

Pendekatan *Self-Sovereign Identity* dan *Blockchain* pada *Smart Egg Incubator*: *Systematic Literature Review*

Denilson Aji Santoso^{*1}, Imam Riadi², Herman³

^{1,3} Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta

² Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta

E-mail: ^{*}12508048014@webmail.uad.ac.id, ² imam.riadi@uad.ac.id, ³hermankaha@uad.ac.id

Abstrak

Implementasi Internet of Things (IoT) pada Smart Egg Incubator sangat krusial untuk memastikan parameter penting dalam penetasan telur terkontrol dengan baik. Namun, arsitektur cloud terpusat rentan terhadap Single Point of Failure (SPoF) serta serangan unauthorized access dan privilege escalation yang dapat memicu kematian embrio massal. Konvergensi Self-Sovereign Identity (SSI) melalui Decentralized Identifiers (DID) dan Verifiable Credentials (VC) dengan smart contract blockchain hadir sebagai solusi otorisasi mesin-ke-mesin (machine-to-machine) dan penyedia audit trail yang tamper-proof. Systematic Literature Review (SLR) hibrida ini bertujuan memetakan lanskap ancaman, mengevaluasi mekanisme mitigasi desentralisasi, serta menyintesis metrik kinerja operasional perangkat dari integrasi teknologi SSI dan Smart Contract Blockchain pada perangkat IoT bersumber daya terbatas (resource-constrained). Berdasarkan protokol PRISMA, dilakukan analisis kritis terhadap 25 artikel primer terkurasi (2022–2026). Hasil sintesis menunjukkan arsitektur hibrida SSI-Blockchain unggul dalam mengeliminasi SPoF dan meningkatkan mitigasi kontrol akses dibandingkan sistem tradisional. Kendati demikian, terdapat trade-off operasional berupa computational overhead, peningkatan latensi, dan limitasi memori mikrokontroler. Sebagai solusinya, penelitian ini merumuskan cetak biru arsitektur kolaboratif berbantuan Edge Gateway lokal dan penyimpanan off-chain berbasis IPFS untuk menjaga efisiensi daya perangkat sekaligus melindungi keselamatan fisik aset biologis secara real-time.

Kata kunci- *Review, Blockchain, Internet of Things, Self-Sovereign Identity, Smart Incubator*

1. PENDAHULUAN

Otomatisasi peternakan modern melalui ekosistem *Internet of Things* (IoT), khususnya pada *Smart Egg Incubator*, terbukti meningkatkan efisiensi operasional dengan menjaga stabilitas suhu, kelembapan, dan pembalikan telur secara *real-time* [1]. Mengingat sensitivitas embrio unggas terhadap deviasi parameter fisik yang dapat memicu kematian massal dan kerugian ekonomi fatal, konsistensi parameter lingkungan mikro inkubasi menjadi sangat krusial [2]. Namun, masifnya adopsi teknologi ini turut membuka celah kerentanan siber pada arsitektur IoT tradisional yang mengancam keandalan operasional sistem di lapangan [3].

Pada implementasi nyata di tingkat peternakan rakyat maupun industri mikro, mayoritas unit *Smart Egg Incubator* dibangun menggunakan mikrokontroler berspesifikasi rendah (*resource-constrained*) seperti ESP32 atau ATmega yang diintegrasikan secara langsung dengan platform *cloud* publik pihak ketiga (misalnya Blynk, ThingSpeak, atau Tuya) [4], [5]. Komunikasi data di lapangan sering kali mengabaikan enkripsi end-to-end dan masih mengandalkan API key atau token plaintext yang tertanam pada firmware kontroler [6], [7]. Arsitektur terpusat ini tidak hanya menciptakan kelemahan *Single Point of Failure* (SPoF) di sisi server [4], [8] tetapi juga menyisakan node tepi tanpa perlindungan verifikasi identitas timbal balik (*mutual authentication*)

[5], [9]. Akibatnya, penyerang pada jaringan lokal maupun publik dapat mengeksploitasi celah tersebut untuk melakukan *unauthorized access*, *session hijacking*, dan *privilege escalation*, serta memanipulasi heater, kipas sirkulasi, atau motor pemutar rak [7], [10], [11]. Serangan *Distributed Denial of Service* (DDoS) pada broker komunikasi dapat melumpuhkan telemetri dan kendali perangkat [9], [12]. Ketiadaan audit trail *tamper-proof* juga melemahkan investigasi forensik atas sabotase operasional di lapangan [13], [14], [15].

Eksplorasi kontrol akses tradisional pada IoT telah memicu gelombang *Systematic Literature Review* (SLR) global serta berbagai studi eksperimental mengenai klasifikasi pola ancaman autentikasi jaringan, namun pemetaan riset terdahulu menunjukkan konvergensi teknologi desentralisasi masih dikaji secara terpisah [16], [17], [18]. Penelitian Singh et.al [19], [20], menyajikan tinjauan sistematis efektivitas arsitektur kontrol akses berbasis *blockchain* terhadap serangan siber umum IoT. Investigasi ini diperkuat oleh Umair et.al [21], melalui uji statistik *Chi-Square* untuk menganalisis hubungan kausalitas antara kerentanan IoT dengan karakteristik solusi *blockchain*. Di sisi lain, pemetaan makro mengenai adopsi IoT pada pertanian pintar dan tantangan privasinya dirangkum oleh Naseer et.al [22]. Sementara itu, aspek pasca-serangan berupa keandalan *log* untuk forensik digital dan validitas *chain of custody* dikaji mendalam oleh Akinbi et.al [23], [10], [24], [25]. Landasan taksonomi standardisasi arsitektur *Self-Sovereign Identity* (SSI) sebagai pengganti tata kelola kredensial terpusat disintesis secara komprehensif oleh Schardong et.al [26].

Studi literatur sistematis (SLR) sebelumnya telah memberikan kontribusi berarti, namun terdapat celah penelitian kritis yang belum terpenuhi karena analisisnya cenderung makro dan mengabaikan batasan *hardware* serta faktor biaya implementasi nyata di lapangan. Riset kontrol akses *blockchain* oleh Singh et al. dan Umair et al. sering mengasumsikan IoT dengan daya komputasi tingkat enterprise dan mengabaikan beban fluktuasi biaya transaksi (*gas fee*). Pemetaan forensik oleh Akinbi et al. kurang menimbang aspek preventif, sedangkan taksonomi SSI oleh Schardong et al. masih human-centered terkait entitas manusia ketimbang interaksi machine-to-machine. Tinjauan IoT agrikultur oleh Naseer et al. menyinggung privasi secara umum tanpa membahas arsitektur kontrol akses yang konkret. Ketiadaan sintesis tersebut menghasilkan kekosongan kerangka kerja keamanan bagi sistem siber-fisik pada *resource-constrained*. Kerentanan kontrol akses pada perangkat dengan memori terbatas (mikrokontroler mikro/mikro-RTOS) merupakan tantangan universal, relevan tidak hanya bagi otomatisasi peternakan mikro, tetapi juga *smart greenhouse*, *smart aquaculture*, *micro-IIoT*, hingga *cold chain monitoring*, yang semuanya menuntut keandalan lingkungan dan determinisme latensi.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan menyusun sebuah Kajian Literatur Sistematis (SLR) hibrida yang mengonvergensi teknologi SSI melalui *Decentralized Identifiers* (DID) dan *Verifiable Credentials* (VC) bersama *Smart Contract Blockchain* untuk mengamankan kontrol akses pada perangkat *resource-constrained IoT*. Dalam penelitian ini, *Smart Egg Incubator* diadopsi sebagai model studi kasus representatif (*archetype/representative benchmark*) dari sistem kendali siber-fisik berdaya rendah. Pemilihan objek ini didasarkan pada karakteristiknya yang memiliki toleransi kesalahan (*fault tolerance*) mendekati nol, di mana keterlambatan aktuasi (*actuator lag*) atau anomali termal sedikit saja dapat merusak aset biologis secara permanen. Dengan demikian, keberhasilan integrasi SSI-*Blockchain* dalam memenuhi batas ambang latensi dan efisiensi memori pada sistem ini akan menjadi bukti kelayakan (*feasibility benchmark*) yang dapat ditransfer ke berbagai arsitektur IoT tepi lainnya. Dengan mengadopsi protokol PRISMA, penelitian ini menyaring dan menganalisis secara kritis 25 artikel primer terpilih (2022–2026) untuk menjawab lima pertanyaan penelitian (*Research Questions/RQ*).

Penelitian ini dirumuskan ke dalam lima pertanyaan utama (*Research Questions*). RQ1 memetakan lanskap ancaman mengenai jenis serangan kontrol akses yang mengancam integritas operasional ekosistem *Smart Egg Incubator*. RQ2 berfokus pada mekanisme mitigasi desentralisasi untuk membedah bagaimana implementasi arsitektur integrasi SSI dan *blockchain* dalam memitigasi serangan tersebut. Selanjutnya, RQ3 mengevaluasi performa siber-fisik terkait metrik validasi dan efektivitas kinerja model SSI-*Blockchain* pada perangkat IoT. RQ4 menyusun

analisis komparatif untuk menelaah keunggulan model integrasi desentralisasi ini dibandingkan dengan arsitektur kontrol akses tradisional berbasis *cloud*. Terakhir, RQ5 mengidentifikasi tantangan teknis utama dalam menerapkan pendekatan SSI dan *blockchain* pada perangkat *Smart Egg Incubator* yang memiliki keterbatasan sumber daya (*resource-constrained*).

Penelitian ini berkontribusi signifikan pada literatur keamanan siber, khususnya integrasi *blockchain* dan IoT, melalui penyusunan taksonomi komprehensif yang memetakan lanskap ancaman kontrol akses, perancangan mekanisme mitigasi hibrida berbasis SSI (*Self-Sovereign Identity*) dan *smart contract*, serta penyintesisan metrik performa siber-fisik operasional. Lebih lanjut, penelitian ini memberikan pembuktian empiris mengenai keunggulan arsitektur desentralisasi dibandingkan dengan sistem *cloud* tradisional, sekaligus mengidentifikasi solusi atas hambatan teknis berupa keterbatasan memori dan daya pada perangkat mikrokontroler di sektor peternakan mikro.

