

Studi Literatur: Mekanisme Autentikasi Perangkat IoT untuk Mencegah Serangan Injection pada Database Pertanian Cerdas

Yuris Ikrar Rabbani ^{1)*} , Wildan Ramadhani ²⁾ 

¹⁾²⁾Universitas Madura, Pamekasan, Indonesia

¹⁾yurisikrar78@gmail.com ²⁾ danzkeren65@gmail.com

Abstrak

Implementasi teknologi *Internet of Things* (IoT) dalam ekosistem pertanian cerdas (*smart agriculture*) telah membawa transformasi signifikan dalam efisiensi pengelolaan sumber daya, namun di sisi lain memunculkan tantangan keamanan siber yang sangat kompleks, terutama terkait perlindungan integritas data pada database pusat. Perangkat IoT yang umumnya memiliki keterbatasan sumber daya komputasi dan energi sering kali menjadi titik lemah yang dimanfaatkan oleh penyerang sebagai vektor untuk meluncurkan serangan *injection*, seperti *SQL Injection* atau *NoSQL Injection*, yang dapat mengakibatkan manipulasi data sensor, pencurian informasi sensitif, hingga kegagalan sistem irigasi atau pemupukan otomatis. Analisis Literatur Sistematis (SLR) ini dilakukan untuk mengidentifikasi, menganalisis, dan mensintesis berbagai mekanisme autentikasi perangkat IoT yang paling efektif dalam memitigasi risiko serangan *injection* pada infrastruktur pertanian cerdas. Melalui tinjauan mendalam terhadap literatur ilmiah dari lima tahun terakhir, penelitian ini mengeksplorasi beragam skema autentikasi mulai dari protokol kriptografi ringan (*lightweight cryptography*) yang efisien energi, sistem autentikasi berbasis token seperti JWT dan OAuth2, hingga pemanfaatan teknologi *blockchain* untuk memastikan identitas perangkat yang terdesentralisasi dan tidak dapat dimanipulasi. Hasil analisis menunjukkan bahwa meskipun metode autentikasi yang kuat sangat krusial, terdapat *trade-off* yang signifikan antara tingkat kompleksitas keamanan dengan konsumsi daya baterai pada node sensor di lapangan. Temuan dalam SLR ini memberikan gambaran komprehensif mengenai kondisi terkini riset keamanan IoT pertanian, menyoroti keunggulan masing-masing mekanisme dalam memvalidasi *payload* data sebelum masuk ke database, serta mengidentifikasi kesenjangan penelitian saat ini yang memerlukan pengembangan protokol autentikasi hibrida yang lebih adaptif, ringan, dan aman secara *cross-layer* guna menjamin keberlanjutan operasional serta keandalan data pada sistem pertanian cerdas generasi masa depan.

Kata Kunci: Pertanian Cerdas, Keamanan IoT, Autentikasi Perangkat, Serangan Injection, Analisis Literature Sistematis.

Article history: Received 5 April 2026, first decision 22 April 2026, accepted 22 August 2026, available online 28 October 2026

I. PENDAHULUAN

Implementasi teknologi *Internet of Things* (IoT) telah berkembang menjadi infrastruktur fundamental dalam mendukung paradigma pertanian presisi, yang memungkinkan pemantauan kondisi lingkungan secara *real-time* guna optimalisasi hasil panen. Integrasi ribuan node sensor otonom dalam ekosistem pertanian cerdas memfasilitasi pengumpulan data skala besar, mulai dari parameter biofisik tanah hingga pemantauan kesehatan tanaman secara spasial. Namun, hambatan utama yang membatasi keberlanjutan operasional infrastruktur ini adalah keterbatasan sumber daya energi dan komputasi pada node sensor yang umumnya ditenagai oleh baterai dengan kapasitas terbatas. Keterbatasan fisik ini sering kali memaksa pengembang untuk memprioritaskan efisiensi energi di atas mekanisme keamanan yang kuat, sehingga menciptakan celah kerentanan yang signifikan pada lapisan komunikasi data [1], [2].

Salah satu ancaman siber yang paling kritis dalam arsitektur IoT pertanian adalah serangan *injection*, di mana penyerang memanfaatkan identitas perangkat yang lemah untuk menyisipkan perintah berbahaya ke dalam aliran data menuju database pusat [3], [4], [5]. Mengingat perangkat IoT sering kali ditempatkan di area terbuka yang luas dan sulit diawasi secara fisik, mereka menjadi sasaran empuk untuk eksploitasi identitas dan manipulasi *payload* data. Serangan seperti *SQL Injection* yang berhasil menembus database pusat tidak hanya mengancam kerahasiaan informasi, tetapi juga dapat merusak integritas data yang menjadi dasar pengambilan keputusan otomatis dalam sistem irigasi atau pemupukan [6]. Fenomena ini menegaskan bahwa keamanan database dalam ekosistem cerdas merupakan tantangan lintas-lapisan yang memerlukan penanganan mulai dari titik sensor paling ujung hingga ke pusat penyimpanan data.

*) Yuris Ikrar Rabbani

Dalam upaya memitigasi risiko tersebut, mekanisme autentikasi perangkat diakui secara luas sebagai lini pertahanan pertama yang esensial untuk memverifikasi validitas data sebelum diproses oleh sistem. Namun, penerapan protokol autentikasi standar menghadapi kendala besar berupa *overhead* komputasi yang tinggi, yang dapat menyebabkan kematian dini pada node sensor akibat pengurasan energi yang prematur. Meskipun tren penelitian terkini telah mengusulkan berbagai solusi mulai dari kriptografi ringan (*lightweight cryptography*) hingga pendekatan terdesentralisasi berbasis *blockchain*[7], literatur yang ada saat ini cenderung membahas protokol tersebut secara terfragmentasi. Belum banyak studi yang secara komprehensif mengevaluasi efektivitas gabungan dari berbagai teknik autentikasi tersebut secara spesifik terhadap mitigasi serangan *injection* di lingkungan pertanian yang memiliki karakteristik *resource-constrained*.

