IADIS International Journal on WWW/Internet
Vol. 24, No. 1, pp. 54-67
ISSN: 1645-7641

A SECURE BLOCKCHAIN FRAMEWORK FOR STANDALONE AND MULTI-INSTITUTION CLINICAL SYSTEMS

Savina Mariettou[1], Constantinos Koutsojannis[2] and Vassilis Triantafyllou[3]
[1]*University of Peloponnese, Electrical and Computer Engineering Department, Patras, Greece.*
[2]*Professor of Medical Physics & Electrophysiology, Director of Health Physics & Computational Intelligence Laboratory, Physiotherapy Department, School of Health Rehabilitation Sciences, University of Patras, Patras, Greece.*
[3]*Professor of Network Technologies and Digital Transformation lab, Electrical and Computer Engineering Department., University of Peloponnese, Patras, Greece.*

ABSTRACT

Despite ongoing advancements in healthcare digitization, current electronic prescription systems still lack essential safeguards for data integrity, transparent traceability, and secure clinical workflows. As a result, inappropriate antibiotic use remains a major public health concern, particularly in the context of rising antimicrobial resistance (AMR). This study introduces a secure prescription architecture that integrates permissioned blockchain technology, smart contract-based validation, and fuzzy logic anomaly detection to ensure end-to-end integrity and process assurance. The first case presents a functional proof-of-concept implementation demonstrating the feasibility of the core validation workflow, cryptographic hashing of prescriptions, and AI-driven access monitoring. The second case extends the system into a multi-warehouse and multi-hospital configuration, where synchronized warehouse nodes maintain a shared ledger for real-time stock visibility, coordinated antibiotic stewardship, and cross-institution interoperability. Overall, across both cases, the proposed framework addresses critical gaps in national e-prescription infrastructures by providing a secure, transparent, and stewardship-aligned platform capable of operating as either a standalone system or an integrated module within broader clinical information environments. This combination of security-by-design mechanisms and stewardship-oriented logic positions the system as a robust foundation for next-generation e-prescription infrastructures.

KEYWORDS

Blockchain, Fuzzy Logic, e-Prescription, Antimicrobial Resistance, Multi-Warehouse, Health-IT Security

1. INTRODUCTION

As information systems become integral to organizational workflows (Alferjanya et al., 2022) and as cyber threats evolve in scale and complexity (Hore et al., 2024), cybersecurity emerges as a central concern. In the healthcare sector, particularly with the increasing reliance on electronic medical records, digital prescribing, and interconnected devices, medical data has become a prime target for cyberattacks. According to recent analyses, healthcare infrastructures face rising threats including ransomware, phishing, and data breaches, highlighting the urgent need for resilient, security-focused architecture (Mariettou et al., 2025a).

While technical intrusions remain a serious concern, risks also emerge from within clinical workflows. Inadequate oversight in antibiotic prescribing poses a significant threat to public health. Antibiotics, while essential for treating bacterial infections, can lead to severe consequences when misused. Poor healthcare system structures often correlate with inappropriate antibiotic use, as clinicians may resort to overprescribing in the absence of adequate diagnostic or monitoring tools, thereby contributing to the growing incidence of antimicrobial resistance (AMR) (Salam et al., 2023; Cotugno et al., 2025). These challenges underscore the need for a secure prescription database with real-time tracking capabilities, which are increasingly recognized as essential to supporting antimicrobial stewardship. However, tracking by itself does not guarantee appropriate use. Stewardship improves only when clinical justification and decision support are incorporated into the prescription workflow as well as AI-based can assist by offering patient-specific guidance while reducing alert fatigue (Sunku et al., 2024).

In this paper, we present the design and implementation of a secure, AI-enhanced, blockchain-based prescription system that supports responsible antibiotic tracking, embeds antimicrobial stewardship logic directly into the workflow, and defends against input-level threats through a fuzzy logic–driven anomaly detection module.

To demonstrate how the architecture performs under different deployment conditions, the system is evaluated through two distinct case studies: a single-warehouse configuration and a distributed multi-warehouse, multi-hospital scenario. Addressing a gap in current e-prescription infrastructures, this paper introduces a unified framework that integrates validation logic, smart-contract enforcement, cryptographic hashing, and adaptive access monitoring for high-risk antibiotics. Beyond the core validation workflow, the architecture is extended into a multi-warehouse environment in which synchronized blockchain nodes maintain consistent drug availability records, enabling scalable and interoperable deployments across distributed clinical settings. By combining clinically grounded decision structures with adaptive cybersecurity mechanisms, the proposed approach moves beyond conventional e-prescription systems and directly supports antimicrobial stewardship principles.

The remainder of this paper is organized as follows: Section 2 reviews related work. Section 3 presents the proposed blockchain-based secure prescription system, including its architecture, security mechanisms, and two case studies, one for the single-warehouse deployment and one for the extended multi-warehouse, multi-hospital scenario. Section 4 provides the evaluation results for both cases. Sections 5 and 6 conclude the paper by discussing the system's implications and outlining directions for future development.

