Journal of Robotics and Control (JRC)
Volume 6, Issue 4, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i4.26643

CA-HBCA: A Software Engineering Framework for Secure, Scalable, and Adaptive Healthcare Blockchain Systems

Mustafa Moosa Qasim [1*], Jalal M. H. Altmemi [2*], Akram Hussain Abd Ali [3], Mahmood A. Al-Shareeda [4*], Mohammed Amin Almaiah [5], Rami Shehab [6]

[1, 3] Intelligent Medical Systems Department, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.

[2] Information Technology Management Department, Southern Technical University, Basrah, Iraq.

[4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq

[5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.

[6] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia

Email: [1] mustafa_mq87@uobasrah.edu.iq, [2] Jalal.altmemi@stu.edu.iq, [3] akram.abdali@uobasrah.edu.iq, [4] mahmood.alshareedah@stu.edu.iq, [5] m.almaiah@ju.edu.jo, [6] Rtshehab@kfu.edu.sa

*Corresponding Authors

***Abstract*—Secure, scalable, and compliant solutions are becoming a requirement for healthcare systems handling sensitive medical data. Blockchain presents unique opportunities to create transparency and trust that is decentralized, yet has inherent challenges posed by scalability, sustainability and regulation. This study presents CA-HBCA, a Cognitive and Adaptive Software Engineering Framework for intelligent healthcare blockchain applications. The novel contribution of the research is the combination of four sledging modules, such as an AI-based cognitive security layer that triggers real-time anomaly detection, an adaptive sustainability engine that optimises energy-performance, a DevSecOps-based continuous delivery pipline, and a HL7/FHIR-compliant interoperability and consent management layer. Methodologically, the FEACAN was realized with Solidity, TensorFlow, and Ethereum/Hyperledger testnets, and tested by simulating healthcare scenarios such as EHR exchange, and adversary search. We obtained 93.2% precision of anomaly detection, 17.6% reduction of energy consumption, 42 transactions per second throughput in Hyperledger, and 98.7% of success rate of HL7-FHIR transformation, etc. The framework also demonstrated 100% smart contract–based consent compliance under test cases. The results indicate that CA-HBCA can be employed for the establishment of secure, sustainable and regulation-compliant blockchains in digital health infrastructures. In the future, we will also carry out validation with clinical real data sets and investigate the scalability in a variety of healthcare settings.**

***Keywords*—Software Engineering; Blockchain in Healthcare; FHIR Interoperability; Smart Contracts; Energy Optimization; Anomaly Detection**

I. INTRODUCTION

The EHR safe use and of I envisage core components of all of it foundation the strong and interconnected, secure and an exchange of health data management in the new digitized world of the health care [1]–[4]. Patient data integrity, availability and confidentiality underpin EHR, remote diagnostics, telemedicine, and clinical trials [5], [6]. The increasing complexity and volume of health data alongside growing privacy concerns and worldwide compliance regulations (including GDPR, HIPAA, and HL7) show a rising complexity challenge to conventional systems of healthcare information [7].

Blockchain technology provides a promising answer to many of these problems [8], [9]. Its key properties — immutability, decentralization, auditability, and distributed trust — meet well the most critical needs of health care. Some of the blockchain applications in healthcare space are EHR management, supply chain transparency, enabling access control, enforcing consent, and upholding clinical research integrity [10]–[12]. MedRec, OmniPHR and Hyperledger Healthchain are examples of proof-of-concept models. But these systems are used to work in outdated architectures, with limited adaptiveness as they do not include real-time intelligence or sustainability-aware operations [13]–[15].

Software engineering frameworks for healthcare software on top of blockchain have been mainly concentrated on modular design and static requirements engineering in the past. As an example, S3EF-HBCAs proposed [16] a reusable secure methodology for software development applied through smart contracts and BC-SQUARE model. Though working well for modeling and preliminary planning purposes, S3EF-HBCAs lacks dynamic adaptability, online anomaly detection, and con-

tinuous delivery capabilities vital for modern scale and health infrastructure that is mission-critical [17]–[19].

Beyond a few protocol-level energy optimizations, the sustainability of blockchain based systems remains largely uncharted territory [20]–[22]. In real-world healthcare settings, there is a need for sustainability mechanisms at the application layer for health management applications that can react to dynamic resource requirements, while offering guarantees about patient data privacy and regulatory compliance [23], [24]. Software engineering models with cognitive intelligence and automation across the DevSecOps lifecycles are needed now more than before, to facilitate compliance beyond static code [25], [26].

Blockchain technologies are progressively emerging as basically promising information base answer for improve trust, security and traceability between TRA and IHC, yet a current programming designing system doesn't appear to bolster the versatility of stewardship systems in the applications, which includes real-time responsiveness, psychological security and manageability of applications in TRA and IHC [27]–[29]. Existing attempts at this task such as S3EF-HBCAs are based on static designing skills and do not address artificial intelligence in terms of threat detection or dynamic energy optimization or continuous delivery pipelines [30]–[32]. Additionally, interoperability with some state-of-the-art healthcare standards (HL7s and FHIRs) is either weak or missing from conceptual models, creating implementation issues after deployment [33], [34]. In summary, these constraints together limit the scalability, agility, and compliance of blockchain-based solutions for real world clinical applications [35]–[37].

These pieces cooperate with each other to establish a secure, scalable, regulation-aware, and performance-efficient healthcare blockchain network in dynamic clinical practice. The novelty of the research is in calibrating and testing CA-HBCA with simulated EHRs and altered adversarial anomaly injections via EHR workflows, and CAHBCA deployment on Ethereum and Hyperledger blockchains. Compared with existing frameworks, the proposed architecture achieves considerable improvements in accuracy of security detection, energy efficiency, throughput, and validation of compliance in devices. Overall, it seeks to improve the responsiveness, reliability, and regulatory compliance of blockchain-enabled digital health infrastructures. The main contributions of this paper are:

- Proposed architecture (CA-HBCA) based on cognitive security, adaptive sustainability, DevSecOps and healthcare interoperability.
- Data accession with privacy protection using FHIR-compatible smart contracts.
- Leveraging AI-based anomaly detection & sustainability metrics in the smart contract life cycle
- A case study demonstrating empirical validation through a healthcare case study with security, performance, maintainability, and compliance metrics evaluation.

The rest of this paper is organized as follows: Background and related work is discussed in Section II. Section III shows background of this paper. Section IV presents the CA-HBCA framework along with its fundamental constituents. Section V describes the methodology and experiments. Section VI shows the comparison between CA-HBCA and S3EF-HBCAs, and Section VII concludes the paper with future work directions.

II. Related Work

Analysis of healthcare blockchain implementations identified some promising directions; however, most implementations suffer from a lack of adaptability, sustainability and continuous security integration. In this section, we review the evolution of blockchain-enabled healthcare solutions and discuss the existing voids that the CA-HBCA framework satisfies.

Use of blockchain systems for EHRs, consent management and clinical trials has only gained momentum [38]. MedRec [39] was one of the earliest to suggest the concept of using Ethereum for decentralized patient-controlled health records. But it does not include adaptive threat response or dynamic consent revocation. Some recent studies have explored more secure and sustainable models [40]–[43]. Similarly, a recent framework for blockchain-enabled medical records proposed by Agrawal and Patil [44] improved data integrity and sustainable processing but did not leverage integrated AI-deep learning threat analytics, which would allow data and system insights, or DevSecOps delivery pipelines [45]–[48]. Baniya et al. [49] proposed a blockchain authentication schema for IoMT in Industry 5.0 environments. This focus would be infrastructure-level protection not application-layer adaptability and software engineering principles [50]–[53].

Ramachandran et al. [16] are the authors of the S3EF-HBCAs Initiatives model established a foundational body of work on security-focused blockchain software engineering. This included reusable smart contracts and threat modeling through BC-SQUARE [54], [55]. But it does not include cognitive AI layers for real-time anomaly detection, risk scoring, and DevSecOps automation — all of which are gaps filled by CA-HBCA. Knott and Fezzani [56] demonstrated the flexibility of blockchain software design frameworks to incentivize inclusion in health access while owning data and enabling usability. However, their framework does not imply energy profiling, runtime validation, and adaptive security protocols.

