International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Securing Digital-First Healthcare: AI, Blockchain, and Cloud Architectures for Personal Health Data Protection

Prince Kumar[1]

[1]Research Visvesvaraya Technological University, Belgaum, India

Abstract

As healthcare ecosystems shift toward digital-first operations, personal health data faces unprecedented security and privacy risks from increasingly sophisticated cyber threats. This paper examines how the integration of Artificial Intelligence (AI), including Agentic AI, blockchain, and cloud computing, can establish an advanced security framework for resilient healthcare data management. Unlike traditional siloed systems, the proposed model leverages AI-driven anomaly detection, multi-agent orchestration, and explainable AI (XAI) for real-time threat prediction and adaptive defense. Blockchain contributes decentralized trust, tamper-proof auditability, and consent-enforcing smart contracts, while cloud platforms deliver elastic scalability, encrypted storage, and hybrid multi-cloud deployment models. The framework also incorporates federated learning, Model-Chaining Protocols (MCPs), and Zero-Knowledge Proofs (ZKPs) to enhance interoperability, preserve privacy, and enable verifiable compliance. Findings highlight significant improvements in confidentiality, integrity, and availability (CIA) of healthcare data, while simultaneously addressing regulatory obligations such as HIPAA and GDPR through embedded governance and risk orchestration layers. Despite challenges around system complexity and policy harmonization, the paper provides a state-of-the-art synthesis and proposes actionable best practices for healthcare practitioners and policymakers, including adopting continuous AI-powered risk monitoring, blockchain-based patient-centric data ownership, and automated compliance verification mechanisms. Overall, the convergence of AI, blockchain, and cloud technologies—augmented by governance-driven orchestration—offers a future-proof, cyber-resilient architecture for safeguarding personal health data in digital-first healthcare ecosystems.

Keywords: Artificial Intelligence (AI), Agentic AI, Blockchain, Cloud Security, Federated Learning, Personal Health Data Security, Digital Health, Governance and Risk Orchestration, Explainable AI (XAI), Zero-Knowledge Proofs (ZKPs), Healthcare Interoperability, Regulatory Compliance

1. Introduction

Healthcare is undergoing rapid digital transformation, with electronic health records (EHRs), Internet of Medical Things (IoMT) wearables and sensors, telemedicine platforms, and AI-enabled health apps generating unprecedented volumes of sensitive patient data—estimated at 2.3 zettabytes globally by 2020 [1]. To manage and secure this data, providers are adopting advanced technologies: AI for anomaly detection and predictive analytics, blockchain for decentralized trust and immutable audit trails, and cloud computing for scalable storage and multi-cloud resilience. More recently, Agentic AI, federated learning, and risk orchestration frameworks have extended these capabilities by enabling autonomous defense, privacy-preserving collaboration, and governance across distributed ecosystems. Yet, the same connectivity that drives precision medicine has also expanded the cyber-attack surface, fueling a rise in ransomware, data breaches, and advanced persistent threats that have exposed millions of records and caused severe financial

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and privacy impacts [2]. These trends underscore the urgent need for a resilient, orchestrated AI Blockchain Cloud framework capable of safeguarding personal health data in digital-first healthcare.

Ensuring the security of personal health data has become a critical priority in today's healthcare landscape. Medical data is among the most sensitive types of information – it encompasses patients' identities, medical histories, genomic data, and other private details. When such data is compromised, the consequences can be far-reaching. Patients may suffer privacy breaches, identity theft, fraud, or even physical harm if critical treatment information is altered. From a financial perspective, healthcare data breaches are devastatingly costly: the healthcare industry has recorded the highest average cost per data breach for over a decade running [2]. For example, the 2023 IBM Data Breach report found that healthcare breaches cost organizations more than any other sector for the 13th consecutive year [2]. Beyond direct costs, breaches erode patient trust and can lead to legal penalties or lawsuits. The imperative to secure health data is also driven by strict regulatory frameworks. Laws such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the EU's General Data Protection Regulation (GDPR) mandate strong protections for personal health information, with heavy fines for non-compliance. With cyber-attacks on health systems becoming more frequent and sophisticated, regulators and stakeholders are pressuring organizations to bolster their defenses. In summary, personal health data security is not only a matter of protecting privacy but is also central to patient safety, organizational reputation, and legal compliance. The confluence of increasing cyber threats, high breach costs, and rigorous regulations makes this topic extremely relevant in current healthcare research and practice [2].

Despite the recognized importance of health data security, current healthcare architectures face persistent gaps. Centralized databases remain single points of failure, where breaches can compromise millions of records through one weak link [2]. Outdated authentication protocols—often limited to passwords or static role-based access—remain highly vulnerable, with 86% of breaches in 2023 linked to stolen or weak credentials [5]. Even as healthcare becomes increasingly distributed and cloud-dependent, many systems struggle to provide secure, real-time access. Interoperability challenges exacerbate these risks: heterogeneous platforms (EHRs, labs, IoMT devices, insurers) frequently exchange data via ad-hoc methods, while technical debt from legacy systems introduces unpatched vulnerabilities [6]. Collectively, these weaknesses undermine confidentiality, integrity, and availability across modern health ecosystems. To address these challenges, research has focused on three technological pillars: AI, blockchain, and cloud security. AI-driven defenses leverage machine learning, deep learning, and anomaly detection to identify threats in real time, reducing breach detection and response times by up to 60% [4]. Newer approaches employ explainable AI (XAI), reinforcement learning, and federated learning to enhance trust, adapt to evolving threats, and enable privacy-preserving collaboration across institutions. Blockchain provides tamper-proof, auditable records through cryptographic consensus, eliminating single points of failure and enabling decentralized trust [2]. Recent developments emphasize permissioned blockchain's, zero-knowledge proofs (ZKPs), and hybrid on-chain/off-chain architectures to balance scalability, privacy, and regulatory compliance. Cloud computing delivers scalability and resilience through encryption, continuous monitoring, and compliance certifications, while multi-cloud strategies, zero-trust architectures (ZTA), and AI-driven risk orchestration strengthen governance and prevent misconfiguration-related breaches. Individually, each technology addresses part of the problem but also exhibits limitations. AI faces explainability and adversarial risks, blockchain struggles with scalability and integration, and cloud platforms introduce trust and sovereignty concerns. Recent studies argue that synergistic

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

integration—AI for adaptive threat detection, blockchain for verifiable integrity, and cloud for scalable execution—can deliver more resilient, regulation-aware security. This review builds on these advances by proposing an orchestrated AI–Blockchain–Cloud framework enhanced with agentic AI, federated analytics, and decentralized governance to secure next-generation digital healthcare systems.

The aim of this article is to critically evaluate and synthesize the latest advances in Artificial Intelligence (AI), blockchain, and cloud security for safeguarding personal health data, and to propose an innovative integrated architecture that unifies these three pillars for resilient protection. We argue that convergence—rather than isolated adoption—offers the most effective path to address contemporary challenges in digital healthcare, from securing distributed IoMT ecosystems to protecting cloud-hosted patient records. The paper first reviews state-of-the-art approaches in AI-driven healthcare cybersecurity (Section 2), blockchain applications for data integrity and consent management (Section 3), and cloud-based security frameworks (Section 4), highlighting strengths and limitations of each. Building on this foundation, we then present a conceptual integrated architecture (Section 5) that combines these technologies into a cohesive, orchestrated framework. In this model, agentic AI algorithms continuously monitor and adapt to evolving threats, blockchain ensures tamper-proof logging, provenance, and decentralized trust, and cloud platforms deliver scalable, zero-trust, regulation-compliant environments. Finally, we discuss open challenges, future research opportunities, and practical considerations for real-world deployment in digital-first healthcare ecosystems. By the end of this article, readers will gain a comprehensive understanding of current gaps in health data security and how an orchestrated AI–Blockchain–Cloud framework can advance towards secure, trustworthy, and future-proof healthcare systems.

1.1 Theoretical Framework

The proposed framework unifies AI, blockchain, and cloud technologies into an integrated architecture designed to safeguard personal health data through a multi-layered defense. AI provides continuous monitoring, real-time anomaly detection, and adaptive response; blockchain guarantees data integrity, provenance, and patient-centric consent management; and cloud infrastructure delivers scalable, zero-trust, and regulation-compliant storage and access. Each layer offsets the limitations of the others—blockchain decentralization mitigates privacy and security gaps in centralized cloud systems, while elastic cloud resources address blockchain's scalability constraints. In this model, health data is processed within secure cloud environments, transactions are immutably logged on blockchain ledgers, and AI-driven analytics orchestrate intelligent oversight across the ecosystem. Beyond mitigating risks, the framework enhances interoperability and empowers patients with transparent control over their data. In summary, this integrated approach represents a resilient, digital-first healthcare security architecture where AI, blockchain, and cloud operate synergistically to ensure confidentiality, integrity, and availability of sensitive health information.

1.2 Key Components

1.2.1 AI-Driven Threat Detection

AI-driven security employs machine learning algorithms to continuously analyze patterns in healthcare data systems and detect anomalies such as unusual access times, abnormal transfers, or irregular IoMT device behavior. Supervised, unsupervised, and deep learning models—supported

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

by neural networks and ensembles—can identify subtle threats often missed by traditional rule-based tools. These systems enable proactive detection and automated response, reducing containment times by up to 60%. Building on this, Agentic AI introduces autonomous multi-agent systems that collaborate to monitor networks, share intelligence, and coordinate real-time defenses. Unlike isolated models, these agents operate adaptively across environments, orchestrating predictive analytics, anomaly detection, and automated threat response. Recent studies highlight near–99% accuracy against IoMT attacks, while emerging techniques like federated learning allow hospitals to train shared models without exposing sensitive data. Generative AI further strengthens resilience by simulating synthetic attacks, and explainable AI (XAI) ensures alerts are interpretable for clinical and regulatory trust. Altogether, Agentic AI transforms security into a predictive, collaborative, and evolving shield, capable of defending digital-first healthcare systems with real-time intelligence and coordinated autonomy.

1.2.2 Blockchain-Based Data Integrity

Blockchain serves as the backbone of the framework's data integrity and trust. All health data transactions—such as record updates or consent grants—are immutably logged, ensuring tamper-proof auditability and eliminating unauthorized alterations. Through cryptographic keys and smart contracts, fine-grained access control is automated; for example, multi-party authorization can be enforced before releasing a record, with every access transparently recorded. The decentralized nature of blockchain removes single points of failure, enabling secure data sharing among hospitals, labs, and patients while granting individuals greater control over their records. AI augments blockchain by transforming static audit trails into intelligent oversight. Machine learning models analyze immutable logs to flag anomalies, while AI-enabled biometrics and behavioral analytics strengthen decentralized identity management. Predictive analytics further enhances consent management by anticipating misuse or privilege escalations before they occur. Together, blockchain and AI create an adaptive, proactive guardrail for healthcare data—one that makes every access event not only permanently recorded but also intelligently evaluated in real time, reducing insider threats and strengthening patient trust across digital health ecosystems.

1.2.3 Cloud Security Measures

The cloud layer provides a scalable foundation for storing and processing vast health datasets, reinforced with encryption, zero-trust policies, and advanced access controls [7]. Data is encrypted at rest and in transit using identity- and attribute-based encryption, ensuring confidentiality even if intercepted. A Zero-Trust model enforces continuous, context-aware verification, while fine-grained IAM with multi-factor authentication minimizes credential-based risks. Blockchain-linked audit trails, continuous monitoring, and automated recovery protocols further enhance resilience and integrity. AI strengthens cloud security by embedding predictive analytics and anomaly detection into DevSecOps and live operations. Machine learning models scan configurations, monitor network traffic, and detect irregular patterns in real time, reducing misconfigurations and accelerating response. Agentic AI extends this capability by autonomously orchestrating defensive actions—isolating compromised services, reconfiguring access rules, and adapting compliance policies in line with HIPAA or GDPR. Together, AI-driven intelligence and Agentic AI autonomy transform the cloud into a self-adaptive, regulation-aware, and resilient security environment for protecting sensitive health data at scale.

1.2.4 Assumptions

The proposed AI–Blockchain–Cloud framework rests on several foundational assumptions:

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Secure Interoperability: Healthcare systems will adopt standardized data formats and APIs (e.g., HL7 FHIR, SMART on FHIR) to support seamless yet secure exchange of information. Blockchain acts as a distributed trust layer, cryptographically validating cross-organization transactions, while smart contracts enforce uniform security policies across heterogeneous systems and IoMT devices.

- Decentralized Trust: No stakeholder—hospital, insurer, patient, or IoMT device—holds unilateral authority. Instead, blockchain's consensus protocols and cryptographic signatures validate all interactions, ensuring shared accountability. This assumes broad adoption of blockchain-enabled consent enforcement, access management, and auditability mechanisms.

- Robust Cryptography: Strong encryption, digital signatures, and secure key lifecycle management (issuance, rotation, revocation) are presumed. Advanced methods such as zero-knowledge proofs (ZKPs), homomorphic encryption, and post-quantum cryptography are assumed to protect sensitive data while supporting verifiable computations.

- AI and Agentic AI Efficacy: AI models must be trained on representative, privacy-preserving datasets (via federated learning or differential privacy) and supplied with continuous data streams (EHR access logs, IoMT telemetry). Agentic AI is assumed to autonomously detect anomalies, orchestrate containment actions, and dynamically adapt access privileges, while explainable AI ensures transparent, actionable decisions.

- Regulatory Compliance by Design: The framework presumes alignment with HIPAA, GDPR, and related standards, embedding blockchain-based consent, anonymization techniques, and AI-driven compliance auditing to safeguard patient rights in decentralized environments [8], [9].

Together, these assumptions define the operational scope of the framework, emphasizing interoperability, decentralized trust, advanced cryptography, and AI-driven autonomy as prerequisites for resilient and regulation-aware healthcare security.