2. METODE PENELITIAN

Kerangka kerja PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) diadopsi dalam penulisan SLR ini sebagai landasan metodologis untuk mewujudkan penemuan yang akurat dan dapat direplikasi [27], [28], [29]. Secara operasional, proses penapisan literatur dijalankan melalui empat tahapan terstruktur: sintesis strategi kata kunci, penyaringan berbasis kriteria inklusi dan eksklusi, penilaian kelayakan artikel (*Quality Assessment/QA*), serta penarikan data inti. Alur sistematis ini dikonfigurasi untuk mengurai lima Pertanyaan Penelitian (*Research Question/RQ*) mengenai konvergensi teknologi SSI (DID/VC) dan *smart contract blockchain* dalam domain pengamanan perangkat *resource-constrained IoT*.

Pencarian literatur dieksekusi melalui dua basis data internasional bereputasi tinggi yang menjadi rujukan utama dalam disiplin ilmu teknik elektro, ilmu komputer, dan keamanan siber, yaitu IEEE Xplore dan ScienceDirect (Elsevier). Pemilihan kedua basis data ini didasarkan pada tingkat kurasi *peer-reviewed* yang ketat serta cakupan komprehensif terhadap publikasi mutakhir di bidang arsitektur *distributed ledger*, *embedded systems*, dan protokol IoT. Untuk membatasi bias dan memastikan relevansi naskah yang terbit dari tahun 2022 hingga 2026.

2.1 Strategi Pencarian

Pencarian literatur menggunakan basis data internasional bereputasi di bidang teknik dan ilmu komputer, yaitu IEEE Xplore serta ScienceDirect. Untuk menyeleksi artikel sesuai ruang lingkup penelitian, sebuah kueri pencarian (*search string*) berbasis operator Boolean (AND/OR) dibangun dengan mengacu pada formulasi kerangka kerja PICO (*Population, Intervention, Comparison, Outcome*). Logika pencarian yang diterapkan mengombinasikan elemen-elemen tersebut melalui formula mendasar: (*Population*) AND (*Intervention*) AND (*Outcome*). Spesifikasi komponen PICO beserta padanan kata kunci penelusuran yang digunakan dalam studi ini dirangkum secara rinci pada Tabel 1.

Tabel 1 Strategi Pencarian Berdasarkan Kriteria PICO

Kriteria	Definisi	Kata Kunci Pencarian
P – Population (Ekosistem IoT <i>Smart Egg Incubator</i>)	Perangkat keras/mikrokontroler dengan sumber daya terbatas (<i>Resource-Constrained IoT</i>) pada sistem Penetas Telur Otomatis (<i>Smart Egg Incubator</i>) yang rentan terhadap manipulasi hak akses.	" <i>smart incubator</i> " OR " <i>egg incubator</i> " OR " <i>resource-constrained IoT</i> " OR " <i>microcontroller</i> "
I – Intervention (Integrasi <i>Self-Sovereign Identity</i> dan <i>Blockchain</i>)	Mekanisme mitigasi desentralisasi berbasis <i>Self-Sovereign Identity</i> (SSI) (menggunakan DID & VC) dan <i>Blockchain</i> (<i>Smart Contract</i>).	" <i>Self-Sovereign Identity</i> " OR " <i>SSI</i> " OR " <i>Decentralized Identifiers</i> " OR " <i>DID</i> " OR " <i>Verifiable Credentials</i> " OR " <i>Blockchain</i> " OR " <i>Smart Contract</i> "
C – Comparison (Model Arsitektur Tradisional)	Arsitektur manajemen hak akses tradisional berbasis Cloud Terpusat (<i>Centralized Cloud Access Control</i>) yang memiliki risiko <i>Single Point of Failure</i> (SPoF).	" <i>Centralized Identity</i> , <i>Traditional Access Control</i> , <i>Cloud-based IoT</i> "
O – Outcome (Efektivitas Mitigasi Serangan Otorisasi dan Eksploitasi Akses)	Peningkatan keamanan hak akses yang <i>tamper-proof</i> , eliminasi risiko <i>Single Point of Failure</i> (SPoF), serta optimalisasi metrik performa (latensi, <i>throughput</i> , dan <i>resource overhead</i>) pada mikrokontroler.	" <i>access control</i> " OR " <i>authorization</i> " OR " <i>privilege escalation</i> " OR " <i>unauthorized access</i> " OR " <i>security metrics</i> "

Protokol pencarian dilakukan menggunakan kombinasi kueri terstruktur berbasis kerangka PICO, yaitu: (*Population*) AND (*Intervention* 1) AND (*Intervention* 2) AND

(*Outcome*). Sintaksis ini dikonfigurasi secara spesifik ke dalam *search string* yang disesuaikan dengan karakteristik basis data IEEE Xplore dan ScienceDirect sebagai berikut:

- a. **String query untuk IEEE Xplore:** (*"smart incubator" OR "egg incubator" OR "resource-constrained IoT" OR "microcontroller" OR "ESP32"*) AND (*"Self-Sovereign Identity" OR "SSI" OR "Decentralized Identifiers" OR "DID" OR "Verifiable Credentials" OR "Blockchain" OR "Smart Contract"*) AND (*"access control" OR "authorization" OR "privilege escalation" OR "unauthorized access" OR "security metrics"*).
- b. **String query untuk ScienceDirect:** (*"smart incubator" OR "constrained IoT"*) AND (*SSI OR Blockchain*) AND (*"access control" OR authorization*).

2. 2 Kriteria Inklusi dan Eksklusi

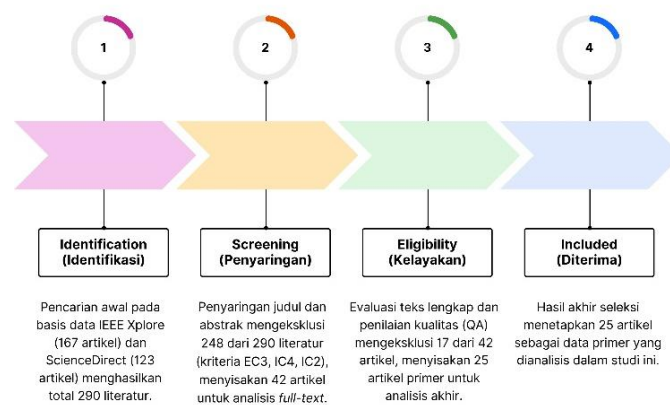
Kriteria inklusi dan eksklusi diterapkan untuk menyaring literatur yang relevan dan berkualitas (Tabel 2). Seleksi memprioritaskan artikel primer (2022–2026) mengenai implementasi teknis SSI dan *blockchain* untuk keamanan IoT [30],[31]. Sebaliknya, artikel berjenis tinjauan pustaka (*review*) serta studi di luar domain arsitektur IoT peternakan mikro berdaya rendah (*resource-constrained*) dieliminasi untuk menjaga orisinalitas data dan menghindari duplikasi informasi dalam literatur.

Tabel 2 Kriteria Inklusi dan Eksklusi

Kode	Kriteria	Keterangan
Inklusi (IC) / (Syarat DITERIMA)		
IC1	Rentang Waktu	Paper diterbitkan antara tahun 2022 hingga 2026 (Data terbaru).
IC2	Kesesuaian Solusi	Studi harus mengintegrasikan <i>Blockchain</i> dan <i>Self-Sovereign Identity</i> (SSI) (seperti W3C DID, <i>Verifiable Credentials</i> , atau ZKP).
IC3	Kesesuaian Masalah	Studi secara eksplisit membahas mitigasi, arsitektur, atau pemodelan keamanan terhadap Serangan Akses Kontrol (<i>Access Control Attacks</i>), manipulasi otorisasi, <i>privilege escalation</i> , atau <i>identity spoofing</i> .
IC4	Kesesuaian Karakteristik	Studi berfokus pada domain <i>Smart Egg Incubator</i> , atau rumpun arsitektur IoT yang setara seperti <i>Smart Agriculture/Farming</i> , Industrial IoT (IIoT), dan perangkat keras dengan sumber daya terbatas (<i>resource-constrained devices</i>).
IC5	Jenis dan Bahasa Dokumen	<i>Original Research Article</i> (Jurnal) dan full text tersedia (dapat diakses/diunduh) dan berbahasa Inggris.
Eksklusi (EC) / (Syarat DITOLAK)		
EC1	Rentang Waktu	Dipublikasikan sebelum tahun 2022.
EC2	Bukan Studi Primer	Dokumen berbentuk <i>review</i> paper lain, survei umum, editorial, laporan industri singkat (<i>whitepaper</i>), tesis/disertasi yang tidak dipublikasikan di jurnal, atau buku chapter.
EC3	Ketidaksesuaian Domain	Studi membahas <i>SSI-Blockchain</i> pada perangkat dengan kapasitas komputasi tinggi atau arsitektur masif, seperti <i>Smart Grid</i> perkotaan, <i>Connected Vehicles</i> (V2X), <i>Healthcare Cloud Systems</i> , atau <i>Cryptocurrency</i> murni yang tidak relevan dengan keterbatasan daya perangkat mikro.
EC4	Fokus Keamanan	Studi IoT- <i>Blockchain</i> yang hanya fokus pada aspek enkripsi <i>data storage</i> , privasi transmisi jaringan, keandalan pasokan energi sensor, atau aspek <i>non-keamanan</i> tanpa menyentuh hak akses/identitas perangkat.
EC5	Data Tidak Lengkap	Artikel yang tidak menyediakan teks lengkap (<i>full-text</i>), naskah abstrak saja, atau merupakan versi duplikat yang lebih pendek dari penelitian yang sudah dipublikasikan lengkap oleh penulis yang sama.