2. RELATED WORK

In our review of 31 recent health security systems (Mariettou et al., 2025a), we identified 11 that utilize blockchain-based approaches to enhance data protection, access control, and system resilience across various healthcare contexts. These systems encompass a diverse range of applications, from IoT-driven health monitoring to decentralized record management, underscoring the versatility and growing role of blockchain in healthcare. Notably, however, none of them explicitly integrates prescription management as a central module, nor do they address antimicrobial stewardship (AMS) as a design priority. A concise overview of the 11 reviewed systems follows, highlighting both their innovations and the gap this study seeks to address. As shown in Table 1, these systems differ in focus and technical design.

Table 1. Overview of selected blockchain-based healthcare security systems, highlighting their focus, architectural components, prevented attacks, and notable features

Authors	Focus	Architecture	Attacks Prevented	Notes
(Puri et al., 2021)	Implant traceability & patient data custody	Smart contracts, secure channels	Impersonation, data leakage	Unique implant IDs; privacy-preserving model
(Abid et al., 2022)	Lightweight transmission for IoMT	E-DPoS consensus, SenCom model	Data tampering, node spoofing	Reputation-based routing is efficient in low-resource settings
(Sharma et al., 2023)	Malware classification with deep learning	Fog computing, federated storage	Botnets, ransomware, trojans	1500 malware types; deep learning model evaluated
(Selvarajan & Mouratidis, 2023)	Hybrid medical data storage	Off-chain via IPFS and cloud	Forgery, unauthorized access	Role-based access control is enabled
(Rani et al., 2023)	IoT-based anomaly detection in clinics	4-layer model (IoT, AI, data nodes)	Data breach, privilege abuse	Smart contracts for access control
(Akinola et al. 2024)	Medical certificate validation	Smart contracts with IoT verification	Phishing, identity theft	5-phase secure workflow
(Mohammed et al., 2023)	Trust-based secure data exchange	ECC, QTRAM model	No replay, privacy leak	Tuna Swarm Optimization; trust scoring logic
(Liu et al., 2024)	Intrusion detection in healthcare networks	4-layer EdDSA-enabled model	Tampering, privacy violation	Remote monitoring, ML-layered smart contracts
(Wu et al., 2024)	EMR exchange with patient control	ECC encryption, smart access policies	Replay, masquerading, and integrity attacks	Cloud integration, customizable permissions

(Mallick et al. 2024)	Decentralized medical file management	Smart contracts, IPFS, fog layer	Forgery, privacy breaches	Self-verifying identities; efficient access
(Idrissi & Palmieri, 2023)	Cloud-backed secure health records	AES, ECC, hybrid storage design	Integrity attack, replay, data breach	Off-chain encrypted storage, performance optimized

While existing blockchain-based healthcare systems offer notable advances in data protection and access control, they rarely address prescribing safety, a gap also highlighted in our literature review. None of the reviewed approaches incorporate stewardship-oriented safeguards, structured antimicrobial justification, or mechanisms for clinically governed authorization. In response, this paper introduces a blockchain-enabled prescription framework that tightly integrates security mechanisms, antimicrobial validation logic, and real-time anomaly detection. By leveraging smart contracts and structured decision workflows, the system establishes a robust and clinically aware prescription process. Furthermore, extends to a distributed multi-warehouse environment, demonstrating how blockchain can support coordinated antibiotic availability and stewardship across multiple institutions.

3. PROPOSED BLOCKCHAIN PRESCRIPTION SYSTEM

The proposed secure, AI-enhanced, blockchain-based prescription system is tailored for the oversight and stewardship of high-risk, high-cost, and last-line antibiotics such as colistin, meropenem, and ceftazidime–avibactam (Zavicefta), which are routinely used in the management of multidrug-resistant Gram-negative pathogens, including Klebsiella pneumoniae (Miller et al., 2024), Pseudomonas aeruginosa (Wu et al., 2024), and Acinetobacter baumannii (Karampatakis et al., 2024). These agents are clinically critical and require strict governance due to limited therapeutic alternatives and the elevated risk of inappropriate selection (Mikhail et al., 2019).

Within this context, the system incorporates all clinically relevant agents commonly placed under antimicrobial supervision protocols. These include last line polymyxins such as Colistin Norma PD.S. Inhaler and Colistin Norma 1,000,000 IU/vial (Stamatiou et al., 2023a; Stamatiou et al., 2023b), carbapenems such as Meropenem 1000 mg/vial (Kane, 2024), inhibitor combinations such as Zavicefta (Momcilovic et al., 2025), and targeted agents such as ertapenem (Banerjee et al., 2025) and fosfomycin (40 mg/ml infusion). Their toxicity profiles, microbiological targeting requirements, and stewardship constraints justify their inclusion in digital oversight mechanisms. To illustrate the rationale for targeting these antibiotics, Table 2 summarizes the main clinical reasons they are considered high-risk and therefore require strict digital supervision.