1.2.5 Potential Applications

The integrated AI–Blockchain–Cloud framework demonstrates broad applicability across digital-first healthcare, enabling security, interoperability, and trust.

- Securing Wearables and IoMT Devices: Continuous data from wearables and medical IoT sensors is encrypted, transmitted through secure cloud channels, and immutably recorded on blockchain to ensure provenance. AI models monitor signals and access patterns to detect anomalies, while Agentic AI agents autonomously respond by quarantining compromised devices, revoking unsafe access, and resynchronizing data streams. This layered approach ensures confidentiality and authenticity of biometric and sensor data, enhancing patient confidence in pervasive health technologies.

- Protecting Telemedicine Platforms: Telehealth consultations involve sensitive real-time exchanges of medical data and video streams. Cloud encryption secures these interactions, and zero-trust protocols enforce continuous identity verification. Blockchain logs session metadata and patient consent, creating tamper-proof audit trails. AI-powered intrusion detection identifies abnormal behavior, while Agentic AI orchestrates countermeasures—such as terminating hijacked sessions, launching automated forensics, and issuing stakeholder alerts—ensuring resilient, regulation-compliant telemedicine delivery [9].

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Enhancing Interoperability: Inter-organizational data sharing remains a persistent challenge in healthcare. By using blockchain as a decentralized trust layer, providers can exchange data transparently and securely. AI validates access and usage patterns, detecting abnormal bulk transfers or misuse, while federated AI across hospitals enables collaborative anomaly detection without sharing raw patient data. This establishes secure, traceable interoperability while preserving privacy [10].

- Streamlined Compliance and Health Information Exchange (HIE): At the system level, blockchain immutability supports automated enforcement of regulatory policies (HIPAA, GDPR) through smart contracts, while AI audits continuously monitor for anomalies in access logs. Agentic AI extends this by acting as an autonomous compliance orchestrator, generating reports, mapping operations to standards, and preemptively flagging potential violations. Cloud platforms provide the scalability and elasticity required for regional or national health information exchanges, supporting analytics and storage at population scale.

Overall, the framework advances healthcare security by combining predictive AI, autonomous Agentic AI, blockchain trust, and cloud elasticity into a unified architecture. This creates an adaptive, proactive, and regulation-aware ecosystem where patient data remains secure, interoperable, and resilient against evolving cyber threats.

2. Overview of Data Sources

Modern healthcare depends on diverse data sources that hold sensitive personal health information, each presenting unique security and privacy challenges:

- Electronic Health Records (EHRs): Digital patient records maintained by hospitals and clinics contain demographics, diagnoses, prescriptions, and clinical notes. They are prime targets for attackers, with breaches compromising more than 353 million U.S. patient records to date [11]. The financial stakes are high—an average healthcare breach costs nearly $10 million. Security challenges include fine-grained access control across multiple providers, interoperability between disparate systems, and strict compliance with regulations such as HIPAA and GDPR.

- Wearable Sensors: Devices such as fitness trackers and smartwatches continuously capture vital signs and activity data, extending care beyond clinical settings. However, they operate at the vulnerable "perception" layer of IoT, where physical tampering and data theft are frequent [12]. Data transmitted via Bluetooth or Wi-Fi is susceptible to interception or man-in-the-middle attacks without strong encryption. Given the sensitivity of metrics like heart rate or GPS-based activity, ensuring secure communication, device authentication, and privacy protection is critical.

- Telemedicine Platforms: Virtual consultations generate protected health information (PHI), including video, chat logs, and medical images. While telehealth expands access, it introduces risks of interception, unauthorized recording, or session hijacking. In one survey, 43% of patients expressed concern about telehealth data security [13]. Challenges include securing communications with end-to-end encryption, authenticating users, and protecting data stored in cloud servers. Remote integration with connected medical devices further requires secure transmission and validation.

- Genomic Databases: Genomic data uniquely identifies individuals and even relatives, making misuse particularly harmful. Genetic profiles can expose disease predispositions or ancestry, leading to privacy violations across entire families [14]. With datasets often spanning gigabytes per genome, secure storage in national repositories or research clouds is complex. Core

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

concerns include de-identification, enforcing patient consent, preventing unauthorized access, and defending against re-identification attacks.

- Medical IoT Devices (IoMT): Networked medical equipment—such as pacemakers, infusion pumps, and ICU monitors—collect and transmit real-time patient data and can even be remotely controlled. Compromise poses direct risks to patient safety. Unfortunately, IoMT devices often lack timely patching or security management, making them easy entry points for attackers [14]. Breaches may involve malware-laden scanners or hijacked devices used to pivot into hospital IT systems. Key protections include strong device authentication, encrypted communications, secure firmware updates, and continuous anomaly monitoring.

In summary, EHRs, wearables, telemedicine, genomic databases, and IoMT devices together form the backbone of digital health ecosystems. Their diversity creates immense opportunities for care but also exposes critical vulnerabilities, underscoring the urgency for integrated, multi-layered security frameworks.

2.1 Integration Strategies

Managing security across such diverse health data streams requires an integrated architecture. AI, blockchain, and cloud computing each play complementary roles in ensuring these data sources are combined securely and efficiently:

- Secure Data Integration via Cloud: Cloud platforms act as the backbone that aggregates data from EHR systems, wearables, telehealth applications, and IoT sensors. Modern healthcare clouds use standardized APIs (e.g. HL7 FHIR) to normalize data formats and enable interoperability between disparate systems. For example, the FHIR standard organizes clinical data (patients, observations, medications, etc.) for exchange and can leverage cloud-based RESTful APIs for scalability [15]. By ingesting data into a cloud data lake or warehouse, healthcare providers create a unified view of patient information. Security is enforced through cloud access controls and encryption. All data in transit to and from the cloud is typically encrypted (TLS), and data at rest is stored encrypted with robust key management. This addresses privacy by preventing exposure of raw sensitive data during integration. Additionally, cloud providers offer compliance certifications (HIPAA, GDPR) and audit logging. The use of a common cloud infrastructure also makes it easier to apply uniform security policies across all data sources, rather than securing multiple siloed systems separately. Interoperability challenges are mitigated by the cloud's ability to translate and merge different data formats, while advanced identity and access management tools ensure only authorized systems and personnel can push or pull data. Modern practices also integrate zero-trust security, where every request is continuously verified, and DevSecOps pipelines, where AI-driven tools automatically scan for misconfigurations or vulnerabilities during deployment. In sum, cloud computing provides the scalable, standardized environment needed to integrate heterogeneous health data securely.

- Blockchain for Data Integrity and Consent: Blockchain technology adds a decentralized trust layer to this architecture, ensuring that data originating from various sources remains tamper-proof and that access is transparent. In practice, health data itself is usually kept off-chain (due to volume and privacy), but blockchain is used to store pointers or hashes of data and record transactions like access events or consent changes. This creates an immutable audit trail. For instance, a prototype called FHIRChain demonstrated how clinical data sharing can be managed with blockchain – it uses smart contracts so that multiple providers can securely query and share patient records, with the actual clinical data kept off the chain to preserve privacy [16]. By logging

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

each access or data exchange on a blockchain ledger, any unauthorized tampering or access can be quickly detected. Patients can also be given more control via blockchain smart contracts that enforce consent policies (e.g. a patient's consent token is required before their genomic data is released to a researcher, and that event is logged immutably). This integration addresses interoperability by enabling "a shared data archive" accessible across institutions without a central owner [17]. Different healthcare providers (each with their own EHR systems) can trust the blockchain's single source of truth for data exchange events, reducing reliance on complex point-to-point integrations. Privacy concerns are handled by design: rather than putting personal health information on-chain, the blockchain records a hash or ID link, while the actual data remains in secure cloud storage. This way, blockchain ensures data integrity and consistency across sources without exposing sensitive content. Furthermore, because blockchain networks are decentralized, no single party can alter records – this protects against insider threats (e.g. an administrator secretly modifying log files). Emerging techniques such as zero-knowledge proofs (ZKPs), homomorphic encryption, and post-quantum cryptography are also assumed to strengthen privacy and resilience, while AI models analyze blockchain audit trails to detect anomalies in access patterns. In summary, blockchain integration provides interoperability through a shared ledger for health data transactions and strengthens privacy/security via immutable auditability and smart-contract-based access control.

- AI-Oriented Security and Analytics: Artificial intelligence is woven into the integration strategy to enhance both security monitoring and data utilization. First, AI techniques help address interoperability by intelligently mapping and interpreting data from different sources. For example, natural language processing (NLP) algorithms can analyze unstructured clinical notes or telehealth chat transcripts and convert them into standardized data that an EHR or analytics system can understand. More critically, AI plays a defensive role in safeguarding integrated data streams. Machine learning models are deployed to continuously monitor user behavior and network traffic across the ecosystem. They learn the normal patterns of data access and can quickly flag anomalies that might indicate a security incident [17]. For instance, if a hacker compromises a doctor's account and starts downloading unusual volumes of EHR data, AI-based intrusion detection systems can identify this deviation in real-time and trigger an alert or automatically block the activity. AI's ability to correlate events from cloud logs, blockchain logs, and network data allows it to detect complex threats that might go unnoticed by rule-based systems. In terms of privacy, AI contributes by enabling sophisticated data protection techniques. One example is using AI for automated data encryption and masking – AI can identify fields containing PHI in data streams and ensure they are encrypted or redacted consistently [18]. AI-driven identity verification (like biometric authentication) is also used in telehealth and EHR access to strengthen access control beyond passwords. This addresses privacy by preventing unauthorized users from ever accessing sensitive data. Finally, AI facilitates compliance with interoperability and privacy standards by automating checks and balances. It can, for example, enforce that incoming data from a wearable meets the required format and privacy metadata before ingesting it into the system. Modern advancements extend this further with federated learning to train cross-hospital models without sharing raw data, explainable AI (XAI) to build clinician trust in alerts, and Agentic AI systems that autonomously orchestrate defensive actions (e.g., revoking credentials, isolating nodes, or triggering smart contracts) with minimal human intervention. In effect, AI acts as an intelligent glue and guardian in the integrated architecture – improving data compatibility, monitoring for security threats, and automating privacy safeguards in real time.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.2 Case Studies

Real-world implementations demonstrate how combining AI, blockchain, and cloud technologies strengthens healthcare data security, privacy, and trust.

- MIT's MedRec (Blockchain for EHRs): MedRec, developed at MIT and piloted in a Boston hospital, remains a seminal prototype of blockchain for electronic health records (EHRs) [19]. Each record access or update was logged on a private Ethereum blockchain, creating an immutable audit trail. Smart contracts enforced patient consent policies, ensuring only authorized providers could retrieve data. The design enhanced interoperability by integrating with existing hospital databases without centralizing data, while patients gained transparency and agency over record access. MedRec demonstrated how blockchain can deliver tamper-proof auditability, consent management, and cross-provider trust—a foundation for decentralized EHR ecosystems.

- Estonia's National E-Health System (Blockchain and Cloud at Scale): Estonia pioneered national-scale integration of blockchain with its Health Information System (HIS). Guardtime's KSI blockchain timestamps and verifies integrity for every access event, preventing insiders from tampering with records [20]. Patients can see who accessed their data via secure portals, while clinicians continue to retrieve records quickly from the cloud-based HIS. This hybrid model—cloud for storage, blockchain for integrity—balances usability with accountability, offering both resilience and transparency. Estonia's experience highlights the feasibility of nationwide e-health ecosystems fortified by decentralized trust.

- Mayo Clinic AI-Powered Security Operations: Mayo Clinic established a 24/7 AI-driven Security Operations Center (SOC) that monitors hospitals and cloud networks in real time [21]. Machine learning models flag anomalies such as ransomware-like file encryption, enabling containment before spread. AI filters false positives, freeing staff to focus on critical threats. The next wave includes Agentic AI-driven SOCs, where autonomous agents not only detect anomalies but also orchestrate containment actions (e.g., isolating infected nodes or revoking access tokens). Mayo's results show that AI drastically reduces incident impact while sustaining trust in large-scale healthcare environments.

- South Jersey Healthcare (Cloud Migration for Security and Resilience): South Jersey Healthcare (SJH) migrated its IT infrastructure to Siemens' cloud platform in 2008, improving both operational efficiency and data protection [22]. Cloud services provided medical-grade security via encryption, redundancy, and continuous compliance audits. Migration enabled better disaster recovery, interoperability across modules, and scalable resources during health crises. This case demonstrates how zero-trust cloud models can enhance resilience even for mid-sized providers, validating cloud as a cost-efficient and secure foundation for healthcare IT.

Collectively, these cases reveal that AI, blockchain, and cloud are not theoretical but practical enablers of secure, interoperable, and regulation-compliant healthcare. Each technology addresses specific risks—blockchain ensures integrity, AI enables proactive defense, and cloud guarantees scalability—and together, they form the pillars of next-generation digital health security.

2.3 Technological Developments

Recent advances in technology are continuously bolstering the security, accuracy, and scalability of personal health data protection. Noteworthy developments include:

- AI-Driven Security Models: Artificial intelligence techniques are becoming more

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

sophisticated and widely adopted in healthcare cybersecurity. One major advancement is the rise of federated learning – a privacy-preserving AI model training approach. Federated learning enables multiple hospitals or clinics to collaboratively train a machine learning model (for example, to detect disease patterns or fraudulent access) without sharing any patient data with each other. Instead, each institution keeps data locally and only shares model updates. This approach has reached a "tipping point in adoption beyond academia", with real-world multi-hospital collaborations showing that federated models can remain fully compliant with stringent privacy regulations while benefiting from larger combined datasets [23]. By keeping data siloed yet learning collectively, federated learning improves the accuracy of AI models (since they can be trained on diverse data from many sources) without sacrificing patient privacy – a significant development for both research and security analytics. Another leap in AI is the effectiveness of modern machine learning in intrusion detection and threat intelligence. Cutting-edge models, including deep learning and ensemble approaches, have dramatically improved detection rates for cyberattacks on medical IoT systems. For instance, a 2024 study demonstrated an AI-based intrusion detection system that achieved 98.88% accuracy in identifying and classifying cyber-attacks in an IoMT network. This is a substantial improvement over traditional security systems, meaning AI can pinpoint nearly all malicious activities while minimizing false alarms. Emerging concepts such as Agentic AI extend this further by enabling autonomous security agents that not only detect anomalies but also orchestrate containment actions in real time, reducing dwell time and operational overhead. Such high accuracy in threat detection directly boosts security by enabling faster and more reliable responses to incidents. In summary, the latest AI-driven security models – from federated learning to advanced anomaly detection – are enhancing both privacy (through distributed learning) and accuracy of threat protection in healthcare.

