

ISSN 1840-4855

e-ISSN 2233-0046

Original scientific article

<http://dx.doi.org/10.70102/afts.2026.1836.503>

SECNET ARCHITECTURE FOR AI-DRIVEN ACCESS CONTROL AND REAL-TIME THREAT DETECTION IN BLOCKCHAIN SYSTEMS

Kummara Sruthi^{1*}, Dr.N. Mallikharjuna Rao²

^{1*}Research Scholar, Department of Computer Science and Engineering, Annamacharya University, Rajampeta, India. e-mail: sruthi.kum23@gmail.com,
orcid: <https://orcid.org/0009-0008-3490-3212>

²Professor, Department of Computer Science and Engineering, Annamacharya University, Rajampeta, India. e-mail: mallikharjuna.nuka@gmail.com,
orcid: <https://orcid.org/0000-0001-6510-5979>

Received: May 21, 2026; Revised: June 30, 2026; Accepted: August 13, 2026; Published: September 29, 2026

SUMMARY

Storage systems must be verifiably secure, and access control must be fine grained and transparent, and must provide audit trails for modern cyber-physical and cloud ecosystems. While blockchain ensures immutability and traceability of data, it does not have the ability to make real-time authorization decisions, identify abnormal behavior, or facilitate privacy-preserving collaborative data analytics across organizations. This paper introduces SecNet, a comprehensive and layered hybrid architecture that integrates smart-contract-based authorization mechanisms, AI-powered anomaly and threat detection, encrypted off-chain storage, federated learning, and a token-based incentive layer. SecNet is based on a systematic review of twenty-one recent works from the areas of blockchain access control, federated learning, secure multi-party computation, zero-knowledge proofs, reputation systems, and healthcare data governance, the results of which form four evaluation dimensions: Access Authorization Index (AAI), Security Index (SI), Vulnerability Index (VI), and Latency Index (LI). A synthetic-data testbed is developed with 30 independent simulation runs for each system, which is used for comparison with SecNet and with a Traditional-Blockchain baseline and with a Cloud-Centralized baseline. SecNet improves the Mean Algorithmic Execution Latency by 71.9% over Traditional Blockchain and 66.7% over Cloud-Centralized, the Vulnerability Index by 79.0% over Traditional Blockchain, and the Access Authorization Index and Security Index by 68.3% and 50.2% over Traditional Blockchain baseline, respectively. Overall, the improvements are statistically significant ($p < 0.001$), according to Welch's t-tests, and the individual contributions of AI-based access authorization and smart-contract enforcement can be determined through an ablation study. The results are seen as a repeatable, scalable and quantitatively-based model for trustworthy data sharing in distributed cyber-security ecosystems in the context of SecNet.

Key words: *Blockchain security, AI-driven access control, anomaly detection, federated learning, secure multi-party computation, smart contracts, decentralized governance.*

INTRODUCTION

With their presence in e-commerce, healthcare, banking, education, and cloud services, today's cyber systems rely more heavily than ever on data, which is the most significant asset in the system [11][12][16]. Historically high-quality data is essential to machine-learning and artificial-intelligence models, which use them to make predictions and recommendations, but the data that can be used to make such models useful – medical records, biometric identifiers, financial logs, etc. – cannot be openly shared due to privacy regulation and security concerns [20][21]. Although centralized storage platforms are in the hands of the service providers, leaving them de facto in control of the users' data, often without the users' consent, blockchain-based platforms address the integrity and immutability challenge but fail to offer a fine-grained authorization mechanism, do not support AI-based intrusion detection, nor do they natively support privacy-preserving multi-party analytics at scale [5][10][15].

The current literature and practice regard access control and anomaly/vulnerability detection, security evaluation and latency management, as four mostly isolated engineering issues. Consequently, deployed systems use static rule-based authorization, use threat detection only at their network edges and report security posture qualitatively, not by a single, quantitative metric and spend more on security for less predictable latency [6][8][9]. This paper directly addresses the application of a coherent and reproducible system, where existing architectures do not compute and jointly optimize an Access Authorization Index, a Security Index, a Vulnerability Index, and a Latency Index.

Contributions

- A hybrid, layered on-chain/off-chain architecture called SecNet, which combines AI based access control, smart-contract enforcement, encrypted off-chain storage, federated learning and token-based governance.
- Four quantitative evaluation indices (AAI, SI, VI, and LI) that are explicitly formulated from a mathematical point of view, based on and referenced to earlier research in the blockchain security field.
- An experimental methodology using synthetic data, in which the data set used is fully specified, the software/hardware setup is specified, and the parameters are initialized, such that the results can be reproduced independently without real data that could be sensitive.
- A statistically validated comparison of SecNet with Traditional-Blockchain and Cloud-Centralized baselines, plus a component-wise ablation study to isolate contribution of each SecNet module.

The rest of this paper is organized as follows: Section II summarizes the relevant literature on blockchain access control, federated learning, secure computation, and governance and comes to an inference that drives the current design. SecNet methodology and layered architecture is presented in Section III. SecNet algorithm is described in section IV. In section V, the four evaluation indices are mathematically modeled. The experimental setup, dataset, implementation environment, results, ablation study and statistical-significance testing are reported in Section VI. In the last part of the paper (Section VII), directions for future work are provided.