Table 2. High-risk antibiotics requiring digital supervision

Antibiotic	Clinical Use	Clinical Oversight Reason
Colistin	Used only when no other antibiotic works	High toxicity, high chance of treatment errors
Meropenem	Powerful "broad" antibiotic for severe infections	Overuse quickly creates resistant bacteria
Zavicefta	Targeted therapy for highly resistant infections	Very expensive; must be used only when absolutely needed
Ertapenem	Treatment for specific resistant bacteria	Not effective for some pathogens → easy to misuse
Fosfomycin	Add-on treatment for extremely resistant cases	Risk of resistance if used incorrectly

Beyond identifying the supervised antibiotics, the system guides the prescriber through a structured digital workflow that records all essential antimicrobial parameters, including infection classification, justification requirements, prior antimicrobial exposure, and pathogen-related details. These inputs ensure consistent documentation and clinician accountability, while remaining aligned with established stewardship practices (Nielsen et al., 2024; Truong & Yamaki, 2018). Once submitted, each prescription request is converted into a secure, traceable sequence of actions: a cryptographic hash is generated, stored on the blockchain, and evaluated through smart-contract rules that check authorization, completeness, and antibiogram compliance. This process transforms the platform from a simple recording tool into a tamper-resistant, auditable prescribing environment.

Because these high-risk antibiotics carry substantial toxicity, complex pharmacokinetic profiles, and high acquisition costs, their use demands strict oversight. The system enforces this through justification steps, antibiogram verification, and immutable auditability, preventing unauthorized use and ensuring that high-risk antibiotics are prescribed only when clinically justified.

The prescribing workflow integrates naturally into clinical practice. After submission, infection classification determines the required level of justification. For supervised antibiotics, brief validation is mandatory; requests may be resubmitted if necessary. When treatment is intended to exceed 14 days, additional approval from an infectious-disease specialist is required before finalization. Once validated, the prescription is confirmed and therapy may begin. This sequential, rule-based approach mirrors real hospital processes and embeds essential safeguards into an efficient, transparent workflow.

At the blockchain layer, the system operates on a permissioned network of clinical, warehouse, ordering, and administrative nodes that collectively maintain the distributed ledger. Three smart contracts regulate system behavior: the Prescription Validation Contract, which verifies authorization, prescription completeness, and antibiogram consistency before writing the hash; the Warehouse Update Contract, which manages stock reservation and availability; and the Audit and Traceability Contract, which records all prescription-related actions to create a tamper-proof clinical audit trail (Puri et al., 2024; Abid et al., 2024). Through smart-contract execution and decentralized consensus, the system ensures that prescriptions remain immutable, verifiable, and transparently traceable across all participating institutions.

3.1 System Architecture

Based on the findings of a national questionnaire conducted among healthcare professionals in Greece, key design priorities were identified for any future digital prescribing system. Participants emphasized the importance of a simplified user interface (UI) with minimal steps required to complete a prescription, alongside system robustness and the ability to operate reliably across different clinical environments (Grammatikopoulou et al., 2024). These practical demands directly informed the design of the proposed system, which integrates core principles of usability, adaptability, and technical security.

To meet these requirements, the system has been developed with a multi-layered architecture that supports modular growth while ensuring data security, prescription traceability, and real-time responsiveness. Each layer encapsulates a distinct set of responsibilities, from user interaction and validation to secure storage and verification. These functional stages are implemented through a layered system architecture, logically structured into three core levels. The system's architecture is illustrated in Figure 1, which outlines the core components and their interactions across three functional layers: user authentication, prescription processing, and secure data storage.

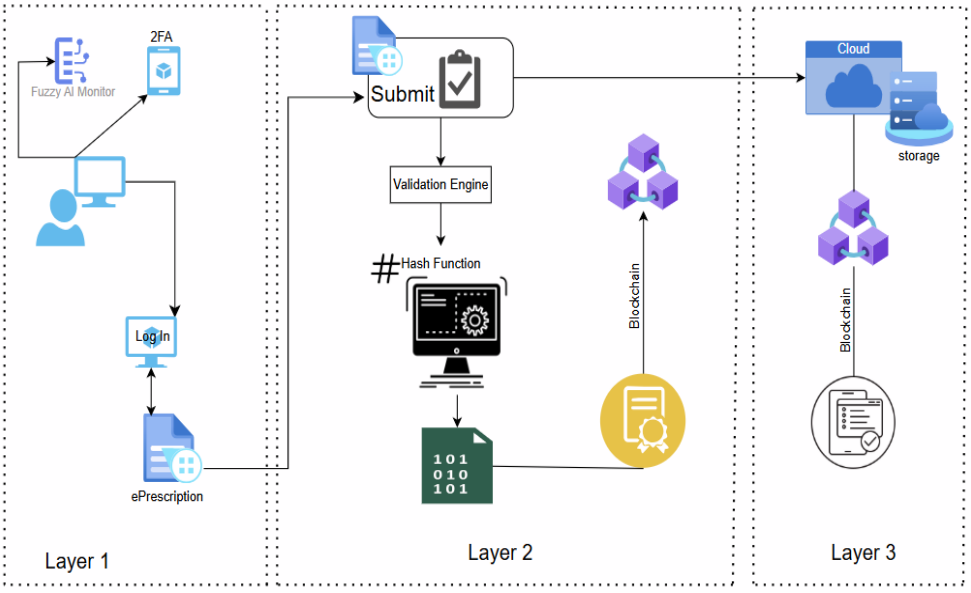

Figure 1. System Model

As shown in Figure 1, the system is organized into three layers, each corresponding to a distinct phase of the prescription lifecycle. It can be installed on an independent server and does not require a connection to a hospital's central infrastructure. The following sections provide a detailed description of the functionality and responsibilities of each layer.