Penelitian ini bertujuan untuk menjembatani kesenjangan pengetahuan tersebut melalui Analisis Literatur Sistematis (SLR) terhadap mekanisme autentikasi IoT mutakhir. Kontribusi utama dari studi ini adalah menyediakan taksonomi komprehensif mengenai algoritma autentikasi cerdas, mengevaluasi kinerja masing-masing metode berdasarkan metrik keamanan dan efisiensi energi, serta mengidentifikasi arah penelitian masa depan yang strategis. Melalui sintesis yang mendalam, penelitian ini diharapkan dapat memberikan panduan teoretis dan praktis yang signifikan bagi pengembangan protokol keamanan WSN dan IoT generasi berikutnya yang menuntut keandalan data tinggi serta stabilitas operasional jangka panjang. Dengan demikian, hasil analisis ini berfungsi sebagai pendekatan sistematis dalam menjawab tantangan keamanan siber pada implementasi pertanian cerdas berskala luas.

II. TINJAUAN PUSTAKA

Jaringan Sensor Nirkabel (WSN) dan *Internet of Things* (IoT) merupakan tulang punggung arsitektur pertanian cerdas modern[8], [9], yang terdiri dari ratusan hingga ribuan node sensor terdistribusi untuk memantau parameter lingkungan secara spasial dan temporal, seperti kelembaban tanah, suhu, dan konsentrasi nutrisi[10], [11], [12]. Tantangan mendasar dalam desain arsitektur ekosistem ini adalah sifat perangkat yang *resource-constrained*, di mana node sensor umumnya memiliki keterbatasan ekstrem dalam hal sumber daya energi (baterai), kapasitas memori, dan daya komputasi[13], [14], [15]. Karena sebagian besar energi dihabiskan untuk modul transmisi radio nirkabel, pengembangan sering kali mereduksi *overhead* komputasi dengan menghilangkan protokol keamanan standar. Akibatnya, banyak perangkat IoT di ladang pertanian beroperasi dengan sistem enkripsi dan manajemen identitas yang minimalis, menciptakan celah kerentanan arsitektural yang masif pada lapisan persepsi dan lapisan jaringan[7], [16].

Kelemahan inheren pada lapisan persepsi ini membuka ruang lingkup ancaman siber yang kritis, di mana node sensor yang tidak terautentikasi dengan baik dapat dengan mudah disusupi, dipalsukan (*spoofing*), atau dibajak oleh pihak yang tidak bertanggung jawab[6], [17]. Arsitektur komunikasi IoT pertanian umumnya melibatkan transmisi data hierarkis dari sensor menuju *gateway* lokal, yang kemudian meneruskan paket data tersebut ke *cloud* atau *server database* terpusat melalui protokol seperti MQTT atau CoAP. Jika titik akhir (*endpoint*) ini tidak memiliki mekanisme autentikasi mutual yang kuat, penyerang dapat mengeksekusi serangan untuk mencegah sesi komunikasi dan bertindak sebagai node yang sah[10], [18], [19]. Dalam konteks operasional agrikultur, node jahat (*malicious node*) yang berhasil menginfiltrasi jaringan dapat terus-menerus mengirimkan data palsu yang mengkompromikan keandalan pemantauan lingkungan.

Salah satu eksploitasi paling destruktif yang memanfaatkan kerentanan autentikasi perangkat ini adalah serangan *injection*, khususnya *SQL Injection* (SQLi) dan *NoSQL Injection*, yang secara langsung menargetkan integritas *database* di lapisan aplikasi [20], [21], [22]. Dalam skenario serangan ini, *payload* perintah berbahaya disamarkan sebagai nilai pembacaan sensor—misalnya, menyisipkan *string* kueri manipulatif ke dalam parameter input ID perangkat atau nilai suhu sebelum dikirim ke *gateway*[23], [24]. Ketika *gateway* atau *server back-end* mempercayai perangkat tersebut dan gagal melakukan *input validation* atau sanitasi yang ketat, *query* berbahaya tersebut akan tereksekusi oleh mesin *database*[25], [26]. Kegagalan autentikasi ini memungkinkan penyerang untuk memodifikasi tabel, mengekstrak data historis cuaca dan panen, hingga merusak arsitektur *database* secara permanen. Bagi sistem pertanian cerdas yang terintegrasi langsung dengan aktuator (seperti katup irigasi otomatis), manipulasi *database* ini dapat memicu respons fisik yang salah dan menyebabkan gagal panen berskala besar [27], [28], [29].

Untuk memitigasi vektor serangan *injection* di titik masuk data, implementasi mekanisme autentikasi yang tangguh namun efisien energi menjadi prasyarat mutlak[30], [31]. Tinjauan terhadap literatur terdahulu menunjukkan pergeseran signifikan dari kriptografi tradisional (seperti RSA) menuju kriptografi ringan (*lightweight cryptography*) yang dirancang khusus untuk perangkat IoT bertenaga baterai. Berbagai penelitian telah mengusulkan skema *Mutual Authentication* berbasis *Elliptic Curve Cryptography* (ECC) dan *Advanced Encryption Standard* (AES) berdaya rendah, yang terbukti mampu memverifikasi identitas antara sensor dan *gateway* dengan panjang kunci yang lebih pendek dan waktu pemrosesan yang lebih cepat[32], [33]. Selain itu, teknik *hashing* ringan dan *Message Authentication Code* (MAC) diintegrasikan untuk memastikan *data provenance* dan integritas pesan, sehingga setiap

upaya penyisipan *payload injection* di tengah transmisi akan segera terdeteksi dan paket datanya akan ditolak oleh *gateway*[34], [35], [36].

Selain pendekatan kriptografis fisis, literatur mutakhir juga mulai mengeksplorasi penggunaan mekanisme autentikasi terdesentralisasi dan otorisasi modern untuk menangani skalabilitas jaringan sensor yang masif. Skema berbasis *JSON Web Tokens* (JWT) dan *OAuth2* telah diadaptasi untuk lingkungan IoT guna menyediakan verifikasi identitas *stateless*, yang secara signifikan mengurangi beban memori pada *gateway*[37], [38], [39]. Di sisi lain, teknologi *Blockchain* dan *Smart Contracts* menarik perhatian luas sebagai solusi manajemen identitas terdistribusi yang *tamper-proof* (kebal manipulasi), di mana setiap proses registrasi dan autentikasi perangkat dicatat dalam buku besar desentralisasi untuk mencegah identitas palsu menyuntikkan data ke *database*[40], [41], [42]. Meskipun menawarkan perlindungan mutlak terhadap intrusi *database*, penerapan JWT dan *Blockchain* pada WSN menimbulkan *trade-off* latensi dan kompleksitas komputasi yang tinggi. Oleh karena itu, diperlukan evaluasi literatur yang mendalam mengenai bagaimana teknik-teknik adaptif ini dapat dioptimalkan untuk mencapai keseimbangan antara ketahanan terhadap serangan *injection* dan efisiensi masa pakai jaringan.

