat pelacak (*Smart Tracker*) yang dipasang langsung pada paket VG, menggunakan Seeed Studio XIAO ESP32-S3 Sense berkamera, modul SIMCom SIM7080G untuk komunikasi *Cat-M*/NB-IoT beserta GNSS, sensor LDR GL5528 dan *micro limit switch* untuk deteksi pembukaan paket, sensor MPU6050 untuk deteksi guncangan, serta baterai LiPo 3,7 V 1500 mAh. Data dikirim melalui protokol MQTT ke *server* VPS dan divisualisasikan pada *dashboard* pemantauan berbasis *website*. Dari sebelas spesifikasi yang ditetapkan, sembilan spesifikasi terpenuhi. Penambahan dimensi perangkat hanya 22 mm dan berat 47 gram, waktu aktivasi di bawah 10 detik, deteksi sabotase berbasis intrusi cahaya 0,46 detik dan berbasis guncangan 0,8 detik, serta biaya perangkat Rp1.450.000 per unit. Pengujian siklus distribusi nyata sejauh ±19 km (n = 43 titik) memperoleh keberhasilan akuisisi koordinat 95,35% dan akurasi posisi 86,05%, sedangkan rasio *real-time* hanya 72,09%. Hasil *User Acceptance Testing* (UAT) menunjukkan tingkat keberhasilan tugas 86,64% dan skor kepuasan 4,4 dari skala 5.**

Kata kunci* — deteksi sabotase, *internet of things*, pelacakan paket, sistem keamanan logistik, *valuable goods

I. PENDAHULUAN

Pertumbuhan pesat industri *e-commerce* global telah mengubah pola konsumsi masyarakat modern, termasuk pembelian barang bernilai tinggi seperti perhiasan, *gadget* premium, dan barang koleksi langka secara daring. Di balik kemudahan tersebut muncul tantangan keamanan pengiriman yang serius. Fenomena pencurian paket atau *porch piracy* di Amerika Serikat mencatat lebih dari 58 juta paket dicuri sepanjang tahun 2024 dengan total kerugian mencapai 12 miliar dolar AS dan nilai rata-rata 204 dolar AS per paket [1]. Sekitar 41% konsumen Amerika melaporkan pernah kehilangan paket yang dikirim ke rumah mereka [2].

Permasalahan menjadi lebih kompleks pada barang berukuran kecil namun bernilai tinggi seperti perhiasan, *chip* elektronik, dan dokumen legal. Barang dengan karakteristik ini mudah disembunyikan tanpa terdeteksi, sementara nilai ekonominya tinggi meskipun volume fisiknya kecil, sehingga pengawasan fisik sulit dilakukan secara efektif [3]. Berbagai penelitian global merespons kondisi tersebut dengan mengembangkan sistem keamanan berbasis IoT dan *blockchain*, yang terbukti mampu meningkatkan jejak pengiriman yang aman, transparan, dan terenkripsi [4], [5].

Kondisi serupa ditemukan pada mitra penelitian, yaitu Kantor Pos Pusat Cimahi, salah satu unit utama PT Pos Indonesia. Rata-rata pengiriman di kantor tersebut mencapai 20.000–25.000 paket per bulan, dengan sekitar 30% di antaranya merupakan barang bernilai tinggi seperti dokumen legal (BPKB, surat tanah) dan emas dengan nilai hingga Rp100 juta per paket. Barang-barang ini diproses menggunakan kode layanan VG (*Valuable Goods*). Meskipun demikian, sistem pelacakan yang diterapkan masih berbasis *barcode* konvensional tanpa dukungan sensor IoT maupun *GPS tracker*, sedangkan pemberitahuan status barang bernilai tinggi kepada kurir masih dilakukan secara manual.

Berdasarkan hasil wawancara dengan supervisor operasional, kehilangan paket paling sering terjadi di area gudang saat proses sortir, bukan pada saat pengiriman. Nilai kerugian rata-rata mencapai Rp200.000–Rp1.000.000 per kasus, dengan penyebab utama berupa kesalahan operasional gudang dan ketiadaan sistem pelacakan digital. Pengawasan yang bersifat reaktif juga menyebabkan proses investigasi dan penentuan sanksi berjalan lambat karena minimnya bukti elektronik pendukung.

Sejumlah solusi yang telah ada belum sepenuhnya menjawab kebutuhan tersebut. Kamera pengawas CCTV seperti produk Hikvision banyak diterapkan di gudang, namun bersifat pasif dan terikat pada titik pemasangan tetap [14]. Perangkat pelacak aset berbasis *Bluetooth Low Energy* seperti Orin TAG memiliki jangkauan terbatas sehingga tidak memadai untuk pemantauan lintas kota [15]. Pendekatan *computer vision* berbasis *deep learning* mampu mendeteksi anomali perilaku secara otomatis [17], [18], tetapi menuntut infrastruktur GPU yang mahal. Sementara itu, pendekatan *blockchain* menjamin integritas data administratif [19]–[21], namun tidak dapat menjamin keamanan fisik paket tanpa dukungan sensor.

