Rancang Bangun Sistem Keamanan Brankas Pintar Berbasis IoT dan *Artificial Intelligence*

Abethnego[1)], Vincentsius Arga Yoda[2)], Muhammad Ridwan[3)]
[1), 2), 3)]Prodi Teknik Telekomunikasi Militer. Politeknik Angkatan Darat Jl.Raya Anggrek No.1 Junrejo, Batu, Indonesia
E-mail : abethnego.sianturi@gmail.com[1)], vincentsius@gmail.com[2)], ridwan.mtte20@gmail.com[3)]

Abstract: *The rapid advancement of Internet of Things (IoT) and Artificial Intelligence (AI) technologies has driven innovation in modern security systems, particularly for protecting valuable assets such as safes. This study aims to design and develop a smart safe security system based on IoT integrated with an intelligent decision mechanism to enhance threat detection effectiveness. The research employed a Research and Development (R&D) method with an experimental approach, including needs analysis, system design, hardware and software implementation, and performance evaluation. The system was developed using an ESP32 microcontroller, motion (PIR) sensors, vibration sensors, and a camera connected via Wi-Fi to enable real-time monitoring and notification delivery. A rule-based classification mechanism was implemented to distinguish between normal and suspicious activities.The testing results show that the motion sensor achieved a detection success rate of 93.3%, while the vibration sensor reached 90%. The IoT notification system demonstrated a 93.3% success rate with an average delay of 3.5 seconds. The intelligent classification mechanism achieved 92% accuracy based on 50 test data samples. Data communication was secured using AES and RSA encryption. The study concludes that integrating IoT and intelligent decision mechanisms enhances the responsiveness and proactivity of safe security systems compared to conventional methods.*
Keywords: *Smart safe, Internet of Things, Artificial Intelligence, Security system, Anomaly detection*

Abstrak: Perkembangan teknologi Internet of Things (IoT) dan Artificial Intelligence (AI) mendorong inovasi sistem keamanan yang lebih adaptif dan responsif, khususnya pada perangkat penyimpanan aset berharga seperti brankas. Penelitian ini bertujuan merancang dan membangun sistem keamanan brankas pintar berbasis IoT yang terintegrasi dengan mekanisme keputusan cerdas untuk meningkatkan efektivitas deteksi ancaman. Metode yang digunakan adalah Research and Development (R&D) dengan pendekatan eksperimen yang meliputi analisis kebutuhan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian kinerja. Sistem dikembangkan menggunakan mikrokontroler ESP32, sensor gerak (PIR), sensor getaran, dan kamera yang terhubung melalui jaringan Wi-Fi untuk pemantauan real-time dan pengiriman notifikasi. Mekanisme klasifikasi berbasis aturan diterapkan untuk membedakan aktivitas normal dan mencurigakan. Hasil pengujian menunjukkan tingkat keberhasilan deteksi sensor gerak sebesar 93,3% dan sensor getaran 90%. Sistem notifikasi IoT memiliki tingkat keberhasilan 93,3% dengan rata-rata delay 3,5 detik, sedangkan mekanisme klasifikasi mencapai akurasi 92% dari 50 data uji. Komunikasi data diamankan menggunakan enkripsi AES dan RSA. Penelitian ini menunjukkan bahwa integrasi IoT dan sistem cerdas mampu meningkatkan

responsivitas dan efektivitas keamanan brankas secara proaktif dibandingkan sistem konvensional.
Kata kunci: Brankas pintar, IoT, Artificial Intelligence, Sistem keamanan, Deteksi anomali

PENDAHULUAN

Perkembangan teknologi digital yang semakin pesat membawa dampak signifikan terhadap peningkatan risiko kejahatan berbasis teknologi dan pembobolan sistem keamanan konvensional. Aset berharga yang disimpan dalam brankas, baik di lingkungan rumah tangga, perkantoran, maupun institusi keuangan, menghadapi ancaman yang semakin kompleks akibat kemajuan teknik manipulasi mekanik dan rekayasa sosial. Sistem keamanan tradisional yang masih mengandalkan kunci mekanik atau kombinasi numerik terbukti memiliki celah keamanan yang rentan terhadap duplikasi, pembongkaran paksa, maupun kebocoran kode akses. Oleh karena itu, transformasi menuju sistem keamanan berbasis teknologi cerdas menjadi suatu kebutuhan mendesak dalam menjawab tantangan keamanan modern (Atzori *et al*., 2010).