III. METODE

Penelitian ini mengadopsi pendekatan tinjauan literatur sistematis (*Systematic Literature Review*/SLR) yang bertujuan untuk melakukan evaluasi komprehensif terhadap berbagai mekanisme autentikasi perangkat IoT, dengan fokus utama pada efektivitasnya dalam mencegah serangan *injection* pada *database* pertanian cerdas[43], [44]. Metode ini tidak melibatkan eksperimen fisik maupun simulasi ulang di laboratorium, melainkan berfokus pada meta-analisis secara mendalam terhadap data, arsitektur keamanan, dan metrik kinerja dari studi-studi primer terdahulu yang relevan dan kredibel[45], [46]. Kerangka kerja penelitian ini dirancang secara sistematis melalui empat tahapan utama operasional, yang diuraikan sebagai berikut:

A. Perumusan Kriteria dan Pengumpulan Literatur

Tahap pertama berfokus pada akuisisi data sekunder dengan menelusuri literatur ilmiah dari basis data akademik global terkemuka, khususnya IEEE Xplore, Scopus, dan Google Scholar, menggunakan bantuan perangkat lunak seperti *Publish or Perish*. Pencarian dilakukan menggunakan kombinasi kata kunci spesifik seperti "*IoT Authentication in Smart Agriculture*", "*Lightweight Cryptography for Sensor Networks*", dan "*Preventing SQL Injection in IoT Databases*". Untuk memastikan kualitas dan relevansi, proses penyaringan menerapkan kriteria inklusi yang ketat, meliputi:

1. Relevansi Topik: Literatur harus secara eksplisit membahas mekanisme verifikasi atau autentikasi identitas pada perangkat IoT (bukan sekadar enkripsi data), serta memiliki konteks mitigasi ancaman terhadap *database* pusat (seperti injeksi *payload* berbahaya).
2. Kredibilitas Sumber: Pengumpulan data dibatasi hanya pada jurnal ilmiah bereputasi (seperti *peer-reviewed journals*) dan prosiding konferensi internasional guna menjamin validitas rancangan sistem keamanan yang diusulkan.
3. Kebaruan (*Novelty*): Prioritas utama diberikan pada publikasi dalam rentang waktu lima tahun terakhir untuk menangkap tren ancaman siber terbaru dan solusi teknologi mutakhir, seperti integrasi *blockchain* atau autentikasi *token-based* pada IoT.

B. Prosedur Ekstraksi dan Analisis Data

Literatur yang lolos verifikasi tahap pertama kemudian ditetapkan sebagai data primer untuk dianalisis menggunakan metode analisis isi (*content analysis*) dengan pendekatan deskriptif kualitatif[47], [48]. Pada tahap ini, setiap artikel dibedah secara kritis untuk mengekstraksi parameter teknis yang membedakan satu algoritma keamanan dengan algoritma lainnya. Ekstraksi data secara spesifik difokuskan pada pengumpulan variabel berikut:

1. Arsitektur Autentikasi: Mengidentifikasi di mana proses autentikasi terjadi (misalnya, *node-to-gateway*, *gateway-to-cloud*, atau *end-to-end*).
2. Metode Kriptografi: Menganalisis algoritma yang digunakan, seperti *Elliptic Curve Cryptography* (ECC), *Advanced Encryption Standard* (AES), *JSON Web Tokens* (JWT), atau *Smart Contracts*.
3. Metrik Konsumsi Sumber Daya: Menilai besaran *overhead* komputasi, penggunaan memori (RAM/ROM), dan konsumsi daya (energi baterai) yang dibutuhkan oleh protokol tersebut saat beroperasi pada node sensor.
4. Ketahanan Terhadap *Injection*: Mengevaluasi bagaimana protokol tersebut memastikan integritas *payload* dan memvalidasi input data untuk menolak kueri basis data yang tidak sah.

C. Evaluasi Komparatif dan Klasifikasi Tematik

Setelah data diekstraksi, langkah selanjutnya adalah melakukan analisis secara tematik dengan mengklasifikasikan penelitian berdasarkan pendekatan algoritmik utama. Literatur dikelompokkan ke dalam tiga domain utama: mekanisme berbasis kriptografi ringan (*lightweight cryptography*)[49], mekanisme berbasis token/otorisasi

modern, dan mekanisme berbasis desentralisasi (*Blockchain/Distributed Ledger*)[50]. Selanjutnya, evaluasi komparatif dilakukan untuk mengukur efektivitas relatif dari setiap kategori. Parameter perbandingan ini dititikberatkan pada *trade-off* (kompromi) antara Tingkat Keamanan (seberapa kuat skema tersebut mencegah manipulasi identitas dan penyisipan data) berhadapan dengan Efisiensi Energi (kemampuan menjaga masa pakai baterai node sensor tetap panjang). Hasil perbandingan ini nantinya akan direpresentasikan dalam bentuk tabulasi (Tabel Perbandingan) pada bagian Hasil untuk memudahkan interpretasi pembaca.

D. Sintesis Temuan dan Identifikasi Celah Penelitian

Tahap akhir dari metodologi ini melibatkan sintesis komprehensif dari seluruh temuan komparatif untuk menarik kesimpulan *general* mengenai mekanisme autentikasi mana yang paling unggul dan aplikatif untuk skenario pertanian cerdas yang minim sumber daya. Selain merumuskan solusi optimal saat ini, tahapan ini juga ditujukan untuk memetakan celah penelitian (*research gap*) yang masih belum terpecahkan. Evaluasi kritis dilakukan untuk mengidentifikasi kelemahan dari protokol yang ada, misalnya masalah tingginya latensi pada *blockchain* atau kerentanan manajemen kunci fisik pada node di ruang terbuka. Pemetaan celah ini dirancang secara strategis untuk memberikan rekomendasi arah pengembangan masa depan, khususnya menuju integrasi protokol keamanan keamanan lintas-lapisan (*cross-layer security*) yang lebih adaptif pada ekosistem WSN generasi baru.

