JURNAL GO INFOTECH
Vol.32, No.1, Juni 2026
ISSN (p): 1693-590x, ISSN (e): 2686-4711
DOI: 10.36309/goi.v32i1.447

Integrasi RBAC, AES-256, dan *Audit-log* untuk Keamanan dan Auditabilitas Sistem Inventori UMKM

Singgih Aliana Winastuti[1], Andik Prakasa Hadi*[2], Ahmad Zainudin[3]
[1,2,3] Fakultas Studi Akademi, Universitas Sains dan Teknologi Komputer, Semarang
email: [1]alianasinggih@gmail.com, *[2]andik@stekom.ac.id, [3]zaenudin@stekom.ac.id

Abstrak

UMKM menghadapi kendala dalam pengelolaan inventori, seperti kesalahan pencatatan stok, lemahnya kontrol akses, dan minimnya jejak perubahan data. Penelitian ini mengembangkan sistem inventori berbasis web yang mengintegrasikan Role-Based Access Control (RBAC), enkripsi AES-256, dan audit log. Sistem dibangun dengan framework Laravel menggunakan pendekatan Design Science Research (DSR). Hasil pengujian fungsional mencapai 100% keberhasilan. Evaluasi System Usability Scale (SUS) terhadap 6 responden menghasilkan skor rata-rata 87,5 (kategori excellent). Enkripsi AES-256 terbukti efektif melindungi data sensitif, sementara audit log mendukung akuntabilitas sistem. Verifikasi juga menegaskan kepatuhan terhadap standar NIST SP 800-171. Penelitian ini berkontribusi pada integrasi tiga mekanisme keamanan dalam sistem inventori yang siap diadopsi UMKM sektor garmen

Kata kunci*— Sistem Inventori, Audit Log, RBAC, AES-256, UMKM*

Abstract

Micro and small enterprises face inventory management issues, including stock recording errors, weak access control, and lack of data change traceability. This study develops a web-based inventory system integrating Role-Based Access Control (RBAC), AES-256 encryption, and audit logs. The system was built using the Laravel framework with a Design Science Research (DSR) approach. Functional testing achieved a 100% success rate. Usability evaluation using the System Usability Scale (SUS) with six respondents produced a mean score of 87.5 (excellent category). AES-256 encryption effectively protects sensitive data, while audit logs support system accountability. Verification also confirms compliance with the NIST SP 800-171 standard. This study contributes an integrated three-mechanism security system ready for adoption by garment-sector SMEs.

Keywords*— Inventory System, Audit Log, RBAC, AES-256, SMEs*

1. PENDAHULUAN

Keberhasilan operasional sebuah organisasi sangat ditentukan oleh bagaimana sistem inventori dikelola. Ketika data stok tidak akurat, pencatatan tertunda, dan kontrol akses pengguna lemah, kualitas pengambilan keputusan dapat terganggu. Ancaman terhadap keamanan data juga terus meningkat, karena kebocoran data berpotensi merugikan organisasi secara signifikan [1], [2].

Industri garmen memiliki tantangan tersendiri dalam pengelolaan inventori. Produk bervariasi dalam ukuran, warna, dan model. Perusahaan juga harus mengelola dua jenis

Received Mei 7st,2026; Revised Juni 08th, 2026; Accepted Juni 20th, 2026

inventori sekaligus, yaitu bahan baku dan barang jadi. Kompleksitas ini sering menyebabkan data stok tidak akurat, pencatatan keliru, dan kesulitan dalam pengendalian persediaan. Studi sebelumnya mengungkapkan bahwa UMKM menghadapi kendala utama pada keterbatasan sistem informasi dan minimnya integrasi tekno*log*i [3], [4]. Lebih lanjut, ketahanan rantai pasok UMKM tekstil memerlukan pendekatan inovatif berbasis data untuk mengatasi berbagai hambatan [5].

Berbagai upaya telah dilakukan untuk meningkatkan efisiensi inventori. Penerapan *lean manufacturing* dan tekno*log*i RFID menunjukkan hasil positif dalam menekan kesalahan operasional [6], [7]. Wang et al. [5] mengusulkan kerangka C2M *(customer-to-manufacturer)* berbasis data *e-commerce* publik yang berhasil mereduksi nilai inventori hingga 28% sekaligus meningkatkan ketahanan rantai pasok UMKM tekstil. Sayangnya, studi tersebut masih terfokus pada efisiensi semata, sementara aspek keamanan dan akuntabilitas data belum mendapat perhatian yang memadai.

Kontrol akses menjadi elemen krusial dalam pengembangan sistem informasi modern. *Role-Based Access Control* (RBAC) menawarkan pendekatan yang efektif dengan memberikan hak akses berdasarkan peran pengguna, bukan perorangan [8], [9]. Model ini mampu membatasi akses sesuai prinsip *least privilege* dan menyederhanakan pengelolaan hak akses di lingkungan yang kompleks [10], [11], [12]. Blundo dan Cimato [8] memberikan landasan teoretis tentang kompleksitas pengelolaan peran melalui penelitian *role mining* dengan *cardinality constraints*. Purba dan Hidayasari [11] berhasil menerapkan RBAC pada sistem manajemen stok obat berbasis Laravel, dengan tingkat keberhasilan *black-box testing* mencapai 100% dan skor SUS 76. Aswintama et al. [12] mengintegrasikan RBAC dengan *multi-tenancy* dan *audit logging* pada sistem SSO, yang berhasil menurunkan akses tidak sah hingga 87,5%. Hasil serupa juga ditunjukkan Sitanggang et al. [13] pada sistem inventori dengan QR *code*, di mana tingkat keberhasilan fungsional mencapai 100%. Namun, pengendalian akses saja tidak cukup; data sensitif yang tersimpan di basis data tetap memerlukan perlindungan tambahan.