Berdasarkan celah tersebut, penelitian ini bertujuan mengembangkan Sistem Keamanan Logistik Terintegrasi berbasis IoT yang mampu (i) melacak posisi paket VG secara *real-time* sepanjang siklus distribusi, (ii) mendeteksi indikasi sabotase berupa pembukaan paket tanpa izin maupun guncangan tidak wajar, (iii) menghasilkan bukti visual otomatis melalui kamera terintegrasi, serta (iv) menyajikan seluruh informasi tersebut pada *dashboard* pemantauan berbasis *website* yang dapat dioperasikan oleh supervisor gudang non-teknis.

II. KAJIAN TEORI

A. Internet of Things pada Rantai Pasok

Penggunaan IoT dalam rantai pasok meningkatkan visibilitas *real-time* atas lokasi dan kondisi barang, seperti suhu, getaran, dan percobaan penyegelan, sehingga mempercepat deteksi insiden serta mengurangi risiko kerusakan maupun kehilangan [9]. Pada lingkungan gudang, sensor IoT dapat memantau kondisi fisik seperti guncangan, kelembapan, suhu, atau paparan cahaya, yang memungkinkan manajemen menerima peringatan dini apabila terjadi anomali pada paket bernilai tinggi [10]. Pengelolaan rantai pasok berbasis IoT juga telah dibuktikan secara sistematis mampumenggantikan pengawasan manual yang rentan terhadap *human error* dengan mekanisme pemantauan otomatis yang lebih andal dan terukur [31].

B. Standar dan Regulasi Acuan

Perancangan sistem mengacu pada tiga landasan utama. Pertama, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mewajibkan penerapan prinsip keamanan,

kerahasiaan, dan integritas data karena sistem memproses informasi sensitif berupa data penerima dan lokasi paket [11]. Kedua, Peraturan Menteri Komunikasi dan Informatika terkait sertifikasi alat dan perangkat telekomunikasi, yang mengatur standar teknis dan keselamatan elektromagnetik bagi setiap modul komunikasi [12]. Ketiga, ISO 28000:2022 tentang *Security and Resilience — Security Management Systems for the Supply Chain* [13], yang diadaptasi melalui tiga prinsip utama, yaitu manajemen risiko berupa pendeteksian dini anomali, ketertelusuran melalui pencatatan aktivitas paket secara digital, serta pengendalian akses data bagi pengguna berwenang.

C. Deteksi Sabotase Berbasis Sensor

Deteksi pembukaan paket tanpa izin dapat dilakukan melalui kombinasi sensor sederhana berbiaya rendah. Sensor *Light Dependent Resistor* (LDR) mendeteksi intrusi cahaya ke dalam kemasan yang seharusnya gelap, dengan karakteristik resistansi mengikuti hukum pangkat terhadap intensitas cahaya. Sementara itu, *micro limit switch* berfungsi sebagai kontak pembukaan yang mengacu pada prinsip kerja detektor intrusi [22]–[24]. Penelitian terdahulu menunjukkan bahwa sensor nirkabel berbiaya rendah efektif digunakan untuk mendeteksi pembukaan dan perusakan kemasan [25]. Deteksi penanganan kasar dilengkapi sensor inersia MPU6050, dengan penerapan *low pass filter* dan validasi ambang batas untuk mengurangi *false positive* akibat guncangan normal selama transportasi.

D. Komunikasi Hemat Daya NB-IoT dan MQTT

Teknologi NB-IoT dan Cat-M dirancang untuk perangkat dengan sumber daya terbatas, menawarkan konsumsi daya rendah dengan cakupan jaringan luas [28], [29]. Protokol MQTT yang bersifat *publish–subscribe* sesuai untuk kondisi tersebut karena ringan dan efisien dalam penggunaan *bandwidth*. Efisiensi pengelolaan data melalui kompresi *payload* dan pemilihan parameter MQTT yang tepat terbukti mampu menurunkan konsumsi energi maupun beban jaringan secara signifikan [34]. Kombinasi mekanisme *deep sleep* dengan *wakeup interrupt* memungkinkan perangkat bertahan pada catu daya baterai selama siklus distribusi berlangsung [16].

III. METODE

Penelitian dilaksanakan dalam empat tahap, yaitu analisis kebutuhan, perumusan spesifikasi, perancangan dan implementasi, serta pengujian. Analisis kebutuhan dilakukan melalui observasi langsung dan wawancara dengan supervisor operasional Kantor Pos Pusat Cimahi. Hasil analisis diterjemahkan menjadi enam batasan sistem (C-01 s.d. C-06), empat spesifikasi fungsional (SF-01 s.d. SF-04), dan tujuh spesifikasi non-fungsional (SNF-01 s.d. SNF-07).

A. Spesifikasi dan Kriteria Kelolosan

Penetapan kriteria kelolosan tidak dilakukan secara sepihak oleh perancang, melainkan melibatkan tiga otoritas. Manajemen kebijakan korporat menetapkan batasan biaya perangkat dan biaya operasional berdasarkan proyeksi *Total Cost of Ownership* (TCO). Supervisor gudang sortir menetapkan batasan fisik dimensi, berat, waktu aktivasi, dan durasi pelatihan berdasarkan *time and motion study* agar perangkat tidak menimbulkan *bottleneck* baru pada alur sortir harian. Otoritas rekayasa menetapkan batasan akurasi lokasi, akurasi waktu, dan waktu deteksi sabotase yang diturunkan dari pemodelan matematis karakteristik sensor LDR, perhitungan *link budget* daya terima sinyal, serta arsitektur manajemen daya.