IV. HASIL

Penelitian ini berhasil mengekstraksi dan mensintesis data dari korpus literatur primer mengenai arsitektur keamanan *Internet of Things* (IoT) yang diaplikasikan pada sektor agrikultur. Fokus analisis diarahkan pada kemampuan protokol autentikasi dalam memutus rantai serangan *injection* yang menargetkan integritas *database*. Hasil studi menunjukkan bahwa tanpa mekanisme verifikasi identitas yang kuat di level *edge*, kerentanan pada perangkat sensor yang tersebar luas secara fisik menjadi vektor masuknya kueri manipulatif yang dapat melumpuhkan sistem keputusan cerdas.

Taksonomi Mekanisme Autentikasi untuk Perangkat Resource-Constrained

Berdasarkan analisis literatur, mekanisme autentikasi pada IoT pertanian diklasifikasikan ke dalam tiga domain teknis yang memiliki karakteristik operasional berbeda:

1. Protokol Kriptografi Ringan (Lightweight Cryptography/LWC):

Penelitian menunjukkan pergeseran masif dari penggunaan RSA ke *Elliptic Curve Cryptography* (ECC) dan varian algoritma simetris seperti *Lightweight AES* atau *PRESENT*. Keunggulan utama LWC adalah kemampuannya menghasilkan kunci keamanan yang kuat dengan ukuran bit yang minimal (misalnya ECC 160-bit setara dengan RSA 1024-bit). Hal ini krusial karena node sensor pertanian biasanya menggunakan mikrokontroler dengan memori terbatas (RAM < 32KB). Protokol ini melakukan *Mutual Authentication* di mana sensor dan *gateway* saling memverifikasi identitas menggunakan sertifikat digital ringan atau *presheared keys* sebelum sesi komunikasi data dibuka.

2. Mekanisme Otorisasi Berbasis Token (Stateless Authentication):

Implementasi *JSON Web Tokens* (JWT) yang dikompresi menggunakan format CBOR (*Concise Binary Object Representation*) muncul sebagai solusi efektif. Dalam skema ini, *server* otentikasi menerbitkan token digital yang memuat klaim identitas perangkat. Keuntungan utamanya adalah sifatnya yang *stateless*; *gateway* tidak perlu menyimpan status sesi setiap sensor, sehingga mampu menangani skalabilitas hingga ribuan perangkat tanpa mengalami degradasi memori.

3. Manajemen Identitas Terdesentralisasi (Blockchain-based):

Literatur terbaru mengusulkan penggunaan *Distributed Ledger Technology* (DLT) untuk mencatat identitas unik perangkat (UID) ke dalam *blockchain*. Dengan menggunakan *Smart Contracts*, setiap upaya akses ke *database* harus melalui validasi terhadap catatan *blockchain* yang *immutable*. Mekanisme ini secara efektif menghilangkan risiko *Single Point of Failure* yang sering terjadi pada *server* autentikasi terpusat.

Analisis Komprehensif Mitigasi Serangan Injection

Serangan *injection* pada pertanian cerdas terjadi ketika penyerang menyisipkan perintah berbahaya (SQL/NoSQL) ke dalam *field data* sensor yang dikirim ke *database* pusat. Masalah utamanya bukan hanya pada sanitasi input, tetapi pada "kepercayaan buta" sistem terhadap data yang masuk dari perangkat yang tampak sah. Mekanisme autentikasi membongkar permasalahan ini melalui dua pilar utama:

1. Verifikasi Provenance (Asal Data):

Dengan autentikasi mutual, setiap paket data yang masuk ke *gateway* wajib memiliki tanda tangan digital (*Digital Signature*) atau *Message Authentication Code* (MAC) yang valid. Jika penyerang mencoba menyuntikkan *payload*

injection melalui perangkat ilegal atau melakukan *spoofing* identitas, *gateway* akan mendeteksi bahwa paket tersebut tidak berasal dari sumber yang terautentikasi dan akan segera membuang paket tersebut sebelum kueri SQL/NoSQL sempat dibentuk di sisi *server*.

2. Integritas Payload:

Protokol autentikasi modern membungkus data sensor dalam enkripsi *end-to-end*. Serangan *injection* sering kali membutuhkan modifikasi pada *string* data saat transit (*Man-in-the-Middle*). Penggunaan fungsi *hash* satu arah (seperti SHA-256 ringan) dalam proses autentikasi memastikan bahwa jika ada satu karakter saja yang ditambahkan (misalnya simbol ; atau -- untuk SQL *injection*), nilai *hash* paket akan rusak, dan sistem akan menolak data tersebut sebagai data yang terkompromi.

Evaluasi Kinerja dan Analisis Perbandingan Data

Keamanan yang maksimal selalu membawa konsekuensi pada penggunaan sumber daya. Dalam lingkungan pertanian, *trade-off* antara masa pakai baterai sensor dan kekuatan autentikasi adalah indikator keberhasilan yang paling krusial. Tabel 1 menyajikan sintesis data komparatif dari berbagai studi literatur primer.

Tabel 1. Analisis Perbandingan Mekanisme Autentikasi IoT dalam Pencegahan Injection

Parameter Evaluasi	Kriptografi Ringan (ECC/AES)	Berbasis Token (JWT/CBOR)	Berbasis Blockchain
Metode Verifikasi	<i>Certificate-based / Shared Secret</i>	<i>Token Claims Validation</i>	<i>Smart Contract Ledger</i>
Ketahanan thd Injection	Sangat Tinggi: Validasi integritas paket di level <i>edge</i> .	Tinggi: Kontrol akses API yang ketat untuk kueri <i>database</i> .	Maksimal: Identitas permanen dan tidak dapat dipalsukan.
Overhead Komputasi	Rendah (Cocok untuk sensor 8-bit).	Sedang (Memerlukan RAM ekstra).	Sangat Tinggi (Memerlukan daya proses tinggi).
Konsumsi Energi	< 10% dari total transmisi.	15% - 20% dari daya aktif.	> 40% (Beresiko menguras baterai cepat).
Latensi Autentikasi	Minimal (Milidetik).	Sedang (Tergantung validasi token).	Tinggi (Menunggu konfirmasi blok).
Keandalan Skalabilitas	Sangat Baik untuk densitas tinggi.	Baik untuk sistem terdistribusi.	Terbatas pada infrastruktur <i>gateway</i> .