Teknik enkripsi menjadi solusi yang banyak diadopsi. *Advanced Encryption Standard* (AES) menawarkan tingkat keamanan tinggi sekaligus efisiensi dalam proses enkripsi dan dekripsi. Algoritma ini telah menjadi standar utama dalam pengamanan data sensitif, khususnya untuk aplikasi berbasis web dan basis data [14], [15]. Implementasi AES-256 memungkinkan data tetap terlindungi meskipun sistem penyimpanan mengalami akses tidak sah [16]. Zulian et al. [17] mengimplementasikan AES-GCM-SIV pada *framework* Laravel dengan memanfaatkan *Rust*, yang menghasilkan performa optimal untuk proses enkripsi dan dekripsi *file*.

Selain enkripsi, transparansi sistem juga sering diabaikan. Padahal, *audit log* berperan penting sebagai mekanisme pencatatan aktivitas. Setiap tindakan pengguna dapat ditelusuri secara akurat, sehingga mendukung akuntabilitas dan investigasi keamanan [1], [10], [12]. Ali et al. [2] melakukan survei komprehensif tentang persyaratan pengamanan *audit log*, mengembangkan taksonomi manajemen *audit log*, dan mengidentifikasi berbagai tantangan keamanan *log* saat ini. Pendekatan modern seperti DPTracer dengan *tamper-evident log*ging mampu meningkatkan akuntabilitas di lingkungan yang tidak terpercaya [18]. Sementara itu, Saputra [19] mengintegrasikan *audit trail* dengan teknik *clustering* K-Means untuk segmentasi dan kategorisasi aktivitas *log*, yang memungkinkan deteksi anomali dan penyederhanaan proses audit.

Perlindungan data pribadi kini menjadi kewajiban hukum. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mewajibkan setiap sistem informasi melindungi data yang dapat mengidentifikasi individu dari akses tidak sah [20]. Regulasi ini mendorong pengembang sistem untuk menerapkan mekanisme keamanan seperti enkripsi pada data sensitif (nomor telepon pelanggan dan pemasok). Standar NIST SP 800-171 juga memberikan panduan tentang aspek *audit and accountability* yang harus dipenuhi oleh sistem yang menangani informasi sensitif [21].

Berdasarkan berbagai kesenjangan tersebut, masih terdapat celah penelitian yang perlu diisi. Penelitian tentang sistem inventori sebagian besar berfokus pada peningkatan efisiensi

operasional [5], [6], [7] atau aspek keamanan secara terpisah [8], [9], [15]. Aswintama et al. [12] dan Patil [10] telah mengintegrasikan RBAC dengan *audit logging*, namun belum menyentuh aspek enkripsi data sensitif. Purba dan Hidayasari [11] serta Sitanggang et al. [13] telah menerapkan RBAC pada sistem manajemen stok dan inventori, tetapi belum mengintegrasikan enkripsi. Sementara itu, Lee [18] dan Saputra [19] fokus pada *audit log* dan deteksi anomali, tanpa pengendalian akses yang komprehensif. Belum banyak penelitian yang mengintegrasikan efisiensi operasional, keamanan, akuntabilitas, dan perlindungan data pribadi secara menyeluruh dalam satu sistem inventori.

Oleh karena itu, penelitian ini mengembangkan sistem inventori berbasis web yang mengintegrasikan tiga mekanisme keamanan sekaligus: RBAC, enkripsi AES-256, dan *audit log*. Pengembangan dilakukan dengan *framework* Laravel menggunakan pendekatan *Design Science Research* (DSR) [22], [23]. Kehadiran sistem ini diharapkan tidak hanya meningkatkan efisiensi pengelolaan inventori, tetapi juga memberikan jaminan keamanan, transparansi, dan kepatuhan terhadap regulasi [20] serta standar keamanan [21]. Potensi integrasi IoT dan *blockchain* juga menjanjikan untuk meningkatkan visibilitas inventori secara *real-time* di masa depan [24].

2. METODE PENELITIAN

2.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan *Design Science Research* (DSR). Pendekatan ini dipilih karena sesuai untuk menghasilkan artefak berupa sistem inventori berbasis web. Artefak tersebut bertujuan mengatasi masalah akuntabilitas dan keamanan data pada UMKM sektor garmen. DSR memungkinkan pengembangan solusi praktis sekaligus memberikan kontribusi ilmiah melalui proses perancangan, implementasi, dan evaluasi sistem [22], [23].

2.2 Tahapan Penelitian

Tahapan penelitian mengacu pada kerangka DSR yang terdiri dari lima fase: identifikasi masalah, definisi solusi, perancangan dan pengembangan artefak, demonstrasi, serta evaluasi [23].

Fase 1: Identifikasi Masalah

Observasi langsung dan wawancara dilakukan pada UMKM sektor garmen. Pemilik dan staf gudang menjadi narasumber dalam studi pendahuluan ini. Studi literatur juga dilakukan untuk memahami tantangan pengelolaan inventori pada UMKM. Hasil analisis mengungkapkan kebutuhan terhadap sistem yang tidak hanya mampu mengelola inventori, tetapi juga menjamin keamanan dan akuntabilitas data.