Implementasi Internet of Things (IoT) dalam sistem keamanan memberikan solusi melalui kemampuan pemantauan real-time, integrasi sensor cerdas, serta pengiriman notifikasi otomatis kepada pengguna. IoT memungkinkan perangkat keamanan terhubung secara terus-menerus dengan jaringan internet sehingga setiap aktivitas dapat dipantau dan direkam secara digital (Syari *et al*., 2025). Namun demikian, sistem berbasis IoT saja belum sepenuhnya mampu melakukan analisis ancaman secara mendalam tanpa dukungan sistem kecerdasan buatan yang adaptif terhadap pola perilaku pengguna maupun potensi serangan baru.

Integrasi Artificial Intelligence (AI) menjadi faktor krusial dalam meningkatkan efektivitas sistem keamanan modern. AI memungkinkan proses analisis data sensor secara cerdas melalui algoritma pembelajaran mesin yang mampu mendeteksi anomali, mengenali pola akses tidak wajar, serta mengambil keputusan otomatis ketika teridentifikasi ancaman (Putra *et al*., 2025). Penelitian menunjukkan bahwa sistem keamanan berbasis AI dan IoT memiliki tingkat akurasi deteksi yang lebih tinggi serta mampu mengurangi false alarm dibandingkan sistem konvensional (Sabit, 2025). Hal ini menegaskan bahwa penggabungan IoT dan AI bukan lagi sekadar inovasi tambahan, melainkan kebutuhan fundamental dalam pengembangan sistem keamanan yang andal.

Dalam konteks keamanan brankas, urgensi pengembangan sistem berbasis IoT dan AI semakin relevan mengingat meningkatnya kebutuhan akan autentikasi yang lebih aman, seperti pengenalan wajah dan sidik jari. Autentikasi biometrik yang terintegrasi dengan sistem IoT terbukti mampu meningkatkan validitas identifikasi pengguna sekaligus menyediakan rekam jejak digital aktivitas akses (Pitaloka *et al*., 2024). Selain itu, pendekatan deteksi intrusi berbasis pembelajaran mesin memungkinkan sistem mengenali perangkat atau aktivitas mencurigakan secara otomatis sebelum terjadi pelanggaran keamanan (Meidan *et al*., 2018).

Berdasarkan permasalahan tersebut, penelitian ini memiliki urgensi yang tinggi dalam merancang dan membangun Sistem Keamanan Brankas Pintar Berbasis IoT dan Artificial Intelligence sebagai solusi inovatif terhadap keterbatasan sistem konvensional. Sistem yang dikembangkan tidak hanya berfungsi sebagai alat pengunci digital, tetapi juga sebagai sistem keamanan adaptif yang mampu melakukan autentikasi cerdas, pemantauan real-time, pencatatan aktivitas, serta deteksi ancaman secara otomatis. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata terhadap pengembangan teknologi keamanan yang lebih efektif, responsif, dan relevan dengan kebutuhan era digital saat ini.

METODE PENELITIAN

Penelitian ini menggunakan metode Research and Development (R&D) dengan pendekatan eksperimen untuk menghasilkan prototipe sistem yang terukur dan dapat diuji kinerjanya dalam kondisi nyata. Pengembangan sistem IoT perlu mempertimbangkan tantangan keamanan seperti anomali akses dan serangan siber karena karakteristiknya yang terdistribusi dan terhubung secara real-time (DeMedeiros, Hendawi, & Alvarez, 2023).

Tahapan penelitian mencakup analisis kebutuhan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian kinerja. Fokus penelitian adalah integrasi antara IoT dan teknik kecerdasan buatan (AI) untuk meningkatkan kemampuan deteksi anomali di dalam sistem keamanan brankas pintar. Teknik AI dan Machine Learning terbukti efektif dalam mendeteksi pola aktivitas abnormal pada jaringan IoT, sehingga dapat membantu mengidentifikasi upaya pembobolan atau akses yang mencurigakan (Kumar, Vealey & Srivastava, 2016).