2.3 Proses Seleksi Studi

Seleksi studi dilakukan berdasarkan protokol *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). Alur seleksi mencakup empat tahap: identifikasi awal, penyaringan (*screening*), penilaian kelayakan (*eligibility*), dan penentuan artikel inklusi akhir. Diagram alir PRISMA pada Gambar 1 mengilustrasikan proses tersebut.



Gambar 1 Diagram PRISMA

Tahap *Identification* (Identifikasi), pencarian awal menghasilkan 290 dokumen dari IEEE Xplore (167) dan ScienceDirect (123). Karena tidak ditemukan duplikasi, 290 artikel dilanjutkan ke tahap penyaringan.

Tahap *Screening* (Penyaringan), 290 artikel dievaluasi berdasarkan judul dan abstrak. Setelah mengeksklusi 248 dokumen berdasarkan kriteria (EC3, IC4, IC2), 42 artikel dilanjutkan ke tahap evaluasi teks lengkap (*full-text review*).

Tahap *Eligibility* (Kelayakan), mengevaluasi teks penuh 42 artikel menggunakan kriteria penilaian kualitas/*Quality Assessment* (QA) (QA1–QA5) (Tabel 3). Penilaian kualitas difokuskan pada lima aspek: metode mitigasi (QA1), pemodelan serangan (QA2), integrasi SSI-*blockchain* (QA3), validasi empiris eksperimental (QA4), dan batasan *resource-constrained* (QA5). Hasil evaluasi mengeksklusi 17 artikel di bawah skor minimum, menyisakan 25 artikel primer untuk diekstraksi dan disintesis.

Tabel 3 Penilaian Kelayakan

Kode	Topik	Pertanyaan Kulitas (<i>Quality Assessment</i>)
QA1	Kejelasan tujuan dan metodologi mitigasi	Apakah tujuan penelitian dan metodologi mitigasi serangan akses kontrol IoT dijelaskan secara eksplisit dan konsisten?
QA2	Pemodelan atau klasifikasi serangan kontrol akses	Apakah paper menyajikan pemodelan atau klasifikasi serangan akses kontrol (<i>unauthorized access/privilege escalation</i>) secara jelas?
QA3	Integrasi hibrida SSI dan <i>blockchain</i>	Apakah mekanisme integrasi SSI (DID/VC) dan <i>blockchain</i> dijelaskan secara rinci beserta logika penegakan kebijakannya (<i>smart contract</i>)?
QA4	Validitas ketersediaan data eksperimen atau bukti empiris kuantitatif	Apakah terdapat data eksperimen, simulasi, atau bukti empiris kuantitatif yang menunjukkan metrik kinerja (seperti latensi, <i>throughput</i> , atau daya)?
QA5	Batasan implementasi pada perangkat <i>resource-constrained</i>	Apakah penelitian mendiskusikan batasan implementasi, tantangan pada perangkat terbatas (<i>resource-constrained</i>), atau celah riset masa depan?

Tahap *Inclusion* (Inklusi) menghasilkan 25 artikel final yang memenuhi seluruh kriteria seleksi dan standar kualitas (QA). Tahap akhir meliputi ekstraksi data dan sintesis kualitatif dari dokumen terpilih untuk menjawab pertanyaan penelitian (RQ). 25 artikel digunakan untuk memetakan implementasi hibrida SSI dan *blockchain* pada ekosistem IoT *Smart Egg Incubator* atau peternakan.

2.4 Ekstraksi dan Sintesis Data

Data dari 25 literatur primer diekstraksi secara sistematis menggunakan matriks Microsoft Excel guna memetakan lima parameter (RQ1–RQ5): jenis serangan kontrol akses, integrasi hibrida SSI-*blockchain*, evaluasi kinerja, komparasi mitigasi arsitektur tradisional, dan tantangan perangkat *resource-constrained*. Melalui analisis tematik dan komparatif, data disintesis guna menemukan *research gap* sekaligus merancang arsitektur keamanan IoT *Smart Egg Incubator*. Meskipun sintesis ini secara komprehensif merangkum data empiris dari 25 literatur primer terpilih, validasi kinerjanya masih didasarkan pada bukti sekunder dari penelitian terdahulu dan belum mencakup pengujian langsung terhadap prototipe fisik *Smart Egg Incubator* di lapangan.

3. HASIL DAN PEMBAHASAN

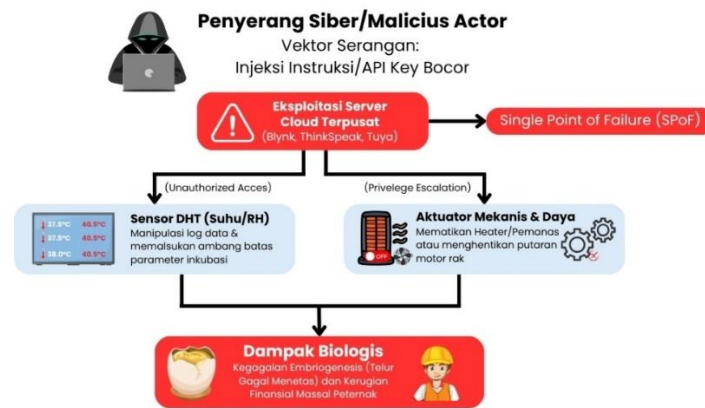
3.1 Lanskap Ancaman dan Vektor Serangan Akses Kontrol pada IoT

Tinjauan sistematis terhadap 25 studi primer mengungkap kerentanan kritis pada arsitektur kontrol akses IoT tradisional akibat ketergantungan mutlak pada model otoritas terpusat (*centralized authority*) seperti platform *cloud* konvensional. Sentralisasi ini menyatukan peran PDP (*Policy Decision Point*) dan PEP (*Policy Enforcement Point*), sehingga eksploitasi pada sektor ini dapat merusak integritas *log* melalui penghapusan jejak aktivitas. Ketidadaan *audit trail* tersebut membuka celah injeksi instruksi ilegal yang memicu anomali fungsional dan kegagalan mekanis pada aktuator fisik (seperti *heater* atau motor penggerak). Berdasarkan temuan tersebut, jenis serangan kontrol akses yang diidentifikasi telah dipetakan secara terstruktur ke dalam taksonomi pada Tabel 4.

Tabel 4 Taksonomi Serangan Akses Kontrol IoT

Kategori Serangan Akses Kontrol	Target Komponen Kritis IoT	Vektor Serangan (<i>Attack Vectors</i>)	Dampak Operasional pada <i>Smart Egg Incubator</i>	Literatur
<i>Unauthorized Access & Unauthorized Modification</i>	IoT Gateways, Sistem Log, Perangkat Akhir Industri (<i>Equipment/Sensors/Actuators</i>), dan <i>State Database</i> (CouchDB).	Eksplorasi kontrol akses terpusat dipicu oleh aturan kaku (<i>static ACL</i>), titik kegagalan tunggal (SPOF), dan proksi <i>cloud</i> yang <i>honest-but-curious</i> .	Penyerang menyusup dan mengubah ambang batas suhu inkubasi atau hak akses operasional, sehingga memicu kebocoran data sensitif.	[32],[33], [34],[35], [36]
<i>Identity Spoofing, Impersonation & Device Cloning</i>	<i>Edge Nodes</i> , Modul Komunikasi, Repositori Data, Entitas Fisik/Kembaran Digital (<i>Digital Twins</i>), dan Klien MQTT.	Kerentanan identitas perangkat mencakup replikasi token, kebocoran kunci API, serangan <i>Sybil</i> , penyusupan entitas palsu, dan pelanggaran privasi operator.	Penyerang mengkloning perangkat suhu untuk mengirim data palsu dan menyembunyikan anomali kondisi inkubasi dari peternak.	[37],[38], [39],[40], [41],[42], [43]
<i>Replay Attack & Denial of Service (DoS/DDoS)</i>	<i>Dedicated Database Storage</i> (DDS), <i>Node Asing</i> , dan Jaringan Komunikasi Data IoT.	<i>Sniffing</i> data akses, serangan <i>brute-force/flooding</i> hak akses, dan penetrasi anomali trafik siber.	Mengakibatkan kongesti jaringan, otorisasi ilegal akibat siaran ulang token, hingga <i>system crash</i> yang menghentikan total pemantauan suhu <i>real-time</i> .	[44],[45], [46],[47], [48]
<i>Privilege Escalation & Insider Threats</i>	<i>Firmware</i> Kontroler, Server Proksi Awan, Dokumen Aktivitas, dan Perangkat IoT Internal Terkompromi.	Serangan <i>privilege escalation</i> (<i>User-to-Root</i>), ancaman orang dalam (<i>insider threat</i>), dan manipulasi node dinamis (<i>on-off attacks</i>).	Eksplorasi <i>privilege escalation</i> oleh akun level rendah untuk menguasai kontrol penuh atas aktuator <i>heater</i> , motor pemutar rak dan kipas sirkulasi.	[49],[50], [51],[52]
<i>Data & Model Poisoning / Fabricated Attacks</i>	Node Kolaborator, Modul Sensor Deteksi, dan Model Pembelajaran Mesin (<i>Machine Learning Model</i>).	Injeksi data rusak/malicious secara sengaja, partisipasi node jahat dalam klaster (<i>Byzantine clients</i>), serta manipulasi data otorisasi hibrida (<i>label-flipping</i> atau <i>backdoor attacks</i>).	Peracunan algoritma otomatisasi pembacaan suhu, sehingga kecerdasan buatan inkubator salah memprediksi waktu penetasan telur ayam atau gagal mendeteksi anomali kerusakan <i>heater</i> .	[53],[54], [55]

Ancaman kontrol akses didominasi oleh *Unauthorized Access* dan *Identity Spoofing*, yang teridentifikasi pada lebih dari separuh literatur (Tabel 4). Kerapuhan verifikasi identitas memungkinkan penyerang melakukan *device spoofing* dan ketidadaan validasi konteks (*context-blind*) untuk menguasai hak akses dan memanipulasi parameter tanpa terdeteksi. Manipulasi ini mengancam operasional *Smart Egg Incubator* yang membutuhkan stabilitas suhu (37,5°C–38°C) dan kelembapan (50%–60%) secara konstan selama 21 hari masa inkubasi. Oleh karena itu, eksploitasi terhadap berbagai celah keamanan yang terpetakan dalam taksonomi serangan kontrol akses tersebut (Tabel 4) akan berdampak fatal pada aspek biologis dan ekonomi akibat kegagalan fisik embrio. Hubungan interaksi antara vektor serangan dan komponen fisik mikrokontroler tersebut diilustrasikan pada Gambar 2.