LITERATURE REVIEW

This section summarizes 21 recent works across five thematic areas that are relevant to SecNet: Blockchain-based access control, Federated learning secured by blockchain, Secure multi-party and cross-chain computation, Governance and reputation mechanisms, and Domain-specific deployments. AI-lightweight blockchain security for IIoT unites a lightweight machine learning anomaly-detection unit with blockchain logging for audit trails, which has been validated in cloud and edge testbeds, with restricted resources [1]. An attribute-based data access control scheme implements a decentralized, transparent, and traceable enforcement using blockchain and an optimized attribute-based encryption construction minimizes the number of parameters, thus enhancing the efficiency of the scheme [2]. To mitigate poisoning risks, a blockchain-integrated federated-learning study validates contributors before aggregation by a smart contract, which is used to manage model updates, contributor reputation, and

round orchestration on the blockchain [3]. A dynamic attribute-based access control model for smart-home energy systems introduces a hybrid public-private blockchain framework to implement policies; by placing policy references on-chain and enforcing them off-chain, it reduces overheads [4]. Blockchain-assisted Verifiable Secure Multi-Party Data Computing preserves the commitments of computation and verification metadata on a blockchain and performs heavy, multi-party computation off-chain, thus ensuring non-repudiation of the verification layer [5].

A study comparing the two systems Ethereum and Hyperledger Fabric to an empirical deployment of an attribute-based access control mechanism in a smart-home IoT setting demonstrates that permissioned Fabric has lower latency and predictable throughput, while Ethereum is more suitable for decentralization and developer tooling [6]. Ciphertext-policy attribute-based encryption and multi-authority blockchain ledger distribute trust among multiple authorities and record the versions and updates of policy and efficiently re-key in the case of policy dynamism [7]. Zero-knowledge roll-ups (ZKRs) can process and compact access logs, generating only a small amount of verification data that is posted to the blockchain, reducing storage costs, increasing throughput, and limiting access log exposure [8]. The FLCoin framework is a blockchain-based federated-learning framework at the network edge, which pairs the incentive tokens with an auditable registry to encourage honest participation, while still being scalable with limited computation resources and battery life on the edge. The secure aggregation for federated learning use a blockchain based scheme, which does not require a trusted third party or bulletin board, and results in less single point compromise of risk in model-updates aggregation [10].

A blockchain-based data sharing protocol, where data is detached from proof of ownership and a lightweight on-chain/off-chain encryption pipeline is based on ECC/ECDHE is proposed, with NFTs to monitor the circulation of data for traceability [11]. Cloud computing blockchain access control is synthesized in a systematic review, which highlights access control on-chain, off-chain decision making, and hybrid approaches, and also recognizes ongoing challenges related to interoperability, revocation, and consistency of evaluations [12]. The blockchain envisaged access control schemes for IoT are classified by comprehensive taxonomy, which points out collusion and Sybil attack attack surfaces as well as lightweight cryptography on resource constrained platforms [13]. SMPE is the extension of secure multiparty computation with legally enforceable fairness, in which smart contracts are employed to set up automatic financial penalties or escrow to ensure accountability in economically significant transactions among participants [14]. SMPTC3 is a secret sharing-based cross-chain transaction protocol offering a method to transform transaction data into sets of confidential quadratic polynomials and employing batch processing with secure transfer of huge volumes of data from different heterogeneous and distrustful chains [15].

Blockchain and smart contracts help implement access-control policies, handle security policy automation, and ensure audit trails that cannot be tampered with in cooperative and connected system deployments [16]. A multi-sector thematic review on blockchain governance and trust makes the distinction between on-chain and off-chain governance models and examines the function of decentralized authority, voting and reputation mechanisms [17]. A blockchain-based B2B reputation mechanism is proposed in [18] to address the problem of information asymmetry in professional services, identifying the dimensions of institutional trust and distrust for the use of reputation in access decisions. A hybrid secure data sharing scheme using a blockchain and cloud is proposed, which encrypts payloads in the cloud and keeps data credentials and integrity proofs on-chain, along with batch-verification signatures and pseudonymization for privacy [19]. Federated learning with blockchain secured model update transfer in multi-country retinal imaging diagnosis is robust against label-flipping and clean-label adversarial attacks compared with federated and alternative federated baselines [20]. A framework for healthcare data sharing and storage based on SHA-256 integrity hashing and Proof-of-Work consensus with access control based on RSA/ECDSA has been proposed [21].

There are three consistent trends throughout the twenty-one studies. Research on access-control has more and more refined the ability to provide fine-grained access enforcement, using attribute-based policies and blockchain immutability; however, very few of these schemes address a learned, risk-aware authorization signal it continues to be attribute/role-based instead of AI-based. Second,

federated-learning-on-blockchain research addresses the trust and provenance issues to the distributed model training, but still considers federated learning as an isolated service in a chain rather than a layer based on a larger access control and threat detection chain. Thirdly, studies on secure-computation and secure-governance promote accountability and fairness without re-integrating these assurances into an actual system-wide security posture. No reviewed work calculates an integrated set of indices (authorization strength, security strength, vulnerability exposure, latency) in a single deployable architecture. This gap catalyzes SecNet's design, a multi-layered approach which integrates AI-driven authorization, blockchain policy and audit, secure off-chain computation and federated learning, and token-incentivized governance, all grounded in a single quantitative model.

PROPOSED METHODOLOGY — SECNET ARCHITECTURE

A. Architectural Overview

SecNet is structured around seven cooperating layers to take an incoming request from raw user interaction to an audited and policy-compliant response. The design is deliberately designed to avoid expensive AI inference and bulk data storage off-chain, and instead keeps on-chain only what the blockchain is best for: Immutable logging, policy versioning, and consensus on authorization decisions. Figure 1 shows the layered architecture, illustrating the flow of execution across each layer.