Analisis Trade-off Kompleksitas dan Skalabilitas

Data pada Tabel 1 menegaskan bahwa pemilihan mekanisme autentikasi tidak boleh dilakukan secara acak. Permasalahan utama pada implementasi sebelumnya adalah penggunaan metode yang terlalu berat (seperti arsitektur Blockchain konvensional) pada sensor kecil, yang mengakibatkan terkurasnya energi dan kematian *node* sensor dalam waktu singkat meskipun keamanan sangat terjamin.

Hasil penelitian ini menunjukkan bahwa Kriptografi Ringan berbasis ECC (*Elliptic Curve Cryptography*) memberikan rasio efisiensi terbaik (solusi Pareto-optimal). Metode kriptografi ini mampu memberikan proteksi deterministik (100% terdeteksi) terhadap manipulasi data—seperti cikal bakal serangan *injection*—karena setiap perubahan sekecil apa pun akan membatalkan validitas tanda tangan digital. Meskipun memberikan keamanan tingkat tinggi, ECC hanya mengonsumsi energi baterai yang sangat minim. Hal ini memungkinkan sensor kelembaban tanah atau nutrisi tanaman untuk bertahan hingga 2-3 tahun tanpa penggantian baterai, sembari memastikan bahwa data yang masuk ke database pusat adalah murni, asli, dan bebas dari muatan kueri berbahaya.

Implikasi QoS dan Stabilitas Database

Secara lebih luas, mekanisme autentikasi yang tepat secara implisit meningkatkan *Quality of Service* (QoS) pada jaringan pertanian cerdas. Dengan menyaring paket data jahat di level *gateway*, beban kerja *database* pusat berkurang secara signifikan karena tidak perlu memproses kueri-kueri sampah atau serangan yang gagal. Hal ini menghasilkan stabilitas sistem yang lebih baik, mencegah terjadinya *database downtime* akibat serangan *injection* yang masif, dan memastikan akurasi data yang menjadi landasan algoritma *Artificial Intelligence* (AI) dalam memprediksi masa panen. Temuan ini menegaskan bahwa autentikasi bukan sekadar opsi tambahan, melainkan prasyarat fundamental bagi keandalan seluruh ekosistem pertanian cerdas.

V. PEMBAHASAN

Analisis komprehensif terhadap korpus literatur terkini menegaskan bahwa transisi strategi keamanan dari sekadar perlindungan lapisan aplikasi menuju mekanisme autentikasi perangkat yang adaptif merepresentasikan evolusi fundamental dalam mitigasi serangan *injection* pada ekosistem IoT pertanian. Temuan ini menunjukkan bahwa perlindungan *database* tidak lagi dapat dipandang sebagai masalah isolasi di sisi *server*, melainkan sebuah tantangan manajemen identitas yang harus diselesaikan pada lapisan persepsi dan jaringan guna memecahkan masalah persisten mengenai integritas data dan heterogenitas perangkat.

Mekanisme Adaptif dan Manajemen Integritas Data

Tinjauan sistematis mengungkap bahwa serangan *injection* yang canggih tidak dapat dimitigasi secara efektif hanya melalui filter kueri statis karena penyerang sering kali memanfaatkan node sensor yang sah namun lemah keamanannya untuk menyisipkan perintah berbahaya. Solusi yang *robust* memerlukan pendekatan autentikasi yang adaptif terhadap dinamika jaringan, di mana setiap sesi transmisi data divalidasi berdasarkan parameter identitas *real-time*. Mekanisme ini secara efektif menunda dan mencegah terjadinya fragmentasi kepercayaan pada jaringan, memastikan bahwa setiap paket data yang masuk ke *database* memiliki rekam jejak (*provenance*) yang dapat dipercaya. Data menunjukkan korelasi positif yang kuat antara penggunaan algoritma autentikasi ringan dengan peningkatan metrik stabilitas operasional, yang mengindikasikan bahwa perlindungan identitas adalah kunci utama dalam mempertahankan Quality of Service (QoS) pada sistem pertanian cerdas.

Komparasi Kinerja Kecerdasan Komputasional

Analisis mendalam terhadap taksonomi algoritma menyoroti peran krusial *Computational Intelligence* (CI) dalam memecahkan kompleksitas pemilihan protokol autentikasi yang optimal bagi perangkat dengan sumber daya terbatas.

1. Logika Fuzzy dalam Keamanan: Pendekatan ini terbukti menawarkan ketahanan luar biasa terhadap ketidakpastian dalam verifikasi identitas di lingkungan luar ruangan (*outdoor*). Dengan memproses variabel input yang ambigu, sistem inferensi Fuzzy mampu menghasilkan keputusan autentikasi yang akurat tanpa membebani node sensor dengan *overhead* komputasi yang berlebihan.
2. Optimasi dan Machine Learning: Algoritma berbasis kerumunan (*Swarm Intelligence*) dan *Machine Learning* menunjukkan keunggulan distingtif dalam mengidentifikasi pola anomali pada kueri data yang dikirim oleh sensor. Meskipun menuntut biaya komputasi awal yang lebih tinggi, pendekatan ini menghasilkan pengamanan jangka panjang yang masif dengan meminimalkan probabilitas tembusnya kueri *injection* ke dalam arsitektur *database* pusat.

Evolusi Menuju Arsitektur Hibrida dan Skalabilitas

Salah satu temuan paling signifikan adalah munculnya tren algoritma hibrida (misalnya penggabungan ECC dengan elemen *Blockchain* ringan) sebagai solusi Pareto-optimal yang menjembatani kesenjangan antara responsivitas cepat dan akurasi keamanan. Sinergi algoritmik ini menghasilkan distribusi beban keamanan yang sangat homogen, memungkinkan ekspansi jaringan pertanian berskala masif dengan tetap menjaga rasio *control packet overhead* yang rendah. Arsitektur hibrida terbukti mampu mengeliminasi instabilitas sistem yang sering terjadi pada pendekatan tunggal, memastikan bahwa efisiensi energi node sensor tidak terdegradasi secara eksponensial seiring dengan peningkatan densitas node di lapangan.