Gambar 2 Alur Vektor Serangan Akses Kontrol Tradisional pada *Smart Egg Incubator*

Alur serangan terhadap sistem kontrol akses tradisional pada *Smart Egg Incubator* secara rinci ditunjukkan pada Gambar 2. Melalui eksploitasi *privilege escalation*, pihak penyerang berpotensi melakukan modifikasi ilegal terhadap aktuator pemanas hingga suhunya melampaui batas kritis 38°C (*overheating*), yang secara fatal mematikan embrio. Selain itu, penyerang dapat menghentikan mekanisme rotasi motor rak secara paksa selama masa inkubasi krusial (hari ke-1 hingga ke-18), sehingga menyebabkan kuning telur menempel pada cangkang dan berujung pada kegagalan proses penetasan. Temuan kritis ini menggarisbawahi urgensi peralihan kontrol akses IoT peternakan menuju arsitektur desentralisasi *tamper-proof*, yang harus mampu mengevaluasi konteks secara adaptif sebelum instruksi dieksekusi oleh mikrokontroler.

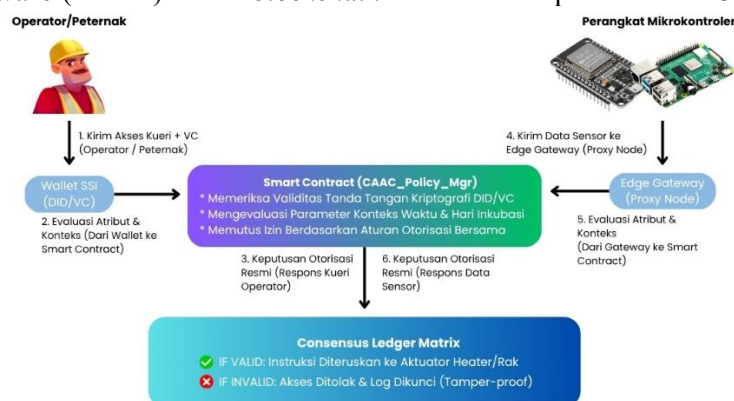
3.2 Mekanisme Mitigasi Desentralisasi Berbasis SSI dan Smart Contract

Untuk memitigasi berbagai spektrum ancaman sistem kontrol akses tradisional, paradigma pertahanan keamanan perlu segera dialihkan dari model kepercayaan terpusat menuju arsitektur terdesentralisasi. Pendekatan inovatif ini secara langsung mengintegrasikan teknologi *Self-Sovereign Identity* (SSI) dan *smart contract* berbasis *blockchain* guna mewujudkan mekanisme validasi hak akses yang dinamis serta otonom. Adapun rincian pemetaan komprehensif yang membahas mengenai literatur terkait, komponen utama, hingga platform desentralisasi dalam strategi mitigasi ini telah dirangkum pada Tabel 5.

Tabel 5 Pemetaan Mekanisme Mitigasi SSI, *Blockchain*, dan Model Akses Kontrol

Model / Logika Kontrol Akses	Komponen SSI yang Digunakan	Platform & Jenis Blockchain	Peran Utama Smart Contract	Literatur
<i>Context-Aware Access Control</i> (CAAC) / <i>Attribute-Based Access Control</i> (ABAC)	Integrasi manifes kebijakan kontekstual berbasis struktur JSON, <i>Verifiable Credentials</i> (VC), dan <i>Selective Disclosure</i> atribut.	<i>Consortium Blockchain: Hyperledger Besu</i> (IBFT 2.0) dengan <i>Hyperledger Fabric</i> <i>Ethereum Private</i>	Sistem ini bertindak sebagai entitas pengelola kebijakan otomatis (<i>smart contract</i> CAAC_Policy_Mgr.sol), memverifikasi aturan akses dinamis (<i>Policy Rule Verification</i>), dan penegak otorisasi <i>on-chain</i> berdasarkan parameter waktu, lokasi, serta status operasional perangkat.	[32],[33], [45],[40], [51],[46], [52]
<i>Capability-Based Access Control</i> (CapBAC)	W3C <i>Decentralized Identifiers</i> (DID), pembuatan tanda tangan kriptografi (Ed25519/ECDSA), dan tokenisasi kemampuan (<i>capability tokens</i>).	<i>Private Blockchain & Directed Acyclic Graph</i> (DAG): <i>Ethereum</i> (Geth) <i>IOTA</i> / <i>Custom Chain</i> <i>Hyperledger Fabric</i>	Mengelola siklus hidup hak akses (<i>Capability Lifecycle Management</i>), memvalidasi delegasi token hak akses antar perangkat tepi (<i>edge devices</i>), serta melakukan pembatalan izin (<i>revocation</i>) secara instan ketika terdeteksi perilaku anomali node.	[44],[37], [38],[43], [56],[47], [48]
<i>Hybrid Intelligent / Privacy-Preserving Access Control</i>	<i>Zero-Knowledge Proofs</i> (ZKP), kriptografi asimetris, dan skema <i>blind signatures</i> untuk anonimitas identitas.	<i>Consortium & Private Blockchain: Ethereum Enterprise</i> <i>Hyperledger Fabric</i> (<i>CouchDB</i>) <i>Quorum</i>	Mengeksekusi verifikasi bukti <i>validity proof</i> tanpa mengungkap identitas asli perangkat (<i>anonimitas</i>), mengevaluasi reputasi node secara cerdas melalui interaksi dengan model <i>Machine Learning / GRU on-chain</i> , dan memblokir <i>Byzantine clients</i> .	[34],[53], [50],[35], [54],[36], [55]

Merujuk pada Tabel 5, mekanisme mitigasi desentralisasi ini dibangun melalui tiga pilar fundamental. Pilar pertama berfokus pada lapisan identitas berbasis *Self-Sovereign Identity* (SSI), memanfaatkan komponen standar W3C yakni *Decentralized Identifiers* (DID) dan *Verifiable Credentials* (VC). Integrasi ini memfasilitasi autentikasi mandiri bagi perangkat maupun operator tanpa ketergantungan pada otoritas sertifikat pihak ketiga. Selanjutnya, pilar kedua mengusung lapisan kontrol akses *context-aware* yang secara signifikan memperluas kapabilitas dari model ABAC dan CapBAC. Sementara itu, pilar ketiga merupakan lapisan penegakan kebijakan (*policy enforcement*) yang mengoptimalkan otomatisasi *smart contract* pada jaringan *consortium* atau *private blockchain* secara *runtime*. Implementasi hibrida pada *Smart Egg Incubator* ini terbukti komprehensif mereduksi risiko otorisasi konvensional melalui eksekusi kebijakan yang bersifat *tamper-proof*. Secara visual, arsitektur logis terkait interaksi desentralisasi antara SSI dan kontrol akses *Context-Aware* (CAAC) di atas *blockchain* diilustrasikan pada Gambar 3.



Gambar 3 Arsitektur Logika Mitigasi Akses Kontrol Berbasis SSI-Smart Contract

Alur mitigasi pengamanan kontrol akses IoT inkubator berbasis *Zero-Trust* ini diimplementasikan melalui integrasi tiga tahapan krusial. Pertama, autentikasi *on-chain* memanfaatkan *Verifiable Credentials* (VC) dan *Decentralized Identifiers* (DID) secara efektif untuk mematahkan serangan *identity spoofing* serta *device cloning* [37], [38], [43]. Kedua, penegakan kebijakan dinamis (CAAC/ABAC) dieksekusi melalui *smart contract* berdasarkan parameter konteks aktual [32], [33], [45]. Sebagai contoh, instruksi ilegal untuk mematikan pemutar rak pada hari ke-10 otomatis diblokir demi menjaga keselamatan embrio. Ketiga, pencatatan setiap kueri menggunakan konsensus IBFT 2.0 pada jaringan Hyperledger Besu guna menghasilkan *audit trail* yang kebal manipulasi maupun ancaman internal (*insider threats*) [32], [46], [52]. Integrasi hibrida antara *Self-Sovereign Identity* (SSI) dan *smart contract* ini terbukti sukses menciptakan lapisan proteksi tangguh bagi ekosistem IoT yang terbatas [34], [57].

3.3 Metrik Kinerja dan Validasi Empiris Sistem Keamanan

Analisis kuantitatif secara komprehensif dilakukan untuk mengevaluasi performa dan ketahanan skema desentralisasi berbasis *Self-Sovereign Identity* (SSI) serta *smart contract blockchain* terhadap stabilitas operasional IoT. Evaluasi ini didasarkan pada tiga parameter utama: latensi respons otorisasi, *throughput* transaksi (TPS), serta kompleksitas komputasi. Berdasarkan tinjauan literatur, karakteristik performa sistem dapat diklasifikasikan ke dalam tiga klaster utama yang merepresentasikan fenomena *trade-off* keamanan siber. Meskipun studi ini tidak membangun instrumen pengujian fisik baru di peternakan, validasi performanya didasarkan pada meta-sintesis data kuantitatif dari 25 literatur primer yang menguji prototipe perangkat keras dan simulator jaringan serta *blockchain* terstandar. Evaluasi mencakup latensi otorisasi, *throughput* transaksi (TPS), dan kompleksitas komputasi. Berdasarkan parameter tersebut, karakteristik performa sistem dikelompokkan ke dalam tiga klaster yang merepresentasikan *trade-off* keamanan siber.