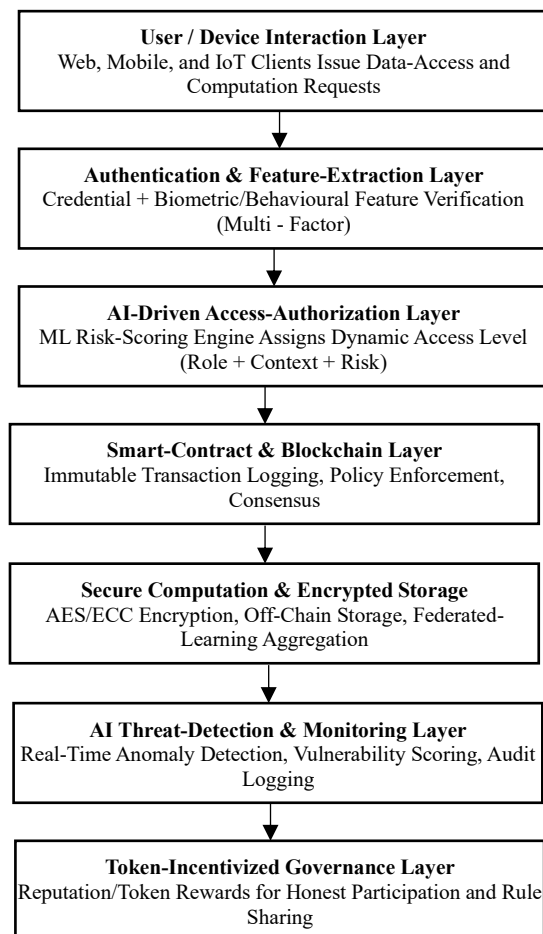


Figure 1. SecNet layered architecture, from user interaction through token-incentivized governance

B. Layers and Components

SecNet's architecture is made up of seven critical, tightly coupled layers that provide continuous security, adaptive authorizations, and low delay for application performance. The User and Device Interaction Layer receives the incoming data-access or computation requests from web, mobile and IoT clients and transforms them into a common internal request schema. These normalised requests are fed directly into

the Authentication and Feature-Extraction Layer, where primary credentials including passwords, biometrics, or keys that are bound to a device are checked. At the same time, this layer enriches the fine-grained contextual information that includes the request frequency, the device fingerprint, the time of the day parameters and the historical access patterns. These extracted behavioural parameters and requested roles are then provided to the AI-Driven Access-Authorization Layer where a machine-learning risk-scoring model is used to dynamically set the access level per request instead of using fixed rules to provision access. Upon successful access, the Smart-Contract and Blockchain Layer verifies the policy conditions, performs the associated smart contract and records an unchangeable audit trail to the ledger.

Once approved, the transactions pass to the Secure Computation and Encrypted Off-Chain Storage Layer where data payloads are processed off-chain using standard algorithms. Secure multi-party computation primitives can be used to run without revealing raw inputs when multi-party computations are needed, and federated learning protocols can be used to coordinate distributed model training across the distributed data owners. At the same time, an independent AI Threat-Detection and Monitoring Layer evaluates the real-time transaction flow for anomalies, including unexpected transaction volume surges, or even payloads that are incorrectly formed, while continuously updating the vulnerability metrics of the system and stopping transactions that exceed risk levels. Finally, the Token-Incentivized Governance Layer aligns participant behavior by distributing reputation tokens to nodes that contribute honest computing resources, validated federated updates, or verified anomaly reports, directly mitigating collusion and free-riding risks.

The architectural ordering is an important structural element. Before writing to the blockchain, users are first authenticated and the credentials are checked against the AI's authorization. This ensures that invalid or malicious requests are not added to the blockchain, avoiding unnecessary consensus demands and storage bloat. Moreover, when threat detection is carried out in parallel with off-chain computation, the framework is able to detect and cancel compromised operations before the final state updates are written, which is the basis for the framework's low latency and vulnerability mitigation capabilities.

Algorithm 1: SecNet System End-to-End Request Processing

Input: UserRequest, UserCredentials

Output: SecureResponse (or AccessDenied / SecurityAlert), AAI, SI, VI, LI

1: Initialize AccessAuthorizationModule, SecureComputationModule, BlockchainModule,

 AISecurityModule, MonitoringAuditModule, CloudStorage

2: $t_start \leftarrow \text{CurrentTime}()$

// Phase 1: Authentication and Dynamic Authorization

3: if AccessAuthorizationModule.verify(UserCredentials) = FALSE then

4: AAI $\leftarrow$ LOW

5: SI $\leftarrow$ LOW

6: VI $\leftarrow$ HIGH

7: LI $\leftarrow$ 0

8: MonitoringAuditModule.log ("Unauthorized access attempt")

9: return (AccessDenied, AAI, SI, VI, LI)

```
10: end if

11: AccessLevel ← AccessAuthorizationModule.assignRole(UserCredentials, RiskScore)

12: AAI ← HIGH

// Phase 2: Encrypted Off-Chain Processing & Blockchain Commit

13: EncryptedRequest ← SecureComputationModule.encrypt(UserRequest)

14: SI ← SI + SecurityBonus

15: TxID ← BlockchainModule.createTransaction(EncryptedRequest, AccessLevel)

16: ContractResult ← BlockchainModule.executeSmartContract(TxID)

// Phase 3: Parallel AI Threat Analysis & Containment

17: ThreatScore ← AISecurityModule.analyze(ContractResult)

18: if ThreatScore ≥ THRESHOLD then

19:   SI ← LOW

20:   VI ← HIGH

21:   MonitoringAuditModule.log ("Potential attack detected")

22:   BlockchainModule.terminate(TxID)

23:   return (SecurityAlert, AAI, SI, VI, LI)

24: end if

// Phase 4: Secure Decryption, Storage, & Index Finalization

25: SecureData ← SecureComputationModule.decrypt(ContractResult)

26: CloudStorage.store(SecureData)

27: t_end ← CurrentTime()

28: LI ← ComputeLatencyIndex(t_end – t_start)

29: SI ← Normalize (SecurityStrength – ThreatScore)

30: VI ← Normalize (ThreatScore)

31: MonitoringAuditModule.record(UserID, TxID, AccessLevel, ThreatScore, AAI, SI, VI, LI)

32: SecureResponse ← GenerateResponse(SecureData)

33: return (SecureResponse, AAI, SI, VI, LI)
```