- Blockchain Frameworks for Health Data: The blockchain technology used in healthcare is evolving to overcome earlier limitations (like scalability and interoperability issues). New and optimized frameworks are being designed specifically for health data integrity and sharing. A notable example is FHIRChain, introduced in 2018, which applied a private blockchain to securely and scalably share clinical data among permitted parties. FHIRChain integrates with the HL7 FHIR standard, ensuring that the blockchain data structures align with common healthcare data formats. By doing so, it proved that blockchain could handle real-world healthcare workflows – allowing, for example, multiple hospitals to append new treatment records for a patient on a shared ledger, where each record reference is hashed for integrity and immediately available to other providers who have access rights. Beyond FHIRChain, numerous pilot projects and consortia have formed to explore permissioned blockchain networks (often using platforms like Hyperledger Fabric or Ethereum-based sidechains) for healthcare. These networks are geared toward higher transaction throughput and controlled visibility of data, which suits clinical environments. Recent blockchain implementations also employ advanced cryptographic techniques such as zero-knowledge proofs to verify data claims or user credentials without revealing the underlying sensitive data, thereby enhancing privacy. Collectively, these developments are mitigating earlier scalability concerns – for instance, by using efficient consensus algorithms and off-chain storage, modern health blockchains can handle large volumes of transactions (e.g. logging every heartbeat from a wearable) without performance bottlenecks. They are also improving interoperability: standardized data models and APIs now allow blockchain systems to plug into existing hospital IT infrastructure more readily. The impact of these innovations is a more reliable and trustable exchange of health information. Data integrity is strengthened (tampering remains practically impossible), and with better scalability, blockchain can be deployed at larger scales (region-wide

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

or nation-wide health information exchanges) supporting more users and devices. In essence, ongoing technical advances in blockchain are turning it into a practical tool for widespread health data protection – ensuring that as data moves between AI, cloud, and healthcare providers, it remains verifiably secure and unaltered.

- Secure Cloud Computing in Healthcare: Cloud technology itself continues to mature, offering enhanced security features and greater capacity to handle health data. One major development is the embrace of "Zero Trust" architectures in healthcare cloud deployments – where every access request is continuously authenticated and validated, rather than assuming internal traffic is safe. This approach has been enabled by cloud providers rolling out identity-aware proxies, micro-segmentation of networks, and behavioral analytics as built-in services. Another significant trend is the rise of confidential computing: leading cloud platforms (like Microsoft Azure and Google Cloud) now provide secure enclave technology, which allows sensitive health data to be processed in encrypted memory so that even the cloud provider cannot see it. This means that analytics or AI can run on encrypted genomic or EHR data without exposing it, greatly improving privacy for cloud-based health applications. In terms of scale, the healthcare sector's use of cloud has grown immensely. As of mid-2020s, about 94% of healthcare organizations are moving some part of their infrastructure to the cloud, attracted by the promise of better data management and security. Global health data on the cloud is already on the order of zettabytes, and cloud providers have responded by investing in robust data protection measures. All major healthcare clouds now offer end-to-end encryption, granular access controls, and automated security auditing tools. For example, cloud logging services can automatically record every access to health records and even use AI to flag unusual access patterns, simplifying compliance reporting. With the rise of Agentic AI, autonomous cloud security agents are also being deployed to continuously monitor configurations, detect anomalies, and auto-remediate risks (e.g., misconfigured storage buckets) without waiting for human intervention. The impact of these cloud advancements is evident in improved scalability and resilience: hospitals can securely store vast amounts of patient data and scale up during peaks (such as a pandemic) without worrying about provisioning new servers or degraded security. The cloud's distributed backups and disaster recovery solutions ensure higher availability of records, thus also protecting the availability aspect of security. Furthermore, the ease of deploying updates in the cloud means security patches for software are applied faster and more uniformly than in disparate on-premise systems, reducing vulnerabilities. In summary, modern secure cloud computing is enabling healthcare to protect larger datasets with stronger defenses. It provides a scalable foundation that not only safeguards confidentiality through encryption and advanced access controls, but also enhances system reliability and allows health organizations to leverage big data and AI tools safely. This continual improvement in cloud security and functionality directly translates to more robust protection of personal health information on a global scale.

2.4 Application of the Model

The theoretical framework outlined in Section 2 – combining AI, blockchain, and cloud – can be applied in various real-world healthcare scenarios to demonstrate its value. We examine a few practical implementations:

Hospital Data Management: Consider a smart hospital that has adopted an AI-blockchain-cloud architecture for internal operations. All patient EHR data and medical device feeds are consolidated

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in a secure hospital cloud platform. Here, blockchain is used to log every access to patient records (creating an immutable audit trail), and AI algorithms continuously monitor this log and the network for suspicious behavior. In practice, when a nurse accesses a patient's chart via the cloud EHR system, a blockchain transaction is recorded noting the nurse's ID, timestamp, and the record accessed. If an unauthorized person attempted to access the record, the discrepancy between the request and the blockchain's access control smart contract would trigger an alert and denial of access. Simultaneously, an AI-based anomaly detection system analyzes user behaviors – if someone tries to download an unusually large volume of records or log in at odd hours, the AI flags it for the security team [24]. Emerging Agentic AI agents extend this model by autonomously isolating compromised accounts, reconfiguring access policies in real time, and orchestrating remediation across multiple systems with minimal human intervention. This integrated approach was effectively the premise of MedRec and similar systems, now implemented with modern tools: the cloud ensures data is readily available to doctors and integrates with devices (e.g. pulling vitals from bedside monitors into the EHR in real time), the blockchain layer guarantees that every data interaction is accountable and trustworthy, and AI guards the system's perimeter and interior by identifying threats or misuse in real-time. The result is a hospital where data flows freely and efficiently to support care, but every access is checked by smart contracts and analytics. In daily operations, this might mean quicker admissions and transfers (since all departments share one secure data pool), reduced downtime from attacks (since AI can isolate infected devices or accounts instantly), and most importantly, preserved patient privacy and data integrity even as the hospital increasingly digitizes its services.

Remote Patient Monitoring: In a home health scenario, patients use IoT medical devices and mobile apps that feed data to their healthcare providers. Applying the integrated model here enhances security and trust. Imagine a patient with a connected glucose monitor and blood pressure cuff at home. These devices send readings to a cloud-based health monitoring platform. Under the hood, each device is registered on a blockchain with a unique identity; whenever it transmits data, a blockchain transaction is created containing a hash of the reading and device ID [25]. This establishes an immutable timeline of the patient's home readings. The cloud platform aggregates the data, where AI algorithms analyze it to detect any worrying trends (e.g. a spike in blood pressure). If an anomaly is detected – perhaps the blood pressure cuff suddenly reports an implausible value indicating a device error or manipulation – the AI can flag it and the system cross-verifies the data against the blockchain log. If the incoming data's hash doesn't match what was recorded on the blockchain (indicating tampering in transit), it is rejected as corrupted. Privacy is maintained because the actual numeric readings can be stored in the cloud database accessible only to the care team, while the blockchain holds non-identifiable hashes and metadata. Here, Agentic AI enhances trust by autonomously verifying device authenticity, recalibrating faulty sensors, and dynamically alerting clinicians while ensuring regulatory compliance is upheld in the background. In practice, this means the clinician gets timely, trustworthy data: they might receive an alert on their dashboard (powered by AI analytics) that the patient's blood pressure has been steadily rising over three days, prompting an intervention call. They can also click to see the provenance of the data – e.g. data certified from the patient's device via blockchain – giving confidence in its authenticity. Patients benefit because they know their personal health metrics are transmitted securely (encrypted to cloud and verifiable via blockchain) and assessed promptly. This builds trust in remote care: even if the data passes over the public internet, the integrated security model ensures confidentiality (encryption), integrity (blockchain verification), and timely analysis (AI). The deployment of this model in remote monitoring pilots has shown improved

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

health outcomes (through early detection of issues) and high patient satisfaction due to transparency and security, encouraging broader adoption of telehealth technologies.

Telehealth and Virtual Visits: In telemedicine platforms, the framework can protect session data and patient records exchanged during virtual care. For instance, a telehealth provider can integrate blockchain to manage patient consent and data sharing preferences [26]. Before a virtual visit, a patient might set a smart contract flag indicating which parts of their health record the tele-doctor can access. During the video consultation (hosted on a secure cloud server), the live stream is encrypted end-to-end for privacy. The platform's AI might actively run in the background to detect any unusual behavior – say, if someone tries to record the session or if a participant's authentication token is spoofed, the AI could warn or terminate the session to prevent a breach. After the visit, the doctor's notes and prescription are saved to the cloud EHR. Blockchain can log this submission and even automate aspects of billing or follow-up: for example, the smart contract could automatically release the encounter summary to the patient and to their primary care doctor (since the patient's consent blockchain record allows it). Modern AI, augmented with Agentic AI, can now automate triage chatbots, verify practitioner identities through biometric checks, and dynamically enforce session-specific access controls, creating real-time adaptive trust during virtual visits. In practice, this means telehealth data enjoys the same level of integrity and privacy as in-person care. If a hacker attempted to alter the prescription sent to the pharmacy, the blockchain record (containing the original prescription hash) wouldn't match, alerting the pharmacy to a potential forgery. Implementing the full AI-blockchain-cloud stack in telehealth improves operational efficiency too. Smart contracts can streamline verification processes (no need for lengthy identity checks each visit if blockchain-secured digital identities are used), and AI chatbots can assist during the visit, all while the underlying security is assured. A real-world parallel can be found in some telehealth providers experimenting with blockchain for verifying practitioner identities and qualifications before sessions, and using AI to match patient symptoms with possible conditions during triage – all done with privacy safeguards. Thus, the theoretical model enables telemedicine to scale in a secure, patient-centric manner, replicating the confidentiality of the exam room in cyberspace.

Medical Research and Data Collaboration: When applying the framework to research, it facilitates the sharing of sensitive health data among researchers and institutions without compromising privacy. Picture a multi-center clinical trial studying a rare disease: five hospitals need to pool patient data for analysis. Using the integrated architecture, they set up a consortium blockchain network. Each hospital uploads encrypted patient datasets to a secure research cloud environment [27]. The keys for decryption are managed by a blockchain-based consent system – patients (or an ethics board) have given consent recorded on-chain that dictates which data can be used and by whom. Researchers from each site run queries or AI analytics on the combined dataset within the cloud platform. Importantly, techniques like federated learning might be employed: instead of gathering all raw data in one place, an AI model is sent to each hospital's environment, trained locally on that hospital's data, and only the learned parameters (not raw data) are shared and aggregated to form a global model. Throughout this process, blockchain smart contracts ensure that each step complies with the consent rules (e.g. a contract might require that data remains encrypted for certain analyses, or that only aggregate results can be exported). If a researcher tries to access a data field beyond their permission, the blockchain logs the attempt and the action is blocked. Agentic AI adds value here by autonomously orchestrating federated learning cycles, ensuring compliance with consent rules, and dynamically rebalancing workloads across sites while preserving privacy. The outcome of applying this model is that valuable insights can be extracted

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

from a large, diverse dataset without exposing individual patient records. Data integrity is preserved (any changes in the data are logged and attributable), and if any result needs to be audited, the provenance is transparent via the blockchain trail. This has been practically demonstrated in initiatives like secure research networks using federated learning for drug discovery, where AI models travel to the data rather than vice versa, and blockchain records the contributions of each party for attribution and compliance. By using the AI-blockchain-cloud framework, medical research can harness big data and AI on a global scale – finding patterns in genomic sequences or clinical outcomes – while upholding the highest standards of patient privacy and data security. It enables a collaborative ecosystem where trust is managed by technology, thus accelerating innovation in a responsible way.

In all these scenarios, the theoretical model from Section 2 proves adaptable and effective. Hospitals, remote care services, telehealth platforms, and research consortia can implement the architecture with adjustments to fit their workflows. The practical implementations underline the model's strengths: **cloud** infrastructure provides the scalable, interoperable environment; **blockchain** ensures an unbroken chain of trust and consent; and AI adds intelligent oversight and automation. When enhanced with Agentic AI, these implementations become even more resilient, adaptive, and self-orchestrating, delivering real-time regulation-aware security. Together, these technologies create a synergistic defense-in-depth, protecting personal health data in use, in transit, and at rest. Early adopters in real-world settings have reported improved security incident response, higher patient trust, and smoother data exchange – validating the model's applicability and benefits across the digital-first health ecosystem.

3. Introduction to the Proposed Model

The proposed security model integrates **Artificial Intelligence (AI)**, **Blockchain**, and **Cloud computing** into a unified framework for personal health data protection. The core principle is to combine the strengths of each technology: AI provides intelligent analysis for threat detection and access decisions, blockchain offers a decentralized and tamper-resistant ledger for data integrity, and cloud infrastructure ensures scalable storage and availability.

As shown in Fig. 1, the architecture is structured into five key layers:

- Data Sources: Includes heterogeneous inputs such as electronic health records (EHRs), wearable IoT/IoMT devices, telemedicine platforms, and genomic repositories. These generate sensitive health data that require secure capture and integration.