The first layer of the system, responsible for interface and authentication, concerns the secure and transparent interaction between the physician and the system. A certified physician logs into the web-based interface using personal credentials. Two-Factor Authentication (2FA)

is enforced, particularly in cases of failed login attempts. In parallel, an AI module based on fuzzy logic continuously monitors login behavior. When multiple failed attempts are detected, the system increases the estimated probability of a pre-attack reconnaissance phase and adapts its security rules accordingly. Once access is successfully granted, the physician proceeds to complete the electronic prescription form.

The second layer handles the system's core functional logic, including prescription validation, hash generation, and blockchain submission. Upon form submission, the entered data is routed through a secure processing and validation mechanism. At this stage, a unique cryptographic hash is generated from the form contents and associated metadata, such as hospital ID and timestamp. This hash is then recorded on the blockchain using smart contracts, ensuring both the integrity and immutability of the transaction. More specifically, this assurance is enforced at the point where the prescription is validated, ensuring that the prescribed drugs cannot be altered. Additionally, this mechanism covers the entire process, from the moment the drugs are ordered from the warehouse until they are administered, capturing even the shortest possible time interval. Consequently, the integration of blockchain technology at this level serves a dual purpose: to guarantee transparency and provide legal-grade traceability for all issued prescriptions.

The third layer ensures data confidentiality and prescription authenticity by combining secure cloud storage with blockchain-based verification. The complete prescription document, along with its associated metadata, is encrypted and securely stored within a cloud infrastructure managed by the healthcare institution. When verification is required, the system compares the document's current content with the corresponding hash stored on the blockchain, allowing for the immediate detection of any discrepancies. Additionally, this layer implements role-based access control, while the use of decentralized, blockchain-based digital identifiers (SSIDs) enhances protection against identity spoofing and unauthorized access.

3.1.1 Layer Framework

The internal operation of the proposed system is organized into a layered framework that clearly separates off-chain logic, smart-contract execution, blockchain governance, and secure data storage. At the core of this design lies a permissioned Hyperledger Fabric network, chosen for its deterministic smart-contract execution, fine-grained access control, and robust identity management. The fuzzy-logic engine operates off-chain to avoid consensus overhead while still influencing the validation pathway through verified events, ensuring modularity and real-time adaptability. The layered structure of the system, illustrated in Figure 2, separates off-chain logic, smart-contract execution, and secure storage.

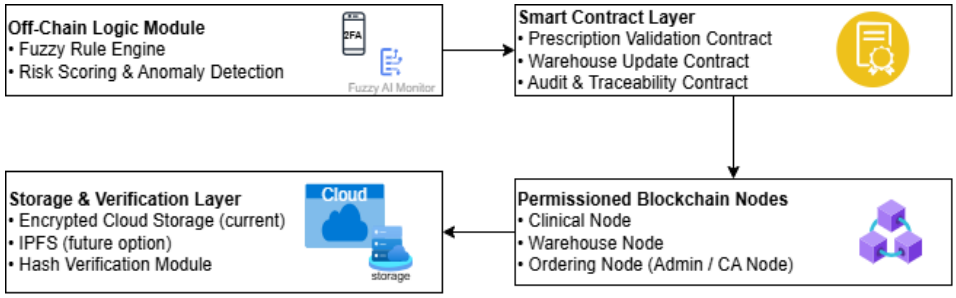

Figure 2. Layer Framework Overview for the single-warehouse deployment

At the core of the blockchain layer are the smart contracts, which define the rules of the system. The Prescription Validation Contract checks that the doctor is authorized, the prescription is complete, and the digital signatures and timestamps are correct before the hash is written to the ledger. The Warehouse Update Contract handles stock reservation and updates to drug availability, while the Audit and Traceability Contract record every action for accountability. These contracts run the same way for every transaction and guarantee that no step can be taken or altered.

The permissioned network is formed by four types of nodes, each with a clear role. Clinical nodes validate and sign prescriptions. Warehouse nodes confirm stock and apply the warehouse-update rules. Ordering nodes create blocks and keep all nodes synchronized, while the certificate-authority node manages identities and access rights. Together, these nodes maintain a shared and tamper-proof ledger. Prescription documents remain encrypted cloud storage, while the blockchain stores only their cryptographic hashes, allowing fast verification without storing sensitive data on-chain.