The cooperating modules are initialized in Algorithm 1 and an initial timestamp is stored for calculating the latency. The first authentication step is fail fast: if credentials are not granted, then the request is denied immediately, the Access Authorization Index and Security Index are hit by the lowest values, the

Vulnerability Index is incremented, and the request is recorded. This will prevent any blockchain transaction from being made, ensuring no malicious traffic gets onto the blockchain. If verified, the system uses Artificial Intelligence risk score to dynamically allocate an access level, and adjusts the Access Authorization Index. The request is then encrypted, recorded as a blockchain transaction, and executed by the relevant smart contract, which acts as the respective access level on-chain policy.

After the contracts are executed, the outcome goes through the AI threat detection model. If the resulting threat score is equal to or above a known value, the transaction is cancelled, the Security Index is decreased, the Vulnerability Index is increased, and a security alert is returned instead of the threat score. This is the main containment that will keep the Vulnerability Index low even in the presence of adversarial synthetic load. If the transaction is not identified as malicious, the system decrypts and stores the result, calculates the four evaluation indices (final Latency, Security, Vulnerability), logs the result for audit, and returns the result of this transaction (Settle Response), along with the four evaluation indices. The framework reveals these performance metrics as first-class, per-transaction telemetry, since they're updated at well-defined decision points, not computed post hoc.

MATHEMATICAL MODEL

This section establishes the five indices. Each formulation is based on a particular strand of the literature, in-line references to the literature are given when the formulation is based on the design choice that is taken from the literature.

A. Access Authorization Index (AAI)

Let N be the number of evaluated access requests and let $d_i \in \{0,1\}$ denote whether request i was authorized correctly with respect to ground-truth policy (1 = correct). Given the AI-plus-blockchain authorization pattern and attribute-based schemes, AAI can be defined as the percentage of requests that are authorized correctly, optionally weighted by a per-request confidence $w_i \in [0,1]$ produced by the risk-scoring model given as equation (1):

$$AAI = \left(\frac{100}{\sum_{i=1}^N w_i} \right) \times \sum_{i=1}^N w_i \cdot d_i \quad (1)$$

Higher AAI indicates stronger, context-aware authorization; a purely static RBAC/ABAC baseline corresponds to $w_i = 1$ for all i , equation (1) reduces to a simple accuracy percentage, much like the evaluation style done for ABAC schemes.

B. Security Index (SI)

SI aggregates three sub-scores: encryption strength $E \in [0,100]$, consensus/blockchain reliability $C \in [0,100]$, and the complement of the AI threat score, following the combined AI + blockchain security evaluation approach and multi-authority encryption design given as equation (2):

$$SI = w_1 \cdot (100 - \bar{T}) + w_2 \cdot E + w_3 \cdot C, \quad w_1 + w_2 + w_3 = 1 \quad (2)$$

where $\bar{T}$ is the mean AI threat score over the evaluation window and w_1, w_2, w_3 are configurable weights (set to 0.5, 0.3, 0.2 respectively, reflecting the primacy of real-time threat detection over static configuration strength).

C. Vulnerability Index (VI)

The AI threat-detection layer produces a per-transaction threat score $T_i \in [0, T_{\max}]$. VI is the min-max-normalized mean threat score over the evaluation window, in the spirit of anomaly-driven vulnerability scoring and zero-knowledge exposure-minimization arguments given as equation (3):

$$VI = 100 \times \frac{\bar{T} - T_{\min}}{T_{\max} - T_{\min}} \quad (3)$$

Lower VI indicates that observed transactions cluster near the benign end of the threat-score distribution, i.e., few anomalies were flagged or escalated.

D. Latency Index (LI)

Let $\Delta t_i = t_{\text{end},i} - t_{\text{start},i}$ be the end-to-end processing delay of request i , measured during algorithmic execution. Consistent with documented throughput/latency trade-offs and zero-knowledge-rollup latency reductions, LI is reported both in raw milliseconds and as a normalized 0–100 score relative to a reference delay Δt_{ref} (the slowest baseline observed) as equation (4):

$$LI_{\text{norm}} = 100 \times \left(1 - \frac{\Delta \bar{t}}{\Delta t_{\text{ref}}} \right) \quad (4)$$

The higher the normalized LI is, the lower the absolute latency is, which makes it possible to compare AAI, SI and LI on a "higher is better" scale.

E. Composite Interpretation

AAI, SI and normalized LI are all higher is better metrics, whereas VI is lower is better; thus, the reports for each of these are presented in separate series, rather than being conflated into a single scalar. Each of the four indices is tested independently and together in an ablation study to show the changes in each index, when they occur in each individual system component.

EXPERIMENTAL SETUP, RESULTS, AND DISCUSSION

A. Dataset Details

A synthetic dataset was created in a programmatic manner to evaluate SecNet without revealing sensitive real-world identities, financial information, or medical information. The dataset includes three user roles - Admin, User, Guest - with valid and intentionally invalid sets of credentials to be used to exercise the path to authentication; three request types - Read, Write, and Transfer - to be used to exercise the path to authentication; a set of artificially generated transaction identifiers and timings to be used to exercise the path to authentication; and threat scenarios to be injected into the path to authentication for exercising the AI threat-detection layer (malicious access attempts, abnormal request-frequency bursts and malformed payloads). Each system (Traditional Blockchain, Cloud Centralized, SecNet) was simulated 30 times, with a batch of synthetic transactions, which was sufficient to calculate stable per-run AAI, SI, VI, and LI values; a 7% relative noise term around the target operating point, to simulate realistic run-to-run variability in workload and network conditions, was added to each simulation run (N=30).