Integrasi *smart contract* dengan model deteksi intrusi cerdas (seperti GRU dan arsitektur VCD-TSNet) mencapai akurasi 99,0% hingga 99,3% dalam memitigasi serangan *flooding* dan DDoS [47], [48], sehingga ketersediaan (*availability*) layanan pemantauan parameter inkubasi

tetap terjaga. Serangan manipulasi data (*payload tampering*) dan injeksi data palsu (*false data injection*) pada *broker* MQTT berhasil dimitigasi dengan akurasi 99,10%–99,88% serta *False Alarm Rate* (FAR) serendah 0,06% menggunakan verifikasi tanda tangan kriptografi berantai dan *split learning* [37], [39], [53], [54]. Penerapan W3C DID dan VC yang dikombinasikan dengan token ERC-721 secara deterministik (100%) menolak perangkat palsu (*Sybil attacks*) dan upaya pembajakan hak akses (*privilege hijacking*) [38], [40], [41].

Pertama, klaster *ultra-fast & lightweight* (ABAC/CapBAC/CAAC) tampil sangat unggul dengan catatan latensi di bawah 100 ms (rata-rata berkisar 42–90 ms) dan kompleksitas konstan. Hal ini krusial demi menjaga stabilitas sistem ketika volume perangkat IoT melonjak [33], [43], [58]. Kedua, klaster *balanced performance* menawarkan arsitektur hibrida adaptif dengan latensi 100–300 ms, yang sangat dipengaruhi oleh stabilitas jaringan tepi (*edge network*) [37], [45]. Terakhir, spektrum *heavy computation & high privacy* (ZKP/GRU) memicu latensi masif mencapai 300–600 ms akibat tingginya beban komputasi proses enkripsi [46], [50], [55].

Operasional *Smart Egg Incubator* memerlukan stabilitas lingkungan yang ketat. Batas toleransi latensi respons aktuator diwajibkan selalu berada di bawah 100 ms menggunakan arsitektur *ultra-fast & lightweight* demi mencegah *actuator lag* maupun penumpukan beban (*bottleneck*) [32], [39]. Meskipun proses penulisan aturan awal (*write operations*) berbasis konsensus membutuhkan waktu hingga 4,7 detik, durasi tersebut dinilai layak (*feasible*). Hal ini dapat diterima karena proses tersebut hanyalah *one-time overhead* pada fase awal siklus masa inkubasi 21 hari [40], [49]. Sebaliknya, operasional harian tetap berjalan super cepat karena secara eksklusif bertumpu pada kueri pembacaan data (*read*) [43], [51]. Hasil pengujian skalabilitas dan pemetaan performa komprehensif dari berbagai literatur utama tersebut dirangkum pada Tabel 6. Sintesis data empiris ini membuktikan kelayakan teknis (*technical feasibility*) arsitektur terdesentralisasi dalam skala laboratorium dan simulasi, meskipun kalibrasi performa dinamis terhadap fluktuasi lingkungan fisik peternakan riil tetap memerlukan validasi eksperimental lebih lanjut.

Tabel 6 Karakteristik Kinerja Empiris Arsitektur Keamanan Desentralisasi

Karakteristik Kinerja	Rentang Latensi	Rentang Throughput	Hasil Pengujian & Mitigasi	Tools / Simulator	Literatur
<i>Ultra-Fast & Lightweight</i> (Skema Kontrol Akses Berbasis Atribut Ringan & Token Kapabilitas)	< 100 ms (Rata-rata: 42 ms – 90 ms)	<i>High Throughput / Scalable</i> (Mampu menangani ratusan hingga ribuan pesan/transaksi per detik secara simultan)	Mengevaluasi aturan akses dengan kompleksitas waktu konstan. Sangat efektif memblokir <i>Unauthorized Access, Identity Spoofing</i> , serta <i>Payload Tampering</i> pada broker pesan (MQTT) secara langsung (<i>runtime</i>).	<i>Hyperledger Besu, Hyperledger Fabric, CouchDB, Go-lang, Ganache, Web3.py, Eclipse Mosquitto MQTT, Docker Containers.</i>	[37],[40], [43],[46], [47],[48], [49],[50], [51],[52], [53]
<i>Balanced Performance</i> (Skema Kontrol Akses Dinamis & Adaptasi Jaringan Tepi)	100 ms – 300 ms (Rata-rata: 110 ms – 250 ms)	<i>Medium Throughput</i> (Kecepatan pemrosesan dibatasi oleh fluktuasi stabilitas jaringan nirkabel tepi atau komputasi lokal node proksi)	Fokus pada penyaringan <i>runtime</i> tingkat lanjut seperti pemutusan konflik kebijakan dinamis (<i>policy deadlocks</i>), pemulihan status otorisasi saat koneksi terputus (<i>intermittent connectivity</i>), serta penjejakan perilaku anomali internal (<i>on-off attacks</i>).	<i>Hyperledger Fabric, State Database (SDB), Ethereum Private Testnet, Python Web3, Remix IDE, NS3, Cooja, Embedded Linux Testbed, Matlab.</i>	[27],[38], [41],[42], [44],[55], [56], [57]
<i>Heavy Computation & High Privacy</i> (Skema Kontrol Akses Hibrida Berbasis Kecerdasan Buatan & Kriptografi Fungsional)	> 300 ms (Rentang: 300 ms – 600 ms, melambat seiring bertambahnya jumlah node kolaborator)	<i>Low Throughput</i> (Mengalami penurunan kecepatan akibat beban komputasi fungsi matematika hibrida atau kompleksitas konsensus kolaboratif)	Memiliki tingkat proteksi privasi tertinggi. Sukses mendeteksi dan mengisolasi serangan penyerang internal tingkat lanjut (<i>insider threats</i>), peracunan model (model <i>poisoning</i>), serta klien <i>Byzantine (backdoor & label-flipping attacks)</i> .	<i>Python, TensorFlow/Keras, PyTorch, PySyft (Federated Learning), Ganache CLI, Go-Ethereum (Geth), Hyperledger Fabric.</i>	[58],[59], [60]

Tabel 6 menunjukkan kelayakan arsitektur desentralisasi berbasis SSI dan *smart contract*. Model ini mengombinasikan proteksi kuat terhadap serangan kontrol akses tradisional dengan performa yang adaptif dan efisien. Ini menegaskan potensinya menjaga keselamatan fisik-biologis *Smart Egg Incubator*. Agregasi data empiris yang diperoleh menunjukkan bahwa batas

kelayakan teknis (*feasibility boundary*) arsitektur desentralisasi telah divalidasi secara kuantitatif pada skala laboratorium dan melalui skenario simulasi. Namun, kalibrasi kinerja secara dinamis terhadap fluktuasi kondisi lingkungan pada peternakan nyata masih memerlukan validasi lebih lanjut. Oleh karena itu, pengujian pada kondisi operasional aktual perlu dilakukan dalam penelitian selanjutnya untuk mengonfirmasi keandalan, skalabilitas, dan adaptabilitas sistem.

3.4 Analisis Komparatif: Model Arsitektur Desentralisasi vs Tradisional

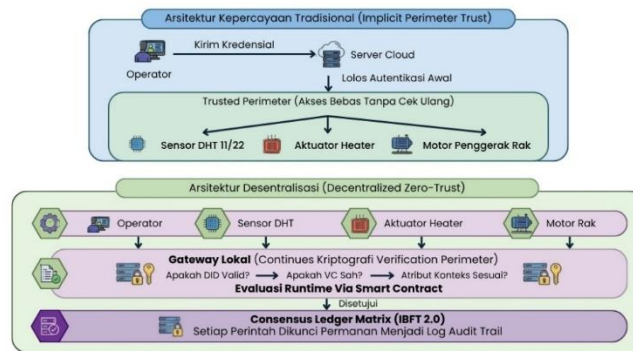
Analisis ini membandingkan kelemahan arsitektur terpusat dengan keunggulan arsitektur desentralisasi berbasis SSI dan *smart contract blockchain*. Perbandingan diklasifikasikan ke dalam empat parameter keamanan kritis: eliminasi *Single Point of Failure* (SPoF), proteksi *log audit trail*, penegakan privasi melalui data minimization, serta pergeseran model kepercayaan (*trust model*). Ringkasan sintesis komparatif arsitektur tersebut dirangkum secara komprehensif pada Tabel 7.

Tabel 7 Analisis Komparatif Efektivitas Keamanan: Tradisional vs Desentralisasi

Parameter Keamanan	Arsitektur Tradisional Terpusat	Arsitektur Desentralisasi Berbasis SSI-Blockchain	Bukti Mekanisme Teknis (Sintesis Literatur)	Literatur
Eliminasi <i>Single Point of Failure</i> (SPoF)	Rentan Tinggi: Seluruh hak otorisasi bertumpu pada satu <i>server cloud</i> tunggal. Jika <i>server</i> lumpuh, seluruh sistem IoT mati total.	Tahan Lumpuh (<i>Robust</i>): Otoritas didistribusikan ke beberapa node validator konsorsium. Sistem tetap hidup selama mayoritas node aktif.	Protokol konsensus <i>enterprise</i> (seperti IBFT 2.0 atau <i>Proof-of-Authority</i>) yang mendistribusikan salinan <i>ledger</i> secara sinkron.	[32],[40], [49],[46]
Integritas Log & Proteksi Audit Trail	Mudah Dimanipulasi: <i>Log</i> aktivitas disimpan dalam database terpusat yang dapat diubah atau dihapus oleh penyerang siber atau insider.	Anti-Manipulasi (<i>Tamper-Proof</i>): Setiap jejak otorisasi akses dikunci secara permanen dan transparan di dalam <i>blok ledger</i> .	Sifat <i>immutability</i> (kekekalan kriptografi) melalui fungsi <i>hashing</i> berantai (<i>blockchain cryptographically linked blocks</i>).	[32],[33], [45],[41], [42]
Prinsip Data Minimization & Privasi	Sangat Lemah: Operator dipaksa mengungkapkan seluruh data kredensial mentah ke server pusat saat meminta hak akses.	Sangat Kuat: Verifikasi dilakukan tanpa mengungkapkan data sensitif operator, melainkan cukup melalui pembuktian klaim.	Implementasi tanda tangan kriptografi asimetris (Ed25519/ECDSA), <i>Verifiable Credentials</i> (VC), atau <i>Zero-Knowledge Proofs</i> (ZKP).	[37],[40], [41],[42], [43],[58], [59]
Model Kepercayaan (<i>Trust Model</i>)	<i>Third-Party Trust</i> : Bergantung penuh pada kejujuran penyedia layanan <i>cloud</i> pihak ketiga atau administrator tunggal.	<i>Decentralized Zero-Trust</i> : Tidak ada entitas yang dipercaya secara buta. Setiap permintaan akses wajib divalidasi kriptografi secara <i>runtime</i> .	Penegakan aturan akses dinamis secara otomatis lewat <i>Smart Contract</i> (CAAC_Policy_Mgr.sol) berdasarkan atribut kontekstual.	[27],[37], [44],[53], [55],[56], [57], [60]