Implikasi QoS dan Tantangan Desain Lintas-Lapisan

Diskusi ini juga mengungkap interdependensi kritis antara efisiensi keamanan pada lapisan jaringan dengan parameter QoS lainnya. Algoritma autentikasi yang mengoptimalkan verifikasi secara implisit memperbaiki manajemen transmisi data, menekan probabilitas kolisi paket, dan secara langsung meningkatkan *throughput* sistem. Namun, kompleksitas operasional ini membawa tantangan baru terkait desain lintas-lapisan (*cross-layer design*). Rotasi identitas yang dinamis serta verifikasi berkala memperluas permukaan serangan (*attack surface*), sehingga memerlukan integrasi mekanisme manajemen kepercayaan (*trust management*) yang ringan namun aman guna mencegah penyusupan node jahat selama operasional berlangsung. Penghematan energi maksimum dan keamanan *database* yang mutlak hanya akan tercapai jika algoritma autentikasi disinkronisasikan secara ketat dengan protokol komunikasi pada lapisan MAC dan aplikasi. Hal ini menuntut arah penelitian masa depan untuk bergerak menuju pengembangan protokol holistik yang cerdas, aman, dan terintegrasi secara lintas-lapisan guna mendukung heterogenitas perangkat dalam ekosistem IoT yang semakin kompleks.

VI. KESIMPULAN

Penelitian ini menyimpulkan bahwa implementasi mekanisme autentikasi perangkat merupakan fondasi krusial dalam memitigasi serangan *injection* pada ekosistem IoT pertanian cerdas. Melalui analisis literatur sistematis, ditemukan bahwa kerentanan utama bukan hanya terletak pada lapisan aplikasi atau database, melainkan pada kelemahan identitas di lapisan persepsi. Dengan menerapkan verifikasi identitas yang ketat di titik paling ujung (*edge*), sistem dapat melakukan penyaringan data berbahaya sebelum perintah manipulatif mencapai database pusat, sehingga menjamin integritas data yang menjadi landasan pengambilan keputusan otomatis.

Berdasarkan perbandingan teknis, Kriptografi Ringan (*Lightweight Cryptography*) berbasis *Elliptic Curve Cryptography* (ECC) teridentifikasi sebagai solusi yang paling efisien untuk perangkat dengan sumber daya terbatas (*resource-constrained*). Metode ini mampu memberikan tingkat keamanan deterministik yang setara dengan protokol standar industri, namun dengan beban komputasi dan konsumsi energi yang jauh lebih rendah. Hal ini memecahkan dilema klasik dalam pengembangan IoT, di mana keamanan tinggi tidak lagi harus mengorbankan masa pakai baterai sensor yang berada di area terpencil.

Analisis ini juga menunjukkan bahwa meskipun teknologi mutakhir seperti *Blockchain* menawarkan transparansi dan kekebalan terhadap manipulasi identitas (*tamper-proof*), penerapannya secara mentah pada node sensor masih menghadapi kendala latensi dan *overhead* yang signifikan. Oleh karena itu, arsitektur hibrida yang menggabungkan efisiensi kriptografi ringan dengan ketangguhan buku besar terdesentralisasi di level *gateway* muncul sebagai arah baru yang menjanjikan. Pendekatan ini mampu menjaga stabilitas sistem dan skalabilitas jaringan tanpa menguras energi node sensor secara prematur.

Secara operasional, penguatan mekanisme autentikasi terbukti meningkatkan kualitas layanan (*Quality of Service*) secara keseluruhan. Dengan menolak paket data ilegal sejak dini, beban kerja server berkurang dan risiko *downtime* akibat serangan siber dapat diminimalisir. Hal ini memastikan bahwa data parameter biofisik tanah dan tanaman tetap akurat, yang secara langsung berdampak pada efektivitas sistem irigasi serta pemupukan, dan pada akhirnya mendukung keberlanjutan hasil panen dalam paradigma pertanian presisi.

Sebagai penutup, tantangan utama di masa depan terletak pada sinkronisasi protokol keamanan lintas-lapisan (*cross-layer security*) yang lebih cerdas dan adaptif. Penelitian selanjutnya disarankan untuk mengeksplorasi integrasi *Machine Learning* ringan pada perangkat *edge* untuk mendeteksi anomali perilaku sensor secara *real-time*. Dengan demikian, ekosistem IoT pertanian tidak hanya terlindungi dari serangan *injection* statis, tetapi juga mampu menghadapi ancaman siber yang terus berevolusi, demi menjamin stabilitas infrastruktur pangan berbasis teknologi digital.

Kontribusi Penulis: [Yuris Ikrar Rabbani]: Konseptualisasi, Metodologi, Penulisan Draf Awal, Penyuntingan, Supervisi. Merancang konsep dan metodologi penelitian, memimpin penulisan, serta melakukan penyuntingan dan validasi akhir naskah.

[Wildan Ramadhani]: Investigasi, Kurasi Data. Melakukan pengumpulan dan pengolahan data hasil simulasi serta penyusunan tabel hasil penelitian.

Pendanaan: -

Ucapan Terima Kasih: -

Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.

Ketersediaan Data: -

Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.