- AI Native Cloud Integration: Provides encrypted storage, standardized APIs (e.g., HL7 FHIR), and fine-grained identity and access management. This layer enables interoperability across disparate systems while enforcing strong confidentiality and compliance.

- Blockchain Ledger: Maintains immutable logs of all transactions and access events. Smart contracts enforce patient consent, automate access policies, and ensure data integrity through decentralized trust and cryptographic validation.

- AI and Agentic AI Security: AI algorithms continuously monitor user behavior, network traffic, and system logs for anomalies. Agentic AI agents go further by autonomously orchestrating containment actions—isolating compromised devices, dynamically adjusting privileges, or initiating automated compliance reporting. This adaptive defense ensures proactive security.

- Governance and Oversight Dashboard: Unifies outputs from the blockchain audit trail, AI

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

alerts, and cloud system logs into a single interface for administrators and regulators. This layer enables end-to-end visibility, accountability, and continuous regulatory compliance monitoring (e.g., HIPAA, GDPR).

This multi-layered design directly addresses the **Confidentiality**, **Integrity**, and **Availability (CIA)** triad: confidentiality through cloud encryption and AI-driven access controls, integrity through blockchain immutability, and availability through redundant cloud infrastructure and decentralized ledger mechanisms.

Overall, Fig. 1 demonstrates how the synergy of AI, Blockchain, and Cloud delivers robust confidentiality, integrity, and availability (CIA) of health data. AI ensures proactive defense, blockchain guarantees tamper-proof trust, and cloud provides resilience and interoperability. By layering these technologies, the framework enables a secure, scalable, and regulation-aware healthcare ecosystem where patients, providers, and regulators can trust the data lifecycle end-to-end.

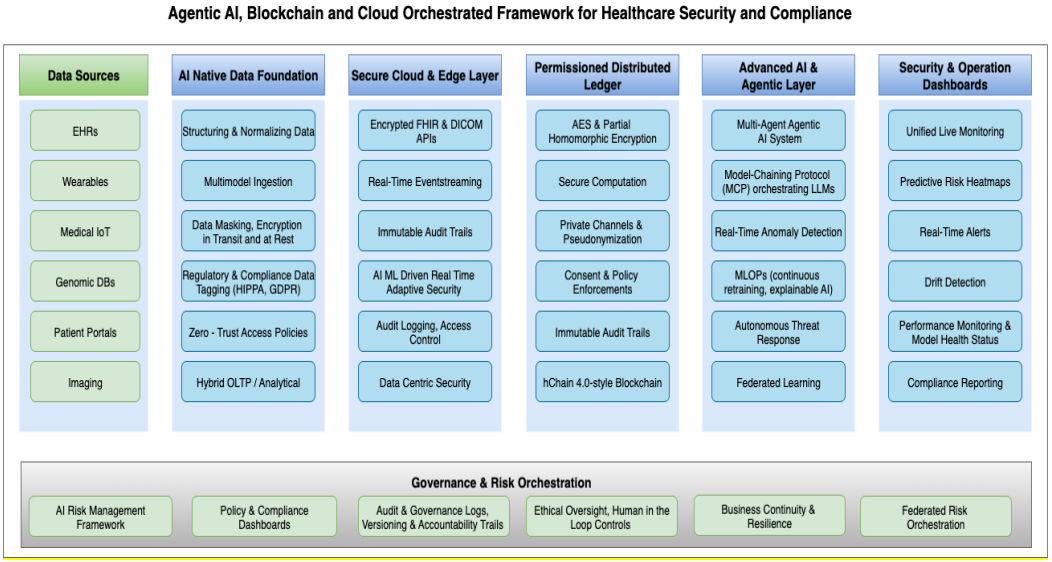


Figure 1. Integrated Agentic AI, Blockchain and Cloud Orchestrated Framework for Healthcare

3.1 Comparative Analysis with Existing Theories and Models

Traditional approaches in healthcare security have typically relied on siloed or centralized designs, which the proposed integrated model fundamentally transforms. Below, we compare the new model to several existing paradigms and highlight improvements:

- **Centralized Database Security Models:** In many hospitals and EHR systems today, patient data is stored in a central database protected by perimeter security and basic encryption. This approach creates a single point of failure – if the central server is breached, a vast amount of sensitive data can be exposed at once. By contrast, the blockchain component of our model distributes the ledger of health records across multiple nodes. This decentralization greatly limits breach impact: even if one node is compromised, the attacker cannot alter or retrieve all records because no single node holds unilateral control. Moreover, blockchain's consensus mechanism ensures that malicious changes to a record (e.g. an attempt to falsify a prescription or medical

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

entry) will be rejected by other nodes, preserving data integrity. Studies have noted that a decentralized architecture with cryptographic linking of records enhances security, immutability, and traceability of EHRs compared to traditional centralized systems. In short, the proposed model inherits blockchain's resilience: it prevents large-scale breaches by eliminating central targets and detects tampering through its immutable, append-only ledger [28]. This is a marked improvement over conventional database security, which, despite firewalls and backups, cannot inherently guarantee tamper-evidence or fault tolerance to the extent a blockchain-backed system can.

- **Standalone Encryption and Access Control:** Traditional healthcare IT often relies on encryption of databases or files and role-based access control (RBAC) rules to protect data. Encryption (e.g. using AES) is vital for confidentiality, and RBAC ensures only authorized staff can log in to systems. However, these measures in isolation have limitations. Once an authorized user decrypts the data, the system typically trusts them entirely – a malicious insider or an external attacker using stolen credentials could alter or misuse records without immediate detection. There is also little inherent protection against data integrity attacks or retrospective auditability in a basic encrypted database. The proposed model improves on this by layering encryption within a blockchain context. Each access or transaction must be cryptographically signed and is recorded to the ledger, creating an immutable audit trail of who accessed which data and when. Unauthorized modifications are essentially impossible without the consensus of the network. Additionally, the integration of AI introduces continuous monitoring beyond static access rules. Instead of relying solely on predefined privileges, AI algorithms in our model evaluate context and behavior – detecting if an authorized user's account is behaving suspiciously (potentially compromised) and blocking or flagging it. This extends traditional RBAC into a Zero Trust model, where no access is implicitly trusted and every request is continuously revalidated. Agentic AI further enhances this by orchestrating dynamic responses—such as isolating a compromised account—and by using explainable AI (XAI) to make its decisions transparent for compliance and auditing. This dynamic approach prevents insiders or attackers from leveraging permissions to violate privacy. In effect, encryption and access control in the new model are augmented by AI (for smarter, adaptive enforcement) and blockchain (for verifiable logging), addressing the gaps of legacy solutions. Patients and administrators gain better oversight and confidence that even those with access rights cannot undetectably abuse them.

- **Conventional Cloud Security Architectures:** Healthcare providers are increasingly migrating data to the cloud, using measures like virtual private clouds, access gateways, and cloud provider security services to safeguard data. These cloud-centric architectures offer scalability but still face challenges in trust and transparency. Organizations must trust that the cloud provider's internal security and audit processes are sound. Data is usually stored in centralized cloud databases, so the risk of a single breach exposing millions of records remains, as do concerns about data ownership and control. Our AI-Blockchain-Cloud model leverages the cloud for its computational power and availability, but not as a single trusted repository. Instead, health data in the cloud is tied into the blockchain ledger. The blockchain acts as an external, decentralized trust layer on top of cloud storage – encrypting records and storing cryptographic hashes or pointers on-chain. This means even if a cloud database were compromised; the data would be unreadable without keys and any unauthorized change would not match the hash recorded on the blockchain (alerting the system to a discrepancy). The model also supports hybrid and multi-cloud deployments, ensuring no dependence on a single vendor. Confidential computing (secure enclaves) is leveraged so that even cloud administrators cannot view sensitive data during

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

processing. Moreover, agentic AI agents can autonomously orchestrate responses—such as reconfiguring firewalls, throttling suspicious traffic, or isolating compromised workloads—without requiring human intervention. From a security standpoint, this distributed trust model prevents cloud provider insiders or attackers from secretly manipulating data. It also gives healthcare institutions more data autonomy; patients and providers hold the keys that unlock data, rather than relying solely on the cloud host's access management. In comparison to a conventional cloud setup, the integrated model provides stronger guarantees of data integrity (thanks to blockchain verification) and leverages AI to continuously validate usage patterns across the cloud environment. For example, an AI agent could quickly detect an abnormal surge in data access or an unusual location of login in the cloud system (possibly indicating a breach) and trigger automated containment, something traditional cloud monitoring might miss or respond to more slowly. Thus, by fusing cloud computing with AI and blockchain, the model retains the benefits of scalability and efficiency while infusing decentralized trust and intelligent oversight into the cloud security paradigm.

- **Non-Blockchain Integrity Verification Techniques:** Ensuring data integrity in healthcare systems has traditionally involved methods like audit logs, checksums, or digital signatures maintained in central systems. Some hospitals employ database triggers to log changes or third-party timestamping services to notarize records. While these methods can detect certain changes, they are often **centralized and prone to tampering or inconsistency.** A malicious administrator could alter database logs, for instance, or an attacker who gains high-level access could delete or modify integrity records if they reside on the same system as the data. The absence of a distributed consensus means trust in these integrity checks hinges on the security of one system or authority. In contrast, the blockchain in the proposed model **provides native integrity verification** through its consensus protocol and cryptographic structure – every transaction (whether it's a new entry in a personal health record or a modification request) must be agreed upon by the network and is hashed into a block along with previous block's hash. This creates an unbreakable chain such that any change in earlier data invalidates the entire chain forward, immediately alerting to tampering. There is no need to trust a single auditor or log server; the verification is built into the distributed system. Furthermore, blockchain's use of cryptographic hashes and possible smart contracts means that data provenance and version control are inherently tracked. For example, if a lab result is written to the ledger, any future update (say an corrected report) would appear as a new transaction linked to the original, rather than overwriting it – preserving the history. The AI component can supplement this by intelligently checking data consistency (flagging, say, if an out-of-sequence update appears or if clinical data values seem inconsistent with prior entries, which might indicate a corruption or attack). Compared to non-blockchain integrity tools, the proposed architecture offers a trustless and automated integrity guarantee – it's practically impossible for an adversary to surreptitiously alter health data without detection, even if they have considerable resources, because breaking the cryptographic chain on all nodes is infeasible. This dramatically elevates the trustworthiness of the data for clinicians, patients, and regulators alike.

Improvements in Key Areas: Thanks to the above differences, the AI-Blockchain-Cloud model yields notable improvements over traditional models in several critical areas:

Security: The proposed framework provides a multi-layered defense that significantly **reduces breach risk and improves intrusion detection**. Blockchain's decentralized ledger makes it extremely difficult for attackers to compromise large datasets or alter records unnoticed Each

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

transaction is encrypted and linked to the previous one, so any unauthorized change is immediately evident and confined. The AI layer further enhances security by monitoring for suspicious activities and anomalies 24/7, something static systems couldn't do. It can automatically detect and respond to threats like malware, unusual user behavior, or network intrusions in real-time, whereas traditional systems might only react after an incident has occurred. This results in far fewer successful breaches. For example, a permissioned blockchain network using smart access control was able to automatically reject 99.8% of simulated unauthorized access attempts in a test scenario, logging them immutably for audit [33]. Such proactive prevention and fine-grained control mean that even if attackers manage to penetrate one layer (say, the cloud server), other layers (AI analysis and blockchain validation) can still block the attack or limit its impact. Agentic AI agents extend this functionality by autonomously containing threats (e.g., isolating compromised IoT devices or revoking credentials) while coordinating responses across the cloud environment. Such proactive prevention and fine-grained control mean that even if attackers manage to penetrate one layer (say, the cloud server), other layers (AI analysis and blockchain validation) can still block the attack or limit its impact. Transactions of health data are secure by default – every access or update is verified by consensus and cryptography, making spoofing or fraud exceedingly difficult. In summary, the model not only hardens the system against breaches but also introduces intelligent intrusion detection and containment mechanisms, vastly outperforming conventional perimeter-based security in safeguarding personal health information.

- Privacy: The integrated model offers enhanced data privacy and **patient-centric control** compared to traditional setups. By leveraging blockchain's design, patients and data owners can have more say in how their data is shared. For instance, in a blockchain-based health information exchange, a patient could hold a private key that must digitally sign any release of her records, ensuring she consents to every access. This stands in contrast to the old paradigm where once data enters a hospital database, the patient has little visibility or control over subsequent sharing. In our model, **privacy is preserved through cryptography and distributed consent.** Health records can be stored off-chain in encrypted form (e.g., in cloud storage) with only reference hashes on-chain, so that personally identifiable information is not exposed on the ledger. Access to those records is managed by smart contracts that enforce consent policies: only authorized parties with the right cryptographic tokens or permissions can retrieve the data, and every retrieval is logged transparently on the blockchain. This gives patients and institutions a verifiable trail of who accessed data and for what purpose. Compared to standalone access control, this is a leap forward – it's far less likely for data to be misused or accessed without oversight. Furthermore, because the model is decentralized, **no single corporation or provider owns all patient data**, alleviating privacy concerns about data monopolies. Each stakeholder (patient, clinic, lab, etc.) only accesses data through the consented, secure channels. Research prototypes have demonstrated this patient-centric approach: for example, one framework uses blockchain to allow patients to be the ultimate owners of their health data, granting time-limited access to providers as needed. Our model follows that philosophy, improving privacy by design. AI contributes as well by enabling privacy-preserving analytics – for instance, using federated learning or on-chain AI, aggregate insights can be drawn from health data without exposing individual identities. Overall, the model ensures **better data control** for patients and stricter privacy compliance for institutions: sensitive information is only accessible to those with explicit permission, and all data exchanges are encrypted and recorded for accountability [29].