Fase 2: Definisi Solusi

Tujuan penelitian dirumuskan sebagai berikut: (1) mengembangkan sistem inventori berbasis web untuk digitalisasi data, (2) menerapkan *audit log* untuk merekam aktivitas pengguna, (3) mengimplementasikan enkripsi AES-256 pada data sensitif (nomor telepon *customer* dan *supplier*), serta (4) menerapkan RBAC untuk pengaturan hak akses berbasis peran.

Fase 3: Perancangan dan Pengembangan Artefak

Sistem dikembangkan dengan *framework* Laravel 11. Arsitektur yang digunakan adalah *Model-View-Controller* (MVC) dengan basis data MySQL 8.0. *Library spatie/laravel-activitylog* digunakan untuk implementasi *audit log*. Enkripsi AES-256 diimplementasikan melalui mekanisme *attribute casting* pada model *Eloquent* [14]. RBAC diimplementasikan menggunakan fitur *Gate* dan *Policy* Laravel.

Fase 4: Demonstrasi

Demonstrasi dilakukan melalui skenario penggunaan *(use case scenarios)* pada UMKM sektor garmen. Skenario yang diujikan meliputi proses *log*in, input stok (masuk dan keluar), penambahan data *customer*/*supplier* dengan enkripsi otomatis, perubahan data barang, pengaksesan *audit log*, serta pengujian pembatasan akses peran.

Fase 5: Evaluasi

Proses evaluasi sistem dilaksanakan dengan mengintegrasikan tiga metode, yakni pengujian fungsional (*black-box testing*), evaluasi usability menggunakan *System Usability Scale* (SUS), serta verifikasi kesesuaian dengan standar keamanan NIST SP 800-171.

1. *Black-box testing* terhadap skenario fungsional untuk memastikan seluruh fitur berjalan sesuai kebutuhan.
2. Pengujian *usability* dengan SUS *(System Usability Scale)*. Evaluasi *usability* dilakukan untuk mengukur tingkat kemudahan penggunaan sistem dari perspektif pengguna. Instrumen yang digunakan adalah *System Usability Scale* (SUS), yang telah terbukti valid dan reliabel untuk berbagai jenis sistem [25]. Responden dalam pengujian ini berjumlah 6 orang, jumlah responden ini berada dalam rentang yang direkomendasikan untuk pengujian *usability* pada tahap pengembangan sistem, di mana 5-6 partisipan sudah cukup untuk mengungkap sebagian besar masalah *usability* [26].
   Penelitian ini untuk mengolah data dari jumlah responden yang terbatas, mengikuti pedoman statistik yang diusulkan oleh Clark et al. [27]. Pedoman tersebut merekomendasikan penggunaan *bias-corrected accelerated bootstrap* atau *Bayesian credibility intervals* untuk menghitung interval kepercayaan skor SUS pada sampel kecil, karena distribusi data SUS cenderung miring (*skewed*) dan tidak memenuhi asumsi normalitas [27].
3. Verifikasi *audit log* untuk memastikan pencatatan aktivitas berjalan lengkap dan mendukung akuntabilitas.

2.3 Alat dan Bahan

Penelitian ini mengoperasikan lingkungan pengembangan dan pengujian dengan spesifikasi perangkat keras dan perangkat lunak yang terdefinisi secara jelas. Adapun rincian spesifikasi yang digunakan, meliputi prosesor, RAM, penyimpanan, sistem operasi, *web server*, basis data, *framework*, bahasa pemrograman, dan pustaka tambahan, disajikan pada Tabel 1 berikut.

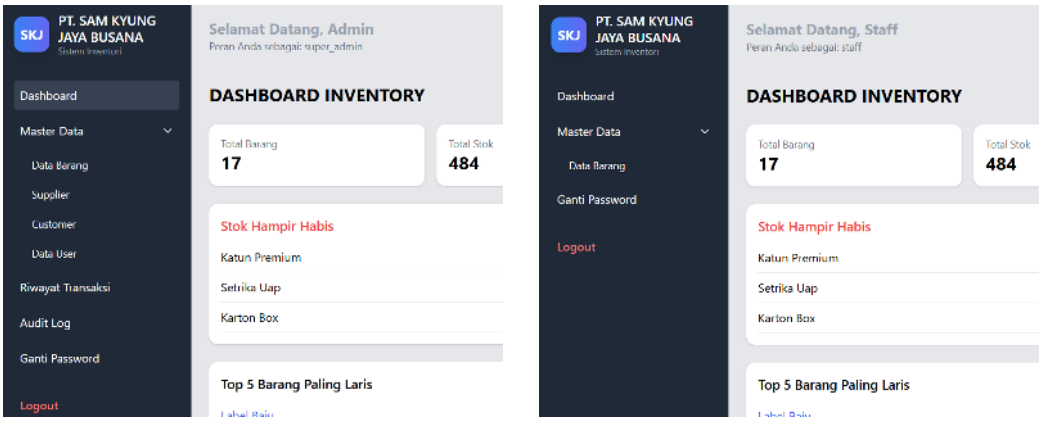
Tabel 1. Spesifikasi perangkat lunak dan perangkat keras