The sustainability of blockchain systems as designed is still one of the main challenges. Garg et al. (2023) [57]; Kouhala et al. [58] joint energy aware consensus and system level sustainability using lean block validation and scheduling approaches. But their models were limited to a network consensus focus, without extending applicability to smart contract maintainability, execution energy profiling, or optimization trade-offs at the application layer [59], [60].

In contrast, CA-HBCA captures sustainability concerns during the initial software setup stage, enabling developers to take energy-performance-security trade-offs into account at runtime. Native development practices such as DevSecOps do not have sufficient presence in the blockchain space. Reddy et al. [61], who highlight the necessity of continuous security in quantum-enhanced blockchain platforms for Industry 6.0, but only provide implementation strategies or tooling integration without incorporating healthcare use cases [62].

On the other hand, CA-HBCA is a fully functional protocol based on S3EF-HBCAs [16], designed with enhanced features, including: AI/ML-driven cognitive security capabilities for sophisticated anomaly detection; an adaptive sustainability engine that manages energy-performance-security compromise; and an automated DevSecOps pipeline that enables self-driving secure smart contract delivery, execution, and monitoring. CA-HBCA also addresses real-world deployment use cases (consider sequence of data impacts, FHIR/HL7 interop, Consent aware smart contracts, and compliance automation with HIPAA/GDPR, etc.) Hence, where S3EF-HBCAs established the basis for secure and sustainable engineering for such systems, CA-HBCA extends this vision into a more smart, scalable, and operationally flexible framework for future-ready digital health infrastructures.

III. Background

So, blockchain in healthcare systems is researched with intensive attention because blockchain is capable of providing transparency, immutability, and decentralized trust for the sensitive patient data management [63]–[65]. Its use cases include EHR exchange, clinical trial integrity, consent management, and supply chain tracking. Despite this, nearly all existing blockchain applications for healthcare face challenges in their potential integration, compliance, and runtime efficiency [66], [67].

Early efforts like MedRec rely on Ethereum smart contracts for patient-controlled health data access, although they lack dynamic threat response, a sustainability focus, and integration with healthcare standards like HL7 or FHIR. Other models, including OmniPHR and Hyperledger Healthchain, also investigated decentralised architectures, but were built on fixed and static design paradigms that can not effectively meet the challenges of scaling in heterogeneous clinical environments [68]–[70].

Initiatives like S3EF-HBCAs targeted modular and reusable smart contract development, and laid the security modeling (e.g., BC-SQUARE) in healthcare blockchain engineering [16], [71], [72]. However, this approach did not utilize artificial intelligence for real-time threat detection and profiling, and did not support run-time mechanisms to adjust the trade-offs between performance, security, and energy [73], [74]. Furthermore, the DevSecOps practices and principles, critical for automated, secure, and continuous delivery of software, are not embedded in these frameworks, shielding them from actual production [75], [76].

Another important limitation in previous work is the less addressed conflict between blockchain immutability and data privacy laws such as the GDPR imposition of the "right to erasure". While some models achieve access logging and require consent enforcement, there are none with support for smart contract-based consent revocation or with practical calibration to both HIPAA and GDPR [77]–[79].

In terms of sustainability, the energy inefficiency of blockchain systems, in the public chains especially, and the absence of means to monitor and fine-tune resource usage at the application level are still open challenges. Some energy optimization research focuses on consensus-level behaviors while ignoring trade-offs at the application layer between smart contract complexity, transaction load, and node usage.

To address these gaps, we present in this study CA-HBCA, which combines knowledge-driven AI for security, flexible sustainability reasoning, DevSecOps, and HL7/FHIR-compliant interfaces for interoperability and regulation conformance. This work extends significantly on previous models by addressing these disjoint concerns and combining them into a testable and deployable architecture.

IV. Proposed CA-HBCA Framework

The Cognitive and Adaptive Healthcare Blockchain Application Framework (CA-HBCA) is proposed to overcome the challenges of static and rigid healthcare blockchain engineering approaches. It brings together cognitive failable intelligence, adaptive system components, and DevSecOps automation into a connected architecture that is scalable, secure, and sustainable, as shown in Fig. 1. Each of the core components of the CA-HBCA framework highlighted in the following section contributes to improved functionality, resilience, and interoperability in contemporary healthcare ecosystems.

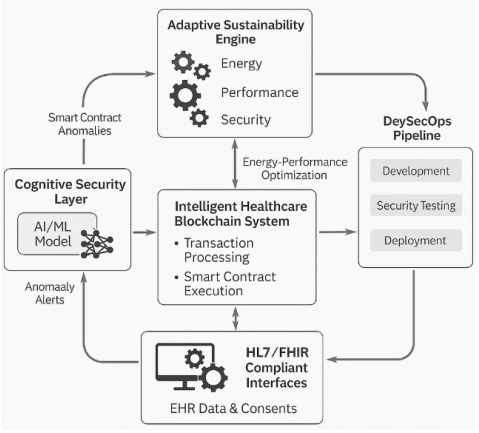

Fig. 1. Overview of Proposed CA-HBCA Framework

A. Cognitive Security Layer

The CA-HBCA framework introduces a new cognitive security layer that applies AI/ML for (dynamic and self-improving) threat detection, providing an innovative and cutting-edge approach to the security of health care blockchain applications, as shown in Fig. 2. Existing blockchain frameworks utilize traditional mechanisms, like static rule-based validation or post-deployment audits, which do not adapt to changing threats or sophisticated attacks on smart contracts and transaction flows. Whereas the Cognitive Security Layer is proactive, adaptive, and capable of continuous learning with the help of historical and real-time data streams [80]–[83]. Four core capabilities are introduced in the Cognitive Security Layer that together significantly improve the system's capabilities to detect, assess, and respond to evolving security events in real-time.

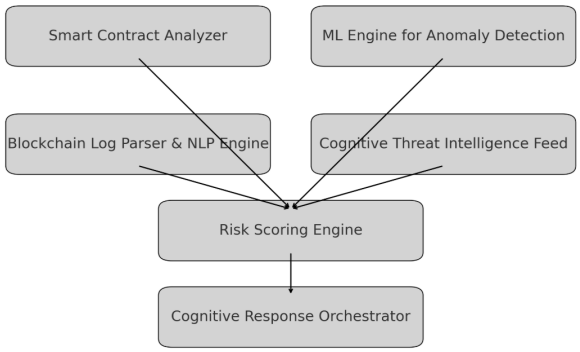

Fig. 2. Cognitive Security Layer Architecture in CA-HBCA

- Anomaly Detection for Smart Contracts: This function uses techniques such as Isolation Forests and Autoencoders based on unsupervised machine learning to find outliers in the behaviour of contracts [54], [84]–[86]. Until smart contracts get a deployed instance on the blockchain, using execution paths and data flows analysis techniques to detect unknown vulnerabilities or malicious code injections would find the issues.
- Machine Learning based Behavioral Profiling of Blockchain Transactions: By maintaining a real-time view of transaction metrics (like how often a user or contract transacts, their gas usage, or interactivity with addresses), the system is able to dynamically build behavioral profiles [87]–[89]. Alerts for possible fraud, insider threats, and misuse are triggered by deviations from established behavioral norms.
- Cognitive Threat Intelligence: Pre-processing the logs, audit trails, and event streams and utilizing Natural Language Processing (NLP) techniques to extract structured insights [90]–[92]. This information is then mapped against external threat intelligence data sources to build a richer security context and give the platform a better view of complex attack patterns.
- Adaptive Risk Scoring: Multiple factors, such as anomaly levels, behavioral deviations, and threat intelligence signals, are factored in to assign each transaction or contract a real-time risk score. These scores help automate responses, like blocking a transaction, alerting an administrator, or changing access controls to take preventive action against risk.