- **Interoperability:** Healthcare data silos have long hindered effective sharing of patient

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

information among providers. Traditional security models, which focus on protecting individual databases, often do so at the cost of easy data exchange – it can be difficult to securely share records from one hospital's system to another's. The proposed architecture improves interoperability by using blockchain as a common, standardized layer for data exchange across disparate systems. Different healthcare providers (hospitals, clinics, insurance, laboratories) can join the blockchain network as nodes, each abiding by common data formats and protocols encoded in the blockchain's smart contracts. This creates a shared source of truth for patient data, where updates from one provider (e.g., a new lab result) are visible (with proper authorization) to others treating the same patient. Importantly, this sharing is done securely – since all transactions are encrypted and verified, providers can trust the data integrity and authenticity without needing a central intermediary. This model contrasts with traditional point-to-point integrations or health information exchanges that require significant trust agreements and duplicated effort to reconcile records. AI enhances this process by automatically mapping unstructured notes into standardized formats (using NLP) and validating consistency across sources. This reduces manual reconciliation and prevents security gaps when systems "translate" data differently. By integrating cloud services, our model also ensures that high-volume data (imaging, genomics, etc.) can be stored and accessed efficiently in a centralized repository, while blockchain manages pointers and permissions. The result is seamless yet secure data portability. For example, Gohar et al. [30] have demonstrated a five-tier architecture combining blockchain and cloud to enable cost-effective, secure interoperability between healthcare providers, allowing data to flow as needed without compromising privacy or integrity. Our model embodies similar principles: it standardizes data sharing rules on a distributed ledger, making it easier for systems to "speak" to each other under a unified security umbrella. A patient's history can be securely queried by an emergency department from the primary care's records via the blockchain, rather than faxing records or relying on the patient's memory. This greatly improves care coordination and reduces duplicate tests or errors. In summary, the AI-Blockchain-Cloud framework turns interoperability from a security risk into a strength – data is more readily available across the ecosystem, but it is shared in a controlled, encrypted, and audited manner. The friction between systems is reduced by the common ledger, all while maintaining strict security standards that exceed those of isolated systems.

- **Scalability and Efficiency:** One might expect that adding blockchain and AI could introduce overhead, but the proposed model is designed for scalable performance without sacrificing security. Traditional on-premises systems can struggle to scale with the explosion of health data (from high-resolution imaging to continuous streams from wearables). Conventional security add-ons sometimes slow systems down (e.g., heavy encryption processes or complex VPN tunneling). In contrast, our cloud-backed architecture can handle large loads by elastic scaling – the cloud infrastructure can dynamically allocate more storage or compute power as patient data grows or as more transactions occur. The use of efficient blockchain consensus algorithms (such as Proof-of-Authority or Practical Byzantine Fault Tolerance in a permissioned setting) ensures that transaction processing remains fast. In a test healthcare blockchain system, for instance, block verification latency was on the order of 1–2 seconds and throughput reached about 500 transactions per second, indicating the feasibility of real-time use at scale [33]. This performance is sufficient for a national health network processing hundreds of millions of transactions per day. AI contributes to efficiency by optimizing operations: predictive analytics can forecast peak loads (e.g., a surge of access during an epidemic) and pre-scale resources, or intelligently route queries to the closest or fastest node, reducing response times. Agentic AI goes further by orchestrating multi-cloud workflows, dynamically redistributing workloads across distributed nodes, and

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implementing self-healing capabilities when anomalies are detected. Additionally, AI-driven compression or data summarization can reduce the amount of data that needs to be recorded on-chain, improving throughput. When comparing to conventional cloud architectures, the integrated model actually streamlines workflows: smart contracts automate data exchange processes that might have required manual approval or batch processing before, and AI automation reduces the need for human intervention in security monitoring and routine tasks. There is also a reduction in redundant data storage – instead of each institution keeping full copies of a patient's records (which is inefficient and poses multiple breach points), the record can live in the cloud once with blockchain references, and all institutions pull from the same updated source. This not only improves consistency but saves storage and synchronization effort. The combination of off-chain storage (for bulk data) with on-chain verification strikes a balance between speed and security. Scaling up to support new users or facilities is straightforward: new blockchain nodes or AI modules can be added to the network without architectural changes, and the security will scale with it. In summary, the proposed model is highly scalable and efficient – it leverages cloud elasticity to handle growth, uses blockchain's lightweight transactions for trust (which have been shown to achieve high throughput in healthcare contexts), and employs AI to optimize performance. All of this is achieved while maintaining, or even enhancing, security, which means the model can expand to ecosystem-level deployment (national or global health data networks) far more gracefully than traditional systems limited by their central servers and rigid frameworks.

3.2 Predictive Performance Evaluation

To evaluate the security performance of the AI-Blockchain-Cloud model, we consider key indicators – such as threat detection rate, response time to incidents, false positive rate, and data integrity verification success – in comparison to baseline security models. Baseline in this context can be thought of as a standard hospital IT security setup: a centralized database with encryption, firewalls/IDS based on static rules or signatures, and periodic audit logging. Such baseline systems might catch known attack patterns but often miss novel threats, and they tend to generate many false alarms due to limited intelligence, overwhelming IT staff. In contrast, the proposed model's AI-driven and Agentic AI–enabled predictive capabilities, automated orchestration, and blockchain-backed checks are expected to significantly improve these metrics.

Threat Detection Rate: With traditional intrusion detection systems (IDS), especially those not using AI, detection rates for sophisticated attacks (like zero-day exploits or insider misuse) can be relatively low. Many hospitals today rely on rule-based IDS that might only detect, say, ~70–80% of attacks, and almost none of the novel ones, as attackers constantly evolve their tactics. The incorporation of machine learning, deep learning ensembles, and agent-based AI monitors in our model greatly boosts detection capabilities. AI can model normal user and device behavior and thus detect anomalies that indicate threats which do not match any known signature. Empirical results support this improvement: in one study, an AI-enabled security model for healthcare achieved about **96% accuracy in distinguishing malicious activities from normal behavior**, far outperforming legacy systems that might only detect clearly known signatures [29]. Another advanced prototype using deep learning for healthcare intrusion detection (part of a blockchain-based framework) reported detection accuracy on the order of 99%, with similarly high recall, when tested against contemporary cyber-attack datasets. Agentic AI further enhances detection by coordinating across nodes, sharing threat intelligence dynamically, and adapting detection strategies in real time. These numbers illustrate the dramatic leap in threat detection the proposed

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

model offers. Essentially, the vast majority of attacks – including subtle ones – can be identified. The blockchain component further aids detection by providing a reliable source of truth for monitoring: because all transactions are recorded, it becomes easier to apply AI analytics to the complete log of events. Any irregular sequence of transactions (e.g., a sudden bulk data extract at 2 AM by a user account) stands out clearly against the normal pattern and can be flagged. In summary, the model's threat detection rate is significantly higher than baseline, meaning it can predict and catch incidents that would have slipped through a traditional security net.

Response Time and Incident Mitigation: In cybersecurity, the time between detecting a threat and neutralizing it is critical. Traditional security operations often involve manual review – for example, an alert triggers and a staff member must investigate and act, which could take hours. During that window, an attacker might already exfiltrate data or cause damage. The proposed model's use of AI enables real-time or near-real-time response, greatly shortening this interval. AI-driven systems can make split-second decisions to isolate a suspicious user or contain a malware outbreak (for instance, by automatically revoking access tokens or spinning up quarantine environments in the cloud) [30]. Agentic AI agents extend this by autonomously executing containment strategies across the cloud–blockchain ecosystem, coordinating with smart contracts to revoke privileges, reroute traffic, or shut down malicious nodes. Additionally, smart contracts on the blockchain can be designed to automatically execute certain actions when specific conditions are met – for example, if an AI flags a transaction as malicious, a smart contract could immediately halt that transaction and alert all network nodes. This level of automation means the **response to threats is often instantaneous or within seconds**, as opposed to the potentially lengthy manual processes in baseline systems. Quantitatively, if a baseline response might take several hours on average to triage and contain a breach (plenty of time for an attacker to steal data), the proposed model could reduce that to seconds or minutes, thereby limiting or preventing data loss. In a simulated environment, AI-based detectors have demonstrated the ability to not only detect but also trigger defensive actions immediately, effectively cutting the "attack dwell time" dramatically. This predictive, fast response capability is a major performance win for the model in practical terms – it turns security from reactive to proactive.

False Positives Rate: A notorious issue with traditional IDS and security alarms is a high false positive rate – benign behavior mistakenly flagged as malicious – which can lead to "alert fatigue" and slow down real incident response. For example, a baseline rule-based system might flood the security team with hundreds of alerts daily, of which only a few are actual threats. The AI in the proposed model is trained to understand context and patterns, which helps **significantly reduce false positives** [31]. Machine learning models can incorporate numerous factors before labeling an event as hostile, whereas a simple rule might trigger on a single unusual data point. As a result, the AI can discern between an actual attack versus, say, an unconventional but legitimate data query by a researcher. Explainable AI (XAI) further supports this by clarifying why an alert was raised, while Agentic AI ensures that only validated, high-confidence alerts escalate for human or automated action. Empirical evidence from healthcare security research shows much improved precision: recent deep learning approaches achieved over **99% precision** in identifying intrusions (meaning almost no false alarms), whereas older methods often had precision in the 80-90% range. In our model's context, this means when an alert is raised by the AI, it is very likely to be a true issue that needs attention. The blockchain's contribution here is indirect but important – the single source of truth it provides eliminates false positives that might arise from inconsistent or out-of-sync logs. In a centralized system, if logs are incomplete or times are skewed, it might appear as if something odd happened (triggering an alert). In the unified ledger, all events are chronologically

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

chained, giving the AI a clean, reliable dataset to learn from and analyze, further minimizing errors. Lower false positives improve overall security performance by allowing both automated systems and human analysts to focus only on genuine threats, thus improving the efficiency of threat handling.

Data Integrity and Verification: The model excels in maintaining and verifying data integrity in ways baseline systems cannot. Traditionally, to ensure data integrity, healthcare IT might perform daily database checksums or have auditors review logs periodically – techniques that are infrequent and can miss intermediate tampering. In contrast, the blockchain continuously verifies integrity with each new block (every transaction confirms the integrity of all previous ones by design). Therefore, any corruption in a patient's record, whether accidental or malicious, is detected immediately when the hashes don't match or consensus fails. The integrity verification success rate of the proposed model is effectively 100% for on-chain data – any single-bit alteration that isn't agreed upon is caught. For off-chain data (like large medical files in cloud storage), the model stores cryptographic fingerprints on-chain, so any discrepancy in the file will be noticed when checked against the fingerprint. Agentic AI contributes by dynamically cross-checking off-chain data with on-chain proofs, initiating corrective workflows (such as rolling back to verified backups) without waiting for manual audits. Baseline systems lack this real-time checking; an attack altering a lab result in a database might go unnoticed until an audit weeks later (if at all), whereas in the blockchain-based model the network would reject the unapproved alteration within seconds. Another aspect is **auditability:** the ease of verifying that data hasn't been tampered with. In our model, auditors (or even patients, through a portal) can quickly query the blockchain to confirm that, for example, a prescription record has not changed since it was issued – the ledger provides a verifiable trail. In legacy systems, this might require combing through log files and hoping they weren't altered. The strength of the model is that it mathematically guarantees data integrity through distributed consensus and hashing. This is a huge performance improvement in terms of trust: stakeholders can rely on the data's accuracy, which is crucial in healthcare where incorrect data can lead to life-threatening decisions.

Taking these indicators together, the predictive and combined approach of AI, blockchain, and cloud shows marked performance improvements. In real-world terms, healthcare organizations adopting this model could expect to prevent a higher percentage of cyber-attacks than those sticking to traditional security – breaches would be prevented or contained in far more instances. They would also notice that their security systems run more autonomously and efficiently: fewer false alarms to investigate, faster reaction to genuine threats, and robust assurance of data integrity and availability. Early implementations and theoretical models suggest that the frequency of security incidents drops and compliance audits become easier (since the evidence of security and data integrity is built into the system). While exact performance gains depend on the scenario, it's reasonable to predict, for example, a substantial increase in threat detection rates (perhaps on the order of 20%+ more threats detected that would have been missed by legacy systems) and a reduction in incident response time from hours to minutes. Such improvements demonstrate the potential of the proposed architecture to significantly harden healthcare environments against cyber threats while maintaining the agility needed in a digital-first health ecosystem.

3.3 Advantages and Innovations of the Proposed Model

Integrating AI, blockchain, and cloud technologies into a single security framework yields **unique**

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

advantages that go beyond the sum of the parts, marking a significant innovation in personal health data security architecture. Here we highlight the standout benefits and how this approach advances the field:

- **Holistic Defense via Layered Synergy:** Perhaps the greatest innovation is the defense-in-depth achieved by the interplay of AI, blockchain, and cloud components. Each technology addresses different dimensions of security, and together they form a robust mesh. Blockchain provides a trustless, tamper-proof foundation – once data is recorded, it's secured by cryptography and consensus, eliminating doubts about its authenticity. AI acts as an intelligent layer on top, predicting and adapting to threats (something static code or traditional systems cannot do), and making real-time decisions to enforce security policies. Cloud technology contributes scalability and reliability, ensuring that the security measures remain effective as data volume and user numbers grow, and that services remain available during peak loads or outages. This combination is innovative because it moves away from relying on any single point of protection; instead, even if one layer encounters a novel threat, another layer can compensate. For example, if an attacker somehow slips past an AI detection (perhaps with a very new attack), the blockchain's immutability could still prevent them from altering any records, containing the damage. Conversely, if someone tried to subvert the blockchain by abusing valid credentials, AI monitoring would catch the unusual usage pattern and trigger a security response. Together, the self-reinforcing loop of AI, Agentic AI, blockchain, and cloud creates a continuously adaptive and collaborative defense mechanism. This self-reinforcing security loop dramatically strengthens protection compared to earlier models. Traditional architectures have discrete security tools working in parallel, whereas our integrated model has them working in tandem, each enhancing the other. This synergy is a novel approach in healthcare, effectively uniting preventive, detective, and corrective controls into one cohesive system.