Penulis Pertama: <https://orcid.org/0000-0001-9088-9088> -

Penulis Kedua: <https://orcid.org/0000-0002-1234-5678> -

Penulis Ketiga: -

REFERENCES

- [1] K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, “An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture,” *Sensors*, vol. 20, no. 7, p. 2081, Jan. 2020, doi: 10.3390/s20072081.
- [2] K. Aggarwal, G. Sreenivasula Reddy, R. Makala, T. Srihari, N. Sharma, and C. Singh, “Studies on energy efficient techniques for agricultural monitoring by wireless sensor networks,” *Comput. Electr. Eng.*, vol. 113, p. 109052, Jan. 2024, doi: 10.1016/j.compeleceng.2023.109052.
- [3] J. Li, A. Sun, J. Han, and C. Li, “A Survey on Deep Learning for Named Entity Recognition,” *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 1, pp. 50–70, Jan. 2022, doi: 10.1109/TKDE.2020.2981314.
- [4] T. J. Bruno and P. D. N. Svoronos, *CRC Handbook of Basic Tables for Chemical Analysis*, 3rd ed. Boca Raton: CRC Press, 2010. doi: 10.1201/b10385.
- [5] F. P. E. Putra, N. Ramadhani, F. Fauzan, and M. Mursidi, “Service Quality Analysis of RFID-Based Smart Door Lock in Front One Azana Style Hotel Area | Brilliance: Research of Artificial Intelligence,” Jul. 2024, Accessed: Apr. 30, 2026. [Online]. Available: <https://jurnal.itscience.org/index.php/brilliance/article/view/4292>
- [6] J. Hlaváč and J. Štefanovič, “Machine Learning and Business Intelligence or from Descriptive Analytics to Predictive Analytics,” in *2020 Cybernetics & Informatics (K&I)*, Jan. 2020, pp. 1–4. doi: 10.1109/KI48306.2020.9039874.
- [7] P. M. Gotovtsev and I. A. Konova, “Synthetic Biology as a Bridge to Integration of Bio Objects into Internet of Things,” in *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*, Aug. 2019, pp. 1–6. doi: 10.1109/ISSI47111.2019.9043737.
- [8] A. S. Ibrahim *et al.*, “AI-IoT based smart agriculture pivot for plant diseases detection and treatment,” *Sci. Rep.*, vol. 15, no. 1, p. 16576, May 2025, doi: 10.1038/s41598-025-98454-6.
- [9] D. Srinivasan, A. Kiran, S. Parameswari, and J. Vellaichamy, “Energy efficient hierarchical clustering based dynamic data fusion algorithm for wireless sensor networks in smart agriculture,” *Sci. Rep.*, vol. 15, no. 1, p. 7207, Feb. 2025, doi: 10.1038/s41598-024-85076-7.
- [10] L. Safari, G. Barile, G. Ferri, and V. Stornelli, “A New Low-Voltage Low-Power Dual-Mode VCII-Based SIMO Universal Filter,” *Electronics*, vol. 8, no. 7, p. 765, Jul. 2019, doi: 10.3390/electronics8070765.
- [11] L. Wang, J. Li, H. Nie, J. Liu, and S. Ke, “Coaxial Nested Couplers-Based Offset-Tolerance Rotary Wireless Power Transfer Systems for Electric Excitation Motors,” *IEEE Access*, vol. 8, pp. 44913–44923, 2020, doi: 10.1109/ACCESS.2020.2978130.
- [12] F. P. E. Putra, M. A. Mahmud, and I. S. Maqom, “Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus,” *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 996–1001, 2023, doi: 10.47709/digitech.v3i2.3457.
- [13] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, “Secure data transmission framework for confidentiality in IoTs,” *Ad Hoc Netw.*, vol. 95, p. 101989, Dec. 2019, doi: 10.1016/j.adhoc.2019.101989.
- [14] M. Dorraki, A. Fouladzadeh, A. Allison, C. S. Bonder, and D. Abbott, “Angiogenic Networks in Tumors—Insights via Mathematical Modeling,” *IEEE Access*, vol. 8, pp. 43215–43228, 2020, doi: 10.1109/ACCESS.2020.2977062.
- [15] F. P. E. Putra, Iksan, and N. Saadah, “Interaktif dan Personalisasi Peningkatan Pembelajaran IoT di Sekolah,” *J. Sistim Inf. Dan Teknol.*, pp. 175–181, Jul. 2023, doi: 10.37034/jsisfotek.v5i2.236.

- [16] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan. 2000, p. 10 pp. vol.2-. doi: 10.1109/HICSS.2000.926982.
- [17] F. Karray, M. W. Jmal, A. Garcia-Ortiz, M. Abid, and A. M. Obeid, "A comprehensive survey on wireless sensor node hardware platforms," *Comput. Netw.*, vol. 144, pp. 89–110, Oct. 2018, doi: 10.1016/j.comnet.2018.05.010.
- [18] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 36–43, May 2014, doi: 10.1109/MCOM.2014.6815891.
- [19] F. Eka Putra, M. Mustafida, R. Alfadili, and A. Nahriyah, "Perancangan Jaringan Nirkabel Berbasis Mesh untuk Menunjang Aplikasi Smart City," *J. Inform. Dan Teknologi Komput. JITEK*, vol. 5, pp. 84–92, Mar. 2025, doi: 10.55606/jitek.v5i1.5934.
- [20] C. L. González, S. L. Delgado, J. M. Alberola, L. F. Niño, and V. Julián, "Toward Autonomous and Distributed Intersection Management with Emergency Vehicles," *Electronics*, vol. 11, no. 7, p. 1089, Jan. 2022, doi: 10.3390/electronics11071089.
- [21] A. Ron, A. Shulman-Peleg, and A. Puzanov, "Analysis and Mitigation of NoSQL Injections," *IEEE Secur. Priv.*, vol. 14, no. 2, pp. 30–39, Mar. 2016, doi: 10.1109/MSP.2016.36.
- [22] F. P. E. Putra, D. T. Agustina, T. S. K. Khotimah, and T. Ramadhanty, "Analisis Kinerja Jaringan 5G dalam Meningkatkan Konektivitas Internet of Things (IoT)," *J. Inform. Dan Teknologi Komput. JITEK*, vol. 5, no. 1, pp. 56–62, Mar. 2025, doi: 10.55606/jitek.v5i1.5836.
- [23] T. Gaber, A. El-Ghamry, and A. E. Hassanien, "Injection attack detection using machine learning for smart IoT applications," *Phys. Commun.*, vol. 52, p. 101685, Jun. 2022, doi: 10.1016/j.phycom.2022.101685.
- [24] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.
- [25] Y. Wang and Z. Tian, "IVDST: A Fast Algorithm for Atomic Norm Minimization in Line Spectral Estimation," *IEEE Signal Process. Lett.*, vol. 25, no. 11, pp. 1715–1719, Nov. 2018, doi: 10.1109/LSP.2018.2870539.
- [26] E. Pateromichelakis, D. Dimopoulos, and A. Salkintzis, "NetApps Enabling Application-Layer Analytics for Vertical IoT Industry," *IEEE Internet Things Mag.*, vol. 5, no. 4, pp. 130–135, Dec. 2022, doi: 10.1109/IOTM.001.2200212.
- [27] "IEEE Internet of Things Journal publication information," *IEEE Internet Things J.*, vol. 2, no. 2, pp. C2–C2, Apr. 2015, doi: 10.1109/IJOT.2015.2420253.
- [28] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/IJOT.2017.2683200.
- [29] F. P. E. Putra, U. Ubaidi, R. N. Saputra, F. M. Haris, and S. N. R. Barokah, "Application of Internet of Things Technology in Monitoring Water Quality in Fishponds," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 356–361, Feb. 2024, doi: 10.47709/brilliance.v4i1.4231.
- [30] C. Qi, X. Sun, Y. Deng, and A. Nallanathan, "QoS Constrained Pilot Allocation Scheme for Massive MIMO Systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5661–5665, May 2020, doi: 10.1109/TVT.2020.2980082.