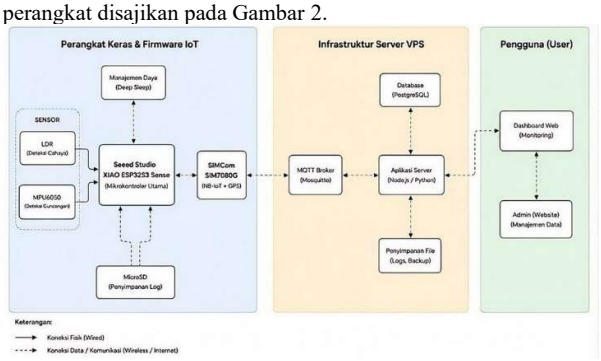
Rangkuman spesifikasi dan kriteria kelolosan disajikan pada Tabel 1.

TABEL 1
Spesifikasi Sistem dan Kriteria Kelolosan

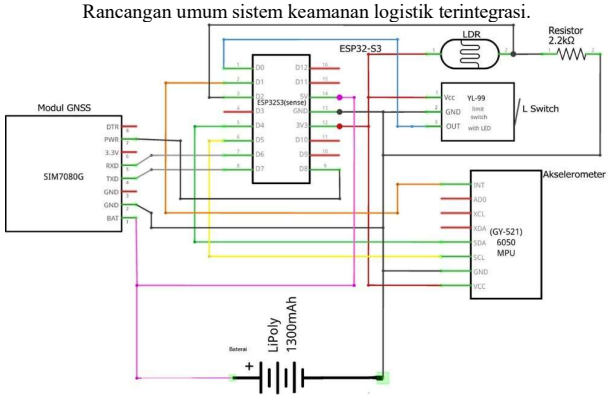
Kode	Parameter	Kriteria Lolos
SF-01	Akurasi lokasi (spasial)	Galat ≤ 10 m
SF-02	Akurasi waktu (temporal)	Galat ≤ 5 detik
SF-03	Deteksi sabotase	Alarm < 1 detik
SF-04	Perekaman sabotase	Foto < 2 detik
SNF-01	Penalti dimensi	≤ 50 mm per sisi
SNF-02	Penalti berat	≤ 50 gram
SNF-03	Penalti aktivasi	< 10 detik
SNF-04	Keramahan pengguna	Navigasi ≤ 60 menit pelatihan
SNF-05	Ketahanan sistem	Tetap berfungsi (debu & tekanan)
SNF-06	Biaya perangkat (BOM)	≤ Rp4.000.000 per unit
SNF-07	Biaya operasional (OPEX)	≤ Rp15.000 per bulan

B. Perancangan Perangkat Keras

Perangkat keras dirancang dengan prinsip dimensi kompak dan konsumsi daya rendah agar tidak menambah volume paket secara signifikan [27]. Seeed Studio XIAO ESP32-S3 Sense dipilih sebagai unit pemroses utama karena telah dilengkapi modul kamera internal untuk dokumentasi visual serta slot *microSD* sebagai media penyimpanan cadangan apabila transmisi data gagal. Modul SIMCom SIM7080G digunakan untuk komunikasi seluler hemat daya berbasis Cat-M dan NB-IoT, sekaligus memanfaatkan fitur GNSS terintegrasi sebagai sumber koordinat presisi. Deteksi sabotase memanfaatkan sensor LDR GL5528 [26] dan *micro limit switch* sebagai pemicu *external interrupt*, serta sensor MPU6050 untuk deteksi guncangan. Catu daya menggunakan baterai Li-Po 3,7 V 1500 mAh, dan seluruh komponen ditempatkan dalam *enclosure* pelindung dari debu dan tekanan mekanis. Rancangan umum sistem ditunjukkan pada Gambar 1, sedangkan diagram skematik rangkaian perangkat disajikan pada Gambar 2.



GAMBAR 1
Rancangan umum sistem keamanan logistik terintegrasi.



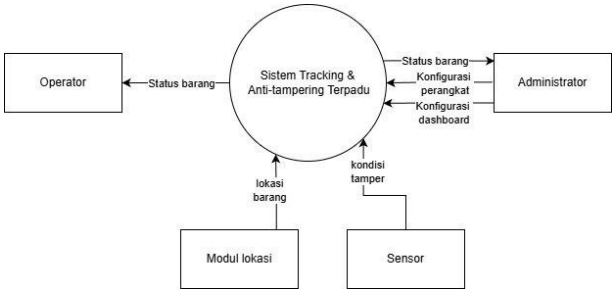
GAMBAR 2
Skematika umum rangkaian listrik perangkat tertempel.