- **Mitigation of a Wide Spectrum of Threats:** The proposed model is designed to counter a broad range of cyber threats that healthcare organizations face, from external hacks to insider misuse, in a more effective manner than legacy solutions. AI algorithms (especially machine learning and deep learning models) bring the power of pattern recognition to detect complex threats like advanced persistent threats or subtle data exfiltration that simple rule-based systems would miss. Blockchain mitigates threats related to data integrity and fraudulent transactions – for instance, it can prevent double-spending of prescriptions or detect if someone tries to retroactively edit a medical record to cover malpractice. Cloud infrastructure, when combined with these, helps absorb and mitigate denial-of-service (DoS) attacks by providing flexible resources and distributed networks (making it harder for an attack to knock out a service). Agentic AI adds resilience by autonomously coordinating distributed responses – isolating compromised IoMT devices, adjusting privileges dynamically, and ensuring continuity of clinical workflows while containing threats. In essence, the integration means multiple threat vectors are addressed simultaneously: network-level attacks, application-level attacks, data-level tampering, and human-factor breaches are all tackled by different parts of the framework. This is a stark improvement from older models, where focus might be on just keeping intruders out, but not on what happens if they get in or if an insider turns malicious. For example, consider ransomware – a major threat to health systems. In the proposed model, ransomware might infiltrate a user's device, but the blockchain-backed data store means the core patient records are versioned and immutable, so ransomware cannot easily encrypt or destroy the only copy of data (there are multiple distributed copies and an immutable history). AI could detect the encryption behavior as anomalous and isolate that node, while cloud

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

backups ensure data availability. Thus, the damage is minimized. This approach essentially future-proofs the security architecture to handle known and unknown threats, because AI can learn new patterns and blockchain provides lasting trust in data, regardless of attack evolution. It's an innovative shift from reacting to known problems, to creating a resilient system that inherently resists a variety of attacks.

- **Enhanced Patient Empowerment and Regulatory Compliance**: By integrating these technologies, the model inherently supports features that improve compliance with healthcare regulations (such as HIPAA, GDPR, and others) and empower patients regarding their data. Blockchain's transparency and immutability mean that audit trails are automatically recorded and cannot be altered – this is a boon for compliance, as demonstrating accountability and traceability of access is straightforward. Every access to a patient's data, every consent given or revoked, and every data transfer is logged indelibly. Regulators can be given access to the ledger (or portions of it) to verify that privacy rules were followed, rather than relying on an organization's internal logs. Smart contracts can even embed regulatory rules (for example, automatically enforce data retention policies or trigger alerts if someone tries to access data in violation of consent), effectively building compliance into the system's logic. From the patient's perspective, this architecture supports granular consent management and data sharing on their terms. The patient could use a secure app (powered by the AI-blockchain network) to decide which doctor or clinic can see which parts of their record and for how long, and this preference would be executed by the system without manual paperwork. This level of control and transparency was hard to achieve in older models where data was locked in each provider's database. Now, with a shared ledger and AI to manage permissions, patients can have unprecedented control and trust. They can even receive real-time notifications (through an AI-driven alert system) when their data is accessed, ensuring nothing happens without their knowledge. These innovations strengthen the patient's trust in digital health ecosystems and directly address privacy regulations that emphasize user rights over data. In fact, the model transforms regulatory compliance from a burdensome process into a mostly automated outcome of the system's normal operations – security and privacy principles are baked in at the architectural level, which is a significant advancement over trying to bolt on compliance after the fact in traditional systems.

- **Scalability, Cost Efficiency, and Future-Proofing:** Another advantage of this integrated approach is that it is inherently scalable and cost-efficient while maintaining security. In the past, achieving higher security often meant expensive proprietary systems and scaling up hardware appliances (like bigger firewalls or more servers for redundancy), which increased costs. Here, by using cloud resources, the model can scale on-demand – you pay for additional compute/storage only when you need it, which is economically efficient for healthcare providers. Blockchain nodes can be lightweight and distributed among participating stakeholders, avoiding the need for a massive central IT infrastructure. There is evidence that combining blockchain and cloud can actually reduce computational costs for the ecosystem while improving security [33]. The reason is that heavy data processing (e.g., AI analytics, bulk storage of images) is offloaded to cloud servers which are optimized for such tasks, whereas the blockchain handles only the smaller, security-critical transactions and references. This division of labor means the system remains high-performance and cost-effective. Over time, as data grows, the marginal cost of securing each additional gigabyte of data is low because the cloud handles it, and the marginal cost of auditing more transactions is low because the blockchain automates it. Moreover, the architecture is modular and future-proof – new advances in AI or new blockchain improvements can be

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

incorporated without overhauling the whole system. For instance, if a more efficient consensus algorithm or a quantum-resistant encryption method becomes available, it can be integrated into the blockchain layer to upgrade security. If new AI models are developed to detect biomedical-specific anomalies (say, looking for patterns of insurance fraud or prescription abuse), they can be deployed in the AI layer. The cloud backbone makes such updates and A/B testing of new security algorithms feasible across the network. This flexibility and adaptability are innovative for healthcare, an industry where IT systems traditionally lag behind cutting-edge tech. The proposed model creates a platform that can evolve with technological advancements, meaning it won't become obsolete as quickly as past systems. In the long run, this can lower the total cost of ownership for security, since the need for manual upgrades or complete replacements is reduced. Hospitals and clinics can subscribe to this security framework as a service (potentially managed in the cloud) rather than investing in a patchwork of separate security solutions. This democratizes strong security – even smaller clinics with limited IT budgets could join the network and benefit from the robust protection, something not possible when only large institutions could afford top-tier security appliances.

The AI-Blockchain-Cloud integrated security model introduces a **paradigm shift** in protecting personal health data. It combines predictive intelligence (AI), autonomous orchestration (Agentic AI), decentralized trust (blockchain), and elastic infrastructure (cloud) into one cohesive framework. It goes beyond incremental improvements, instead offering a transformative approach where confidentiality, integrity, and availability are enforced through a coordinated trio of advanced technologies. The model not only remedies many weaknesses of existing systems (single points of failure, static rules, poor interoperability) but also creates new capabilities (like intelligent threat prediction and patient-governed data sharing) that were not feasible before. By mitigating diverse cyber threats, strengthening privacy, enabling seamless yet secure data exchange, and providing a scalable, compliant infrastructure, this innovative architecture paves the way for safer adoption of digital and data-driven healthcare. It advances the state of the art in healthcare security, showing how emerging technologies can be harmoniously combined to achieve robust protection in modern health ecosystems. Ultimately, such a model helps ensure that as healthcare becomes increasingly digital-first, security and trust keep pace, thereby protecting patients and empowering healthcare providers in the digital age.

4. Implications for Practitioners

Healthcare providers, IT professionals, and administrators can adopt the AI–Blockchain–Cloud architecture framework by aligning it with their existing health IT systems and workflows. Rather than a disruptive overhaul, new security solutions should be layered onto current electronic health record (EHR) platforms and databases to ensure continuity and interoperability [34]. A phased implementation is prudent – starting with pilot projects to validate the framework's effectiveness and then scaling up once trust and efficacy are established. Practitioners should also involve multidisciplinary teams (clinicians, IT staff, and compliance officers) early in the process to address concerns and tailor the framework to clinical needs.

- **Incremental Integration:** Blend blockchain, AI, and cloud tools with legacy systems via APIs and middleware, instead of replacing core systems outright. This integration facilitates data exchange and a smoother transition without interrupting care delivery [34]. For example, a blockchain layer can mirror key data from an EHR, providing an immutable audit trail, while AI models run in parallel to existing monitoring systems for anomaly detection. Agentic AI agents can orchestrate across these layers – automatically updating access rules, synchronizing consent

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

policies, or reconciling discrepancies between blockchain logs and cloud storage.

- **Workforce Training and Buy-In:** Invest in comprehensive training programs to upskill healthcare staff on these technologies. Lack of understanding and training is a well-documented barrier to adopting AI in healthcare [35]. Clinicians and administrators need to learn how AI-driven alerts or blockchain-based data sharing work in practice. By improving digital literacy, organizations can mitigate user resistance and build trust in the new tools. Leadership should also champion the initiative and clearly communicate its patient safety and efficiency benefits to gain buy-in.

- **Interoperability and Standards Compliance:** Plan for data standardization and interoperability from the outset. A major challenge is the lack of uniform data standards across systems – without alignment, integrating multiple providers' systems on a blockchain is difficult [36]. To overcome this, organizations should use existing health data standards (like HL7 FHIR for data formats) and ensure the new framework conforms to those. Engaging vendors that support industry standards and participating in interoperability initiatives can reduce integration friction. Federated learning across providers and standardized blockchain APIs can further support secure multi-institutional data sharing, while embedded compliance checks help maintain HIPAA and GDPR alignment automatically.

- **Security and Key Management:** Adopting blockchain and cloud solutions introduces new operational considerations, such as managing cryptographic keys and access rights. Healthcare IT teams should follow "zero trust" security principles and robust identity management. Best practices include enforcing strong access controls, encryption of data in transit and at rest, and regular security audits of AI algorithms [36]. Such measures help maintain confidentiality of personal health information within the new framework.

- **Pilot Testing and Incremental Rollout:** Start with limited-scope deployments (e.g. a departmental pilot or a subset of anonymized patient data) to evaluate performance and address issues on a small scale. Use insights from the pilot to refine the integration process. Gradually expand the implementation once the solution is validated. This iterative approach allows practitioners to learn and adjust, minimizing disruptions. Throughout, gather feedback from end-users (doctors, nurses, IT staff) to improve usability.

4.1 Overcoming Adoption Challenges

Implementing an AI–Blockchain–Cloud architecture will come with challenges, but there are strategies to tackle them. One common hurdle is the technical complexity – many organizations lack in-house expertise in these emerging technologies. To address this, healthcare IT departments can partner with experienced technology providers or consultants for initial deployments, while simultaneously training internal teams. The use of Agentic AI orchestration tools can further ease technical integration by automating interoperability tasks such as aligning blockchain audit trails with cloud databases and dynamically adjusting access policies. Establishing a cross-functional governance committee can help manage the change; this team would set guidelines for usage, monitor progress, and ensure that the new system aligns with clinical workflows and privacy requirements. Another challenge is cultural resistance: clinicians may be wary of AI recommendations or new data-sharing processes. Clear communication about how the framework enhances (and does not replace) clinicians' decision-making is vital. Early involvement of clinical champions who advocate for the system can help in easing fears. Finally, resource constraints (time, budget) can slow adoption. Organizations should build a business case that highlights long-

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

term savings from prevented breaches and improved efficiency to justify the upfront investment. Phased implementation is recommended, beginning with pilot projects in high-impact areas (such as telehealth or IoMT security) and then expanding incrementally across departments. Leveraging cloud scalability and modular blockchain deployment ensures costs are distributed over time, while AI-driven predictive analytics can forecast ROI and security improvements. By anticipating these challenges and proactively developing mitigation strategies, practitioners can more readily embrace the integrated security framework and realize its benefits.

4.2 Policy Considerations

The convergence of AI, blockchain, and cloud in healthcare security has significant regulatory and policy implications. Existing regulations like HIPAA, GDPR, and various national health data laws provide important guardrails, but they were not written with these advanced technologies in mind. Policymakers and compliance officers must therefore interpret and possibly update these frameworks to accommodate the new security models.

- **Ensuring Compliance with Privacy Laws:** The AI–Blockchain–Cloud framework must be implemented in a way that adheres to patient privacy and data protection laws. For instance, using a public, permissionless blockchain to store patient data would likely violate privacy regulations – a public ledger's transparency is incompatible with HIPAA's strict confidentiality requirements [37]. To remain compliant, healthcare organizations should favor private or consortium blockchains where access is restricted to authorized parties. Similarly, cloud providers hosting health data must sign Business Associate Agreements and offer robust security measures in line with HIPAA. It's worth noting that data location is a regulatory factor as well: health data stored on foreign cloud servers might fall under other jurisdictions' laws. Policymakers may need to clarify or strengthen data sovereignty rules. For example, guidance from HHS emphasizes that even if cloud servers are overseas, U.S. health data must still comply with HIPAA standards. Organizations might choose cloud regions carefully or opt for "sovereign cloud" solutions that keep data within certain geographic or legal boundaries. In the EU, the GDPR's requirements add another layer of complexity – particularly the "right to erasure." Blockchain's immutable ledger means once data is recorded, it cannot be easily deleted, posing a conflict with GDPR's right to be forgotten. Proposed solutions involve off-chain storage of personal data (so that on-chain entries can be erased by deleting the off-chain link) with on chain hashes, redactable cryptography or innovative cryptographic techniques to edit or revoke access to on-chain data. Regulators may need to explicitly allow such approaches or create exceptions to reconcile blockchain immutability with privacy rights.

- **Updates to Regulatory Frameworks:** Regulatory bodies should proactively update and refine healthcare data security guidelines to account for AI and blockchain. Currently, a lack of clear regulation or guidance on these technologies can itself be a barrier – uncertainty may discourage healthcare organizations from innovating [38]. Governments and health authorities could establish clearer standards for AI in healthcare, such as requiring algorithmic transparency and validation for AI tools that handle patient data. For blockchain, standards on security, node accountability, and data handling should be developed to ensure any distributed ledger usage still upholds privacy obligations. Efforts are already underway in some jurisdictions (for example, the FDA in the U.S. has been exploring regulatory frameworks for AI/ML in medical devices, and the EU is working on an AI Act) to ensure algorithmic accountability. These need to be harmonized with health-specific laws. Policy sandboxes could also be useful – regulators can allow pilot implementations of AI or blockchain in a controlled environment to observe compliance challenges

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and refine rules accordingly. The overarching goal should be to provide a robust governance framework that encourages innovation in security while protecting patient rights. This might include updated accreditation or certification for health AI systems, and guidelines on conducting risk assessments for AI and blockchain deployments.