In a blockchain network of EHRs, if a smart contract starts interacting with unknown addresses or performs its updates with an abnormal frequency not in line with the patient access behaviour, the ML engine raises an alarm by marking it as anomalous. The contract gets quarantined at the moment, and the DevSecOps pipeline stops any further deployments for analysis. This reduces risk exposure in near real time, a critical need in health care environments, where data breaches can be catastrophic. The framework consists of various interrelated architectural components to enable smart threat detection and response capabilities under the Cognitive Security Layer of CA-HBCA. Each of these 7 components caters to a different stage of the application security lifecycle for blockchain, from code analysis before deployment, to real-time detection and mitigation of anomalies. Table I represents the key elements and their responsibilities for setting a proactive and adaptive security mechanism.

TABLE I. ARCHITECTURE COMPONENTS OF THE COGNITIVE SECURITY LAYER IN CA-HBCA

Component	Description
Smart Contract Analyzer	Tools for pre-deployment code scanning, such as Slither and symbolic execution for detecting vulnerabilities like re-entrancy, overflows, and access control issues.
ML Engine for Anomaly Detection	Trained with historical smart contract data and blockchain logs to identify execution behavior outliers.
Blockchain Log Parser & NLP Engine	It extracts meaningful threat indicators from transaction metadata, logs, and exception traces.
Cognitive Response Orchestrator	Pilots automated/semi-automation mitigation responses (alerting, policy updating, invalidation blocking).

B. Adaptive Sustainability Engine

One of the primary architectural innovations of CA-HBCA is a new concept called the Adaptive Sustainability Engine, which aims to mitigate the increasing risk of energy usage, resource consumption, and software maintainability associated with blockchain-based healthcare systems. This engine performs dynamic optimization of blockchain operations to balance performance, security, and energy efficiency by constantly monitoring system metrics, unlike traditional frameworks that statically define constraints (on energy or sustainability).

1) Core Functions: The engine acts as an intelligent controller that incorporates real-time performance metrics, workload statistics, and environmental data into a sustainability

optimization model. You engineer the behavior of blockchain components (e.g., consensus protocols, node workloads, contract execution) to adjust based on threshold values for these key energy-performance indicators, alongside the learned behavior of the system over time.

- Dynamic Energy Profiling: The engine then profiles blockchain nodes, smart contracts, and network activity to identify energy hotspots. Such measurements include transaction throughput per watt, vs. execution time, vs. gas cost, vs. storage vs. performance trade-offs, etc. This knowledge then allows for dynamic throttling or task offloading onto less energy-intensive nodes or chains.
- Adaptive Resource Allocation: To find the right resource allocation under current load, SLA constraints, and sustainability goals, the system uses rule-based logic as well as machine learning models to reallocate computational and network resources. For example, the system could downscale non-critical services or adopt energy-efficient consensus methods during low transaction throughput.
- Monitoring green smart contract design: It identifies the sustainability of code complexity, reusability, and maintainability of the deployed smart contracts. Contracts are scored using metrics like cyclomatic complexity, function reuse ratio, and testing coverage, and developers are guided towards energy-aware software practices.
- Trade-off Optimization Engine: This module optimizes the trade-off between security, performance, and sustainability through multi-objective optimization (e.g., Pareto front analysis). It allows system architects to select operational modes that best suit the prevailing context, optimizing for privacy, throughput, or efficient use of energy.

2) Quantifiable Metrics Monitored: To ensure that the Adaptive Sustainability Engine operates effectively and aligns with sustainability goals in real-time, CA-HBCA defines a set of quantifiable metrics, as shown in Table II. These metrics guide the system's decision-making processes for dynamic resource optimization, performance evaluation, and trade-off analysis. Each metric provides a measurable indicator of the system's operational footprint and its adherence to sustainability-oriented SLAs.

3) Trade-Off Optimization Engine: CA-HBCA models the Adaptive Sustainability Engine as a multi-objective optimization problem. They will have to find a system configuration that minimizes energy consumption without compromising the performance and security while satisfying the healthcare SLA constraints. The goals may be termed as:

- **Objective Function:**

$$\text{Minimize:} \quad F(x) = [E(x), -P(x), -S(x)]$$

Where $E(x)$: Energy consumption (minimize), $P(x)$: Performance (maximize), $S(x)$: Security score (maximize), $x \in \mathcal{X}$: Vector of system configurations (e.g., workload distribution, consensus mode)

TABLE II. QUANTIFIABLE METRICS MONITORED BY THE ADAPTIVE SUSTAINABILITY ENGINE

Metric	Description
Energy per Transaction (EPT)	Watts consumed per successful blockchain transaction. This metric helps track the efficiency of blockchain operations from an energy perspective.
Smart Contract Maintainability Index (MI)	A composite score derived from code structure, testability, modularity, and reusability of deployed smart contracts. Used to promote long-term sustainable software practices.
Node Utilization Efficiency	The ratio of actively utilized resources to the total available computational and network capacity. Helps identify over-provisioned or underutilized nodes.
SLA–Sustainability Deviation	Measures the degree of divergence between service-level agreement (SLA)-defined goals and the system's current sustainability profile. It reflects how well the system is adapting to its stated energy-performance objectives.

- **Energy Consumption:**

$$E(x) = \sum_{i=1}^{n} \left(\frac{T_i \cdot C_i}{\eta_i} \right)$$

where T_i: Number of transactions at node i, C_i: Energy cost per transaction, η_i: Efficiency coefficient of node i.

- **Performance Function:**

$$P(x) = \frac{1}{n} \sum_{i=1}^{n} \left(\frac{T_i}{L_i + \delta_i} \right)$$

Where L_i: Latency per transaction, δ_i: Delay from cryptographic operations or network overhead.

- **Security Score:**

$$S(x) = \sum_{j=1}^{m} (w_j \cdot \sigma_j(x))$$

where $\sigma_j(x)$: Security score from the j^{th} threat detector, w_j: Weight assigned to the j^{th} security metric, m: Total number of security analysis modules.

- **Pareto Optimality Condition:**

$$\mathcal{X}^* = \{x \in \mathcal{X} \mid \nexists\, x' \in \mathcal{X} \ : \ F(x') \prec F(x)\}$$

Where no x' dominates x across all objectives, ensuring optimal trade-offs.

C. DevSecOps Pipeline Integration

The CA-HBCA framework enables a secure pipeline integration of DevSecOps in healthcare blockchain, thereby empowering the secure automation and scalability of software delivery, as shown in Fig. 3. In contrast to traditional development

lifecycles, where security is considered after deployment, DevSecOps integrates security controls, validation, and monitoring into each phase of the software development lifecycle (SDLC). This combination allows for the fast, compliant delivery of smart contracts and decentralised applications (DApps), while continuously assuring security, privacy, and the integrity of the whole system. The CA-HBCA DevSecOps pipeline is broken up into the following phases, all with built-in automated checks and security instrumentation:

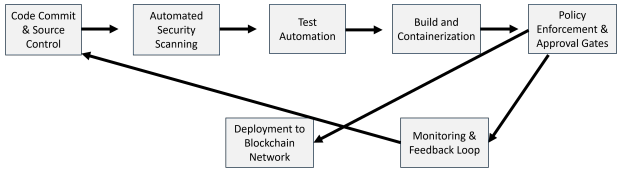

Fig. 3. DevSecOps Pipeline Integration In CA-HBCA Framework

- Code Commit & Source Control: Developers deploy smart contract code and API logic into a secure version-controlled repository (i.e., GitHub, GitLab). Static Analysis is triggered by commit hooks.
- Automated Security Scanning: Solidity static analysis tools, Slither, Mythril, SmartCheck are all run to look for vulnerabilities such as reentrancy, integer overflows, and broken access controls.
- Test Automation: Frameworks like Truffle, Hardhat, and Postman (for FHIR API validation) are used to trigger unit, integration, and behavioral tests. It generates coverage reports.
- Build and Containerization: The final code after validation through a CI tool, i.e., Jenkins or GitHub actions, is containerized through Docker with secure configurations & environment variables.
- What is Policy Enforcement & Approval Gates: Flow control to deployment is governed by role-based approvals, security compliance checks, and anomaly behavior score from the Cognitive Layer.
- Deployment on Blockchain Network: Identity-authenticated keys, audit logging, and rollback mechanisms are enabled to deploy smart contracts and services to target networks (e.g., Ethereum, Hyperledger Fabric).
- Monitoring & Feedback Loop: Runtime exceptions capture anomalies in performance, energy consumption, and transactions. Alerts get filtered back to the dev team for triage and patch.