C. Perancangan Perangkat Lunak

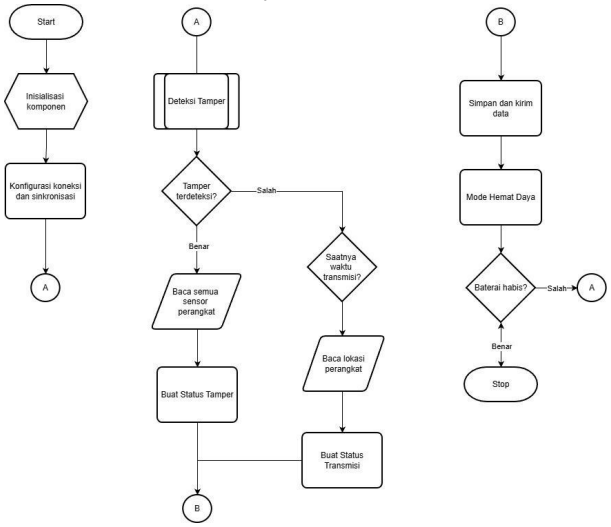
Firmware perangkat diimplementasikan menggunakan bahasa C++ dengan fokus pada efisiensi daya. *Firmware* mengatur siklus hidup perangkat antara mode *deep sleep* dan aktif, serta mengemas data sensor dalam format JSON ringkas sebelum dikirim ke *server* melalui jaringan seluler. Ketika sensor LDR atau *limit switch* memicu interupsi, perangkat bangun dari mode tidur dan menjalankan rutin *run_tamper_sequence* untuk mengaktifkan kamera dan mendokumentasikan kondisi paket.

Pada sisi *server*, sebuah *Virtual Private Server* (VPS) menjalankan aplikasi *back-end*, *broker* MQTT, dan basis data secara berkelanjutan. *Server* ini juga menjalankan logika keamanan tingkat tinggi seperti penghitungan *geofencing* dan manajemen autentikasi akses. Platform pemantauan berbasis *website* menampilkan koordinat paket pada peta digital Leaflet/OpenStreetMap, grafik

status sensor, panel informasi perangkat, serta notifikasi otomatis ketika terjadi anomali. Sistem juga menyediakan fitur *generate* kode QR yang memungkinkan pelacakan paket langsung melalui *smartphone* tanpa perlu masuk ke sistem admin. Perhitungan jarak antartitik pelacakan menggunakan algoritma Haversine. Aliran data sistem secara keseluruhan digambarkan pada DFD Level 0 (Gambar 3), sedangkan alur kerja firmware perangkat ditunjukkan pada Gambar 4.



GAMBAR 3
DFD Level 0 sistem Smart Tracker.



GAMBAR 4
Flowchart alur kerja perangkat utama.

D. Skenario Pengujian

Pengujian dilakukan dalam tiga tahap yang saling melengkapi. Pengujian internal berbasis *white box* memeriksa kebenaran logika internal berupa pembacaan sensor, alur kondisi pemicuan alarm dan kamera, penjadwalan pengiriman data, serta manajemen daya. Pengujian internal berbasis *black box* menguji perilaku sistem terhadap masukan tanpa melihat kode, mencakup akurasi lokasi dan waktu, respons deteksi dan perekaman, penalti dimensi, berat, dan aktivasi, ketahanan, serta biaya. Pengujian eksternal berupa UAT menilai penerimaan dan kemudahan penggunaan sistem oleh supervisor gudang pada skenario kerja nyata.

Pengujian dilaksanakan pada 15–17 Juni 2026, dengan pengujian internal di laboratorium pengembangan dan pengujian eksternal di area Kantor Pos Pusat Cimahi. Setiap pengukuran kuantitatif diulang minimal tiga kali, sedangkan pengujian deteksi sabotase dilakukan sebanyak 36 kali pengulangan untuk memperoleh keandalan statistik yang lebih baik. Sebagai pelengkap, dilaksanakan satu pengujian eksternal tambahan berupa simulasi siklus distribusi nyata dengan intervensi pengembang diminimalkan hanya pada tahap aktivasi awal, mengingat pengujian integrasi pada kondisi operasional nyata memberikan bukti kelayakan yang lebih kuat dibandingkan pengujian pada lingkungan terkontrol semata [32], [33].

IV. HASIL DAN PEMBAHASAN

A. Implementasi Perangkat

Seluruh rancangan pada bagian sebelumnya diwujudkan menjadi purwarupa fungsional yang siap diuji pada kondisi operasional nyata. Komponen elektronik dirakit mengikuti skematika pada Gambar 2, kemudian dikemas dalam *enclosure* pelindung dan ditempatkan pada rongga bagian atas kemasan, tepat di atas barang yang dikirim. Posisi ini dipilih agar tuas *micro limit switch* bersentuhan langsung dengan penutup kemasan, sehingga aksi menutup paket sekaligus menjadi mekanisme pengaktifan sistem keamanan tanpa memerlukan langkah tambahan dari petugas sortir. Hasil implementasi perangkat pada paket VG ditunjukkan pada Gambar 5.