Arsitektur desentralisasi hibrida *consortium blockchain* mengeliminasi risiko SPoF pada platform *cloud* konvensional untuk melindungi siklus biologis embrio *Smart Egg Incubator*. Melalui pengalihan otoritas ke *edge gateways*, fungsi otorisasi tetap berjalan via *node* validator lain saat terjadi kegagalan sistem atau serangan DoS. Selain menjamin kontinuitas operasional, otomatisasi *smart contract* pada *ledger immutable* dengan *hashing* kriptografi berantai berhasil menutup celah manipulasi internal (*insider threats*). Mekanisme ini menghasilkan *audit trail* yang valid sebagai bukti forensik digital yang sah untuk akuntabilitas sistem.

Integrasi arsitektur *decentralized zero-trust* dan prinsip *data minimization* berbasis DID dan VC berhasil meningkatkan proteksi perangkat *resource-constrained*. Dengan memverifikasi tanda tangan digital secara *runtime* via *smart contract*, model ini mengeliminasi risiko kebocoran *API key*, kata sandi terpusat, dan *identity spoofing*. Keamanan berlapis menggunakan *nonce* unik dan *timestamp* kontekstual juga efektif menangkal *privilege escalation* serta *replay attack*. Keunggulan utama skema desentralisasi ini terletak pada transformasi batas keamanan (*security perimeter*) yang menggeser paradigma struktural *implicit trust* tradisional, di mana entitas dalam jaringan dianggap aman setelah autentikasi awal, menuju model *Decentralized Zero-Trust Architecture* yang visualisasinya diilustrasikan pada Gambar 4.



Gambar 4 Perbandingan Model Kepercayaan Terpusat vs Model *decentralized zero-trust*

Analisis Gambar 4, arsitektur tradisional (*Implicit Perimeter Trust*) memiliki titik eksekusi kaku berupa *Single-Boundary Perimeter*, di mana autentikasi awal pada *cloud* membuka akses implisit ke seluruh sistem *Smart Egg Incubator*. Model ini sangat rentan karena kebocoran token API atau eksploitasi server memungkinkan penyerang mengambil alih kendali penuh. Akibatnya, instruksi fatal seperti manipulasi pemanas atau penghentian rotasi rak akan langsung dieksekusi oleh mikrokontroler tanpa adanya verifikasi ulang di tingkat lokal.

Sebaliknya, model *Decentralized Zero-Trust* menerapkan prinsip *never trust, always verify* menggunakan *continuous cryptographic verification perimeter* pada gateway lokal. Melalui *Smart Contract (CAAC_Policy_Mgr.sol)*, setiap instruksi divalidasi secara *runtime* kesesuaiannya dengan DID, VC, serta konteks operasional harian. Arsitektur ini mampu mengisolasi dampak serangan; meskipun kredensial operator terkompromi, instruksi ilegal tetap diblokir jika menyalahi parameter siklus inkubasi. Akhirnya, seluruh *log* otorisasi dikunci permanen melalui konsensus IBFT 2.0 sebagai *audit trail* yang *tamper-proof* untuk melindungi keselamatan fisik embrio.

3.5 Tantangan Implementasi Keamanan pada Resource-Constrained

Integrasi SSI dan *smart contract* terbukti memperkuat kontrol akses, namun adopsinya pada perangkat *edge* terkendala oleh keterbatasan sumber daya perangkat keras. Mikrokontroler tipikal pada *Smart Egg Incubator*, seperti ESP32/ATmega memiliki kapasitas memori dan komputasi yang sangat terbatas (SRAM 2–520 KB, Flash 4–16 MB, clock 16–240 MHz). Berdasarkan sintesis 25 literatur primer, penerapan mekanisme desentralisasi memicu empat kendala teknis utama dikelompokkan ke dalam empat tantangan utama pada Tabel 8 yang saling terikat.

Tabel 8 Tantangan pada Perangkat *Resource-Constrained*

Jenis Tantangan Fisik	Implikasi Teknis	Dampak & Parameter Beban Kerja	Optimalisasi Arsitektur Ringan (<i>Lightweight</i>)	Literatur
<i>Computational Overhead</i>	Operasi kriptografi asimetris intensif dan fungsi matematika hibrida memicu beban pemrosesan CPU dan RAM yang teramat tinggi.	Biaya komputasi (<i>gas cost</i>) untuk <i>deployment</i> awal <i>smart contract</i> pengelola kebijakan adalah sebesar 2.090.226 gas.	Mendelegasikan proses penandatanganan aturan (<i>on-chain signing</i>) berat ke lapisan <i>edge proxy node</i> .	[37],[57], [58],[59], [60]
Masalah <i>Ledger Bloat</i>	Akumulasi pencatatan tanda tangan data log transaksi bervolume besar secara berkala membebani kapasitas penyimpanan lokal node.	Ukuran basis data <i>ledger</i> lokal membengkak seiring bertambahnya data transaksi kontrol akses hibrida dari sensor.	Pemanfaatan arsitektur penyimpanan terdesentralisasi <i>off-chain</i> menggunakan IPFS.	[37],[38], [41],[43], [47]
Konsumsi Energi / Daya	Aktivitas penyaringan anomali runtime intensif dan enkripsi asimetris di level perangkat fisik menguras daya dengan sangat cepat.	Implikasi langsung pada peningkatan latensi jaringan lokal dan beban kerja <i>hardware</i> yang memicu disipasi panas.	Penggunaan algoritma kriptografi kurva eliptik yang efisien (ECC) atau pemangkasan fitur model <i>lightweight</i> .	[37],[44], [49],[50], [52]
<i>Intermittent Connectivity</i>	Kegagalan sinkronisasi status identitas desentralisasi saat node tepi mengalami gangguan sinyal nirkabel lokal.	Terputusnya pelacakan sesi otorisasi (<i>connectivity tracking failure</i>) pada arsitektur hibrida terdistribusi.	Implementasi mekanisme <i>embedded linux testbed</i> untuk menjaga konsistensi hak akses lokal sementara.	[27],[42], [46],[48], [51],[53], [55], [56]

Pada jaringan *public blockchain* (*Ethereum*), eksekusi *smart contract* menimbulkan biaya transaksi (*gas fee*) yang tinggi dan fluktuatif; proses *deployment smart contract* pengelola kebijakan (CAAC_Policy_Mgr.sol) mengonsumsi 2.090.226 unit *gas* [32], sementara registrasi identitas awal membutuhkan 285.836 unit *gas* [37]. Guna mengeliminasi beban biaya operasional bagi peternak kecil, literatur merekomendasikan migrasi ke *consortium blockchain* (Hyperledger Besu/Fabric) berbasis konsensus IBFT 2.0 atau arsitektur *Directed Acyclic Graph* (DAG/IOTA) yang beroperasi secara *feeless* (bebas biaya *gas*) [32], [56].

Beban komputasi kriptografi asimetris yang berat (seperti bilinear pairings pada ZKP dengan latensi 12,9–17,9 ms) memicu lonjakan arus kerja hingga >150–240 mA, yang berdampak pada pemborosan daya dan disipasi termal mikrokontroler [40], [50]. Masalah penyimpanan (*ledger bloat*) diselesaikan melalui sistem hibrida *off-chain* berbasis IPFS (InterPlanetary File System) [43], [49]. Data log berukuran besar dari sensor DHT diunggah ke IPFS, sementara *smart contract* hanya menyimpan nilai *hash* kriptografi 32-byte sebagai sidik jari digital *tamper-proof* untuk menjamin resiliensi penyimpanan jangka panjang [40], [45].

Efisiensi komunikasi antara mikrokontroler dan *edge gateway* ditingkatkan menggunakan kriptografi ringan berbasis ECC (seperti Ed25519) [46], [51]. Metode ini memberikan keamanan tinggi dengan ukuran kunci lebih pendek, sehingga meminimalkan beban CPU, RAM, dan daya [52], [54]. Kolaborasi antara efisiensi perangkat dan kapasitas *edge node* ini membuktikan bahwa model pertahanan *zero-trust* berbasis SSI dan blockchain sangat layak (*feasible*), aman, dan siap menjaga keberlanjutan siklus *Smart Egg Incubator* [39], [49]. Namun, mengingat analisis performa ini berbasis sintesis literatur, evaluasi empiris secara langsung tetap direkomendasikan guna memvalidasi ketahanan sistem terhadap gangguan fisik serta variasi pasokan daya di lapangan.