3.2 Security considerations and AI integration

The proposed system incorporates a three-layer security framework to address four key threat categories: identity impersonation, credential compromise, order tampering, and data leakage. User identities are protected through blockchain-based digital identifiers (SSIDs) and advanced cryptographic methods. Crucially, smart contracts form an important part of the blockchain layer, automating the validation, ordering, and immutability of prescription workflows. These contracts ensure that once a prescription is approved, it cannot be modified, thus supporting traceability, accountability, and regulatory compliance. Additional safeguards include TLS 1.3, ECC-based certificates, and strict role-based access controls, which preserve data confidentiality and prevent unauthorized system interactions. At the core of adaptability lies an AI module powered by fuzzy logic, which continuously monitors user access patterns. When anomalies such as repeated failed logins or irregular activity are detected, the system dynamically updates its rule sets, enhancing its ability to respond to emerging threats. It is worth noting that, due to its autonomous operation and online connectivity, the system may be targeted by external factors beyond the hospital’s internal network. Such threats can be mitigated by leveraging blockchain-based security measures. To illustrate the system's adaptive detection capabilities, a sample of fuzzy logic rules used for identifying anomalous behavior is presented in Figure 3.

```
(defrule Rule1-CriticalSuspicion
   (LoginAttempt (user ?u) (failedAttempts high) (retryRate fast) (ipDistribution diverse))
   =>
   (assert (Suspicion (user ?u) (level 0.95)))
)

(defrule Rule2-WeightedAdjustment
   (Suspicion (user ?u) (level ?x))
   (PatternHistory (user ?u) (weight ?w&:(> ?w 0.5)))
   =>
   (bind ?adjusted (min 1.0 (+ ?x (* 0.1 ?w))))
   (retract (Suspicion (user ?u) (level ?x)))
   (assert (Suspicion (user ?u) (level ?adjusted)))
)

(defrule Rule3-UpdateRules
   (NewThreatSignal (pattern ?p) (severity high))
   =>
   (assert (UpdateFuzzyRules (source ?p)))
```

Figure 3. Algorithm – Fuzzy Intrusion Detection Logic (CLIPS Representation)

These rules form the basis of the system's adaptive intrusion detection strategy and are actively employed during runtime to adjust access control decisions. Importantly, the security framework, including smart-contract validation, blockchain-anchored identity management, and fuzzy-logic anomaly detection, remains fully operational in Case 2, demonstrating that the core validation logic scales to the multi-warehouse architecture.

3.3 Case study 2: Multi-Warehouse and Multi-Hospital Deployment

Building on the Layer 2 validation workflow, the system is extended to operate across multiple warehouse and hospital units. In this multi-hospital configuration, the blockchain layer functions as a shared distributed ledger maintained by several synchronized warehouse nodes. The validation steps, hashing process, and auditability remain unchanged, but the ledger is now jointly managed by multiple institutions.

This distributed setup enables consistent multi-site availability checks and coordinated dispensing across locations where warehouse facilities may operate in different parts of the same city or region. Each warehouse node records updates through the Warehouse Update Contract, ensuring that reservation and dispensation events are propagated to all participating nodes. The extended ledger configuration and its interaction across warehouse nodes are illustrated in Figure 4.

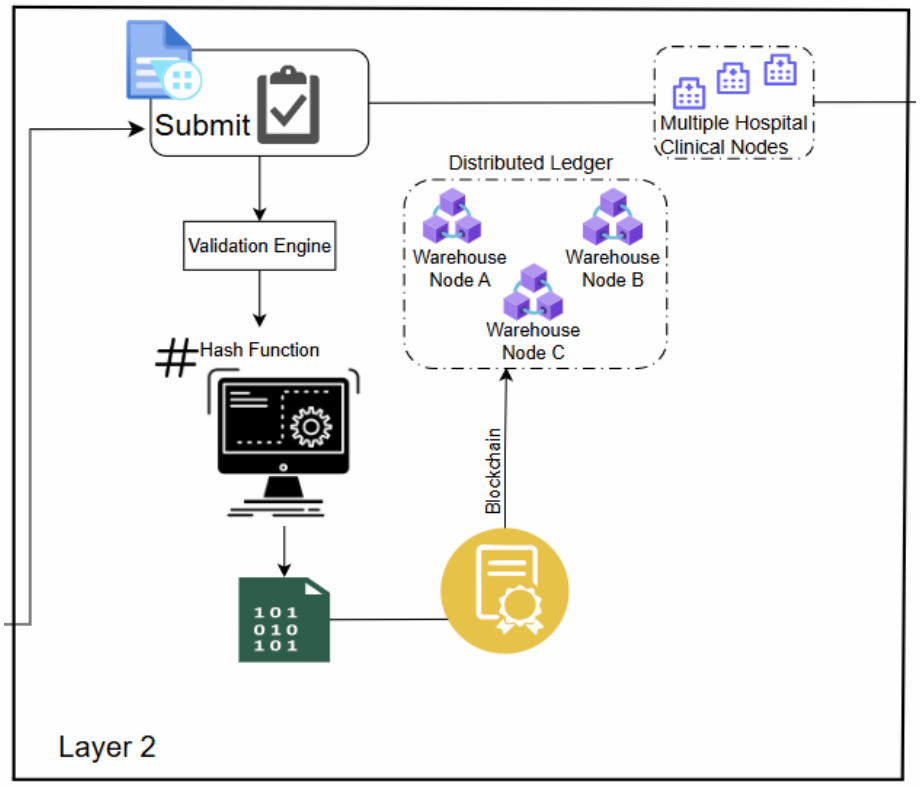

Figure 4. Extended Layer 2 architecture with synchronized warehouse nodes and multiple hospitalsαι