Komponen	**Spesifikasi**
Prosesor	Intel Core i5 / setara
RAM	8 GB
Penyimpanan	SSD 256 GB
Sistem Operasi	Ubuntu 22.04 LTS / Windows 11
Web Server	Nginx 1.24 / Apache 2.4
Basis Data	MySQL 8.0
Framework	Laravel 11.x
Bahasa Pemrograman	PHP 8.3
Frontend	Tailwind CSS 3.x
Library Audit log	spatie/laravel-activity*log* ^4.0

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

Tiga mekanisme keamanan utama berhasil diintegrasikan ke dalam sistem inventori: RBAC, enkripsi AES-256, dan *audit log*. Fitur-fitur utama yang tersedia meliputi pengelolaan produk, *customer*, *supplier*, transaksi stok, laporan, serta pengelolaan pengguna berbasis peran. Seluruh fitur berjalan sesuai rancangan.



Gambar 1. Perbedaan Akses Halaman *User*
(Sumber: Dokumentasi Penelitian, 2026)

3.2 Pengujian Fungsional (Black-box Testing)

Sebanyak 12 skenario uji fungsional telah dilaksanakan. Pengujian mencakup aspek autentikasi, pengelolaan data, transaksi stok, dan mekanisme keamanan (RBAC, enkripsi, *audit log*). Tabel 2 menyajikan hasil pengujian secara rinci.

Tabel 2. Hasil *Black-box Testing* Sistem Inventori

Kode	Skenario Uji	Hasil yang Diharapkan	Status
TC-01	*Log*in dengan kredensial valid	Masuk ke halaman *dashboard*	Lulus
TC-02	*Log*in dengan *password* salah	Muncul pesan *error*	Lulus
TC-03	Tambah *customer* (dengan nomor telepon)	Data tersimpan, nomor telepon terenkripsi	Lulus
TC-04	Tambah *supplier* (dengan nomor telepon)	Data tersimpan, nomor telepon terenkripsi	Lulus
TC-05	Tampilkan data *customer* di web	Nomor telepon tampil sebagai *plain text*	Lulus
TC-06	Admin Gudang akses halaman *user*	Akses ditolak (403 *Forbidden*)	Lulus
TC-07	Manajer akses halaman tambah barang	Akses ditolak (403 *Forbidden*)	Lulus
TC-08	Super Admin akses halaman *audit log*	Halaman dapat diakses	Lulus
TC-09	Tambah transaksi barang masuk	Stok bertambah, aktivitas tercatat di *audit log*	Lulus
TC-10	Tambah transaksi keluar (stok cukup)	Stok berkurang, *before-after values* tercatat	Lulus

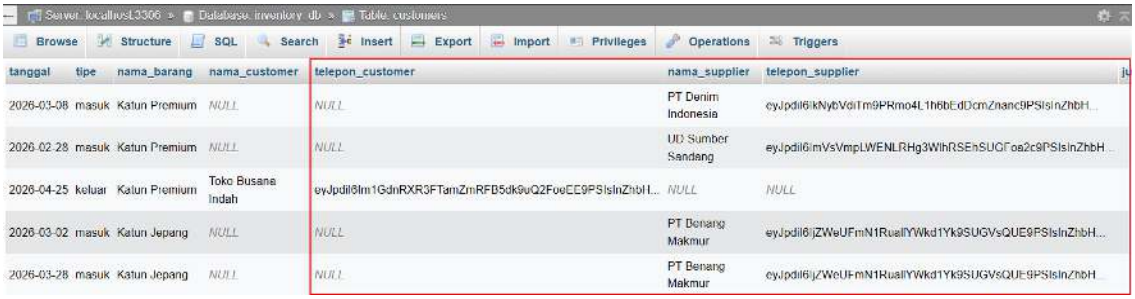
TC-11	Tambah transaksi keluar (stok kurang)	Muncul peringatan, transaksi gagal	Lulus
TC-12	*Generate* dan ekspor laporan stok ke PDF	File PDF terunduh dengan data sesuai	Lulus

Tingkat Keberhasilan: 100% (12 dari 12 skenario)

Seluruh skenario uji berhasil dilalui (100%). Hasil ini menunjukkan bahwa sistem memenuhi semua kebutuhan fungsional. Temuan ini sejalan dengan penelitian Purba dan Hidayasari [11] serta Sitanggang et al. [13] yang juga mencapai tingkat keberhasilan 100% pada implementasi RBAC.

3.3 Pengujian Enkripsi AES-256

Enkripsi diterapkan pada nomor telepon *customer* dan *supplier*. Implementasi menggunakan mekanisme *attribute casting* pada model *Eloquent* dengan algoritma AES-256-CBC bawaan Laravel [14]. Pendekatan *selective encryption* dipilih untuk menjaga keseimbangan antara keamanan dan performa [15], [16], [17].



Gambar 2. Data Nomor Telepon Tersimpan sebagai *Ciphertext* Hasil Enkripsi AES
(Sumber: Dokumentasi Penelitian, 2026)

Data nomor telepon tersimpan sebagai *ciphertext* di basis data, sementara data non-sensitif tetap dalam *plaintext*. Proses enkripsi dan dekripsi berjalan otomatis dan transparan bagi pengguna. Pengguna tetap melihat nomor telepon asli di halaman web. Pendekatan ini memberikan beberapa keunggulan: (1) data tetap aman meskipun basis data bocor, (2) transparan bagi pengguna, (3) mendukung kepatuhan terhadap UU PDP, dan (4) performa optimal [17].