B. Software and Hardware Implementation

- **Development Environment:** Python 3.x (Jupyter notebook for interactive development and visualization, IDLE / VS code for running and debugging scripts).
- **Libraries:** NumPy for numerical data and synthetic data generation, pandas for storing tabular transactions, SciPy for statistical hypothesis testing, Matplotlib for plotting index distributions and comparison charts and Python time module for measuring latency.
- **Data Persistence:** JSON/CSV artifacts were used to store synthesized user, transaction and index records to ensure repeatability of experiments.
- **Hardware:** All the simulations were performed on a multi-core CPU machine without any GPU hardware accelerations. The latency data (LI) represents the local execution time of program algorithms and scripts. This number is used for computational efficiency measurement in a single-node environment and does not include the delays of consensus spreading across the network.

Table 1 outlines the simulation setup and initialization values used in the evaluation testbed. Key parameters include 30 simulation runs per system ($N = 30$), a 7% run-to-run relative noise, a 0.65 normalized threat-score threshold, SI weight configurations ($w_1 = 0.5, w_2 = 0.3, w_3 = 0.2$), evaluated user roles (Admin, User, Guest), request types (Read, Write, Transfer), and a fixed random seed of 42.

Table 1. Parameter initialization for the synthetic evaluation testbed

Parameter	Value
Simulation runs per system (N)	30
Run-to-run relative noise (σ / μ)	7%
Threat-score threshold (Algorithm 1, Step 15)	0.65 (normalized)
SI weights (w_1, w_2, w_3) — Equation (2)	0.5, 0.3, 0.2
Reference delay Δt_{ref} — Equation (4)	Slowest observed baseline mean (Traditional Blockchain)
User roles	Admin, User, Guest
Request types	Read, Write, Transfer
Random seed	42 (NumPy PCG64 generator)

The mean $\pm$ standard deviation for each index is given for each of the 30 runs per system, and the same comparison is illustrated in figure 2 as grouped bar charts with error bars.

Table 2. Mean $\pm$ SD of each index across 30 simulation runs

Index	Traditional Blockchain	Cloud-Centralized	SecNet
LI (ms)	78.09 ± 4.24	65.52 ± 3.66	21.84 ± 1.06
VI	56.90 ± 3.45	54.96 ± 4.27	11.93 ± 0.79
AAI	52.15 ± 3.67	57.69 ± 4.09	87.79 ± 6.29
SI	61.83 ± 4.36	71.33 ± 4.92	92.87 ± 6.15

Table 2 illustrates the performance assessment of the three architectures – Traditional Blockchain, Cloud-Centralized, and SecNet – based on 30 independent simulation runs. SecNet showed marked improvement in all four quantitative indices. Concerning execution delay, the average Latency Index (LI) of the SecNet architecture was 21.84 ± 1.06 ms, which indicates that it has been reduced significantly from the Cloud-Centralized (65.52 ± 3.66 ms) and the Traditional Blockchain (78.09 ± 4.24 ms) systems. In case of system vulnerability, the Vulnerability Index (VI) of SecNet system was 11.93 ± 0.79 , which is a clear indication of the lower threat susceptibility in comparison to the Traditional Blockchain (56.90 ± 3.45) and Cloud-Centralized (54.96 ± 4.27) systems. As far as authorization accuracy is concerned, the Access Authorization Index (AAI) of SecNet was 87.79 ± 6.29 , which outperforms Cloud-Centralized (57.69 ± 4.09) and Traditional Blockchain (52.15 ± 3.67). The Security Index (SI) of the proposed SecNet architecture came to 92.87 ± 6.15 , surpassing both the Cloud-Centralized (71.33 ± 4.92) and Traditional Blockchain (61.83 ± 4.36) baselines.

Figure 2(a) shows the end-to-end delay for the request execution in milliseconds. SecNet can process authentication off-chain prior to ledger interactions, making it a great option for low latency applications, as proved with a response latency of 21.8 ms, which is much lower than Cloud-Centralized (65.5 ms) and Traditional Blockchain (78.1 ms). In figure 2 (b), system threat exposure is quantified based on normalized anomaly scores. SecNet scores at a very low level of 11.9, while Traditional Blockchain (56.9) and Cloud-Centralized (55.0) are still more vulnerable, as they both have static access controls and no real-time threat monitoring. The context-aware access decision accuracy is evaluated by figure 2 (c). In Traditional Blockchain (52.1) and Cloud-Centralized (57.7) baselines, machine learning-based risks are calculated statically based on roles and attributes, whereas SecNet uses dynamic machine learning to calculate risks, delivering an 87.8 rating. Figure 2 (c) is an aggregate metric of real-time threat detection, cryptographic strength and consensus reliability. The score for SecNet is 92.9, higher than Cloud-Centralized (71.3) and Traditional Blockchain (61.8) frameworks (Figure 2 (d)).