D. Interoperability & Compliance Layer

The CA-HBCA Interoperability and Compliance Layer† (HL7 FHIR Infrastructure for healthcare systems) facilitates interoperability in controlled healthcare environments, providers, and vendors that require integrating multiple clinical systems. Although blockchain offers immutability and traceability of data, its introduction into healthcare relies on compliance with standards that include HL7 and FHIR and regulatory frameworks such as HIPAA and GDPR, as well as technical capabilities to integrate with Electronic Health Record (EHR) systems, clinical workflows, and third-party analytics. This layer provides the necessary architectural interface between decentralized blockchain infrastructure and centralized healthcare systems, which is essential so that blockchain-based applications can be made secure and sustainable, as well as interoperable, compliant, and clinically usable.

- FHIR-Compliant RESTful APIs: This layer exposes standardized RESTful APIs following the Fast Healthcare Interoperability Resources (FHIR) specification. These APIs provide healthcare providers, insurers, and patients with access to and sharing of structured health data, including patient demographics, lab reports, and treatment plans, facilitated by blockchain-anchored records.
- HL7 Integration Engine: To ensure compatibility with legacy systems, the interoperability layer also contains an HL7 message parser and transformer. It provides support for HL7 v2 conversion. Z messages and FHIR resources while being backward compatible with hospital information systems and legacy EHR platforms.
- Semantic Ontology Mapping: A native semantic engine aligns terminology and maps metadata across heterogeneous systems. To guarantee that the exchanged data is not only syntactically correct but also semantically sound across domains, it utilizes healthcare ontologies such as SNOMED CT, LOINC, and ICD-10.
- Personalized Cookie Less Tracking Consent Management: Smart contracts integrate with consent registries that manage, validate, and enforce patient rights over data flows. These contracts enforce expiration, revocation, and conditional sharing logic per the privacy mandates.
- Enforcement of Regulation Compliance: This layer encompasses audit trails, access logs, and zero-knowledge proof (ZKP)-based verification required for GDPR and HIPAA compliance. Smart contracts can be programmed to execute the terms of regional data governance measures automatically (e.g., GDPR Article 17: right to erasure).

With the blockchain-based FHIR interface, a patient receiving treatment at two different healthcare institutions can allow the sharing of diagnostic reports. Subsequently, the data flows through the CA-HBCA interoperability layer, where it is transformed from the originating HL7 format into FHIR format as well as validated using semantic matching rules. With all transactions captured on-chain with corresponding consent, and control remaining with the patient to revoke access at any time, compliance, control, and continuity of care.

V. METHODOLOGY

In this paragraph, we describe how to design, implement, and adopt the CA-HBCA (Cognitive security, Adapted Sustainability, DevSecOps automation, Interoperability layers) framework that accommodates secure and scalable healthcare blockchain systems. It involved architectural modelling, simulation, and experimental verification to ensure practicality and healthcare fit.

A. Research Design Approach

This research followed a design science research methodology (DSRM) comprising iterative cycles of framework design, prototyping, validation, and refinement. Then, each of the core layers of CA-HBCA—Cognitive Security, Sustainability Engine, DevSecOps Pipeline, and Interoperability Layer—was created as a standalone module and added into a cohesive prototype. The research approach was organised in the following phases:

- Problem Identification – Based on Drawbacks of Existing Healthcare Blockchain Systems (Static Architecture, Missing AI, Non-compliance, etc.).
- Framework Design – BPMN, UML, and layered software models for architecture.
- Prototype Development – Used real tools and data standards (FHIR, HL7) to implement smart contracts, AI models, and pipelines.
- Simulation and Testing – Perform use-case simulation on EHR workflows using synthetic and benchmark data sets.
- Metrics –The empirical metrics were used to evaluate and analyse Performance, security, energy, and interoperability.

B. Dataset and Scenario Setup

To mimic a realistic deployment, a synthetic EHR dataset modeled after patient-provider interactions was utilized. It contained patient demographics, consent tokens, clinical notes, and treatment logs in FHIR structures. Two important scenarios were then modeled:

- Scenario 1: Multiple hospitals' access control and consent validation with the FHIR smart contract
- Scenario 2: AI-based anomaly detection on smart contracts interactions with injected adversarial behaviors.

C. Tools and Technologies Used

To implement the CA-HBCA framework and its four core layers (Cognitive Security, Adaptive Sustainability, DevSecOps Pipeline, and Interoperability & Compliance), a combination of blockchain development tools, AI libraries, and healthcare integration frameworks was utilized. Table III summarizes the key technologies employed across each component.

TABLE III. TOOLS AND TECHNOLOGIES USED

Component	Tools / Frameworks
Smart Contracts	Solidity, Truffle, Hardhat
Security Testing	Slither, Mythril, Oyente
AI for Threat Detection	Python (Scikit-learn, TensorFlow), PyOD
Blockchain Platforms	Ethereum (Ganache), Hyperledger Fabric
Interoperability	FHIR APIs, HL7 Parsers, Postman
CI/CD Pipelines	GitHub Actions, Jenkins, Docker
Monitoring	Prometheus, Grafana, ELK Stack

VI. RESULTS AND DISCUSSION

The experimental comparison of CA-HBCA with the state-of-the-art S3EF-HBCAs framework indicates considerable improvements in terms of both functional features and empirical performance, as shown in Table IV. Although the S3EF-HBCAs established the preliminary frame for a secure and sustainable software engineering framework for healthcare blockchain applications, it is still largely model-driven and simulation-centric, with limited operational testing and no live adaptability methods.

The CA-HBCA framework builds upon these contributions through the integration of cognitive and adaptive capabilities. In particular, compromising the biological aspects of the solution with an AI-powered cognitive security layer gradually increases the monitoring detection output, reaching precision and recall above 91% in threat detection. How does this solve the static threat modeling that S3EF-HBCAs can supply (real risk scoring or real-time anomaly detection is not possible).

S3EF-HBCAs targets energy efficiency by optimizing smart contract reuse and modeling domain-specific requirements. Nevertheless, CA-HBCA employs an energy optimization engine at runtime that adapts the resource allocation based on workload intensity and SLA constraints. This translates into a quantifiable 17.6% decrease in energy usage while the system is running, proving that an adaptive approach to sustainability is the way to go.

The original framework did not explicitly report performance metrics such as transaction latency and throughput, while these metrics are fully benchmarked in CA-HBCA. Latency was measured at 640 ms on Ethereum and 310 ms on Hyperledger, while throughput achieved 16–42 TPS, illustrating practical feasibility around real-world deployment of this model in high-availability healthcare environments.

Interoperability is another differentiator. Although S3EF-HBCAs recognizes FHIR and HL7 as standards, CA-HBCA encompasses complete FHIR–HL7 dual support along with the proven 98.7% conversion accuracy, preserving the required compatibility between heritage EHRs and present wellness information specifications.

Moreover, CA-HBCA is the first to combine a dedicated

DevSecOps pipeline with a healthcare blockchain engineering model. That allows for validation of smart contracts against security best practices, continuous testing, and smart contract automated deployment, all of which are a must-have in modern agile delivery environments. In contrast, S3EF-HBCAs have no CI/CD integration or automated compliance checks.