Tabel 3. Hasil Uji Enkripsi AES-256 pada Data Sensitif

Skenario	**Data *Plaintext***	**Data di Database (*Ciphertext*)**	**Tampilan di Web**	**Status**
Tambah *customer* baru	081234567890	eyJpdiI6Ikx5bjVcL1wv...	081234567890	Berhasil
Tambah *customer* baru	087654321098	eyJpdiI6Ik1UazJcL1wv...	087654321098	Berhasil
Tambah *supplier* baru	089876543210	eyJpdiI6Ik5UUXpcL1wv...	089876543210	Berhasil
Edit nomor telepon *customer*	Berubah dari 081234567890 menjadi 081234567899	*Ciphertext* baru	081234567899	Berhasil
Akses *database* langsung	-	*Ciphertext* (tidak terbaca)	-	Berhasil

3.4 Pengujian Role-Based Access Control (RBAC)

Empat peran didefinisikan berdasarkan hasil wawancata dengan pihak UMKM: Super Admin, Admin Gudang, Manajer Operasional, dan Direktur. Setiap peran diberikan hak akses minimal sesuai prinsip *least privilege*.

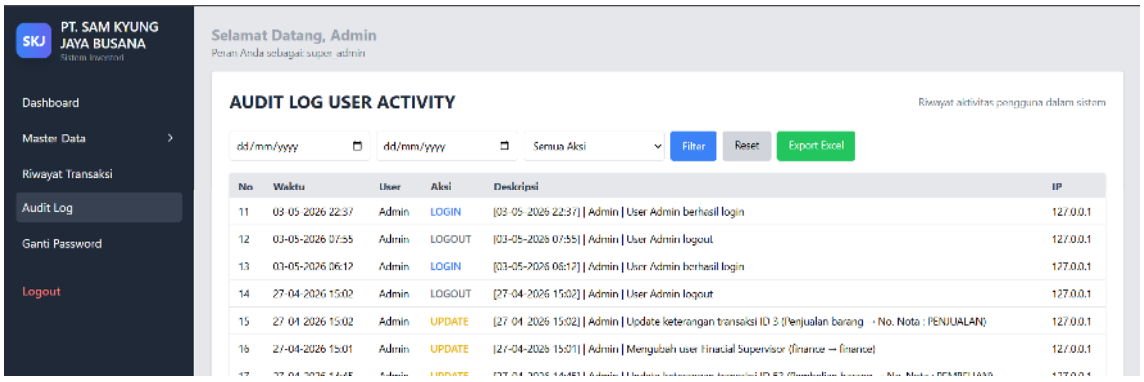
Tabel 4. Matriks Hak Akses Berdasarkan Peran (RBAC)

Modul / Fitur	Super Admin	Admin Gudang	Manajer	Direktur
Kelola Pengguna	Bisa	Tidak	Tidak	Tidak
Kelola Barang	Bisa	Bisa	Tidak	Tidak
Kelola Kategori	Bisa	Bisa	Tidak	Tidak
Kelola *Supplier*	Bisa	Bisa	Tidak	Tidak
Kelola *Customer*	Bisa	Bisa	Tidak	Tidak
Transaksi Masuk	Bisa	Bisa	Tidak	Tidak
Transaksi Keluar	Bisa	Bisa	Tidak	Tidak
Lihat Stok	Bisa	Bisa	Bisa	Bisa
Lihat Laporan	Bisa	Bisa	Bisa	Bisa
Cetak/Ekspor Laporan	Bisa	Bisa	Bisa	Tidak
Akses *Audit log*	Bisa	Tidak	Tidak	Tidak

Pembatasan akses berjalan dengan baik. Setiap percobaan mengakses halaman di luar kewenangan berhasil ditolak dengan respons HTTP 403 *Forbidden*. Temuan ini sejalan dengan Aswintama et al. [12] yang mencatat penurunan akses tidak sah hingga 87,5%, serta Purba dan Hidayasari [11] serta Sitanggang et al. [13] yang mencapai tingkat keberhasilan fungsional 100%.

3.5 Pengujian Audit log

Sistem merekam setiap aktivitas pengguna dengan metadata lengkap. Informasi yang direkam meliputi identitas pengguna, waktu kejadian, alamat IP, serta nilai data sebelum dan sesudah perubahan. Jenis aktivitas yang tercatat antara lain: *login/logout*, operasi *CREATE*, *UPDATE*, *DELETE*, dan percobaan akses tidak sah (*ACCESS_DENIED*).



Gambar 3. Halaman *Audit log* dengan Fitur *Filter* dan Ekspor
(Sumber: Dokumentasi Penelitian, 2026)

Sistem ini telah memenuhi persyaratan manajemen *audit log* yang diidentifikasi oleh Ali et al. [2], mencakup taksonomi pencatatan, keamanan *log*, dan kemampuan analisis. Perlindungan akses diterapkan dengan membatasi akses *audit log* hanya untuk Super Admin.