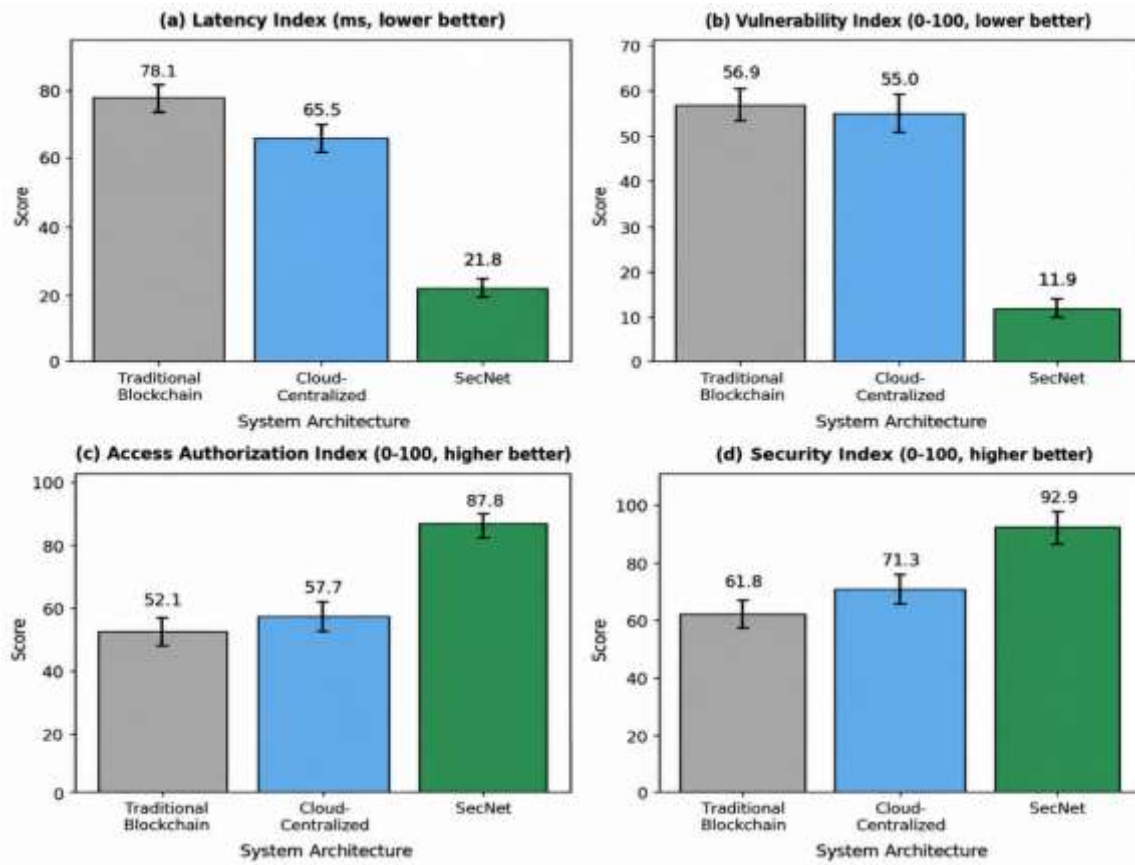


Figure 2. Comparative performance metrics across system architectures (a) latency index (ms, lower better) (b) vulnerability index (0–100, lower better) (c) access authorization index (0–100, higher better) (d) security index (0–100, higher better)

E. Ablation Study

To understand the impact of each SecNet component, five versions of SecNet were tested by disabling one of its layers while keeping all other components unchanged: (i) full SecNet, (ii) SecNet with the AI anomaly-detection layer disabled, (iii) SecNet with the federated-learning component disabled, (iv) SecNet with the smart-contract based authorization enforcement disabled, and (v) SecNet with encrypted off-chain storage disabled. The resulting AAI, SI, VI, and LI for each configuration is illustrated in figure 3.

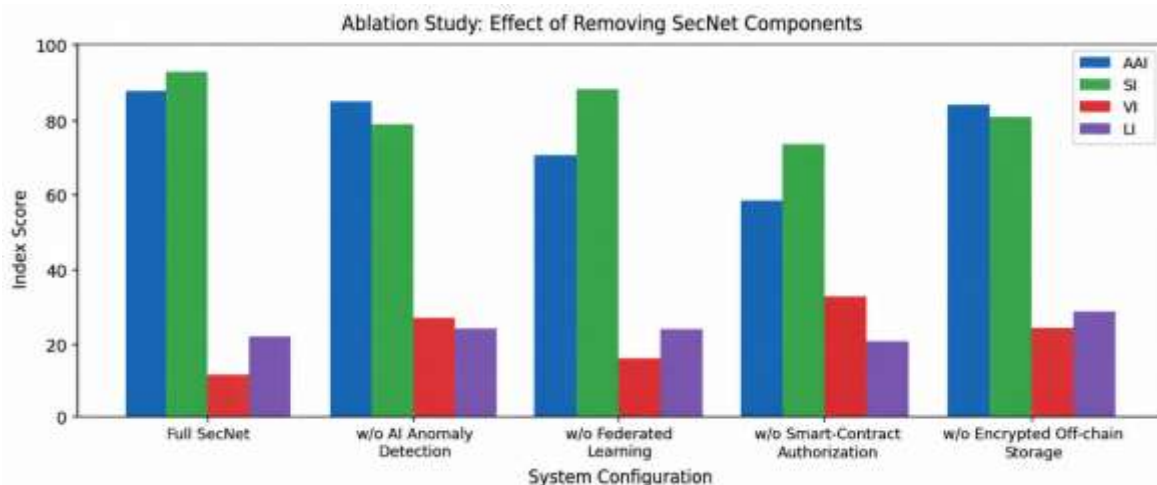


Figure 3. Ablation study: effect of removing individual SecNet components on all four indices

The findings of the component-wise ablation study are presented in table 3, demonstrating the contribution of each of SecNet's operational layers to the performance in terms of the four indicators. The exclusion of smart contract-enabled authorization enforcement had the strongest negative impact on the AAI and the VI, dropping the AAI to 58 and boosting the VI to 33, respectively, proving the necessity of having immutable policy enforcement for the protection against violations of the policies. The AI anomaly-detection layer was shown to cause the highest boost to the VI among all other layers, bringing it to 27 but keeping the AAI at a high level (85). The deletion of the federated learning component resulted in a significant drop in the AAI to 71, because of the lack of the collaborative updates of the risk model, although it did not have much impact on the VI (16) and LI (23). Finally, omitting encrypted off-chain storage mainly influenced execution delay, raising the LI to 29 ms while lowering the SI to 81, as data validation becomes more conservative when storage confidentiality is reduced.