4. KESIMPULAN

Tinjauan sistematis ini memetakan arsitektur terdesentralisasi sebagai solusi keamanan mutakhir bagi ekosistem IoT peternakan, dengan menempatkan *Smart Egg Incubator* sebagai model studi kasus representatif. Kerentanan mendasar pada kontrol akses konvensional umumnya bersumber dari serangan *unauthorized access*, *identity spoofing*, dan *privilege escalation* yang mengeksploitasi arsitektur *cloud* terpusat, sehingga berisiko memicu manipulasi parameter fisik yang berdampak fatal terhadap viabilitas embrio. Studi ini membuktikan bahwa integrasi hibrida antara *Self-Sovereign Identity* (SSI), melalui *Decentralized Identifiers* (DID) dan *Verifiable Credentials* (VC), bersama *smart contract blockchain* mampu mengeliminasi *Single Point of Failure* (SPoF), menyediakan jejak audit yang *tamper-proof*, serta menegakkan otorisasi *zero-trust* antarmesin (*machine-to-machine*) secara adaptif.

Dari segi implementation feasibility dan tingkat kesiapan teknologi, adopsi desentralisasi penuh pada peternakan skala mikro saat ini tergolong *conditionally feasible*. Keterbatasan sumber daya mikrokontroler murah (ESP32 SRAM 520 KB), tingginya *overhead* komputasi dan energi kriptografi asimetris, serta instabilitas jaringan nirkabel lokal merupakan faktor penghambat utama. Solusi kelayakan teknis dan ekonomi bertumpu pada *tiered edge-assisted framework*: mengalihkan beban konsensus dan komputasi berat ke unit *Edge Gateway* lokal (Raspberry Pi 4), memanfaatkan *consortium blockchain* nirbiaya (*feeless*), dan menerapkan penyimpanan *off-chain* IPFS (*hash 32-byte*) guna memitigasi risiko *ledger bloat*.

Terlepas dari keunggulan keamanannya, arsitektur ini menghadapi *trade-off* operasional pada perangkat IoT terbatas (*resource-constrained*), seperti *computational overhead*, lonjakan latensi validasi (300–600 ms pada ZKP), dan ancaman *ledger bloat* pada SRAM mikrokontroler. Solusi arsitektur hibrida berbasis *Edge Gateway* lokal dan *off-chain* IPFS mampu mereduksi latensi tersebut ke tingkat aman (<100 ms). Kendati demikian, penelitian ini memiliki tiga keterbatasan utama: (1) evaluasi performa masih bertumpu pada sintesis data sekunder tanpa implementasi fisik lapangan; (2) sumber literatur terbatas pada basis data IEEE Xplore dan ScienceDirect (2022–2026); serta (3) evaluasi *Total Cost of Ownership* (TCO) bagi peternak mikro belum divalidasi secara empiris.

5. SARAN

Untuk menjembatani temuan teoretis ke penerapan praktis, penelitian lanjutan perlu memvalidasi efisiensi daya, disipasi termal, dan latensi *handshake* DID/VC secara empiris pada *testbed* mikrokontroler murah (ESP32) dan *Edge Gateway* lokal (Raspberry Pi 4). Integrasi pada infrastruktur inkubasi eksisting (*legacy systems*) dapat mengadopsi pendekatan *retrofit* melalui *middleware plug-and-play* (jembatan protokol MQTT/RESTful API), sehingga peningkatan keamanan tercapai tanpa merombak sensor dan aktuator mekanis terpasang.

Guna memastikan keberlanjutan adopsi pada peternakan skala mikro dengan sumber daya terbatas, rencana pengembangan selanjutnya diwajibkan mengikuti peta jalan prioritas (*staged priority roadmap*) bertahap: (1) Prioritas Pertama (Reduksi Biaya Implementasi): mengeliminasi biaya gas transaksi melalui platform *consortium/DAG feeless* serta memanfaatkan *shared edge gateway* untuk menekan belanja modal awal (*CapEx*); (2) Prioritas Kedua (Efisiensi Energi dan Stabilitas Node): mengimplementasikan modul kriptografi ringan *Pairing-Free ECC* (Ed25519) guna menekan konsumsi daya mikrokontroler dan menjaga ketahanan terhadap intermitensi jaringan nirkabel lokal; serta (3) Prioritas Ketiga (Ketahanan Keamanan Lanjutan): menguji resiliensi sistem terhadap simulasi serangan multi-vektor kompleks (DDoS dan *data poisoning*) serta memvalidasi keandalan forensik log audit *tamper-proof* di lapangan..

DAFTAR PUSTAKA

- [1] A. U. Bhuiyan *et al.*, *IoT Enabled Smart Egg-incubator with Remote Monitoring and Control System*, vol. 1, no. 1. Association for Computing Machinery, 2024. doi: 10.1145/3723178.3723193.
- [2] K. S. Masia, P. A. Idowu, K. A. Nephawe, J. N. Ngcobo, M. C. Modiba, and T. J. Mpofo, "Effect of incubation temperature on hatchability , chick quality and post-hatch performance – Review," *Anim. Sci. Genet.*, vol. 21, no. 4, pp. 59–87, 2025, doi: 10.5604/01.3001.0055.2705.
- [3] A. O. Adewusi, N. R. Chiekezie, and N. L. Eyo-udo, "Securing smart agriculture : Cybersecurity challenges and solutions in IoT-driven farms," *World J. Adv. Res. Rev.*, 2022, doi: <https://doi.org/10.30574/wjarr.2022.15.3.0887>.
- [4] R. K. Maddumala, "Global Journal of Engineering Innovations & Interdisciplinary Research Comparison of Edge vs . Cloud Computing Architectures in IoT-Based Smart Agriculture Systems," *Glob. J. Eng. Innov. Interdiscip. Res.*, vol. 5, no. 6, pp. 1–6, 2025, doi: <https://doi.org/10.33425/3066-1226.1180>.
- [5] I. Riadi and P. A. Raharja, "Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 135–143, 2019, doi: <https://dx.doi.org/10.14569/IJACSA.2019.0101118>.
- [6] T. Irlon, Muryanto and A. Alvionita, "IoT Security Model with Machine Learning and Edge Computing for Smart Poultry Farm," *Interdiscip. Soc. Stud.*, 2024, doi: <https://doi.org/10.55324/iss.v4i3.876>.
- [7] I. Riadi and W. P. Wicaksono, "Implementasi Quality of Service M enggunakan Metode Hie rarchical Token Bucket Landasan Teori," *JUSI*, vol. 1, no. 2, pp. 93–104, 2011.
- [8] F. Albanna and I. Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 1, pp. 173–178, 2017.
- [9] H. Wintolo, I. Riadi, and A. Yudhana, "Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 11, pp. 2323–2331, 2025, doi: <https://doi.org/10.18280/ijssse.151112>.
- [10] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack using Open Web Application Security Project (OWASP) Framework," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 6, pp. 1363–1371, 2017.

-
- [11] T. Rochmadi, I. Riadi, and P. Yudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Appl.*, vol. 164, no. 8, pp. 31–37, 2017.
 - [12] S. Rudrakar, P. Rughani, and L. Sadineni, "Digital forensics and incident response management model for IoT based agriculture," *Sci. Rep.*, pp. 1–23, 2025, doi: <https://doi.org/10.1038/s41598-025-02635-2>.
 - [13] P. Widiandana and I. Riadi, "Forensik Digital Cyberbullying pada Grup WhatsApp Menggunakan National Institute of Standards and Technology," *Insect (Informatics Secur. J. Tek. Inform.*, vol. 12, no. 01, 2026, doi: <https://doi.org/10.33506/insect.v12i01.5275>.
 - [14] R. Umar, I. Riadi, and R. S. Kusuma, "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method," *Int. J. Informatics Dev.*, vol. 10, no. 1, pp. 53–61, 2021, doi: <https://doi.org/10.14421/ijid.2021.2423>.
 - [15] I. Riadi, Sunardi, and Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *JURTI*, vol. 3, no. 1, pp. 87–95, 2019.
 - [16] M. Campoverde-molina, "Computers & Security Cybersecurity in smart agriculture : A systematic literature review," *Comput. Secur.*, vol. 150, no. December 2024, 2025, doi: <https://doi.org/10.17632/5ddfvwfj9p.1>.
 - [17] I. Riadi and R. Umar, "Experimental Study of Honeypot-Based Cyber Attack and Data Collection in Campus Network Environment," *Int. J. Informatics Comput.*, vol. 8, no. 1, 2026, doi: 10.35842/ijicom.
 - [18] I. Riadi, S. Winiarti, H. Yuliansyah, and M. 'Arif Bin Mohamad, "Machine Learning Model for Classifying the Severity Level of Cyber Security Attacks," *Int. J. Adv. Intell. Informatics*, 2026, doi: https://ijain.org/index.php/IJAIN/article/view/2245%7Cto_array%3A0.
 - [19] R. Singh, D. Kukreja, and D. K. Sharma, "Blockchain-enabled access control to prevent cyber attacks in IoT: Systematic literature review," *Front. Big Data*, 2023, doi: <https://doi.org/10.3389/fdata.2022.1081770>.
 - [20] A. Kurniawan and I. Riadi, "Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior," *Int. J. Netw. Secur.*, vol. 20, no. 5, pp. 836–843, 2018, doi: DOI: 10.6633/IJNS.201809 20(5).04.
 - [21] M. K. Umair and M. S. Khan, "Systematic Literature Review on Blockchain Based IoT Solutions," *ICCK Trans. Adv. Comput. Syst.*, 2026, doi: <http://dx.doi.org/10.62762/TACS.2025.327681>.
 - [22] A. Naseer, M. Shmoon, T. Shakeel, S. U. Rehman, A. Ahmad, and V. Gruhn, "A Systematic Literature Review of the IoT in Agriculture—Global Adoption, Innovations, Security, and Privacy Challenges," *IEEE Access*, vol. 12, pp. 60986–61021, 2024, doi: 10.1109/ACCESS.2024.3394617.
 - [23] A. Akinbi and A. M. Ismael, "Forensic Science International : Digital Investigation A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models," vol. 43, 2022, doi: 10.1016/j.fsidi.2022.301470.
 - [24] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, pp. 219–227, 2018, doi: <http://dx.doi.org/10.28932/jutisi.v4i2.769>.
 - [25] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," *Prosiding*, vol. 2, no. 1, pp. 159–163, 2016.
 - [26] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors*, pp. 1–43, 2022, doi: <https://doi.org/10.3390/s22155641>.
 - [27] N. M. Banua and Q. W. Boon, "Blockchain for Security and Privacy: A Systematic Literature Review," *Appl. Inf. Technol. Comput. Sci.*, vol. 5, no. 1, pp. 1360–1382, 2024, doi: <https://doi.org/10.30880/aitcs.2024.05.01.078>.
 - [28] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, and E. Albassam, "Blockchain-Based Secured Access Control in an IoT System," *Appl. Sci.*, pp. 1–16, 2021, doi:
-