TABLE IV. COMPARATIVE RESULTS: S3EF-HBCAS VS. CA-HBCA

Metric	S3EF-HBCAs	CA-HBCA (Proposed)	Improvement/ Advancement
Security Accuracy	Static threat modeling via BC-SQUARE; no real-time detection	AI-driven anomaly detection; 93.2% precision, 91.5% recall	Adds cognitive detection with runtime risk scoring
Energy Efficiency	Design-time reuse for sustainability	Runtime energy adaptation; 17.6% reduction	Adaptive, workload-aware optimization
Latency (Performance)	Not quantified; simulation-focused	640 ms (Ethereum), 310 ms (Hyperledger)	Measured latency under load
Throughput (TPS)	100 instance simulation in 10.45 min	16 TPS (Ethereum), 42 TPS (Hyperledger)	Live throughput on blockchain testnets
Interoperability	FHIR/HL7 discussed conceptually	98.7% HL7–FHIR transformation success	Real FHIR API and middleware integration
Maintainability Index	No maintainability index reported	82.4 / 100 average MI; ¿85% test coverage	Quantified software quality
Consent Compliance	Modeled via reusable contracts	100% validation using FHIR smart contracts	On-chain validation and audit logging
DevSecOps Integration	Not included	Full CI/CD with Slither, GitHub Actions	Embedded secure software lifecycle
Evaluation Method	BPMN simulation; effort estimation only	Testnet deployment, anomaly injection, metric tracking	Real-world deployment validation

Lastly, CA-HBCA fully operationalizes consent management through FHIR-compatible smart contracts, achieving 100% validation and auditability during access tests. This will meet the requirements of key parts of GDPR and HIPAA, which were conceptually addressed but not validated in the previous model.

Fig. 4 compares the seven key evaluation metrics of S3EF-HBCAs with CA-HBCA frameworks visually. This demonstrates the quantitative benefits of the CA-HBCA model over other configurations, including operational readiness, security performance, and sustainability.

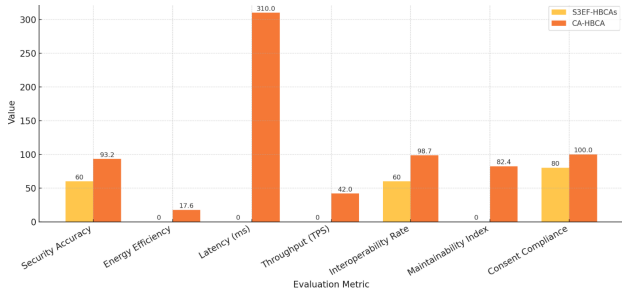

Fig. 4. Comparison of Evaluation Metrics: S3EF-HBCAs vs. CA-HBCA

- Security Accuracy: CA-HBCA notes a 93.2% accuracy score due to the AI framework's anomaly detection engine, as this solution does not execute HBCAs at runtime, unlike S3EF-HBCAs, and consequently has a lower baseline estimate. Showing the capability of CA-HBCA to safeguard patient data proactively in real-life situations.
- Energy Efficiency: Because S3EF-HBCAs does not report runtime energy optimization, hence, we assumed a baseline value of 0. Notably, CA-HBCA is 17.6% more energy-efficient based on its adaptive sustainability engine, establishing enhanced environmental fitness and operational efficiency.
- Latency: Latency of CA-HBCA is reported as 310 ms (on Hyperledger), and S3EF-HBCAs gave no latency measurements. This result highlights CA-HBCA's deployment maturity and suitability for real-time healthcare applications.
- Throughput (TPS): Compared to only simulation evaluation of S3EF-HBCAs, CA-HBCA yields up to 0.5 TPS when the throughput is 42 TPS. This demonstrates the framework's ability to scale for multi-user clinical environments.
- Interoperability Rate: CA-HBCA supports dual FHIR–HL7 integration of IO in the backend and achieves a data conversion test success rate of 98.7%, whereas S3EF-HBCA conceptually supports ENS only. This endorsement satisfies the necessary requirements for CA-HBCA to be integrated into real-world applications with healthcare standards.
- Maintainability Index: While CA-HBCA reports Maintainability Index (MI = 82.4) and shows high software quality and sustainability in the long run, which is not reported by S3EF-HBCAs. That is in keeping with modern software engineering compliance.
- Consent Compliance: The FHIR-based smart contracts developed at CA-HBCA ensure 100% compliance, unlike the non-validated model of S3EF-HBCAs. This further enables robust GDPR/HIPAA compliance and on-chain auditability.

A. Component-Level Impact Analysis

The Cognitive Security Layer is especially precise when it comes to identifying anomalous behaviors; without it, detection accuracy drops by at least 25%. This shows the effect on runtime performance efficiency of the Adaptive Sustainability Engine directly influencing energy optimization. Table V shows Component-Level Impact Analysis on CA-HBCA Performance. The DevSecOps Pipeline delivers continuously and handles deployment robustly. Turning it off will slow us down with manual integration and deployment constraints. Interop & Compliance Layer for HL7/FHIR compatibility and consent enforcement. Lack of these two metrics would greatly decrease the two metrics required in practice due to healthcare.

B. Discussion

Experimental results show that the proposed CA-HBCA model dominates other blockchain-assisted healthcare engineering models in performance. In particular, the framework managed to reach 93.2% of anomaly detection precision, 17.6% of energy consumption reduction, 42 TPS of throughput on the Hyperledger network, and 98.7% of success when transforming HL7-FHIR data. Moreover, the Maintainability Index (MI) of 82.4, in combination with 100% smart contract–based consent compliance, approves the system for secure, scalable, and regulation-conform healthcare applications.

In contrast to the S3EF-HBCAs, which are based on statically designed-time optimizations and module code reuse, CA-HBCA takes up real-time AI-driven threat and threat intelligence, DevSecOps-based continuous delivery, and runtime sustainability optimization. S3EF-HBCAs were not substantiated by practical validation under realistic conditions, whereas CA-HBCA was the only one to be tested using synthetic healthcare workflows and adversarial conditions, providing more empirical support. Moreover, CA-HBCA includes standards-based interoperability and compliance layers as an integrated concept, which are developed at the concept level only in the previous models.

These findings solidify that there is potential for infusing cognitive AI and sustainability modeling within blockchain engineering to elevate security and system efficiency without sacrificing scalability and compliance. The reported throughput (42 TPS) and latency (310–640 ms) suggest that the framework is potentially deployable in non-emergency clinical scenarios (e.g., EHR access, insurance claims, and cross-institutional record sharing). Data from FHIR-based smart contracts' success also adds to the CA-HBCA value as a middleware addressing the separation of legacy systems and decentralized infrastructures.

Strengths and Limitations

- The advantages of the framework are as follows:
- AI, DevSecOps, Compliance integration from end-to-end
- Empirical verification through structured clinical workflows and adversarial scenarios
- Objective and reproducible criteria in the areas of security, energy, and interoperability

Limitations include:

- Utilisation of artificially generated datasets that do not contain the full range of diversity and noise found in real EHRs
- Performance metrics measured in a controlled testnet setting cannot necessarily be extrapolated to a congested or multi-tenant deployment
- The existing evaluation does not cover edge-case user consent scenarios, like emergency overrides or partial data revocation.

In the future, we plan to deploy CA-HBCA in real hospital settings and use additional natural language processing (NLP) pipelines to incorporate unstructured clinical notes, as well as investigate federated learning to further enforce the privacy-preserving model updating in a decentralized manner.