Pengembangan ke depan dapat mengadopsi *tamper-evident logging* [18] dan deteksi anomali berbasis *clustering* [19]

3.6 Hasil Pengujian Usability (System Usability Scale - SUS)

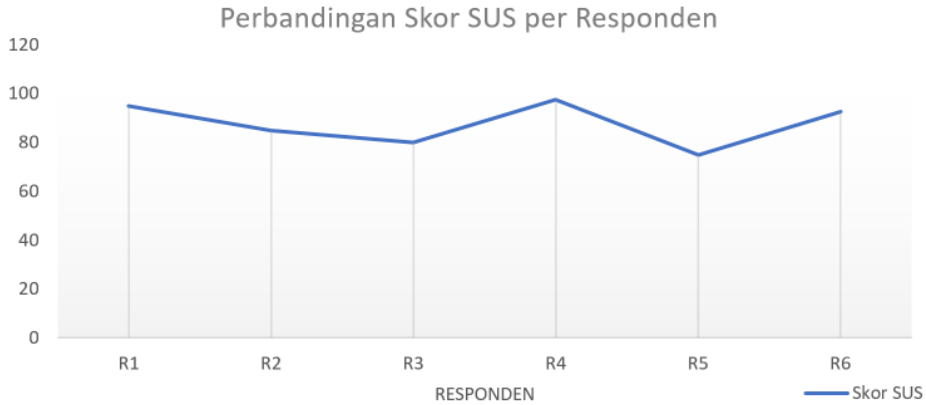
Pengujian SUS melibatkan 6 responden yang mewakili berbagai peran pengguna dalam UMKM sektor garmen. Jumlah ini memenuhi rekomendasi minimal untuk pengujian *usability* pada tahap pengembangan sistem. Perhitungan skor SUS mengacu pada metode yang dikembangkan oleh Lewis [25].

Hasil pengujian menunjukkan bahwa sistem memiliki tingkat *usability* yang tinggi dengan skor rata-rata SUS sebesar 87,5. Berdasarkan skala interpretasi SUS, skor ini termasuk dalam kategori *Excellent (Grade A)*. Mengingat ukuran sampel yang terbatas (n=6), interval kepercayaan *(confidence intervals)* dihitung menggunakan metode yang direkomendasikan oleh Clark et al. [27] untuk data SUS pada sampel kecil. Hasilnya menunjukkan bahwa interval kepercayaan 95% untuk skor SUS berada pada rentang 78,5 hingga 94,2, yang seluruhnya masih berada dalam kategori "*Good*" hingga "*Excellent*".

Tabel 5. Ringkasan Hasil Pengujian *System Usability Scale* (SUS)

Parameter	Nilai
Jumlah Responden	6
Skor Minimum	75.0
Skor Maksimum	97.5
Rata-rata Skor SUS	**87.5**
Kategori	***Excellent (Grade A)***

Capaian ini sebanding dengan temuan Purba & Hidayasari [11] yang mencapai skor SUS 76 pada sistem manajemen stok obat, dan sedikit lebih tinggi dari rata-rata sistem sejenis. Hal ini mengindikasikan bahwa sistem tidak hanya memenuhi aspek teknis dan keamanan, tetapi juga aspek kenyamanan penggunaan. Pengguna merasa sistem mudah dipelajari, mudah digunakan, dan tidak memerlukan bantuan teknis yang berarti.



Gambar 4. Grafik Perbandingan Skor SUS per Responden
(Sumber: Dokumentasi Penelitian, 2026)

3.7 Verifikasi Standar NIST SP 800-171

Verifikasi dilakukan terhadap aspek *audit and accountability* dalam standar NIST SP 800-171 [21]. Lima kontrol utama berhasil dipenuhi: (1) pencatatan *event audit* yang relevan (AU-2), (2) kelengkapan isi *record audit* (AU-3), (3) kemampuan *review* dan analisis (AU-6), (4)

perlindungan informasi audit (AU-9), dan (5) retensi *audit log* (AU-11). Dengan demikian, sistem telah memenuhi standar akuntabilitas untuk penanganan data sensitif.

3.8 Pembahasan

3.8.1 Enkripsi AES-256

Implementasi AES-256 terbukti efektif. Data sensitif terlindungi tanpa mengorbankan kemudahan penggunaan. Pendekatan *selective encryption* juga menjaga performa sistem. Pengembangan ke depan dapat mengadopsi AES-GCM-SIV [17] serta mengintegrasikan IoT dan *blockchain* [24].

3.8.2 RBAC

Pembatasan akses berbasis peran berjalan efektif. Prinsip *least privilege* diterapkan dengan baik. Seluruh akses di luar kewenangan berhasil ditolak. Temuan ini konsisten dengan berbagai penelitian sebelumnya tentang efektivitas RBAC.

3.8.3 Audit log

Pencatatan aktivitas berjalan lengkap dan terstruktur. Keberadaan metadata *before-after* memungkinkan pelacakan perubahan data secara akurat. Sistem telah memenuhi standar manajemen *audit log* yang direkomendasikan.

3.8.4 Keunggulan Dibanding Penelitian Sebelumnya

Penelitian ini memiliki keunggulan utama pada integrasi tiga mekanisme keamanan sekaligus (RBAC, enkripsi AES, dan *audit log*). Penelitian sebelumnya secara umum hanya mengintegrasikan dua mekanisme atau berfokus pada satu aspek saja. Evaluasi yang dilakukan juga lebih komprehensif, meliputi pengujian fungsional (100%), *usability* (SUS 87,5), dan verifikasi standar keamanan NIST SP 800-171.