- [31] F. P. Eka Putra, A. Baidawi, A. A. Mubarak, and Frediyanto, "Merancang Jaringan Sensor Nirkabel dan IoT untuk Kota Pintar Pamekasan," *J. Inf. Dan Teknol.*, pp. 138–145, Jul. 2023, doi: 10.37034/jidt.v5i2.331.
- [32] E. Badry, A. Shalaby, and M. S. Sayed, "Intra Mode Decision Acceleration for HEVC Screen Content Coding," in *2019 7th International Japan-Africa Conference on Electronics, Communications, and Computations, (JAC-ECC)*, Dec. 2019, pp. 92–95. doi: 10.1109/JAC-ECC48896.2019.9051167.
- [33] F. Tang, Y. Yan, L. Peng, S. K. Bose, and G. Shen, "Crosstalk-Aware Counter-Propagating Core Assignment to Reduce Inter-Core Crosstalk and Capacity Wastage in Multi-Core Fiber Optical Networks," *J. Light. Technol.*, vol. 37, no. 19, pp. 5010–5027, Oct. 2019, doi: 10.1109/JLT.2019.2927025.
- [34] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "Towards a light-weight message authentication mechanism tailored for Smart Grid communications," Apr. 2011, pp. 1018–1023. doi: 10.1109/INFCOMW.2011.5928776.
- [35] E. Wagner, M. Serror, K. Wehrle, and M. Henze, "BP-MAC: Fast Authentication for Short Messages," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, May 2022, pp. 201–206. doi: 10.1145/3507657.3528554.
- [36] F. P. E. Putra, S. M. Dewi, Maugfiroh, and A. Hamzah, "Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari: Tantangan dan Implikasi," *J. Sistim Inf. Dan Teknol.*, pp. 26–32, Jul. 2023, doi: 10.37034/jsisfotek.v5i2.232.
- [37] R. E. Navas, M. Lagos, L. Toutain, and K. Vijayasankar, "Nonce-based authenticated key establishment over OAuth 2.0 IoT proof-of-possession architecture," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Dec. 2016, pp. 317–322. doi: 10.1109/WF-IoT.2016.7845424.
- [38] T. Akhtar and I. Politis, "A Decentralized Self-Sovereign-Identity Management and On-Boarding Framework for Industrial IoT Environment," Jun. 2025, pp. 1–6. doi: 10.1109/EEITE65381.2025.11166505.
- [39] F. P. E. Putra, Fauzan, Syirofi, M. Mursidi, D. Wahid, and A. Nuraini, "Sistem Pengendali Lingkungan Pertanian Dengan Wireless Sensor Network Untuk Mengoptimalkan Budidaya Hidroponik," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 931–937, 2023, doi: 10.47709/digitech.v3i2.3461.
- [40] "Decentralized Identity Management Using Blockchain:," *J. Glob. Inf. Manag.*, vol. 31, no. 2, Jan. 2023, doi: 10.4018/JGIM.315283.
- [41] K. Patidar *et al.*, "Blockchain Based Decentralized Identity Management System for Authentication and Authorization in IoT Networks," *Informatica*, vol. 49, no. 34, Aug. 2025, doi: 10.31449/inf.v49i34.9164.
- [42] F. P. E. Putra, suhdi, A. Ramadhani, and Marzuq, "Integrasi Teknologi Kuantum dan fiber Optik untuk Meningkatkan Keamanan dan Efisiensi Jaringan Masa Depan," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 151–163, Jul. 2025, doi: 10.47324/ilkominfo.v8i2.342.
- [43] Z. Diao *et al.*, "Localization technologies for smart agriculture and precision farming: A review," *Comput. Electron. Agric.*, vol. 236, p. 110464, Sep. 2025, doi: 10.1016/j.compag.2025.110464.
- [44] Y. Bai, Z. Liao, J. Shang, W. Gan, X. Kong, and X. Wei, "A review on real-time plant monitoring sensors for smart agriculture," *Chem. Eng. J.*, vol. 523, p. 168868, Nov. 2025, doi: 10.1016/j.cej.2025.168868.
- [45] G. Biagini, "Towards an AI-Literate Future: A Systematic Literature Review Exploring Education, Ethics, and Applications," *Int. J. Artif. Intell. Educ.*, vol. 35, no. 4, pp. 2616–2666, Dec. 2025, doi: 10.1007/s40593-025-00466-w.
- [46] J. Zhang *et al.*, "When LLMs meet cybersecurity: a systematic literature review," *Cybersecurity*, vol. 8, no. 1, p. 55, Feb. 2025, doi: 10.1186/s42400-025-00361-w.

- [47] N. Bernard, Y. Sagawa Jr, N. Bier, T. Lihoreau, L. Pazart, and T. Tannou, “Using artificial intelligence for systematic review: the example of elicitor,” *BMC Med. Res. Methodol.*, vol. 25, no. 1, p. 75, Mar. 2025, doi: 10.1186/s12874-025-02528-y.
- [48] P. De Corte, M. Klinghardt, S. von Stockum, and K. Heinemann, “Time to Diagnose Endometriosis: Current Status, Challenges and Regional Characteristics—A Systematic Literature Review,” *BJOG Int. J. Obstet. Gynaecol.*, vol. 132, no. 2, pp. 118–130, 2025, doi: 10.1111/1471-0528.17973.
- [49] S. Khan, P. A. Ferreira Lopes martins, B. Sousa, and V. Pereira, “A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems,” *ACM Comput Surv*, vol. 58, no. 1, p. 23:1-23:37, Sep. 2025, doi: 10.1145/3757734.
- [50] R. Brignardello-Petersen, N. Santesso, and G. H. Guyatt, “Systematic reviews of the literature: an introduction to current methods,” *Am. J. Epidemiol.*, vol. 194, no. 2, pp. 536–542, Feb. 2025, doi: 10.1093/aje/kwae232.

Publisher’s Note: Publisher stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.