TABEL 2
Hasil Pengujian Deteksi dan Perekaman Sabotase (n = 36)

Parameter	Rata-rata	Status Kelolosan
Jeda aktuasi alarm (SF-03)	0,46 detik	Lolos
Jeda pengambilan foto (SF-04)	2,40 detik	Tidak lolos
Deteksi guncangan MPU6050 (SF-03)	0,80 detik	Lolos



GAMBAR 5
Implementasi perangkat Smart Tracker pada paket Valuable Goods.

Sebagaimana terlihat pada Gambar 5, perangkat menempel rapat pada sisi dalam kemasan tanpa mengubah bentuk luar paket, sehingga keberadaannya tidak mudah dikenali dari tampak luar. Kondisi ini penting untuk menjaga fungsi pengamanan tetap tersembunyi sekaligus memastikan penambahan dimensi dan bobot tetap berada dalam batas yang ditetapkan pada SNF-01 dan SNF-02. Purwarupa inilah yang selanjutnya digunakan pada seluruh rangkaian pengujian yang dibahas pada sub-bab berikutnya.

B. Hasil Pengujian Akurasi Lokasi dan Waktu

Pengujian akurasi lokasi dilakukan pada empat kondisi lingkungan yang berbeda dengan membandingkan koordinat yang ditampilkan sistem terhadap posisi fisik perangkat. Hasil pengujian dirangkum pada Tabel 2.

TABEL 3
Hasil Pengujian Akurasi Lokasi dan Waktu

Kondisi Pengujian	Rerata Selisih Jarak	Rerata Selisih Waktu
Tempat terbuka, sedikit halangan ke langit	0,4 m	26 detik
Tempat terbuka, langit dihalangi beton dan seng	1 m	12 detik
Tempat tertutup, satu lantai di bawah atap beton dan seng	2 m	21 detik
Area jalanan dikelilingi bangunan tinggi	5,4 m	16 detik

Akurasi lokasi memenuhi kriteria SF-01 dengan selisih posisi tertinggi 5,4 m pada area jalanan yang dikelilingi bangunan tinggi, masih jauh di bawah ambang batas 10 m. Sebaliknya, akurasi waktu tidak memenuhi kriteria SF-02. Selisih waktu berkisar 12 hingga 26 detik, melampaui batas galat 5 detik. Penyebab utamanya adalah proses pemulaian ulang modul GNSS, akuisisi lokasi awal, dan inisialisasi transmisi yang secara kumulatif menambah waktu pengiriman data.

C. Hasil Pengujian Deteksi dan Perekaman Sabotase

Pengujian deteksi pembukaan paket melalui intrusi cahaya dilakukan sebanyak 36 kali pengulangan dengan mengukur dua parameter, yaitu jeda aktuasi alarm dan jeda pengambilan foto. Hasil rangkuman disajikan pada Tabel 3.

Perangkat berhasil mendeteksi interupsi fisik dengan rata-rata 0,46 detik, jauh di bawah kriteria 1 detik. Namun, jeda pengambilan foto rata-rata 2,40 detik melampaui kriteria 2 detik. Penyebab utamanya adalah latensi *cold-start* modul kamera setelah bangun dari mode *deep sleep* serta waktu komputasi pengemasan berkas gambar. Sebagai jalur deteksi alternatif, mekanisme berbasis guncangan menggunakan MPU6050 dengan klasifikasi tingkat keparahan MILD, MODERATE, SEVERE, dan EXTREME merespons dengan rata-rata 0,8 detik, sehingga tetap memenuhi kriteria SF-03. Penerapan *low pass filter* dan validasi ambang batas terbukti efektif membedakan guncangan normal selama transportasi dari benturan yang mengindikasikan sabotase.

D. Hasil Pengujian Spesifikasi Non-Fungsional

Seluruh spesifikasi non-fungsional terpenuhi kecuali biaya operasional. Pemasangan *enclosure* memberikan penambahan dimensi 22 mm dan penambahan bobot 47 gram, keduanya di bawah ambang batas 50 mm dan 50 gram. Integrasi aktivasi melalui *dashboard* dan kode QR menghasilkan waktu aktivasi di bawah 10 detik sehingga tidak menimbulkan hambatan pada alur sortir. Pengujian ketahanan berupa penaburan debu dan penekanan masing-masing selama 10 menit tidak mengganggu fungsi sensor maupun transmisi data. Akumulasi biaya pengadaan seluruh komponen elektronik dan fabrikasi pelindung menghasilkan total BOM sekitar Rp1.450.000 per unit, jauh di bawah batas Rp4.000.000.

Spesifikasi biaya operasional (SNF-07) tidak terpenuhi. Fleksibilitas perangkat dalam memanfaatkan jaringan Wi-Fi memang mampu mengeliminasi biaya kuota seluler pada area yang terjangkau, namun penggunaan optimal di luar wilayah tersebut tetap memerlukan jaringan seluler sehingga biaya operasional melampaui Rp15.000 per bulan per unit.

E. Hasil User Acceptance Testing

UAT dilaksanakan oleh tiga orang supervisor gudang non-teknis setelah memperoleh pelatihan singkat, kemudian masing-masing menyelesaikan serangkaian tugas tanpa instruksi tambahan. Hasil pengujian disajikan pada Tabel 4.