The architecture preserves the transparency, immutability, and prescription-integrity guarantees of the single-warehouse model while adding horizontal scalability and institutional interoperability. As a result, the system can support coordinated antimicrobial resource management across multiple healthcare sites.

3.3.1 Layer Framework (Case 2)

The extended deployment broadens the original layer framework into a distributed configuration incorporating multiple warehouse nodes and additional hospital units. Each warehouse node maintains its own inventory records while participating in the shared permissioned ledger, enabling unified high-level availability information across connected locations.

In this configuration, the Warehouse Update Contract executes across all warehouse nodes, coordinating reservation and decrementing operations in a consistent manner. This supports settings where multiple warehouses must collaborate to meet clinical demand. The node architecture also expands to include multiple clinical nodes, allowing hospitals within the same network to validate prescriptions and access synchronized availability information.

Although the set of smart contracts remains identical to Case 1, their operational scope increases. The Warehouse Update Contract serves as the central mechanism for multi-site availability checks, while the Audit and Traceability Contract provides a unified cross-institution audit trail. Overall, this distributed framework supports coordinated antibiotic stewardship across participating healthcare institutions.

4. EVALUATION

To assess the feasibility and robustness of the proposed system, a fully functional proof-of-concept implementation was developed. Physicians access the system through a secure web interface that enforces two-factor authentication and integrates a fuzzy AI module monitoring login behavior in real-time. This logic, implemented in CLIPS, dynamically adjusts suspicion levels and triggers security responses based on anomalous patterns. Once a prescription is completed, it is validated, hashed, and recorded through smart contracts, while the full data is encrypted and stored securely. Access is controlled via role-based permissions and digital signatures, confirming the system's technical viability for sensitive clinical environments.

Beyond the technical validation, brief feedback from healthcare professionals indicated that the prototype workflow was clear and that the justification fields for high-risk antibiotics were considered useful for stewardship. In addition, basic security and performance checks confirmed low-latency processing and effective anomaly detection by the fuzzy logic module.

Finally, the system addresses core threat categories through a layered defense. Table 3 summarizes the mapping of threats to countermeasures.

Table 3. Threat–Countermeasure Mapping in the Proposed Prescription System

Threat Category	Countermeasure	Mechanism
Identity impersonation	Blockchain-based identifiers (SSIDs)	Unique, decentralized IDs prevent spoofing and misuse
Credential compromise	Two-factor authentication + fuzzy monitoring	Real-time anomaly detection of login behavior
Prescription tampering	Smart contracts + cryptographic hashing	Immutable blockchain records ensure integrity and traceability
Data leakage	TLS 1.3 + encrypted cloud storage	Secure transmission and encrypted off-chain data storage

This layered approach demonstrates how the system integrates both technical safeguards and clinical oversight, ensuring that prescription integrity and data confidentiality are preserved throughout the workflow.

4.1 Evaluation of Case 2

The evaluation of the multi-warehouse deployment examined whether the extended architecture could maintain synchronization, consistency, and operational stability under distributed conditions. Using the Case 1 prototype with simulated multi-warehouse behavior, the analysis assessed the system's ability to coordinate updates across warehouse nodes and provide clinicians with consistent high-level availability responses.

Simulated multi-site reservation scenarios showed that the Warehouse Update Contract propagated updates uniformly across participating nodes, avoiding inconsistencies and supporting the intended use of the architecture in settings with geographically dispersed warehouses. Hypothetical multi-hospital workflows further demonstrated that clinical nodes could access a unified availability view through the shared ledger. The smart-contract logic maintained the traceability and immutability guarantees previously validated in Case 1. The main capabilities demonstrated through these evaluations are summarized in Table 4.

Table 4. Capabilities Demonstrated in Multi-Warehouse Architecture (Case 2)

Capability / Challenge	**Mechanism in Case 2**	**Benefit**
Multi-site availability	Distributed warehouse nodes	Consistent availability responses
Synchronized updates	Warehouse Update Contract	Uniform state propagation across nodes
Cross-institution access	Multiple clinical nodes in shared ledger	Unified high-level availability view

Overall, these capabilities indicate that the extended architecture can operate reliably in settings where warehouse facilities, whether hospital-based or external, are distributed across different locations, within the same city or across wider regions, and require coordinated availability through a shared ledger.