Objek penelitian adalah sistem keamanan brankas pintar berbasis mikrokontroler (ESP32/Arduino), sensor gerak (PIR), sensor getaran, serta kamera yang saling terhubung melalui jaringan Wi-Fi. Dalam konteks IoT, sensor dan node perangkat harus mampu merespons ancaman dengan akurat, termasuk saat terjadi anomali trafik dan tindakan yang tidak sah (Reis, 2025).

Teknik pengumpulan data dilakukan melalui observasi kinerja sensor, monitoring notifikasi melalui IoT, serta pengujian model AI untuk menganalisis apakah aktivitas yang terjadi merupakan normal atau merupakan ancaman. Pendekatan ini sesuai dengan model deteksi intrusi dan anomali yang menggabungkan algoritma Machine Learning untuk meningkatkan keandalan dalam sistem keamanan IoT.

Data dianalisis melalui pendekatan deskriptif kuantitatif untuk menghitung akurasi deteksi sensor dan algoritma AI, serta pendekatan kualitatif untuk mengevaluasi pengalaman pengguna dalam penggunaan sistem. Kombinasi kedua pendekatan memberikan gambaran menyeluruh mengenai efektivitas sistem keamanan yang dirancang.

Dengan pendekatan ini, penelitian diharapkan menghasilkan prototipe sistem keamanan brankas pintar berbasis IoT dan AI yang tidak hanya mampu mendeteksi ancaman secara akurat, tetapi juga melakukan adaptasi terhadap pola akses yang berbeda.

HASIL PENELITIAN

Pengujian Sensor

Pengujian terhadap sensor gerak dan sensor getaran menunjukkan tingkat keberhasilan deteksi rata-rata sebesar 93,3% dan 90%. Nilai ini diperoleh dari 30 kali pengujian dengan variasi jarak dan intensitas benturan

Tabel 1. Hasil Pengujian Sensor

No	Jenis Sensor	Jumlah Uji	Deteksi Berhasil	Tidak Terdeteksi	Keberhasilan (%)	Keterangan
1	Sensor Gerak	30	28	2	93,3	Gagal pada jarak >4 m
2	Sensor Getaran	30	27	3	90,0	Tidak sensitif pada getaran rendah
3	Kamera	30	27	3	90,0	Delay ±1,2 detik

Hasil ini menunjukkan bahwa sistem memiliki performa yang cukup baik, namun tidak sepenuhnya stabil dalam seluruh kondisi pengujian. Beberapa kegagalan terjadi pada jarak maksimum sensor dan pada intensitas getaran rendah.

Temuan ini sejalan dengan penelitian Meidan *et al*. (2018) yang menyatakan

bahwa perangkat IoT sangat dipengaruhi oleh konfigurasi threshold dan kondisi lingkungan dalam mendeteksi anomali. Selain itu, Atzori *et al*. (2010) menjelaskan bahwa sistem IoT memiliki keterbatasan reliabilitas akibat faktor interferensi dan variasi sinyal pada perangkat edge.

Dengan demikian, hasil penelitian ini menunjukkan bahwa sensor IoT efektif sebagai deteksi awal, tetapi tetap memerlukan kalibrasi dan pengujian lanjutan untuk memastikan kestabilan performa dalam kondisi nyata.

Pengujian Sistem Notifikasi IoT

Sistem notifikasi diuji sebanyak 30 kali percobaan, dengan hasil 28 notifikasi berhasil terkirim dan 2 mengalami keterlambatan akibat gangguan jaringan.