- <https://doi.org/10.3390/app11041772>.
- [29] R. Mubarak, I. Riadi, and T. Sutikno, "Integration of blockchain and cryptographic algorithms for education certification and verification : a systematic literature," *J. Soft Comput. Explor.*, 2026, doi: <https://doi.org/10.00000/joscex.0000.00.00.000>.
 - [30] A. Odeh and A. A. Taleb, "Federated Learning and Blockchain Framework for Scalable and Secure IoT Access Control," *Comput. Mater. Contin.*, vol. 84, no. 1, pp. 447–461, 2025, doi: <https://doi.org/10.32604/cmc.2025.065426>.
 - [31] S. A. Fadhel and A. S. Nori, "Lam-Iot : Lightweight Authentication Model for Monitoring Systems in Iot-Enabled Smart Homes Based on Did Using Iota," *Int. J. Comput. Digit. Syst.*, vol. 18, no. 1, pp. 1–13, 2025, doi: <http://dx.doi.org/10.12785/ijcds/1571111345>.
 - [32] M. M. Merlec and H. P. In, "SC-CAAC: A Smart-Contract-Based Context-Aware Access Control Scheme for Blockchain-Enabled IoT Systems," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19866–19881, 2024, doi: 10.1109/JIOT.2024.3371504.
 - [33] M. Usman, M. S. Sarfraz, M. U. Aftab, U. Habib, and S. Javed, "A Blockchain Based Scalable Domain Access Control Framework for Industrial Internet of Things," *IEEE Access*, vol. 12, pp. 56554–56570, 2024, doi: 10.1109/ACCESS.2024.3390842.
 - [34] A. Ferrer-Rojas, B. T. Maharaj, and M. C. Hlophe, "Blockchain-Enhanced Attribute-Based Encryption Architecture With Feasibility Analysis," *IEEE Access*, vol. 13, pp. 57629–57638, 2025, doi: 10.1109/ACCESS.2025.3554643.
 - [35] H. Cheng and J. Lu, "Blockchain-assisted attribute-based multi-keyword search for dynamic encrypted data in cloud-edge-IoT," *Internet of Things*, vol. 36, no. December 2025, p. 101838, 2026, doi: 10.1016/j.iot.2025.101838.
 - [36] P. Liu, Q. He, B. Zhao, B. Guo, and Z. Zhai, "Efficient Multi-Authority Attribute-Based Searchable Encryption Scheme with Blockchain Assistance for Cloud-Edge Coordination," *Comput. Mater. Contin.*, 2023, doi: 10.32604/cmc.2023.041167.
 - [37] D.-M. Ngo, D. Lightbody, A. Temko, C. C. Murphy, and E. Popovici, "A Scalable Security Approach in IoT Networks: Smart Contracts and Anomaly-Based IDS for Gateways Using Hardware Accelerators," *IEEE Access*, vol. 12, pp. 159519–159533, 2024, doi: 10.1109/ACCESS.2024.3486605.
 - [38] Y. Ding, J. Yu, S. Li, H. Sato, and M. G. Machizawa, "Data Aggregation Management With Self-Sovereign Identity in Decentralized Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 6, pp. 6174–6189, 2024, doi: 10.1109/TNSM.2024.3451995.
 - [39] A. A. M. Sharadqh *et al.*, "Hybrid Chain : Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment," *IEEE Access*, vol. 11, no. March 2023, pp. 27433–27449, 2025, doi: 10.1109/ACCESS.2023.3256277.
 - [40] Y. Kunwei, Y. Bo, W. Tao, and Z. Yanwei, "Zero-Cerd : A Self-Blindable Anonymous Authentication System Based on Blockchain," vol. 32, no. 3, 2023, doi: 10.23919/cje.2022.00.047.
 - [41] U. Khalil *et al.*, "Extending ERC721 : Design and implementation of a novel secure NFT framework for IoT asset authentication in cyber-physical systems," *Blockchain Res. Appl.*, vol. 7, no. 2, p. 100456, 2026, doi: 10.1016/j.bcr.2026.100456.
 - [42] S. Suhail, M. Iqbal, R. Hussain, S. Ur, R. Malik, and R. Jurdak, "TRIPLE: A blockchain-based digital twin framework for cyber – physical systems security," *J. Ind. Inf. Integr.*, vol. 42, no. July 2023, p. 100706, 2024, doi: 10.1016/j.jii.2024.100706.
 - [43] P. S. Akshatha and S. M. D. Kumar, "MQTT and blockchain sharding : An approach to user-controlled data access with improved security and efficiency," *Blockchain Res. Appl.*, vol. 4, no. 4, p. 100158, 2023, doi: 10.1016/j.bcr.2023.100158.
 - [44] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology," *IEEE Access*, vol. 11, pp. 36379–36398, 2023, doi: 10.1109/ACCESS.2023.3265349.
 - [45] I. Mustafa, A. Salimi, and M. Scriney, "Secure IoT Communication and Policy Enforcement Framework (SCOPE)," *IEEE Internet Things J.*, vol. 13, no. 3, pp. 4546–

-
- 4563, 2026, doi: 10.1109/JIOT.2025.3633459.
- [46] I. Kulkarni, G. Rathee, C. Abdelaziz, and N. Jaglan, "Adaptive ML-blockchain framework for intrusion detection and trust management in IoT networks," *Sustain. Cities Soc. Adv.*, vol. 2, no. 2, p. 100055, 2026, doi: 10.1016/j.scsadv.2026.100055.
 - [47] Z. Gao and W. Yan, "The real-time data processing framework for blockchain and edge computing," *Alexandria Eng. J.*, vol. 120, pp. 50–61, 2025, doi: <https://doi.org/10.1016/j.aej.2025.01.092>.
 - [48] H. Huang, P. Ye, M. Hu, and J. Wu, "A multi-point collaborative DDoS defense mechanism for IIoT environment," *Digit. Commun. Networks*, vol. 9, no. 2, pp. 590–601, 2023, doi: 10.1016/j.dcan.2022.04.008.
 - [49] G. Baralla, L. Cocco, M. Di Francesco, and R. Tonelli, "Integrating Blockchain, SSI, and RBAC for the Secure Management of Defense Heritage Buildings," *IEEE Access*, vol. 13, pp. 86290–86307, 2025, doi: 10.1109/ACCESS.2025.3570809.
 - [50] M. M. Asiri, H. Alfraihi, and Y. Said, "Securing Consumer Electronics Devices : A Blockchain-Based Access Management Approach Enhanced by Deep Learning Threat Modeling for IoT Ecosystems," *IEEE Access*, vol. 12, no. July, pp. 110671–110680, 2024, doi: 10.1109/ACCESS.2024.3441094.
 - [51] S. Siddiqui, S. Hameed, S. Attique, J. Arshad, and Y. Ahmed, "A smart-contract-based adaptive security governance architecture for smart city service interoperations," *Sustain. Cities Soc.*, vol. 113, no. December 2023, p. 105717, 2024, doi: 10.1016/j.scs.2024.105717.
 - [52] W. Jiang, Z. Lin, and J. Tao, "An access control scheme for distributed Internet of Things based on adaptive trust evaluation and blockchain," *High-Confidence Comput.*, vol. 3, no. 1, p. 100104, 2023, doi: 10.1016/j.hcc.2023.100104.
 - [53] V. Dineshbabu and M. Vigenesh, "SecureFLACF : Secure Federated Learning Access Control Framework with Blockchain-Infused Intrusion Detection System for IIoT," vol. 21, pp. 939–966, 2025, doi: 10.13052/jmm1550-4646.2155.
 - [54] C. Beis-penedo, R. P. Díaz-redondo, A. Fernández-vilas, M. Fernández-veiga, and F. Troncoso-pastoriza, "HLF-FSL : A decentralized federated split learning solution for IoT on hyperledger fabric," *Array*, vol. 29, no. January, p. 100685, 2026, doi: 10.1016/j.array.2026.100685.
 - [55] W. Issa, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "DT-BFL: Digital Twins for Blockchain-enabled Federated Learning in Internet of Things networks," *Ad Hoc Networks*, vol. 178, p. 103934, 2025, doi: <https://doi.org/10.1016/j.adhoc.2025.103934>.
 - [56] D. Bernal, O. Ledesma, P. Lamo, and J. Bermejo, "IOTA-Based Authentication for IoT Devices in Satellite Networks," *Comput. Mater. Contin.*, 2025, doi: 10.32604/cmc.2025.069746.
 - [57] V. Dineshbabu and M. Vigenesh, "SecureFLACF: Secure Federated Learning Access Control Framework with Blockchain-Infused Intrusion Detection System for IIoT," *J. Mob. Multimed.*, vol. 21, no. 5, pp. 939–966, 2025, doi: 10.13052/jmm1550-4646.2155.
 - [58] S. K. Lee, M. M. Merlec, N. K. Sinai, S. Hong, and H. P. In, "ZK-Sandbox : Zero-Knowledge Data Sandbox System for Enhancing End-to-End Security and Privacy of Verifiable Credentials," *IEEE Internet Things J.*, vol. PP, no. X, p. 1, 2026, doi: 10.1109/JIOT.2026.3662381.
-