TABEL 4
Hasil User Acceptance Testing

Kode	Skenario	Keberhasilan	Skor (1–5)
UAT-01	Login	100% (3/3)	5
UAT-02	Pemantauan lokasi	66,6% (2/3)	4
UAT-03	Notifikasi sabotase	100% (3/3)	5
UAT-04	QR tracking	100% (3/3)	5
UAT-05	Navigasi umum	66,6% (2/3)	3
—	Rata-rata keseluruhan	86,64%	4,4

Tingkat keberhasilan tugas rata-rata 86,64% dengan skor kepuasan 4,4 dari skala 5 menunjukkan bahwa sistem dapat dioperasikan secara mandiri oleh pengguna non-teknis, sehingga memenuhi batasan C-03 dan spesifikasi SNF-04. Skenario dengan skor terendah adalah pemantauan lokasi dan navigasi umum, yang mengindikasikan perlunya penyederhanaan alur antarmuka pada kedua fitur tersebut.

F. Hasil Pengujian Siklus Distribusi Nyata

Pengujian tambahan dilakukan melalui simulasi siklus distribusi VG yang sesungguhnya, meliputi pengambilan paket, pemrosesan di Kantor Pos Pusat Cimahi, pengiriman menuju lokasi tujuan melalui kondisi jalan raya nyata, hingga pengembalian perangkat ke titik asal. Perjalanan berlangsung sekitar 2 jam 10 menit dengan jarak sekitar 19 km sekali jalan, menghasilkan 43 titik data. Titik akhir berjarak hanya sekitar 23 meter dari titik keberangkatan. Rekapitulasi hasil validasi disajikan pada Tabel 5.

TABEL 5
Rekapitulasi Validasi Data Siklus Distribusi (n = 43)

Parameter	Data Valid	Persentase
Koordinat terbaca	41 / 43	95,35%
Timestamp ditampilkan	43 / 43	100,00%
Kecepatan terbaca	41 / 43	95,35%
Koordinat mendekati posisi aktual	37 / 43	86,05%
Timestamp mendekati waktu aktual	31 / 43	72,09%

Ditinjau dari ketertelusuran lokasi, tingkat keberhasilan akuisisi koordinat mencapai 95,35% dengan akurasi posisi 86,05% pada rute yang mencakup jalan raya, perlintasan kereta api, dan area padat lalu lintas. Hasil ini memberikan bukti triangulasi yang memperkuat status lolos SF-01 pada skenario distribusi jarak jauh. Sebaliknya, rasio *real-time* hanya mencapai 72,09%, dengan penurunan paling nyata pada fase pengiriman (65,0%) dan fase pengembalian (63,6%). Klaster titik dengan stempel waktu nyaris identik mengindikasikan penundaan pengiriman telemetri saat perangkat bergerak pada kecepatan tinggi dalam durasi panjang, konsisten dengan keterbatasan *bandwidth* dan latensi publikasi MQTT pada jaringan NB-IoT. Temuan ini memperkuat secara empiris status tidak lolos SF-02 dengan sampel yang jauh lebih besar dibandingkan pengujian terkontrol sebelumnya.

Seluruh siklus *round-trip* berhasil diselesaikan oleh kurir tanpa satu pun intervensi teknis pengembang selama transit, dan perangkat kembali dalam kondisi berfungsi baik. Dua kegagalan total akuisisi koordinat yang terjadi berturut-turut menjelang akhir siklus menjadi catatan tambahan, berpotensi terkait penurunan kualitas sinyal GNSS pada rute tertentu atau akumulasi beban pemrosesan setelah periode aktif lebih dari dua jam.

G. Analisis Kelayakan Ekonomi

Proyeksi kelayakan finansial disusun berdasarkan volume rata-rata
22.500 paket per bulan dengan proporsi paket VG sebesar 27,5%. Pengadaan awal 1.914 unit perangkat memerlukan CAPEX sekitar Rp2,10 miliar, dengan OPEX data komunikasi sekitar Rp62,05 juta per bulan dan biaya pemeliharaan serta kalibrasi berkala sekitar Rp205,20 juta per tahun. Total *Cost of Ownership* tahun pertama pada skenario dasar diperkirakan mencapai Rp3,05 miliar. Analisis sensitivitas menunjukkan nilai TCO bergerak pada rentang Rp1,50 miliar hingga Rp5,16 miliar, dengan fluktuasi yang dikendalikan secara sensitif oleh efisiensi tata kelola waktu resirkulasi perangkat. Oleh sebab itu, skema *piloting* terbatas disarankan sebelum implementasi penuh guna mengukur nilai riil parameter tersebut secara empiris di lapangan.