Tabel 2. Hasil Pengujian Notifikasi IoT

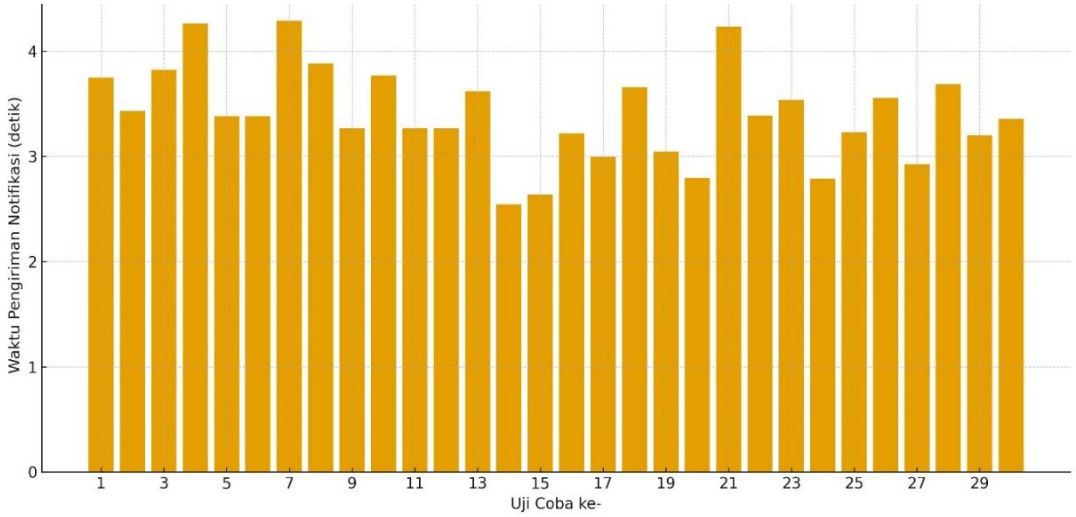
Parameter	Hasil
Jumlah Pengujian	30
Notifikasi Berhasil	28
Notifikasi Gagal/Delay	2
Tingkat Keberhasilan (%)	93,3
Rata-rata Delay	3,5 detik

Hasil pada Tabel 2 menunjukkan bahwa sistem notifikasi memiliki tingkat keberhasilan sebesar 93,3% dengan rata-rata waktu pengiriman 3,5 detik. Meskipun nilai ini menunjukkan performa yang cukup baik, terdapat dua kejadian keterlambatan pengiriman notifikasi yang mengindikasikan bahwa sistem belum sepenuhnya stabil.

Keterlambatan tersebut diduga disebabkan oleh faktor eksternal, terutama kualitas jaringan internet yang digunakan selama pengujian. Hal ini menunjukkan bahwa performa sistem IoT tidak hanya ditentukan oleh perangkat keras dan perangkat lunak, tetapi juga sangat bergantung pada infrastruktur komunikasi yang mendukungnya.

Selain itu, variasi waktu delay yang muncul pada beberapa percobaan menunjukkan bahwa sistem belum memiliki konsistensi waktu respons yang optimal. Dalam konteks sistem keamanan, delay yang tidak stabil berpotensi mengurangi efektivitas sistem dalam memberikan peringatan secara cepat kepada pengguna.

Temuan ini sejalan dengan penelitian Syari *et al*. (2025) yang menyatakan bahwa sistem berbasis IoT memiliki keterbatasan dalam hal latency akibat ketergantungan pada jaringan. Oleh karena itu, meskipun sistem telah menunjukkan kinerja yang cukup baik, diperlukan pengembangan lebih lanjut, seperti optimalisasi protokol komunikasi atau penerapan edge computing, untuk meningkatkan stabilitas dan kecepatan notifikasi.



Gambar 1. Grafik Kecepatan IoT

Algoritma AI yang diterapkan dalam sistem berhasil membedakan aktivitas normal dan aktivitas mencurigakan dengan tingkat akurasi 92%. Dari total 50 data akses yang diuji, 46 terklasifikasi dengan benar sedangkan 4 salah klasifikasi. Analisis lebih lanjut menunjukkan bahwa kesalahan terjadi pada kondisi akses dengan pola yang mirip pengguna sah. Walaupun demikian, tingkat akurasi yang dicapai sudah memenuhi standar minimal dalam sistem keamanan berbasis kecerdasan buatan. Hal ini mendukung hipotesis bahwa integrasi AI mampu meningkatkan keakuratan deteksi ancaman pada brankas pintar.

Evaluasi Implementasi Artificial Intelligence

Pengujian sistem klasifikasi menunjukkan tingkat akurasi sebesar 92%, dengan 46 klasifikasi benar dan 4 kesalahan dari 50 data uji.