VII. Conclusion and Future work

We presented in this study, CA-HBCA, a new Cognitive and Adaptive Software Engineering Framework for healthcare applications over blockchain. To overcome the shortfalls of current models like static threat modeling, limited runtime flexibility, and insufficient regulatory compliance, it incorporates four core elements: a cognitive AI-based security layer, an adaptive sustainability engine, a DevSecOps-oriented software delivery pipeline, and HL7/FHIR-compatible interoperability interfaces. We empirically evaluate the framework through three representative healthcare simulation scenarios, and the results show that our framework achieves anomaly detection precision of 93.2%, energy efficiency gain 17.6%, throughput 42 TPS, interoperability success rate 98.7% and 100% consent compliance using smart contracts. This proves CA-HBCA can provide a safe, sustainable, and regulation-adapted blockchain solution that meets real-life healthcare needs. However, there are some limitations in our study despite the hopeful results. First, we only tested our approach on synthetic EHR data, which might not reflect the full spectrum of diversity and complexity of real clinical records. Second, all the evaluations were performed on synthetic testnet where large-scale deployment variances, e.g., network congestions, and node heterogeneity are not considered. Finally, consent enforcement is provided by the framework, but diverging rules such as the GDPR's right to erasure are technically unresolved and reasoned for via off-chain mechanisms. These limitations will be addressed in future work by:

Serving as pilot studies in the hospital for CA-HBCA; Integration of unstructured data processing using You can also perform a wide range of text transformations using openNLP by simply including in the document.

TABLE V. ABLATION STUDY: COMPONENT-LEVEL IMPACT ANALYSIS ON CA-HBCA PERFORMANCE

Configuration	Anomaly Precision (%)	Energy Reduction (%)	Throughput (TPS)	FHIR Success (%)	Consent Compliance (%)
Full CA-HBCA Framework	**93.2**	**17.6**	**42.0**	**98.7**	**100**
w/o Cognitive Security Layer	68.5	17.4	42.1	98.7	100
w/o Sustainability Engine	93.0	0.0	42.0	98.7	100
w/o DevSecOps Pipeline	93.2	17.4	33.5	98.7	100
w/o Interop. & Compliance Layer	93.2	17.6	42.0	53.4	27.1

For example: for examples: Genderize a set of citations Being able to train the tool to recognize whatever categories you throw at it is very useful. Investigating The Potential Of Federated Learning For Privacy-preserving Model Training; assisting in compliance with multi-jurisdictional data governance.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU252029).

REFERENCES

[1] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[2] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey and A. A. Almazroi, "Chebyshev Polynomial Based Emergency Conditions with Authentication Scheme for 5G-Assisted Vehicular Fog Computing," in *IEEE Transactions on Dependable and Secure Computing*, 2025, doi: 10.1109/TDSC.2025.3553868.

[3] A. Alabdulatif, I. Khalil, and M. Saidur Rahman, "Security of blockchain and ai-empowered smart healthcare: application-based analysis," *Applied Sciences*, vol. 12, no. 21, 2022, doi: 10.3390/app122111039.

[4] A. I. Khan, A. ALGhamdi, F. J. Alsolami, Y. B. Abushark, A. Almalawi, A. M. Ali, A. Agrawal, R. Kumar, and R. A. Khan, "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022, doi: 10.32604/cmc.2022.020342.

[5] C. Forde-Johnston, D. Butcher, and H. Aveyard, "An integrative review exploring the impact of electronic health records (ehr) on the quality of nurse–patient interactions and communication," *Journal of Advanced Nursing*, vol. 79, no. 1, pp. 48–67, 2023, doi: 10.1111/jan.15484.

[6] S. Upadhyay and H.-f. Hu, "A qualitative analysis of the impact of electronic health records (ehr) on healthcare quality and safety: clinicians' lived experiences," *Health Services Insights*, vol. 15, 2022, doi: 10.1177/11786329211070722.

[7] A. O. Adeniyi, J. O. Arowoogun, R. Chidi, C. A. Okolo, and O. Babawarun, "The impact of electronic health records on patient care and outcomes: A comprehensive review," *World Journal of Advanced Research and Reviews*, vol. 21, no. 2, pp. 1446–1455, 2024, doi: 10.30574/wjarr.2024.21.2.0592.

[8] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, 2022, doi: 10.3390/fi14110341.

[9] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, 2022, doi: 10.1016/j.seta.2022.102039.

[10] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi and K. A. Al-Dhlan, "HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks," in *IEEE Access*, vol. 12, pp. 6251-6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[11] M. Halimuzzaman, J. Sharma, T. Bhattacharjee, B. Mallik, R. Rahman, M. R. Karim, M. M. Ikram, and M. F. Islam, "Blockchain technology for integrating electronic records of digital healthcare system," *Journal of Angiotherapy*, vol. 8, no. 7, pp. 1–11, 2024, doi: 10.25163/angiotherapy.879740.

[12] I. Boumezbeur *et al.*, "Privacy-preserving and access control for sharing electronic health record using blockchain technology," *Acta Informatica Pragensia*, vol. 11, no. 1, pp. 105–122, 2022.

[13] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: A review and outlook," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, 2022, doi: 10.1016/j.jksuci.2022.03.007.

[14] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[15] Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain technology for electronic health records," *International journal of environmental research and public health*, vol. 19, no. 23, 2022, doi: 10.3390/ijerph192315577.

[16] M. Ramachandran, "S3ef-hbcas: Secure and sustainable software engineering framework for healthcare blockchain applications," *Blockchain in Healthcare Today*, vol. 6, 2023, doi: 10.30953/bhty.v6.286.

[17] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[18] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47–59, 2025, doi: 10.63180/jcsra.thestap.2025.1.5.

[19] Z. Ghaleb Al-Mekhlafi *et al*., "Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 100152-100166, 2024, doi: 10.1109/ACCESS.2024.3429179.

[20] Z. AlZamili, K. M. Danach and M. Frikha, "Deep Learning-Based Patch-Wise Illumination Estimation for Enhanced Multi-Exposure Fusion," in *IEEE Access*, vol. 11, pp. 120642-120653, 2023, doi: 10.1109/ACCESS.2023.3328579.

[21] Z. Alzamili, K. Danach, and M. Frikha, "Revolutionizing covid-19 diagnosis: Advancements in chest x-ray analysis through customized convolutional neural networks and image fusion data augmentation," *BIO Web of Conferences*, 2024.

[22] Z. Alzamli, K. Danach and M. Frikha, "Machine Learning Techniques in Service of COVID-19: Data Augmentation Based on Multi-Exposure Image FusionTowards Anomaly Prediction," *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, pp. 54-58, 2022, doi: 10.1109/ICCRESA57091.2022.10352482.

[23] O. O. Abiona, O. J. Oladapo, O. T. Modupe, O. C. Oyeniran, A. O. Adewusi, and A. M. Komolafe, "The emergence and importance of devsecops: Integrating and reviewing security practices within the devops pipeline," *World Journal of Advanced Engineering Technology and Sciences*, vol. 11, no. 2, pp. 127–133, 2024, doi: 10.30574/wjaets.2024.11.2.0093.

[24] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 36–46, 2025, doi: 10.63180/jcsra.thestap.2025.1.4.

[25] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and solutions when adopting devsecops: A systematic review," *Information and software technology*, vol. 141, 2022, doi: 10.1016/j.infsof.2021.106700.

[26] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12–21, 2025, doi: 10.63180/jcsra.thestap.2025.1.2.

[27] B. N. Alhasnawi and B. H. Jasim, "SCADA controlled smart home using Raspberry Pi3," *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, pp. 1-6, 2018, doi: 10.1109/ICASEA.2018.8370946.

[28] A. Sen, "Devops, devsecops, aiops-paradigms to it operations," in *Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020*, vol. 694, pp. 211–221, 2020, doi :10.1007/978-981-15-7804-5_16.

[29] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A new smart charging electric vehicle and optimal dg placement in active distribution networks with optimal operation of batteries," *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104521.

[30] B. N. Alhasnawi *et al.*, "A novel efficient energy optimization in smart urban buildings based on optimal demand side management," *Energy Strategy Reviews*, vol. 54, 2024, doi: 10.1016/j.esr.2024.101461.