- **Global and National Coordination:** Healthcare data often crosses borders (especially in cloud-based systems or international research collaborations), so policy coordination is important. International standards bodies (like ISO or IEEE) and collaborations between countries can help create interoperable security standards. National healthcare data laws may need revisions to address cross-border data exchange facilitated by cloud and blockchain networks. Policymakers should clarify how data residency requirements apply in the cloud era and possibly negotiate treaties or agreements for health data sharing with strong security (similar to how international financial data is regulated). In essence, as personal health data flows through AI algorithms, blockchain networks, and cloud servers, the legal accountability for data breaches or misuse must be clearly defined across all involved entities (e.g., delineating the responsibilities of healthcare providers vs. cloud vendors vs. AI software providers).

- **Equitable Access and Ethical Use:** Another critical policy consideration is ensuring equitable access to the benefits of secure digital health ecosystems. Policymakers should guard against a scenario where only large, resource-rich hospitals can deploy advanced AI-blockchain security, leaving smaller clinics more vulnerable. This could widen health IT disparities. Governments can promote equity by providing funding or incentives (grants, subsidies, public-private partnerships) for smaller providers to upgrade their security infrastructure. Additionally, establishing national interoperability and security standards can level the playing field by making it easier and more affordable for all players to adopt compliant solutions. On the ethical front, regulations should ensure that the use of AI and data sharing via blockchain does not inadvertently harm patients – for example, algorithms should be audited for biases that could unfairly target or exclude certain groups. Data governance policies must also uphold that patients retain agency over their personal health information. Frameworks like GDPR already emphasize patient consent and control, and these principles should carry into any new security architecture. Policymakers might require that any AI or blockchain application in health includes patient opt-in/opt-out mechanisms and transparency about how data is used. Ultimately, aligning with the principle that digital health innovations should be "ethical, safe, secure, reliable, and equitable" for all people, regulators and lawmakers should continuously update laws like HIPAA, GDPR, and others to reflect the realities of AI-driven, blockchain-secured health data management.

- **Recommendations for Policymakers:** In summary, policymakers are advised to: (a) Modernize health data regulations to explicitly address AI algorithms, blockchain data storage, and cloud services – providing clarity on compliance requirements for each. (b) Enhance oversight by developing certification programs or audits for AI and blockchain systems used in healthcare, ensuring they meet security and privacy benchmarks. (c) Foster collaboration between technologists, healthcare professionals, and legal experts (e.g., through advisory councils or working groups) to stay ahead of emerging security issues. (d) Promote standards and interoperability, possibly by supporting open standards for health data exchange on blockchain and encouraging the use of interoperable cloud services, so that security improvements can be shared across the health system. (e) Ensure equity in adoption by supporting initiatives that bring these advanced protections to underserved clinics and populations – for instance, funding pilot programs in rural healthcare or training programs nationwide. By considering these policy measures,

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

governments and institutions can create an environment where AI–Blockchain–Cloud security architectures flourish in a responsible, lawful, and inclusive manner.

4.3 Future Research Directions

While integrating AI, blockchain, and cloud technologies shows promise for strengthening personal health data security, several open research questions and challenges remain. Addressing these will require concerted efforts from researchers in computer science, healthcare informatics, cybersecurity, and beyond. Key directions for future investigation include:

- **Blockchain Scalability and Performance:** Current blockchain implementations (especially in healthcare, which can generate large volumes of data) face throughput and scalability limitations. As medical data grows, researchers are exploring ways to make blockchain networks more efficient and scalable for health applications [39, 40]. Proposed solutions such as sharding, sidechains, or off-chain transactions need further study to determine their efficacy in a healthcare context. For example, how can a nationwide health information blockchain handle thousands of transactions per second (e.g., real-time patient monitoring data) without compromising security? Additionally, energy consumption and cost of blockchain operations are concerns; future research might focus on energy-efficient consensus algorithms suitable for health data exchange. Exploring integration of blockchain with quantum-resistant cryptography and next-generation distributed storage could also future-proof adoption. Solving these issues is critical for widespread adoption – if every hospital in a country were to use blockchain for medical records, the system must scale accordingly.

- **AI Bias and Fairness in Security Analytics:** The use of AI in healthcare security (such as AI systems monitoring access logs or predicting potential breaches) must be approached with caution regarding bias. We know from clinical AI applications that algorithms can perpetuate or even amplify biases present in training data, leading to unfair outcomes. In the security domain, an AI might inadvertently give more false alarms on certain user groups or overlook threats if the data is skewed. This is an emerging area where research is needed to ensure AI-driven security tools are fair and trustworthy. Techniques to audit and mitigate AI bias should be applied in this context. For instance, developing discrimination-aware algorithms that consciously minimize bias in decision-making can help [41]. Researchers should test security AIs with diverse datasets to evaluate performance across different scenarios and user demographics. Moreover, explainable AI (XAI) is important – security personnel will need to understand an AI's reasoning (e.g. why it flagged an activity as suspicious) to trust and effectively use these tools. Future studies may also examine "Agentic AI" in security, where autonomous agents collaborate to defend systems; such systems will require fairness, transparency, and accountability guardrails.

- **Cloud Security and Data Sovereignty:** As healthcare continues its migration to cloud infrastructures, questions around data sovereignty and cloud security architecture remain open. One research avenue is developing "sovereign cloud" solutions for healthcare, which combine the scalability of public clouds with guarantees about data location and jurisdiction. Sovereign clouds aim to keep sensitive health data under national or organizational control, addressing legal requirements and patient trust concerns [42]. Studying the trade-offs of such architectures (e.g., slightly higher latency or cost in exchange for greater control) would be valuable. Additionally, techniques like confidential computing and advanced encryption (homomorphic encryption, secure multi-party computation) in cloud environments are ripe for exploration. These could allow cloud-based AI processing of health data while keeping the data encrypted to the cloud provider – a

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

promising concept for preserving privacy. Researchers should also explore robust cloud incident response for health data: how to quickly detect and recover from breaches in a cloud-hybrid environment that uses blockchain logging and AI monitoring. This includes investigating methods for continuous compliance auditing in the cloud, since regulations may require proof that data was handled according to policy even when using external cloud services.

- **Federated and Privacy-Preserving Machine Learning:** With privacy a paramount concern, federated learning has emerged as a compelling research direction for healthcare. Federated learning allows training machine learning models across multiple hospitals or devices without centralizing the sensitive data – only model updates are shared, not raw patient data [43]. This approach can enable collaborative security analytics, such as hospitals jointly developing an AI model to detect cyber threats or fraud, without exposing their underlying patient data to each other. Research is needed to tailor federated learning to healthcare security use cases: for example, creating algorithms that detect unusual access patterns or malware infections by learning from multiple institutions' experiences, all while each institution's data stays local. Early studies highlight that federated models can indeed enhance privacy-preserving analytics by aggregating insights rather than raw data, reducing the risk of data exposure. However, challenges remain in ensuring these distributed models are accurate and in handling issues like heterogeneous data (different hospitals may have very different IT systems and threat landscapes) and communication overhead. Another related area is secure multi-party analytics – beyond model training, federated query systems could allow, say, a consortium of hospitals to run joint analyses on security logs or genomic data with cryptographic guarantees that no single party sees the others' data. This overlaps with blockchain (for trust and auditability) and is a rich interdisciplinary research niche combining cryptography, ML, and health informatics.

- **Cross-Disciplinary Collaboration and Governance:** Effective research and development in this domain will require multidisciplinary efforts. Future studies should not just focus on technical aspects in isolation, but also involve social science, legal, and clinical expertise. For example, investigating the human factors of these security architectures – how do healthcare workers interact with AI alerts or blockchain systems? Ethnographic studies or human-computer interaction research can improve the usability and integration of these tools in real hospital environments. Legal research is also needed to keep pace with technological capabilities: scholars in law and ethics could propose new regulatory models or frameworks (such as data trusts or revised consent models) that better fit AI-blockchain ecosystems. Healthcare outcomes research can examine whether these security enhancements translate into tangible benefits like reduced data breaches or improved patient confidence, and how that impacts overall care delivery. We also foresee the establishment of testbeds or simulation environments where interdisciplinary teams can evaluate new ideas safely – for instance, a simulated hospital IT environment where new AI algorithms or blockchain protocols are trialed and assessed from both a security and a clinical workflow perspective. In essence, future research should be highly collaborative: technologists working hand-in-hand with healthcare providers, ethicists, and policymakers. Such collaborations will help ensure that innovations are not just technically sound, but also practical, ethical, and aligned with healthcare's mission.

By pursuing these research directions, the community can address key gaps in our knowledge. Questions about how to scale blockchain, eliminate AI biases, enforce data sovereignty, and leverage federated learning must be resolved to fully realize the potential of the AI–Blockchain–Cloud paradigm. The coming years offer an exciting opportunity for researchers from

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

cybersecurity, medicine, and policy fields to jointly advance the frontiers of secure digital health.

5. Practical Simulation: Anomaly Detection on Hospital Data Objective

This simulation explores how AI-driven anomaly detection can be applied to hospital data as an initial proof-of-concept for the broader AI–Blockchain–Cloud framework. The focus is on identifying unusual patient records that deviate from population norms based on behavioral and health-related features. Such anomalies may reflect:

- Outliers in healthcare utilization
- Atypical clinical conditions
- Or potential data quality issues

The goal is to assist in risk profiling, resource planning, or quality assurance.

Methodology

1. Dataset

i. Source: https://www.kaggle.com/datasets/ibnarahat/hospital-data?resource=download

ii. Variables considered for anomaly detection:

- Age
- BMI
- Annual_Visits
- Avg_Stay_Duration
- Total_Spending

2. Preprocessing

- Dropped rows with missing values in selected features
- Focused on numeric variables to support Isolation Forest modeling

3. Model

i. Used Isolation Forest, an unsupervised learning algorithm designed to:

- Isolate anomalies by recursively partitioning data
- Score points based on how quickly they become isolated

ii. Parameters:

- contamination = 0.03 (expecting ~3% of the data to be anomalous)
- random state = 42 for reproducibility

4. Evaluation Metrics

i. Traditional supervised metrics were not applicable.

ii. Instead, anomalies were assessed via:

- Model anomaly scores, and

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Z-score deviations from baseline norms.

This approach is consistent with emerging explainable AI (XAI) practices, offering interpretable outputs for clinicians.

Observations

i. 4 patient records were detected as anomalies out of the full dataset

ii. These anomalies showed extreme values or rare combinations in the chosen features

iii. Most impactful deviations were seen in:

- BMI (very low or very high)
- Total Spending (exceeding the usual range)
- Avg Stay Duration (7 days, when typical is 1–5)
- Annual Visits (8 visits, compared to norm of 1–6)

Findings

Patient ID	Key Reasons for Being Flagged
P10003	Low BMI (16), only 1 visit, very low spending (410)
P10005	High BMI (30), 8 visits, long stay (7 days), high spending (2100)
P10007	Extremely low BMI (13.6), lower than clinical norms
P10089	Highest BMI (50.65), 8 visits, longest stay (7 days), highest spending (2306.5)

- These cases represent extreme resource usage or clinical profiles
- No indication of incorrect data — they are valid but rare cases

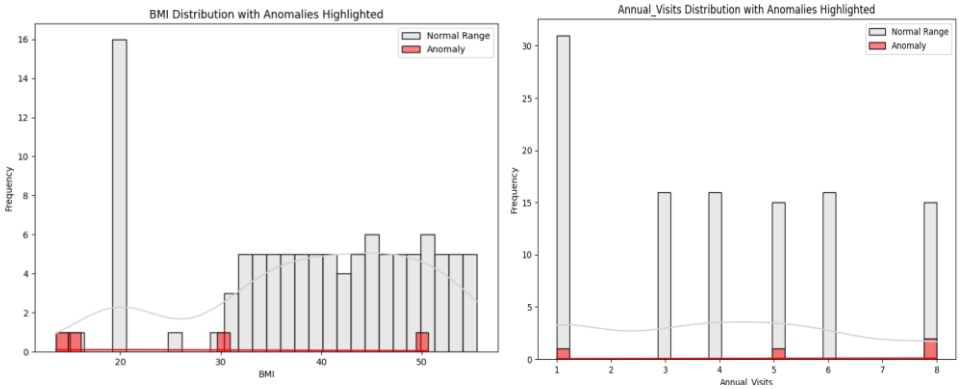
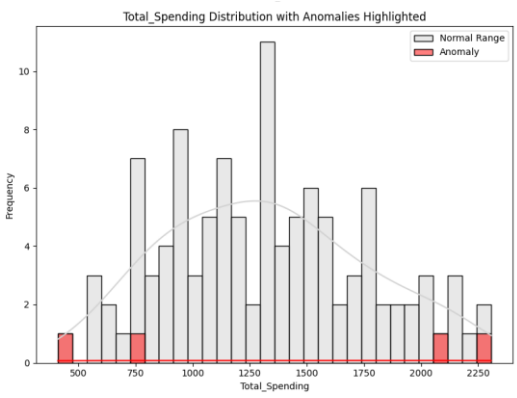


Figure 2: BMI Distribution with Anomalies Highlighted

Figure 3: Annual Visits Distribution with Anomalies Highlighted

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



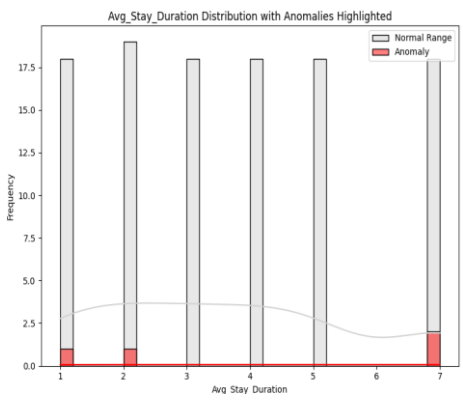


Figure 4: Total Spending Distribution with Anomalies Highlighted

Figure 5: Average Stay Duration Distribution with Anomalies Highlighted

Figure 2 histogram illustrates the distribution of Body Mass Index (BMI) values across all patients. Normal cases are shown in light gray, while anomalous BMI values—identified using the Isolation Forest algorithm—are shown in red. Anomalies typically fall at extreme low or high BMI values, suggesting that patients with underweight or severely overweight profiles may exhibit unusual healthcare patterns. Figure 3 displays the distribution of the number of annual hospital visits per patient. Most patients have moderate visit frequencies, while anomalies (in red) tend to occur at very low (1) or unusually high visit counts. These cases may indicate patients who rarely seek care despite chronic needs or, conversely, high-frequency users with outlier characteristics in spending or stay duration. Figure 4 shows how long patients typically stay in the hospital during a visit. The red-highlighted anomalies are concentrated at unusually short (1 day) or long (7+ days) durations, which deviate from the norm. These outliers could reflect patients with complex medical conditions, inefficient treatment cycles, or exceptional recovery times. Figure 5 shows total healthcare spending per patient. Most patients incur moderate costs, but anomalies (red bars) cluster at the low end (e.g., around $410) and high end (above $2000). These deviations may be due to billing errors, insurance limitations, or special treatment requirements—indicating financial outliers in the healthcare system.