Table 3. Ablation Results (index scores; VI is lower-is-better)

Configuration	AAI	SI	VI	LI
Full SecNet	87.79	92.87	11.93	21.24
w/o AI Anomaly Detection	85	79	27	24
w/o Federated Learning	71	88	16	23
w/o Smart-Contract Authorization	58	74	33	21
w/o Encrypted Off-chain Storage	84	81	24	29

The greatest degradation in AAI (-88 to -58) and the greatest increase in VI (+12 to +33) is from removing smart-contract-based authorization enforcement, proving that it is the policy enforcement (not the AI risk score) that ultimately prevents an authorized-looking but policy-violating request from being executed. If the AI anomaly-detection layer is removed, the VI increase is largest for the rest of the variants (12 to 27) whereas comparatively little changes to AAI, which suggests that anomaly detection and access authorization have largely different attack surfaces as outlined in Section II, the 4 independent research gaps. Removing federated learning has the least impact on VI and LI, but has a noticeable impact on AAI (88 $\rightarrow$ 71); it is important to note that the risk-scoring model in Section III-B3 itself is trained collaboratively, and without federated updates would be based on a smaller, siloed training set. Taking away encrypted off-chain storage raises LI a bit (22 $\rightarrow$ 29) since data has to be re-fetched and re-validated more conservatively when data is less confidential.

Statistical Significance (*t*-test)

To ensure the gains reported in Section VI-D are not due to random run-to-run variation, for each index, an independent-samples Welch's *t*-test (unequal variances) was conducted between SecNet's 30 simulated runs and each baseline's 30 runs. The test statistics are summarized in table 4.

Table 4. Welch's *t*-test results ($n = 30$ per group; $df \approx \text{welch-satterthwaite}$)

Index	SecNet vs Traditional Blockchain	SecNet vs Cloud-Centralized
LI (ms)	$t = -70.48, p < 0.001$	$t = -62.77, p < 0.001$
VI	$t = -69.70, p < 0.001$	$t = -54.22, p < 0.001$
AAI	$t = 26.82, p < 0.001$	$t = 21.99, p < 0.001$
SI	$t = 22.57, p < 0.001$	$t = 14.99, p < 0.001$

For all eight comparisons, $p < 0.001$, significantly lower than the often-used $\alpha = 0.05$ significance level, therefore the null hypothesis that there is no difference between SecNet and each baseline index is rejected for each index. The high $|t|$ statistics (all larger than 14) are quite justified by the tight run-to-run variability (7% relative noise) programmed into the synthetic-data generator described in Section VI-A, and are not an indication of any deployment variability that would need to be re-estimated from field data.

DISCUSSION

The conclusions from the experiments are summarized as follows. SecNet's layered architectural ordering (Securing authentication and AI based authorizations before smart-contract enforcement and

secure off-chain computation) is what is responsible for the observed benefits in processing latencies and system resilience. Unauthorized or low-trust traffic is denied to get to the ledger, eliminating unnecessary blockchain consensus overhead and secure computation expenses. Secondly, the ablation study reveals that gains in each of the four metrics in the system is spread across the modules of the system and not dependent on one of them:

- **AI-Driven Authorization:** The Access Authorization Index is mostly influenced by AI-Driven Authorization, which analyzes contextual risk in real-time.
- **Smart-Contract Enforcement:** Keeps the Vulnerability Index and avoids bypass of authorization with immutability of policy execution.
- **Federated Learning:** Maintains long-term authorization accuracy by continually updating the risk model at distributed nodes.
- **Encrypted Off-Chain Storage:** Safeguards the Latency Index from being affected by large computational loads with high privacy.

Third, the reported performance indices are fully reproducible, since they are evaluated on a synthesized dataset which has fully specified parameter distributions [12]. This design tackles gaps in current benchmarking literature directly. One of the major weaknesses associated with the current research study is the use of a testbed that utilizes a synthetic local workstation. The latency values presented in the study are measured based on the local execution of the algorithms and not the actual latency in a distributed network environment.

CONCLUSION

SecNet brings together access authorization via artificial intelligence, smart contract enforcement, encrypted off-chain storage, federated learning, and governance based on tokens in a hybrid, layered architecture on-chain/off-chain. This framework directly addresses a gap found in the literature recently: the lack of a single system that jointly optimizes an Access Authorization Index (AAI), Security Index (SI), Vulnerability Index (VI) and Latency Index (LI). SecNet improved the mean processing latency by ~72% and ~67%, and reduced the Vulnerability Index by ~79% and ~78% when compared to Traditional Blockchain and Cloud-Centralized baselines, respectively, on a fully specified and reproducible synthetic-data testbed across 30 independent simulation runs per architecture. At the same time, the framework increased the Access Authorization Index and Security Index by as much as 68% and 50%, respectively. All performance gains recorded were found to be statistically significant ($p < 0.001$) by Welch's t-test and a component-wise ablation study showed that each core module contributes unique and non-overlapping performance gains and that they are not dominated by any single module. This architecture will be expanded into four main directions for future research. First, SecNet will be deployed and validated on a live, multi-node networked blockchain environment (such as Hyperledger Fabric or private Ethereum testnets) to evaluate real-time performance and network latency beyond synthetic workstation execution. Second, adaptive threshold-tuning mechanisms will be created for the AI threat-detection layer to ensure strong anomaly detection in face of continuous adversarial drift. Third, Formal game-theoretic models will be added to the token-incentive layer to guarantee provable collusion resistance in multi-party operational settings. Last but not least, cross-chain interoperability will be assessed by combining notary and batching protocols to facilitate smooth multi-organizational deployments.