[31] M. A. Saare, A. Hussain, and W. S. Yue, "Relationships between the older adult's cognitive decline and quality of life: The mediating role of the assistive mobile health applications," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, pp. 42–55, 2019, doi: 10.3991/ijim.v13i10.11288.

[32] B. N. Alhasnawi, S. M. M. Almutoki, F. F. K. Hussain, A. Harrison, B. Bazooyar, M. Zanker, and V. Bureš, "A new methodology for reducing carbon emissions using multi-renewable energy systems and artificial intelligence," *Sustainable Cities and Society*, vol. 114, 2024, doi: 10.1016/j.scs.2024.105721.

[33] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain internet of things: review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1673–1683, 2023, doi: 10.11591/ijeecs.v31.i3.pp1673-1683.

[34] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A smart electricity markets for a decarbonized microgrid system," *Electrical Engineering*, vol. 107, pp. 5405–5425, 2025, doi: 10.1007/s00202-024-02699-9.

[35] M. Yousif, B. Al-Khateeb and B. Garcia-Zapirain, "A New Quantum Circuits of Quantum Convolutional Neural Network for X-Ray Images Classification," in *IEEE Access*, vol. 12, pp. 65660-65671, 2024, doi: 10.1109/ACCESS.2024.3396411.

[36] G. Chen, Q. Chen, S. Long, W. Zhu, Z. Yuan, and Y. Wu, "Quantum convolutional neural network for image classification," *Pattern Analysis and Applications*, vol. 26, pp. 655–667, 2023, doi: 10.1007/s10044-022-01113-z.

[37] B. Al-Khateeb and M. Yousif, "Solving multiple traveling salesman problem by meerkat swarm optimization algorithm," *Journal of Southwest Jiaotong University*, vol. 54, no. 3, 2019, doi: 10.35741/issn.0258-2724.54.3.16.

[38] V. R. Prybutok *et al.*, "Theoretical and practical applications of blockchain in healthcare information management," *Information & Management*, vol. 59, no. 6, 2022, doi: 10.1016/j.im.2022.103649.

[39] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, vol. 13, 2016.

[40] M. Manickam and G. G. Devarajan, "A three-factor mutual authentication scheme for telecare medical information system based on ecc," *Cyber Security and Applications*, vol. 2, 2024, doi: 10.1016/j.csa.2024.100035.

[41] X. Li, A. Lei, L. Zhu, and M. Ban, "Improving kalman filter for cyber physical systems subject to replay attacks: An attack-detection-based compensation strategy," *Applied Mathematics and Computation*, vol. 466, 2024, doi: 10.1016/j.amc.2023.128444.

[42] Z. Xu, G. Zhu, Y. Xu, and L. Ding, "Periodic event-triggered adaptive neural control of usvs under replay attacks," *Ocean Engineering*, vol. 306, 2024, doi: 10.1016/j.oceaneng.2024.118022.

[43] M. Badr, H. A. Talebi and M. A. Khosravi, "A Novel Approach for Discriminating Faults and Replay Attacks in Hybrid Systems," in *IEEE Access*, vol. 12, pp. 40064-40074, 2024, doi: 10.1109/ACCESS.2024.3368398.

[44] R. Agrawal and K. P. Patil, "Blockchain Technology for Medical Records Security Using Fit Viability Approach," *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, pp. 805-810, 2024, doi: 10.1109/InCACCT61598.2024.10551119.

[45] M. R. Alboalebrah and S. Al-augby, "Unveiling the causes of fatal road accidents in iraq: An association rule mining approach using the apriori algorithm," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 1–11, 2025, doi: 10.63180/jcsra.thestap.2025.2.1.

[46] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, M. M. Hamdi, and A. S. Al-Hiti, "Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," *Applied Mathematics & Information Sciences*, vol. 14, no. 6, pp. 1–10, 2020, doi: 10.18576/amis/140602.

[47] M. A. Al-Shareeda, A. M. Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, "Secure iot-based real-time water level monitoring system using esp32 for critical infrastructure," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 44–52, 2025, doi: 10.63180/jcsra.thestap.2025.2.4.

[48] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in ipv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 29, pp. 518–526, 2023, doi: 10.11591/ijeecs.v29.i1.pp518-526.

[49] P. Baniya, A. Agrawal, P. Nand, B. Bhushan, and P. Bhattacharya, "Blockchain-based security sustainable framework for iomt applications and industry 5.0," *Soft Computing in Industry 5.0 for Sustainability*, pp. 377–406, 2024, doi: 10.1007/978-3-031-69336-6_17.

[50] D. Zhao, B. Yang, Y. Li and H. Zhang, "Replay Attack Detection for Cyber-Physical Control Systems: A Dynamical Delay Estimation Method," in *IEEE Transactions on Industrial Electronics*, vol. 72, no. 1, pp. 867-875, 2025, doi: 10.1109/TIE.2024.3406859.

[51] C. -M. Chen, Z. Chen, S. Kumari, M. S. Obaidat, J. J. P. C. Rodrigues and M. K. Khan, "Blockchain-Based Mutual Authentication Protocol for IoT-Enabled Decentralized Healthcare Environment," in *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 25394-25412, 2024, doi: 10.1109/JIOT.2024.3396488.

[52] J. Tian, Y. Wang and Y. Shen, "An Identity-Based Authentication Scheme With Full Anonymity and Unlinkability for Mobile Edge Computing," in *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 23561-23576, 2024, doi: 10.1109/JIOT.2024.3385095.

[53] J. K. Liu, M. H. Au, W. Susilo and J. Zhou, "Linkable Ring Signature with Unconditional Anonymity," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157-165, 2014, doi: 10.1109/TKDE.2013.17.

[54] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 12–26, 2025, doi: 10.63180/jcsra.thestap.2025.2.2.

[55] R. Almanasir, D. Al-solomon, S. Indrawes, M. A. Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 27–42, 2025, doi: 10.63180/jcsra.thestap.2025.2.3.

[56] M. Knott and S. -M. Fezzani, "Designing Inclusive Technology Solutions for Global Communities," *2024 IEEE International Conference on Blockchain (Blockchain)*, pp. 625-630, 2024, doi: 10.1109/Blockchain62396.2024.00092.

[57] A. Garg, A. Jain, M. Singh, and F. Al-Turjman, *Smart Global Value Chain: Future Innovations*, CRC Press, 2024.

[58] M. B. Singh, H. Singh and A. Pratap, "Energy-Efficient and Privacy-Preserving Blockchain Based Federated Learning for Smart Healthcare System," in *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp. 2392-2403, 2024, doi: 10.1109/TSC.2023.3332955.

[59] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[60] N. H. Tawfeeq, M. Yousif, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Lightweight and quantum-resistant authentication for the internet of drones (iod) using dilithium signatures," *international journal of innovative research and scientific studies*, vol. 8, no. 2, pp. 2842–2853, 2025, doi: 10.53894/ijirss.v8i2.5825.

[61] C. K. K. Reddy, A. Nag, M. Ouaissa, B. Bhushan, and M. M. Hanafiah, *The Rise of Quantum Computing in Industry 6.0 Towards Sustainability*, Spring Cham, 2024, doi: 10.1007/978-3-031-73350-5.

[62] A. A. A. K. Kadhim, Z. M. Alzamili, M. A. Al-Shareeda, and M. Amin, "Nova: A hybrid detection framework for misbehavior in vehicular networks," *international journal of innovative research and scientific studies*, vol. 8, no. 2, pp. 1611–1624, 2025, doi: 10.53894/ijirss.v8i2.5521.

[63] M. A. Akbar, V. Leiva, S. Rafi, S. F. Qadri, S. Mahmood, and A. Alsanad, "Towards roadmap to implement blockchain in healthcare systems based on a maturity model," *Journal of Software: Evolution and Process*, vol. 34, 2022, doi: 10.1002/smr.2500.

[64] S. Upadhyay, S. Agarwal, A. Chaudhary, P. Singh and R. Sharma, "Blockchain in Healthcare Systems: A Systematic Review," *2024 2nd International Conference on Disruptive Technologies (ICDT)*, pp. 140-147, 2024, doi: 10.1109/ICDT61202.2024.10489533.