H. Keterbatasan dan Pengembangan Lanjutan

Sistem masih memiliki sejumlah keterbatasan. Akurasi pelacakan menurun pada area tertutup karena ketergantungan penuh pada modul GNSS. Uji ketahanan yang dilakukan bersifat *ad-hoc* dan belum mencapai standar sertifikasi *Ingress Protection* (IP) formal. Skala UAT juga masih terbatas pada tiga responden di satu lokasi. Untuk pengembangan lanjutan, penambahan metode pelacakan dalam ruangan melalui kombinasi *Bluetooth Low Energy*, RFID, atau *Wi-Fi positioning* disarankan agar ketertelusuran tetap terjaga selama fase penyimpanan di gudang tertutup. Sertifikasi perangkat sesuai ketentuan Kementerian Komunikasi dan Digital diperlukan untuk memenuhi batasan C-02, disertai pengujian ketahanan berstandar IP bersertifikat. Perluasan UAT ke lebih banyak responden dan lokasi akan meningkatkan validitas hasil evaluasi. Selanjutnya, integrasi dengan platform digital internal PT Pos Indonesia memungkinkan verifikasi status, deteksi anomali, dan investigasi kehilangan berjalan otomatis. Terakhir, penerapan enkripsi *end-to-end* pada seluruh jalur transmisi telemetri beserta mekanisme manajemen *consent* diperlukan untuk memenuhi ketentuan UU PDP sebagaimana ditetapkan pada batasan C-01.

V. KESIMPULAN

Penelitian ini berhasil mengembangkan Sistem Keamanan Logistik Terintegrasi berbasis IoT untuk pemantauan paket *Valuable Goods* di lingkungan operasional PT Pos Indonesia, khususnya Kantor Pos Pusat Cimahi. Sistem mengintegrasikan mikrokontroler berkamera Seeed Studio XIAO ESP32-S3 Sense, modul komunikasi SIMCom SIM7080G berbasis Cat-M/NB-IoT dengan GNSS, sensor LDR GL5528, *micro limit switch*, dan sensor MPU6050, dengan transmisi data melalui protokol MQTT menuju *server* VPS dan *dashboard* pemantauan berbasis *website*.

Dari sebelas spesifikasi yang ditetapkan, sembilan spesifikasi berhasil dipenuhi. Akurasi lokasi memenuhi kriteria dengan galat maksimum 5,4 m pada pengujian terkontrol dan tingkat akurasi posisi 86,05% pada siklus distribusi nyata sejauh ±19 km. Deteksi sabotase berbasis intrusi cahaya merespons dengan rata-rata 0,46 detik dan deteksi berbasis guncangan 0,8 detik. Penambahan dimensi perangkat hanya 22 mm dan berat 47 gram, waktu aktivasi di bawah 10 detik, dan biaya perangkat Rp1.450.000 per unit. UAT memperoleh tingkat keberhasilan tugas 86,64% dengan skor kepuasan 4,4 dari skala 5.

Dua spesifikasi belum terpenuhi, yaitu akurasi waktu (SF-02) akibat latensi akuisisi GNSS dan publikasi MQTT pada jaringan NB-IoT, serta biaya operasional (SNF-07) yang melampaui ambang batas ketika perangkat beroperasi di luar jangkauan Wi-Fi. Meskipun demikian, hasil pengujian membuktikan bahwa sistem mampu menggantikan pengawasan manual yang rentan terhadap *human error* dengan pemantauan otomatis, deteksi dini anomali, dan ketertelusuran digital berkelanjutan. Catatan mengenai akurasi pelacakan di area tertutup, sertifikasi ketahanan formal, dan skala UAT yang terbatas menjadi dasar bagi pengembangan selanjutnya menuju implementasi massal.

REFERENSI

[1] M. Adkins, "Package Theft Annual Report and Statistics," Security.org, Nov. 2024. [Online]. Available: https://www.security.org/package-theft/annual-report/

[2] J. R. Evans, "Porch Pirates Report," ValuePenguin, Oct. 2024. [Online]. Available: https://www.valuepenguin.com/porch-pirates-report

[3] "Package Theft Statistics (2025): Number per Year, Costs & Trends," Capital One Shopping, Jun. 2025. [Online]. Available: https://capitaloneshopping.com/research/package-theft-statistics/

[4] V. Aleksieva, H. Valchanov, A. Haka, and D. Dinev, "Logistics Model Based on Smart Contracts on Blockchain and IoT," Engineering Proceedings, vol. 41, no. 1, 2023, doi: 10.3390/engproc2023041008.

[5] A. Soni, "IoT & Blockchain for Cargo Monitoring," IBM. [Online]. Available: https://www.ibm.com/think/topics/iot-blockchain-for-cargo-monitoring

[6] M. G. Cedillo-Campos, J. E. Flores-Franco, and D. Covarrubias, "A physical internet-based analytic model for reducing the risk of cargo theft in road transportation," Comput. Ind. Eng., vol. 190, p. 110016, Apr. 2024, doi: 10.1016/j.cie.2024.110016.

[7] K. V. Queiroz, J. M. Abe, J. G. M. dos Reis, and M. Renon, "Analysis of Strategies to Combat Cargo Theft and Robbery in Peripheral Communities of São Paulo, Brazil, Using a Paraconsistent Expert System," Logistics, vol. 9, no. 1, Mar. 2025, doi: 10.3390/logistics9010037.