5. DISCUSSION

The proposed system demonstrates how combining decentralized architectures, smart-contract enforcement, and adaptive AI-driven monitoring can address persistent challenges in prescription security and antimicrobial stewardship. By anchoring prescription events to a permission blockchain, the system introduces verifiable integrity guarantees and prevents post-issuance modifications, limitations frequently observed in traditional e-prescription platforms (Mariettou et al., 2025b). Accountability becomes an inherent property of the workflow rather than an externally imposed control mechanism.

A key innovation of architecture lies in the fuzzy-logic module, which provides real-time behavioral monitoring and dynamically adjusts security thresholds based on detected anomalies. Unlike conventional rule-based login controls, this mechanism evaluates uncertain or borderline user behaviors and identifies reconnaissance patterns early, strengthening protection against credential misuse. Its off-chain operation preserves modularity while still influencing on-chain validation pathways, forming a coherent multi-layer security strategy.

From a clinical perspective, the system embeds essential antimicrobial stewardship principles directly into the prescribing workflow. Through structured justification fields, infection-specific logic, and validation checks for high-risk antibiotics, it promotes rational and well-documented antimicrobial use. This alignment of security logic with clinical reasoning distinguishes the system from prior blockchain-based health security models, which typically focus on data custody rather than stewardship-oriented governance.

Beyond the single-site implementation, the multi-warehouse and multi-hospital extension highlights the scalability of the architecture. Synchronized ledger updates across distributed warehouse nodes enable consistent multi-site availability information and support collaboration

across institutions. This distributed configuration offers a pathway toward shared resource coordination within broader healthcare networks.

In practice, the system can operate autonomously or integrate with existing Hospital Information Systems (HIS) through standard interoperability mechanisms. This allows prescription, identity and stock data to flow smoothly between platforms, supporting gradual and non-disruptive adoption.

Overall, the system brings together traceability, adaptive security, and stewardship-aligned decision structures. By improving consistency, auditability, and coordinated stock management, the architecture can support more appropriate antimicrobial use. These improvements are associated in the literature with reduced antimicrobial resistance and more efficient hospital resource utilization. The evaluation suggests that architecture not only addresses technical security gaps but also strengthens clinical governance in contexts where responsible antibiotic use is a priority.

6. CONCLUSION AND FUTURE WORK

This work presents a secure and intelligent prescription system that integrates permissioned blockchain technology with adaptive, behavior-aware access controls to support responsible antibiotic use. Architecture ensures verifiable integrity through immutable on-chain records and efficient smart-contract validation, while behavior-based access protection strengthens defense against credential misuse. The system operates autonomously yet can integrate with hospital information infrastructures, confirming its flexibility across diverse deployment environments.

The multi-warehouse case study demonstrates the system's capacity to support distributed healthcare networks. By maintaining synchronized availability information across warehouse nodes, the architecture enables coordinated resource management across institutions.

Future work will focus on extending the system to additional clinical scenarios, evaluating performance under real-world operational loads, and refining the user interface for broader clinical adoption. A key direction involves enriching the AI module to detect prescribing anomalies, such as atypical dosages or recurrent high-risk drug patterns, while maintaining strict data-privacy boundaries.

REFERENCES

Abid, A., Cheikhrouhou, S., Kallel, S., Tari, Z. & Jmaiel, M. (2024). A smart contract-based access control framework for smart healthcare systems. *The Computer Journal*, Vol. 67, No. 2, pp. 407-422. doi:10.1093/comjnl/bxac183. 363

Akinola, O., Akinola, A., Oyekan, B., Oyerinde, O., Adebiyi, H. F., & Sulaimon, B. (2024). Blockchain-Enabled Security Solutions for Medical Device Integrity and Provenance in Cloud Environments. *International Journal of Innovative Science and Research Technology (IJISRT)* IJISRT24APR225, 123-135. doi:10.38124/ijsrmt.v3i4.27

Alferjanya, A., Musaed Al-mwald, M. N. and Alias, R. B. (2022). *The Effect of Cyber Security Knowledge on Employees' Personal Growth: An Empirical Study in Private Hospitals in Libya and Yemen*. *Health Education and Health Promotion*, Vol. 10, No. 2, pp. 369-375.

Banerjee, B., Kaur, M., Sharma, A., Priya, A. & Singh, A. (2025). Some commercially available β-lactam antibiotics. In J. M. Khurana and B. Banerjee (eds.) *Bioactive Four-Membered Heterocycles: Natural Products, Green Synthesis and Bioactivity*, Vol. 7. De Gruyter, Berlin, pp. 1-38.

Cotugno, S. et al. (2025). Antimicrobial resistance and migration: interrelation between two hot topics in global health. *Annals of Global Health*, Vol. 91, No. 1, 12. doi:10.5334/aogh.4628

Grammatikopoulou, M. et al. (2024). Electronic prescription systems in Greece: a large-scale survey of healthcare professionals' perceptions. *Archives of Public Health*, Vol. 82, No. 1. doi:10.1186/s13690-024-01304-6

Hore, K. et al. (2024). Cybersecurity and critical care staff: A mixed methods study. *International Journal of Medical Informatics*, Vol. 185, 105412. doi:10.1016/j.ijmedinf.2024.105412

Idrissi, H. & Palmieri, P. (2023). Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems. *The Journal of Supercomputing*, Vol. 80, No. 5, pp. 6622-6660.