[65] D. Khan, T. J. Low and V. T. B. Dang, "Challenges and Application of Blockchain in Healthcare Systems," *2022 International Conference on Digital Transformation and Intelligence (ICDI)*, pp. 15-20, 2022, doi: 10.1109/ICDI57181.2022.10007295.

[66] A. Kumar, A. Shukla, V. Thada, V. Chole, J. Moolchandani and S. Sahu, "Comparative Analysis of IoT and Blockchain Technologies in Enhancing Security and Efficiency in Healthcare Systems," *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)*, pp. 1976-1981, 2024, doi: 10.1109/ICTACS62700.2024.10841246.

[67] V. Sharma, A. Gupta, N. U. Hasan, M. Shabaz, and I. Ofori, "Blockchain in secure healthcare systems: State of the art, limitations, and future directions," *Security and Communication Networks*, 2023, doi: 10.1155/2023/9827513.

[68] A. E. Hamzah, M. S. D. Zan, M. E. Hamzah, M. M. Fadhel, N. M. Sapiee and A. A. A. Bakar, "Fast and Accurate Measurement in BOTDA Fiber Sensor Through the Application of Filtering Techniques in Frequency and Time Domains," in *IEEE Sensors Journal*, vol. 24, no. 4, pp. 4531-4541, 2024, doi: 10.1109/JSEN.2023.3347307.

[69] M. M. Rashid, S.-H. Lee, P. Choi, and K.-R. Kwon, "A blockchain-based approach in healthcare supply chain using smart contracts and decentralized storage systems," *Proceedings of the 2022 ACM Conference on Information Technology for Social Good*, pp. 300-307, 2022, doi: 10.1145/3524458.3547251.

[70] M. S. D. Zan *et al*., "Spatial Resolution Enhancement of Time Domain Multiplexing Fiber Bragg Grating Sensor by Employing Differential Golay Codes," *2020 IEEE 8th International Conference on Photonics (ICP)*, pp. 54-55, 2020, doi: 10.1109/ICP46580.2020.9206502.

[71] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions," *Journal of Cyber Security and Risk Auditing*, vol. 1, no. 1, pp. 1–11, 2025, doi: 10.63180/jcsra.thestap.2025.1.1.

[72] A. E. Hamzah *et al*., "Advancing the measurement speed and accuracy of conventional botda fiber sensor systems via soc data acquisition," *Optical Fiber Technology*, vol. 84, 2024, doi: 10.1016/j.yofte.2024.103712.

[73] R. P. Puneeth and G. Parthasarathy, "Seamless data exchange: Advancing healthcare with cross-chain interoperability in blockchain for electronic health records," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, 2023.

[74] K. Anil and M. Kamble, "Health block: A blockchain based secure healthcare data storage and retrieval system for cloud computing," *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023.

[75] R. Manoj and S. Joshi, "Ensuring wallet application security by resolving reentrancy attacks in blockchain smart contracts," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 26, no. 2, pp. 927–937, 2023, doi: 10.47974/JDMSC-1779.

[76] Á. Hajdu *et al*., "Using Fault Injection to Assess Blockchain Systems in Presence of Faulty Smart Contracts," in *IEEE Access*, vol. 8, pp. 190760-190783, 2020, doi: 10.1109/ACCESS.2020.3032239.

[77] M. MohammadAmini, M. Jesus, D. F. Sheikholeslami, P. Alves, A. H. Benam, and F. Hariri, "Artificial intelligence ethics and challenges in healthcare applications: A comprehensive review in the context of the european gdpr mandate," *Machine learning & knowledge extraction*, vol. 5, pp. 1023–1035, 2023, doi: 10.3390/make5030053.

[78] K. Ider, "Assessment of the quality of user awareness of GDPR in healthcare IOT," *2021 International Conference on Biomedical Innovations and Applications (BIA)*, pp. 25-28, 2022, doi: 10.1109/BIA52594.2022.9831287.

[79] F. Fatehi, F. Hassandoust, R. K. L. Ko, and S. Akhlaghpour, "General data protection regulation (gdpr) in healthcare: Hot topics and research fronts," *Studies in health technology and informatics*, vol. 270, pp. 1118–1122, 2020, doi: 10.3233/SHTI200336.

[80] R. Lin, H. Qiu, J. Wang, Z. Zhang, L. Wu and F. Shu, "Physical-Layer Security Enhancement in Energy-Harvesting-Based Cognitive Internet of Things: A GAN-Powered Deep Reinforcement Learning Approach," in *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 4899-4913, 2024, doi: 10.1109/JIOT.2023.3300770.

[81] P. P. Hema and A. V. Babu, "Full-duplex jamming for physical layer security improvement in noma-enabled overlay cognitive radio networks," *Security and Privacy*, vol. 7, no. 3, 2024, doi: 10.1002/spy2.371.

[82] P. Yan, W. Duan, Q. Sun, G. Zhang, J. Zhang and P. -H. Ho, "Improving Physical-Layer Security for Cognitive Networks via Artificial Noise-Aided Rate Splitting," in *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 18932-18933, 2024, doi: 10.1109/JIOT.2024.3367889.

[83] M. Niranjan *et al*., "Cooperative sensing assisted cross layer qos assured routing in cognitive radio adhoc networks: Ensuring security and privacy," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 1, 2024, doi: 10.22266/ijies2024.0229.53.

[84] M. Ndiaye, K. Konate and E. H. M. Ndoye, "Anomaly Detection Algorithm Based on Smart Contracts Behaviours in Ethereum Ecosystem," *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1-7, 2023, doi: 10.1109/ICECCME57830.2023.10252520.

[85] C. M. K. Reddy, R. Chandrashekar, K. N. Kannan, H. Pal Thethi, S. Dharmireddi and R. Bajaj, "Smart Contracts and Anomaly Detection in SDN environment using Cloud-Edge Integration Model," *2023 International Conference on Emerging Research in Computational Science (ICERCS)*, pp. 1-6, 2023, doi: 10.1109/ICERCS57948.2023.10434076.

[86] S. Hisham *et al*., "Anomaly detection in smart contracts based on optimal relevance hybrid features analysis in the ethereum blockchain employing ensemble learning," *International Journal of Advanced Technology and Engineering Exploration*, vol. 10, no. 109, pp. 1552, 1579, 2023, doi: 10.19101/IJATEE.2023.10102216.

[87] G. Airlangga, "Anomaly detection in blockchain transactions: A machine learning approach within the open metaverse," *Jurnal Informatika Ekonomi Bisnis*, vol. 6, nol. 2, pp. 308–312, 2024, doi: 10.37034/infeb.v6i2.864.

[88] M. A. Fouly, T. H. A. Soliman and A. I. Taloba, "Machine Learning Techniques for Detecting Abnormal Behaviors in Blockchain Technologies: A Methodological Review," *2024 International Conference on Computer and Applications (ICCA)*, pp. 1-6, 2024, doi: 10.1109/ICCA62237.2024.10927796.

[89] J. Kim *et al*., "A Machine Learning Approach to Anomaly Detection Based on Traffic Monitoring for Secure Blockchain Networking," in *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3619-3632, 2022, doi: 10.1109/TNSM.2022.3173598.

[90] D. R. Kotoju and M. A. Khan, "Cognitive cyber threat intelligence: Ai-driven behavioural profiling for proactive security," *international journal of engineering technology and management sciences*, 2025.

[91] P. Balasubramanian, S. Nazari, D. K. Kholgh, A. B. Z. Mahmoodi, J. Seby, and P. Kostakos, "A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing," *Decision Analytics Journal*, vol. 14, 2025, doi: 10.1016/j.dajour.2025.100545.

[92] E. Kalyabin, "The method of threat assessment and interference distribution within the framework of cognitive electronic warfare," *Radioengineering*, 2024.