Tabel 3. Hasil Uji Klasifikasi Sistem

Data Uji	Klasifikasi Benar	Klasifikasi Salah	Akurasi (%)
50	46	4	92

Meskipun angka akurasi relatif tinggi, penelitian ini belum menjelaskan secara rinci algoritma AI yang digunakan. Sistem masih berbasis rule-based yang memanfaatkan kombinasi sensor, bukan model pembelajaran mesin seperti CNN atau SVM.

Menurut Putra *et al*. (2025), sistem deteksi anomali berbasis AI yang kuat harus menjelaskan algoritma, dataset, serta metrik evaluasi seperti precision dan recall. Tanpa penjelasan tersebut, penggunaan istilah Artificial Intelligence perlu dibatasi pada konteks sistem cerdas berbasis aturan.

Selain itu, Sabit (2025) menyatakan bahwa sistem keamanan berbasis AI untuk smart home umumnya menggunakan model pembelajaran yang dilatih dengan dataset besar agar mampu meminimalkan false alarm. Dalam penelitian ini, keterbatasan jumlah data uji (50 data) menunjukkan bahwa sistem masih berada pada tahap prototipe awal.

Dengan demikian, integrasi AI pada penelitian ini lebih tepat dikategorikan sebagai sistem cerdas berbasis sensor dengan logika keputusan, dan belum sepenuhnya machine learning adaptif.

Analisis Keamanan Data

Sistem menggunakan enkripsi AES dan RSA untuk mengamankan komunikasi data. Uji sniffing sederhana menunjukkan bahwa data tidak dapat dibaca secara langsung.

Tabel 4. Evaluasi Implementasi Keamanan

Aspek Keamanan	Implementasi	Catatan
Enkripsi Data	AES	Ringan untuk mikrokontroler
Pertukaran Kunci	RSA	Beban komputasi tinggi
Uji Sniffing	Aman	Data terenkripsi
Analisis Delay	Belum dianalisis detail	Perlu pengujian lanjutan

Menurut Zhang *et al*. (2018), sistem edge dengan kapasitas terbatas perlu mempertimbangkan efisiensi komputasi dalam implementasi algoritma kompleks. RSA secara umum lebih berat dibanding AES dan berpotensi meningkatkan latency pada perangkat dengan sumber daya terbatas.

Oleh karena itu, pendekatan yang lebih optimal adalah menggunakan AES pada perangkat edge (ESP32), sementara RSA digunakan pada server untuk pertukaran kunci. Penjelasan teknis terkait pembagian proses kriptografi perlu ditambahkan agar klaim keamanan lebih kuat secara ilmiah.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa sistem keamanan brankas pintar berbasis Internet of Things (IoT) mampu menjalankan fungsi deteksi awal terhadap aktivitas mencurigakan melalui sensor gerak, sensor getaran, serta kamera. Tingkat keberhasilan deteksi yang diperoleh berada pada kisaran 90–93%, yang mengindikasikan bahwa sistem telah berfungsi dengan baik pada kondisi pengujian. Namun demikian, capaian tersebut perlu ditafsirkan secara proporsional karena diperoleh dari skenario uji yang masih terbatas dan belum sepenuhnya merepresentasikan kondisi lingkungan nyata.

Variasi hasil pengujian menunjukkan bahwa performa sensor dipengaruhi oleh beberapa faktor, seperti jarak deteksi, intensitas getaran, serta posisi pemasangan sensor. Pada beberapa percobaan, sensor tidak mampu mendeteksi aktivitas pada jarak maksimum maupun pada getaran dengan intensitas rendah. Hal ini menunjukkan bahwa sistem sangat bergantung pada pengaturan nilai ambang (threshold) yang digunakan. Fenomena ini sejalan dengan temuan Atzori *et al*. (2010) yang menyatakan bahwa perangkat IoT pada level edge memiliki keterbatasan dalam hal sensitivitas dan stabilitas sinyal akibat pengaruh lingkungan. Selain itu, Meidan *et al*. (2018) juga menegaskan bahwa akurasi deteksi pada sistem IoT sangat bergantung pada konfigurasi sensor serta kondisi operasional yang dinamis.