Experimental Results and Insights

The experiment successfully demonstrated that:

- Isolation Forest is effective in flagging unusual records in healthcare datasets.
- Anomalies provide valuable insights for clinical review, policy refinement, and targeted interventions.
- The approach is scalable, unsupervised, and adaptable, making it well-suited for real-world hospital analytics and integration into next-generation AI–Blockchain–Cloud security architectures.

9. Conclusion

In summary, this review highlights that integrating artificial intelligence (AI), Agentic AI, blockchain, and cloud architectures provides a multifaceted defense for digital-first healthcare systems. Each technology complements the others: AI can detect anomalies and strengthen access controls, agentic AI extends this by orchestrating multi-agent collaboration and adaptive decision-making across dynamic health data ecosystems, blockchain ensures data integrity and secure

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

sharing, and cloud platforms offer scalability and connectivity. Together, these innovations greatly enhance the security, privacy, and interoperability of personal health data. By combining these tools, healthcare providers can create an ecosystem where sensitive health information is protected at every stage – from storage and transmission to analysis – without sacrificing the seamless data exchange needed for quality care. This synergy not only fortifies data protection but also lays the groundwork for more patient-centric and trustworthy digital health services.

Real-World Implications: The practical benefits of these integrated solutions are far-reaching. For healthcare providers, robust security and interoperability mean they can confidently adopt electronic health records and telemedicine platforms, improving clinical workflows and patient outcomes. Secure, interoperable data sharing enables doctors, hospitals, and laboratories to access up-to-date patient information instantly, leading to better-informed decisions and coordinated care. For policymakers and regulators, the convergence of AI, blockchain, and cloud in healthcare offers new tools to enforce privacy laws and data standards automatically – for example, smart contracts on blockchain could verify consent or compliance in real-time. Explainable AI (XAI) further enhances accountability by ensuring that AI-driven alerts or decisions can be interpreted and audited. Industry stakeholders, including health IT companies and insurers, stand to gain from reduced fraud, improved auditability, and higher public trust in digital health services. Ultimately, patients benefit from these real-world advances through improved data privacy, faster services, and confidence that their personal health data is handled securely and transparently. The adoption of these technologies thus promises a safer and more efficient healthcare system that aligns with both clinical needs and regulatory requirements.

Challenges and Considerations: Despite the clear advantages, there are important challenges and considerations when implementing AI, blockchain, and cloud security in healthcare. Regulatory hurdles remain a top concern – many of these technologies outpace current health data regulations, creating uncertainty around compliance and standards. Issues like data residency, consent management, and the right to be forgotten (especially relevant to immutable blockchain records) require careful navigation by regulators and stakeholders. Implementation complexity is another barrier: integrating blockchain networks or AI-driven security into legacy hospital systems can be technically daunting and resource-intensive. There is often a shortage of skilled personnel (for example, blockchain developers or AI specialists) to drive these projects, and interoperability standards are still maturing. Technological constraints also persist. Blockchain systems, in their current form, can suffer from scalability and performance limitations, especially under the heavy data loads of nationwide health systems. AI models, while powerful, may introduce bias or errors if not properly trained and audited – a serious concern in healthcare where fairness and accuracy are paramount. Likewise, relying on cloud infrastructure means healthcare organizations must trust external providers and ensure robust encryption and cyber-defense measures are in place to prevent breaches. Agentic AI adds another challenge: while it enables adaptive orchestration of decisions across multiple systems, governance frameworks must evolve to ensure these autonomous agents remain transparent, ethical, and aligned with clinical priorities. Acknowledging these challenges is crucial: stakeholders must approach digital health security with both optimism and caution, addressing legal, technical, and ethical considerations upfront to fully realize the benefits of these tools.

Future Research Directions: Looking ahead, further research and development are needed to overcome current limitations and refine these security architectures. Blockchain scalability is a priority area – future work should explore advanced consensus algorithms, side-chains, or hybrid

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

architectures that can handle large volumes of health data and transactions with low latency. Research is already underway to improve blockchain performance for healthcare as data volumes grow, but more is required to ensure these systems can scale nation-wide without compromising security or speed. AI bias in healthcare security is another critical field of study. As AI systems take on roles in detecting security threats or managing patient identities, researchers must develop techniques to ensure these models are fair, transparent, and free of bias. This includes using diverse training data, auditing AI decisions, and incorporating explainability so that automated security decisions can be trusted in clinical environments. In the realm of cloud computing, privacy-preserving techniques are an evolving frontier. Future research should expand on methods like differential privacy and homomorphic encryption that allow health data to be analyzed or processed in the cloud while mathematically guaranteeing patient privacy. For instance, major cloud providers have begun offering differential privacy tools to help obscure patient identities in datasets, and ongoing work on fully homomorphic encryption promises the ability to compute on encrypted medical data without ever exposing it in plaintext. Additionally, advances in secure multi-party computation and federated learning could enable collaborative analytics across hospitals without pooling sensitive data centrally. Exploration of Model-Chaining Protocols (MCPs) and agentic AI frameworks will also be vital to orchestrate interoperability between AI agents, blockchain nodes, and cloud systems in a secure and verifiable way. Research into these areas – along with studies on improving interoperability standards and reinforcing smart healthcare devices against cyberattacks – will be essential to keep pace with the evolving threat landscape. By prioritizing these topics, the academic and tech communities can close gaps in our current systems and drive innovations that make digital health security future-proof.

In conclusion, the protection of personal health data in an era of digital-first healthcare should be a collective priority. We call on healthcare organizations, technology developers, and regulators to work collaboratively in adopting and refining the AI, blockchain, and cloud innovations discussed in this review. Healthcare institutions should actively pilot and implement these solutions – for example, deploying blockchain-based record systems or AI-driven intrusion detection – to safeguard patient data and build trust in digital services. Technology providers and developers are encouraged to engage with clinicians and IT teams to tailor their tools to real-world clinical workflows, ensuring that security enhancements also promote usability and interoperability. At the same time, regulators and policymakers must update frameworks and guidelines to support these advancements, providing clear standards (such as for blockchain data management or AI algorithm transparency) and incentivizing compliance with security best practices. Cross-sector collaboration is vital: establishing partnerships, consortia, and open forums where insights are shared will accelerate learning and address challenges more efficiently than any stakeholder could alone. By taking collective action, the healthcare industry can create a robust, secure-by-design digital health ecosystem. The path forward demands both innovation and vigilance – with all parties championing data protection – so that the full potential of digital health can be realized without compromising the privacy and security of the individuals it serves.

References

[1] Moore, J., & Guichot, Y. D. (2024, January 5). How to harness the power of health data to improve patient outcomes. World Economic Forum.

[2] Doughman, S. (2023, December 5). How blockchain can improve data security in healthcare. World Economic Forum.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[3] Alabdulatif, A., Khalil, I., & Rahman, M. S. (2022). Security of blockchain and AI-empowered smart healthcare: Application-based analysis. Applied Sciences (Switzerland), 12(21), 11039.

[4] Arefin, S. (2024). Strengthening healthcare data security with AI-powered threat detection. International Journal of Scientific Research and Management, 12(10), Article EC02.

[5] Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business.

[6] Lindquist, M. (2024, June 24). Interoperability in healthcare explained. Oracle Health.

[7] Ismail, L., & Damaševičius, R. (2021). Integrated Blockchain-Cloud Architecture for Healthcare. Encyclopedia.

[8] Arefin, S. (2024). Strengthening healthcare data security with AI-powered threat detection. International Journal of Scientific Research and Management, 12(10).

[9] Taherdoost, H. (2023). Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives. Sci, 5(4), 41.

[10] Vukotich, G. (2023). Healthcare and cybersecurity: Taking a zero trust approach. Health Services Insights, 16, 11786329231187826.

[11] Xeven Solutions. (n.d.). 5 top healthcare data security challenges and solutions. Xeven Solutions Blog.

[12] Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., & Yongchareon, S. (2024). Health IoT threats: Survey of risks and vulnerabilities. Future Internet, 16(11), 389.

[13] Empeek. (2023). Telehealth privacy concerns, regulations, and the vulnerable areas to focus on. Empeek Blog.

[14] Bonomi, L., Huang, Y., & Ohno-Machado, L. (2020). Privacy challenges and research opportunities for genomic data sharing. Nature Genetics, 52(7), 646–654.

[15] CSRWire. (2023). AI and IoT cybersecurity considerations for healthcare. CSRWire Press Release.

[16] CapTech Consulting. (2023, December 18). Combining blockchain and AI to foster trust in healthcare. CapTech Insights Blog.

[17] Clindcast. (2023). FHIR and blockchain revolutionizing health data security. Clindcast Healthcare IT Blog.

[18] Tagde, P., Tagde, S., Bhattacharya, S., Tagde, M., Haldar, R., & Usmani, A. (2021). Blockchain and artificial intelligence technology in e-health. Environmental Science and Pollution Research, 28(38), 52810–52831.

[19] Putty, C. (2023). Safeguarding patient data: AI's role in healthcare cybersecurity. Thoughtful Blog.

[20] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data. MIT Media Lab White Paper.

[21] e-Estonia Briefing Centre. (n.d.). Estonian e-health records. e-Estonia.

[22] DigitalDefynd. (2025). Top 10 healthcare cybersecurity case studies [2025]. DigitalDefynd Insights.

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] Healthcare and Hospital Management. (n.d.). Case study – Reaching for healthcare IT value in the cloud. HHM Global Articles.

[24] Röhm, R., Dobson, E., & Prieto, J. T. (2024). Toward a tipping point in federated learning in healthcare and life sciences. NPJ Digital Medicine, 7(1), 159.

[25] Alsolami, T., Alsharif, B., & Ilyas, M. (2024). Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the Internet of Medical Things. Sensors, 24(3), 1112.

[26] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267–278.

[27] Myers, K., & O'Donnell, S. (2023). Is cloud computing in healthcare the key to securing data? Centric Consulting Blog.

[28] Al-Khasawneh, M. A., Faheem, M., Alarood, A. A., Habibullah, S., & Alzahrani, A. (2024). A secure blockchain framework for healthcare records management systems. Healthcare Technology Letters.

[29] Elvas, L. B., Serrão, C., & Ferreira, J. C. (2023). Sharing health information using a blockchain. Healthcare (Basel), 11(2), 170.

[30] Gohar, A. N., Abdelmawgoud, S. A., & Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. IEEE Access, 10, 92137–92157.

[31] Jadav, D., Patel, D., Gupta, R., Jadav, N. K., & Tanwar, S. (2022). BaRCODe: A blockchain-based framework for remote COVID detection for Healthcare 5.0. In 2022 IEEE International Conference on Communications Workshops (pp. 782–787). IEEE.

[32] Kumaar, M. A., Samiayya, D., Vincent, D. R., Srinivasan, K., Chang, C.-Y., & Ganesh, H. (2022). A hybrid framework for intrusion detection in healthcare systems using deep learning. Frontiers in Public Health, 9, 824898.

[33] Bathushaw, M. H., & Nagasundaram, S. (2024). The role of blockchain and AI in fortifying cybersecurity for healthcare systems. International Journal of Computational and Experimental Science and Engineering, 10(4), 300–307.

[34] Peremore, K. (2023, July 31). Challenges with using blockchain technology in healthcare. Paubox.

[35] Ahmed, M. I., Spooner, B., Isherwood, J., Lane, M., Orrock, E., & Dennison, A. (2023). A systematic review of the barriers to the implementation of artificial intelligence in healthcare. Cureus, 15(10), e46454.

[36] Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health, 6, Article 1359858.

[37] Amod, F. (2024, June 28). How cloud storage location affects HIPAA compliance. Paubox.

[38] Bayle, A., Koscina, M., & Perez-Lapillo, O. (2018). When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry. In 2018 IEEE/WIC/ACM

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

International Conference on Web Intelligence (pp. 788–792). IEEE.

[39] World Health Organization. (2021). Global strategy on digital health 2020–2025. World Health Organization.

[40] Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., & Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-health. Environmental Science and Pollution Research, 28(38), 52810–52831.

[41] Mennella, C., Maniscalco, U., De Pietro, G., & Esposito, M. (2024). Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. Heliyon, 10(4), e026297.

[42] Olaoye, F., & Egon, A. (2024). Federated learning for privacy-preserving security analytics. ResearchGate.

[43] Adcock, D. (2023, September 5). Building patient trust with the sovereign cloud. Healthcare Outlook.

Received: August 09, 2025