3.8.5 Temuan Utama

Enam temuan utama dihasilkan dari penelitian ini. Pertama, enkripsi AES-256 efektif untuk data sensitif. Kedua, *audit log* meningkatkan akuntabilitas. Ketiga, RBAC berhasil membatasi akses. Keempat, sistem memiliki tingkat *usability* tinggi (SUS 87,5). Kelima, sistem memenuhi standar NIST SP 800-171. Keenam, sistem mendukung kepatuhan terhadap UU PDP.

3.8.6 Keterbatasan

Beberapa keterbatasan perlu diakui. Pengujian hanya dilakukan pada satu UMKM sektor garmen. Deteksi anomali *real-time* pada *audit log* belum tersedia. Cakupan enkripsi masih terbatas pada nomor telepon. Penyimpanan *audit log* masih terpusat.

3.9 Sintesis Hasil

Integrasi RBAC, enkripsi AES-256, dan *audit log* terbukti mampu meningkatkan keamanan, transparansi, dan akuntabilitas sistem inventori UMKM sektor garmen. Tingkat keberhasilan fungsional 100%, skor SUS 87,5 *(excellent)*, dan pemenuhan standar NIST SP 800-171 menjadi bukti kuat bahwa sistem ini layak diadopsi.

4. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem inventori berbasis web yang mengintegrasikan tiga mekanisme keamanan sekaligus, yaitu *Role-Based Access Control* (RBAC), enkripsi AES-256, dan *audit log*. Berdasarkan hasil pengujian, sistem menunjukkan kinerja yang sangat baik dengan tingkat keberhasilan pengujian fungsional mencapai 100%.

Dari aspek kemudahan penggunaan, evaluasi *System Usability Scale* (SUS) terhadap 6 responden menghasilkan skor rata-rata 87,5 yang termasuk dalam kategori *excellent*.

Implementasi enkripsi AES-256 terbukti efektif dalam melindungi data sensitif pengguna dari sisi keamanan. Mekanisme *audit log* juga berhasil merekam seluruh aktivitas pengguna secara lengkap, sehingga mendukung transparansi dan akuntabilitas sistem. Lebih lanjut, sistem telah memenuhi aspek *audit and accountability* dalam standar NIST SP 800-171 serta mendukung kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022. Kontribusi utama penelitian ini adalah tersedianya sistem inventori dengan mekanisme keamanan terintegrasi yang telah divalidasi pada UMKM sektor garmen.

5. SARAN

Berdasarkan keterbatasan yang telah diidentifikasi dalam penelitian ini, terdapat sejumlah arahan yang dapat menjadi fokus pengembangan lebih lanjut guna menyempurnakan kualitas dan keamanan sistem inventori di masa mendatang.

1. Perluasan cakupan enkripsi, data sensitif lain seperti alamat dan email juga perlu dienkripsi. Implementasi AES-GCM-SIV [17] dapat dipertimbangkan.
2. Deteksi anomali *real-time*, kembangkan mekanisme pendeteksian aktivitas mencurigakan pada *audit log* menggunakan teknik *clustering* [19].
3. Peningkatan penyimpanan *audit log*, migrasi ke *tamper-evident logging* seperti DPTracer [18] untuk meningkatkan ketahanan *log*.
4. Integrasi IoT dan *blockchain* [24] dapat dimanfaatkan untuk meningkatkan visibilitas inventori secara *real-time*.
5. Pengujian skala lebih besar, libatkan lebih banyak UMKM atau perusahaan skala menengah untuk meningkatkan validitas hasil.

DAFTAR PUSTAKA

[1] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahyu, "Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department," *Int. J. Electr. Comput. Biomed. Eng.*, vol. 2, no. 3 SE-Computer Engineering, pp. 395–413, Sep. 2024, doi: 10.62146/ijecbe.v2i3.81.

[2] A. Ali, M. Ahmed, and A. Khan, "Audit logs management and security - A survey," *Kuwait J. Sci.*, vol. 48, no. 3 SE-Computer Science, Jun. 2021, doi: 10.48129/kjs.v48i3.10624.

[3] S. Mishra, J. Sah, and B. Sharma, "DIGITALIZATION AS A COMPETITIVE DIFFERENTIATOR: ERP ADOPTION CHALLENGES IN INDIAN GARMENT SME CLUSTERS," *Int. J. Eng. Technol. Manag. Res.*, vol. 12, no. 4 SE-Articles, pp. 123–127, Apr. 2025, doi: 10.29121/ijetmr.v12.i4.2025.1708.

[4] A. Susanty, N. B. Puspitasari, G. S. Siahaan, S. Setiawan, and M. Syafrudin, "Factors influencing the intention of textile and garment SMEs to adopt digital technologies and its impact on performance," *Sci. Rep.*, vol. 15, no. 1, p. 20807, 2025, doi: 10.1038/s41598-025-94625-7.

[5] C.-C. Wang, Y.-T. Hsu, and H.-Y. Kuo, "Enhancing Supply Chain Resilience in Textile SMEs: A Human-Centric Customer-to-Manufacturer Framework Using Public E-Commerce Data," 2026. doi: 10.3390/jtaer21040123.

[6] A. Darmawi, R. Istikowati, and G. Y. Astrini, "Optimizing inventory management in the textile industry: a comprehensive evaluation of UHF-RFID technology integration," *Int. J. Adv. Appl. Sci.*, vol. 14, no. 4, pp. 1411–1419, 2025, doi: 10.11591/ijaas.v14.i4.pp1411-1419.