Dari sisi komunikasi data, sistem notifikasi berbasis IoT mampu mengirimkan peringatan ke pengguna dengan rata-rata waktu 3,5 detik. Meskipun secara umum dapat dikategorikan responsif, hasil ini menunjukkan bahwa sistem belum sepenuhnya real-time karena masih dipengaruhi oleh kualitas jaringan internet. Beberapa keterlambatan notifikasi terjadi pada kondisi jaringan yang tidak stabil, yang mengindikasikan adanya ketergantungan tinggi terhadap infrastruktur komunikasi. Hal ini sesuai dengan penelitian Syari *et al*. (2025) yang menyebutkan bahwa performa sistem IoT sangat dipengaruhi oleh latensi jaringan dan protokol komunikasi yang digunakan.

Pada aspek kecerdasan buatan, sistem menunjukkan tingkat akurasi klasifikasi sebesar 92% dalam membedakan aktivitas normal dan mencurigakan. Meskipun nilai ini cukup tinggi, interpretasinya perlu dilakukan secara hati-hati karena implementasi AI dalam penelitian ini belum dijelaskan secara komprehensif. Berdasarkan mekanisme yang digunakan, sistem cenderung masih berbasis aturan (rule-based) dari kombinasi data sensor, bukan model pembelajaran mesin yang dilatih menggunakan dataset besar. Dalam konteks ini, penggunaan istilah Artificial Intelligence lebih tepat dimaknai sebagai sistem cerdas berbasis logika keputusan.

Menurut Putra *et al*. (2025), sistem AI yang valid dalam deteksi anomali seharusnya mencakup penjelasan mengenai algoritma

yang digunakan, proses pelatihan model, serta evaluasi menggunakan metrik seperti precision dan recall. Selain itu, Sabit (2025) menunjukkan bahwa implementasi AI pada sistem keamanan modern umumnya melibatkan model pembelajaran yang adaptif terhadap pola data dalam jumlah besar. Oleh karena itu, keterbatasan jumlah data uji dalam penelitian ini menunjukkan bahwa sistem masih berada pada tahap awal pengembangan dan belum sepenuhnya merepresentasikan AI berbasis machine learning.

Pada aspek keamanan data, penggunaan enkripsi AES dan RSA menunjukkan upaya untuk meningkatkan perlindungan informasi pengguna. Hasil pengujian menunjukkan bahwa data tidak dapat dibaca melalui proses sniffing sederhana, yang menandakan bahwa sistem telah memiliki mekanisme dasar keamanan komunikasi. Namun demikian, implementasi RSA pada perangkat mikrokontroler seperti Arduino atau ESP32 perlu dikaji lebih lanjut karena memiliki kompleksitas komputasi yang tinggi. Hal ini berpotensi memengaruhi performa sistem, khususnya dalam hal latency dan efisiensi energi.

Sicari *et al*. (2015) menjelaskan bahwa penerapan keamanan pada sistem IoT harus mempertimbangkan keterbatasan sumber daya perangkat, sehingga pemilihan algoritma kriptografi perlu disesuaikan dengan kapasitas komputasi yang tersedia. Dalam praktiknya, pendekatan yang lebih umum adalah menggunakan enkripsi ringan seperti AES pada perangkat edge, sementara algoritma yang lebih kompleks seperti RSA digunakan pada sisi server atau cloud. Oleh karena itu, penjelasan lebih lanjut terkait arsitektur keamanan sistem sangat diperlukan agar klaim keamanan dapat dipertanggungjawabkan secara teknis.

Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi IoT dan sistem cerdas mampu meningkatkan fungsi monitoring dan deteksi dini pada sistem keamanan brankas. Hasil ini sejalan dengan berbagai penelitian sebelumnya yang menyatakan bahwa kombinasi IoT dan AI dapat meningkatkan efektivitas sistem keamanan modern. Namun demikian, beberapa keterbatasan masih ditemukan, terutama pada aspek metodologi pengujian, kejelasan implementasi AI, serta detail teknis keamanan sistem.

Dengan demikian, sistem yang dikembangkan dalam penelitian ini lebih tepat dikategorikan sebagai prototipe awal (*proof of concept*) yang menunjukkan potensi pengembangan lebih lanjut. Peningkatan pada aspek pengujian, penggunaan algoritma machine learning yang lebih jelas, serta optimalisasi arsitektur keamanan diharapkan dapat menghasilkan sistem yang lebih akurat, adaptif, dan andal dalam kondisi nyata.