[8] X. Liang, S. Fan, J. Lucy, and Z. Yang, "Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network,"

[9] Reliab. Eng. Syst. Saf., vol. 226, Oct. 2022, doi: 10.1016/j.ress.2022.108702.

[10] F. Alghamdi, "The Role of IoT in Real-Time Supply Chain Visibility and Risk Management," Global Journal of Management and Business Research, no. 08, pp. 13–14, 2025, doi: 10.34257/gjmbravol25is5pg13.

[11] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management," Future Internet, vol. 11, no. 161, pp. 1–22, 2019.

[12] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jakarta, 2022. [Online]. Available: https://peraturan.go.id/id/uu-no-27-tahun-2022

[13] Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 tentang Penyelenggaraan Jasa Telekomunikasi. Jakarta, 2019.

[14] "ISO 28000:2022 — Security and resilience — Security management systems — Requirements." [Online]. Available: https://www.iso.org/standard/79612.html

[15] "Hikvision Indonesia — Leading the future of AIoT." [Online]. Available: https://www.hikvision.com/id/

[16] "Orin TAG — GPS Tracker Orin Indonesia." [Online]. Available: https://orin.id/orintag/

[17] A. Sorensen et al., "Modeling and Experimental Validation for Battery Lifetime Estimation in NB-IoT and LTE-M," IEEE Internet Things J., vol. 9, no. 12, pp. 9804–9819, Jun. 2022, doi: 10.1109/JIOT.2022.3152173.

[18] J. S. Kang, J. K. Kang, S. Son, S. H. Park, E. J. Jung, and G. R. Cho, "Image Enhancement Method for Detection in Logistics Loading and Unloading Robots," IEEE Access, vol. 13, pp. 143678–143687, 2025.

[19] L. M. Wastupranata, S. G. Kong, and L. Wang, "Deep Learning for Abnormal Human Behavior Detection in Surveillance Videos — A Survey," Electronics, vol. 13, no. 13, 2024, doi: 10.3390/electronics13132579.

[20] M. Andoni et al., "Blockchain Technology in the Supply Chain: A Systematic Literature Review," IEEE Access, vol. 8, pp. 21681–21700, 2020.

[21] L. Ran, Z. Shi, and H. Geng, "Blockchain Technology for Enhanced Efficiency in Logistics Operations," IEEE Access, vol. 12, pp. 152873–152885, 2024.

[22] B. C. Cheong, "Leveraging blockchain for enhanced transparency and traceability in sustainable supply chains," Discov. Anal., vol. 3, no. 1, 2025, doi: 10.1007/s44257-025-00032-7.

[23] "Tiny detect switches serve multiple uses in IoT," Embedded.com, Nov. 2021. [Online]. Available: https://www.embedded.com/tiny-detect-switches-serve-multiple-uses-in-iot/

[24] EN 50131-2-6:2008, Alarm systems — Intrusion and hold-up systems — Part 2-6: Opening contacts (magnetic). CENELEC, 2008.

[25] EN 50131-2-10:2018, Alarm systems — Intrusion and hold-up systems — Part 2-10: Lock state contacts (magnetic). CENELEC, 2018.

[26] W. Wang, A. Sadeqi, H. R. Nejad, and S. Sonkusale, "Cost-effective wireless sensors for detection of package opening and tampering," IEEE Access, vol. 8, pp. 117122–117132, 2020.

[27] "GL5528 Photoresistor (Light Dependent Resistor) Datasheet," Electronic Components Manufacturer, 2020.

[28] S. Arif, M. A. Khan, and S. U. Rehman, "Machine Learning Based Channel Estimation for Low-Power Internet of Things (LP-IoT) Devices: A Probabilistic Analysis," IEEE Access, vol. 13, pp. 38470–38483, 2025.

[29] R. B. Salikhov, "Internet of Things (IoT) Security Alarms on ESP32-CAM," J. Phys. Conf. Ser., vol. 2096, no. 1, 2021.

[30] O. S. Althobaiti and M. Dohler, "Narrowband-Internet of Things Device-to-Device Simulation: An Open-Sourced Framework," Sensors, vol. 21, no. 5, 2021.

[31] A. K. Junejo, M. Breza, and J. A. McCann, "Threat modeling for communication security of IoT-enabled digital logistics," Sensors, vol. 23, no. 23, p. 9500, Nov. 2023.

[32] S. Taj, A. S. Imran, Z. Kastrati, S. M. Daudpota, R. A. Memon, and J. Ahmed, "IoT-based supply chain management: A systematic literature review," Cluster Computing, vol. 26, pp. 3995–4015, 2023.

[33] M. Bures et al., "A multimethod study of Internet of Things systems testing in industry," IEEE Trans. Softw. Eng., vol. 50, no. 1, pp. 1–20, 2024.

[34] B. Marculescu et al., "A systematic review of IoT systems testing: Objectives, approaches, tools, and challenges," IEEE Trans. Softw. Eng., vol. 50, no. 3, pp. 452–481, 2024.

[35] M. Has, D. Kreković, M. Kušek, and I. Podnar Žarko, "Efficient data management in agricultural IoT: Compression, security, and MQTT protocol analysis," Sensors, vol. 24, no. 11, p. 3517, 2024.