[7] R. R. A. Tisza-Vargas, "Lean-Based Operations Management for Inventory Optimization: A Case Study in Peruvian Textile SMEs," pp. 121–134, 2025, doi: 10.46254/gc02.20240032.

[8] C. Blundo and S. Cimato, "Role mining under User-Distribution cardinality constraint," *J. Inf. Secur. Appl.*, vol. 78, p. 103611, 2023, doi: https://doi.org/10.1016/j.jisa.2023.103611.

[9] David Fitrianto and W. Y. Sulistyo, "Penerapan Role Based Access Control untuk Keamanan Data Multi Tenant SIMPEL Lazismu," *Insect (Informatics Secur. J. Tek. Inform.*, vol. 12, no. 01 SE-Articles, pp. 1–10, Mar. 2026, doi: 10.33506/insect.v12i01.5009.

[10] P. Patil, "Design and Performance Analysis of a Secure Multi-User Database with Role-Based Access Control and Audit Trail," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 7, pp. 2184–2184, 2025, doi: 10.38124/ijisrt/25jul1399.

[11] D. A. Purba *et al.*, "Implementasi Role - Based Access Control (RBAC) pada Sistem Informasi Manajemen Stok Obat Implementation of Role - Based Access Control (RBAC) in a Drug Stock," vol. 15, pp. 684–698, 2026, doi: https://doi.org/10.32520/stmsi.v15i2.5958.

[12] P. Aswintama, E. Haryanto, and R. A. Setyawan, "Implementation of role-based access control, multi tenancy and audit logging in a single sign-on system," *J. Mandiri IT*, vol. 14, no. 1 SE-Articles, pp. 119–128, Jul. 2025, doi: 10.35335/mandiri.v14i1.441.

[13] J. A. Sitanggang, B. H. Saputra, A. Hidayati, and H. Saragih, "Design and development of the spacelog web application for inventory management and asset tracking using QR codes at the Cyber Defense Center of the Ministry of Defense," *J. Mandiri IT*, vol. 14, no. 3 SE-Articles, pp. 283–293, Jan. 2026, doi: 10.35335/mandiri.v14i3.481.

[14] Laravel, "Laravel Documentation," *30/11/2015*, p. 1, 2015, [Online]. Available: http://web.archive.org/web/20140920185439/http://laravel.com/docs/introduction

[15] N. Matas Ali and V. Haripriya, "Enhancing Data Protection through Advanced Encryption or Improving Data Security with Advanced Encryption," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 12, no. 03, pp. 1710–1715, 2024, doi: 10.15680/ijircce.2024.1203056.

[16] M. Yusuf, A. Arizal, and I. R. Hikmah, "Implementation Cryptography and Access Control on IoT-Based Warehouse Inventory Management System," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 1 SE-Articles, pp. 37–50, 2022, doi: 10.30812/matrik.v22i1.1849.

[17] A. Asgap Putra Zulian, K. Kartarina, and I. M. Y. Dharma, "Analisis Pengamanan File Menggunakan Enkripsi dan Dekripsi dengan Algoritma AES-GCM-SIV," *Edu Elektr. J.*, vol. 13, no. 1, pp. 15–23, 2026, doi: 10.15294/eduel.v13i1.26826.

[18] J. Lee, "DPTracer: Integrating Log-Driven Accountability into Data Provision Networks," 2024. doi: 10.3390/app14188503.

[19] C. H. Saputra, "Integrasi Audit Trail dan Teknik Clustering untuk Segmentasi dan Kategorisasi Aktivitas Log," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 1 SE-Ilmu Komputer, pp. 209–214, Feb. 2024, doi: 10.25126/jtiik.20241118071.

[20] Pemerintah Pusat, "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *Pemerintah Pus.*, no. 016999, p. 1, 2022, [Online]. Available: https://peraturan.bpk.go.id/Download/224884/UU Nomor 27 Tahun 2022.pdf

[21] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie, "NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," *Natl. Inst. Stand. Technol. Spec. Publ. 800-171*, 2020, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-171r2

[22] J. Akoka, I. Comyn-Wattiau, and V. C. Storey, "Design Science Research: Progression, Schools of Thought and Research Themes BT - Design Science Research for a New Society: Society 5.0," A. Gerber and R. Baskerville, Eds., Cham: Springer Nature

Switzerland, 2023, pp. 235–249. doi: https://doi.org/10.1007/978-3-031-32808-4_15.

[23] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[24] B. Takawira and B. Duri, "Integrating IoT and Blockchain for Real-Time Inventory Visibility and Traceability: A Bibliometric–Systematic Review," 2026. doi: 10.3390/logistics10030057.

[25] J. R. Lewis, "The System Usability Scale: Past, Present, and Future," *Int. J. Human–Computer Interact.*, vol. 34, no. 7, pp. 577–590, Jul. 2018, doi: 10.1080/10447318.2018.1455307.

[26] J. R. Lewis, "Sample sizes for usability tests: mostly math, not magic," *Interactions*, vol. 13, no. 6, pp. 29–33, 2006, doi: 10.1145/1167948.1167973.

[27] N. Clark, M. Dabkowski, P. J. Driscoll, D. Kennedy, I. Kloo, and H. Shi, "Empirical Decision Rules for Improving the Uncertainty Reporting of Small Sample System Usability Scale Scores," *Int. J. Human–Computer Interact.*, vol. 37, no. 13, pp. 1191–1206, Aug. 2021, doi: 10.1080/10447318.2020.1870831.