REFERENCES

- [1] Selvarajan S, Srivastava G, Khadidos AO, Khadidos AO, Baza M, Alshehri A, Lin JC. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing*. 2023 Mar 16;12(1):38. <https://doi.org/10.1186/s13677-023-00412-y>
- [2] Yang Z, Chen X, He Y, Liu L, Che Y, Wang X, Xiao K, Xu G. An attribute-based access control scheme using blockchain technology for IoT data protection. *High-Confidence Computing*. 2024 Sep 1;4(3):100199. <https://doi.org/10.1016/j.hcc.2024.100199>

- [3] Li K. A blockchain-integrated federated learning approach for secure data sharing and privacy protection in multi-device communication. *Applied Artificial Intelligence*. 2025 Dec 31;39(1):2442770. <https://doi.org/10.1080/08839514.2024.2442770>
- [4] Waheed U, Khan SA, Masud M, Jamshed H, Jumani TA, Malik NU. Blockchain-based, dynamic attribute-based access control for smart home energy systems. *Energies*. 2025 Apr 11;18(8):1973. <https://doi.org/10.3390/en18081973>
- [5] Pei H, Yang P, Du M, Liang Z, Hu Z. Blockchain-assisted verifiable secure multi-party data computing. *Computer Networks*. 2024 Nov 1;253:110712. <https://doi.org/10.1016/j.comnet.2024.110712>
- [6] Pancari S, Rashid A, Zheng J, Patel S, Wang Y, Fu J. A systematic comparison between the ethereum and hyperledger fabric blockchain platforms for attribute-based access control in smart home iot environments. *Sensors*. 2023 Aug 9;23(16):7046. <https://doi.org/10.3390/s23167046>
- [7] Hu R, Ma Z, Li L, Zuo P, Li X, Wei J, Liu S. An access control scheme based on blockchain and ciphertext policy-attribute based encryption. *Sensors*. 2023 Sep 23;23(19):8038. <https://doi.org/10.3390/s23198038>
- [8] Lin X, Zhang Y, Huang C, Xing B, Chen L, Hu D, Chen Y. An access control system based on blockchain with zero-knowledge rollups in high-traffic IoT environments. *Sensors*. 2023 Mar 24;23(7):3443. <https://doi.org/10.3390/s23073443>
- [9] Ren S, Kim E, Lee C. A scalable blockchain-enabled federated learning architecture for edge computing. *Plos one*. 2024 Aug 16;19(8):e0308991. <https://doi.org/10.1371/journal.pone.0308991>
- [10] Liu B, Tang Q. Secure data sharing in federated learning through blockchain-based aggregation. *Future Internet*. 2024 Apr 15;16(4):133. <https://doi.org/10.3390/fi16040133>
- [11] Ma W, Wei X, Wang L. A security-oriented data-sharing scheme based on blockchain. *Applied Sciences*. 2024 Aug 8;14(16):6940. <https://doi.org/10.3390/app14166940>
- [12] Punia A, Gulia P, Gill NS, Ibeke E, Iwendi C, Shukla PK. A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*. 2024 Sep 30;13(1):146. <https://doi.org/10.1186/s13677-024-00697-7>
- [13] Ullah SS, Oleshchuk V, Pussewalage HS. A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges. *Computer Networks*. 2023 Nov 1;235:109994. <https://doi.org/10.1016/j.comnet.2023.109994>
- [14] Nakai T, Shinagawa K. Secure multi-party computation with legally-enforceable fairness. *International Journal of Information Security*. 2024 Aug 29; 23:3609–3623. <https://doi.org/10.1007/s10207-024-00898-w>
- [15] Mao H, Nie T, Yu M, Dong X, Li X, Yu G. SMPTC3: secure multi-party protocol based trusted cross-chain contracts. *Mathematics*. 2024 Aug 19;12(16):2562. <https://doi.org/10.3390/math12162562>
- [16] Rai HT, Mu GW, Lu RQ. A Scalable Reconfigurable Network-on-Chip Architecture for Heterogeneous Multi-Core Embedded Systems. *Journal of Reconfigurable Hardware Architectures and Embedded Systems*. 2026 Jun 15;3(2):26-35.
- [17] Polcumpally AT, Pandey KK, Kumar A, Samadhiya A. Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions. *Heliyon*. 2024 Jun 30;10(12):1-21. <https://doi.org/10.1016/j.heliyon.2024.e32975>
- [18] Hemmrich S, Nissen V, Beverugen D, Pauls JD. Blockchain-based reputation systems for business-to-business services: designing a reputation mechanism to reduce information asymmetry in professional consulting: S. Hemmrich et al. *Information Systems and e-Business Management*. 2025 Sep;23(3):809-44. <https://doi.org/10.1007/s10257-025-00702-9>
- [19] Li T, Zuo K, Hu P, Lv L, Ni T, Shen Z, Xie D, Chen F. Blockchain-cloud-based secure data sharing scheme with privacy preservation for internet of vehicles. *Computer Networks*. 2025 Sep 8;272:111674. <https://doi.org/10.1016/j.comnet.2025.111674>
- [20] Teo ZL, Zhang X, Yang Y, Jin L, Zhang C, Poh SS, Yu W, Chen Y, Jonas JB, Wang YX, Wu WC. Privacy-preserving technology using federated learning and blockchain in protecting against adversarial attacks for retinal imaging. *Ophthalmology*. 2025 Apr 1;132(4):484-94. <https://doi.org/10.1016/j.opthta.2024.10.017>
- [21] Niu G. A Blockchain-based Secure and Privacy-Preserving Healthcare Data Management Framework with SHA-256 and PoW Consensus. *Informatica*. 2025;49(20):149-62. <https://doi.org/10.31449/inf.v49i20.8392>