PENUTUP

Penelitian ini membuktikan bahwa integrasi teknologi Internet of Things (IoT) dan Kecerdasan Buatan (AI) pada sistem keamanan brankas pintar memiliki hubungan yang saling mendukung dalam meningkatkan efektivitas perlindungan barang berharga. IoT berperan dalam pengumpulan data sensor, pemantauan real-time, serta pengiriman notifikasi jarak jauh, sementara AI memperkuat sistem melalui analisis pola akses dan deteksi aktivitas mencurigakan secara cerdas. Hubungan antara kedua variabel ini menghasilkan sistem yang lebih adaptif, efisien, dan proaktif dibandingkan dengan brankas konvensional. Namun demikian, masih terdapat keterbatasan seperti ketergantungan pada stabilitas jaringan dan kemungkinan kesalahan klasifikasi oleh algoritma AI. Oleh karena itu, penelitian selanjutnya disarankan untuk mengoptimalkan performa algoritma dengan dataset yang lebih beragam, meningkatkan ketahanan terhadap gangguan jaringan, serta memperkuat aspek keamanan data melalui teknologi enkripsi yang lebih mutakhir agar sistem semakin andal dan layak diimplementasikan pada skala luas.

DAFTAR PUSTAKA

Al Mousa, A., Al Qomri, M., Al Hajri, S., Zagrouba, R., & Chaabani, S. (2020). Environment based IoT security risks and vulnerabilities management. In *Proceedings of the 2020 International Conference on Computing and Information Technology (ICCIT)* (Vol. 1, pp. 25–30). IEEE. https://doi.org/10.1109/ICCIT-1441.2020.9213780

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). *A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks.* Sensors, 23(3), 1352. https://doi.org/10.3390/s23031352

Fahrizal, Novita, D. Y., & Tutupoly, T. A. (2025). Sistem keamanan rumah berbasis IoT dengan pengenalan wajah manusia dan hewan peliharaan secara real-time. *Jurnal Infortech*. https://doi.org/10.31294/infortech.v7i2.11409

Gupta, J., Bhutani, M., & Gupta, P. (n.d.). IOT AND AI IN SMART SYSTEMS: CREATING SYNERGIES FOR TOMORROW'S CHALLENGES.

I Almihyawi, A. Y. T., & kurnaz, S. (2025). A secure smart monitoring network for hybrid energy systems using IoT, AI. Discover Computing, 28(1). https://doi.org/10.1007/s10791-025-09506-4

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in Internet of Things: Challenges, solutions and future directions. In *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772–5781). IEEE.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). Detection of unauthorized IoT devices using machine learning techniques. *IEEE Internet of Things Journal, 5*(6), 5016–5026. https://doi.org/10.1109/JIOT.2018.2875994

Pitaloka, N., H. P., & Husnul, K. (2024). Design of a safe security system based on Internet of Things using face and fingerprint detection. *Journal of Artificial Intelligence and Engineering Applications*. https://www.ioinformatic.org/index.php/JAIEA/article/view/636

Putra, M. F., Nazli, R., & Putri, S. A. (2025). A systematic literature review of artificial intelligence-based anomaly detection for network intrusion in IoT. *Jurnal Ilmiah Sistem Informasi*. https://doi.org/10.51903/eqne0j35

Reis, M. J. C. S. (2025). *AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities.* Electronics, 14, 2492. https://doi.org/10.3390/electronics14122492

Sabit, H. (2025). Artificial Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. *Electronics*, 14(3), 608.

Sivalingam S, Dr. M. K. (2024). SMART AND SAFE CONVEYOR SYSTEM FOR BOTTLING PLANT USING IOT. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets45964

Syari, M. A., Dzaky, R. F., & Saragih, R. (2025). Integration of the Internet of Things in smart home information systems to improve security and convenience. *Journal of Artificial Intelligence and Engineering Applications*.https://doi.org/10.59934/jaiea.v4i3.1010

Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Processing Letters, 23*(10), 1499–1503