Kane, Z. A. (2024). *Application of mechanistic and mixed effect modelling in the elucidation of developmental factors influencing oral absorption and bioavailability in children*, Doctoral dissertation, University College London.

Karampatakis, T., Tsergouli, K. & Behzadi, P. (2024). Pan-genome plasticity and virulence factors: a natural treasure trove for Acinetobacter baumannii. *Antibiotics*, Vol. 13, No. 3, 257. doi:10.3390/antibiotics13030257

Liu, Y., Wang, X., Zheng, G., Wan, X. & Ning, Z. (2024). An AoI-aware data transmission algorithm in blockchain-based intelligent healthcare systems. *IEEE Transactions on Consumer Electronics*, Vol. 70, No. 1, pp. 1180-1190. doi:10.1109/TCE.2024.3365198

Mallick, S. R. et al. (2024). A lightweight, secure, and scalable blockchain-fog-iomt healthcare framework with ipfs data storage for healthcare 4.0. *SN Computer Science*, Vol. 5, No. 1, 198.

Mariettou, S., Koutsojannis, C. & Triantafillou, V. (2025a). Artificial Intelligence and Algorithmic Approaches of Health Security Systems: A Review. *Algorithms*, Vol. 18, No. 2, 59.

Mariettou, S., Koutsojannis, C. and Triantafyllou, V. (2025b). A Secure Prescription System with Machine Learning for SQL Injection Detection. *Computer Networks and Communications*, Vol. 3, No. 2, pp. 59–72. doi:10.37256/cnc.3220257145

Mikhail, S. et al. (2019). Evaluation of the synergy of ceftazidime-avibactam in combination with meropenem, amikacin, aztreonam, colistin, or fosfomycin against well-characterized multidrug-resistant Klebsiella pneumoniae and Pseudomonas aeruginosa. *Antimicrobial agents and chemotherapy*, Vol. 63, No. 8, pp. 10-1128. doi:10.1128/AAC.00779-19

Miller, J. C., Cross, A. S., Tennant, S. M. & Baliban, S. M. (2024). Klebsiella pneumoniae Lipopolysaccharide as a Vaccine Target and the Role of Antibodies in Protection from Disease. *Vaccines*, Vol. 12, No. 10, 1177. doi:10.3390/vaccines12101177

Mohammed, M. A. et al. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, Vol. 129, 107612. doi:10.1016/j.engappai.2023.107612. 376

Momcilovic, M. et al. (2025). Continuous infusion versus intermittent dosing of ceftazidime/avibactam in critically ill patients with Klebsiella pneumoniae OXA-48 or Pseudomonas aeruginosa infections: a single-center randomized open-label trial (ZAVICONT). Rationale and design. *Frontiers in pharmacology*, Vol. 16, 1618987. doi:10.3389/fphar.2025.1618987

Nielsen, N. D. et al. (2024). When to Stop Antibiotics in the Critically Ill?. *Antibiotics*, Vol. 13, No. 3, 272. doi: 0.3390/antibiotics13030272

Puri, V., Kataria, A. & Sharma, V. (2024). Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. *Transactions on Emerging Telecommunications Technologies*, Vol. 35, No. 4, e4245. doi:10.1002/ett.4245. 361

Rani, S., Chauhan, M., Kataria, A. & Khang, A. (2023). IoT equipped intelligent distributed framework for smart healthcare systems. In V. Rishiwal et al. (eds) *Towards the Integration of IoT, Cloud and Big Data. Studies in Big Data*, Vol 137. Springer, Singapore. doi:10.1007/978-981-99-6034-7_6

Salam, M. A. et al. (2023). Antimicrobial resistance: a growing serious threat for global public health. *Healthcare*, Vol. 11, No. 13, 1946. doi:10.3390/healthcare11131946

Stamatiou, R. et al. (2023a). Colistin Effects on Emphysematous Lung in an LPS-Sepsis Model. *Antibiotics*, Vol. 12, No. 12, 1731. doi:10.3390/antibiotics12121731

Stamatiou, R. et al. (2023b). Critical-illness: combined effects of colistin and vasoactive drugs: a pilot study. *Antibiotics*, Vol. 12, No. 6, 1057. doi:10.3390/antibiotics12061057

Selvarajan, S. & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Scientific Reports*, Vol. 13, No. 1, 7107. doi:10.1038/s41598-023-34354-x. 368

Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J. & Trivedi, M. C. (2023). EHDHE*: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Information Sciences*, Vol. 629, pp. 703-718. doi:10.1016/j.ins.2023.01.148.366

Sunku, S. S., Varuni, H. K. & Vinodha, K. (2024). Leveraging Permissioned Blockchain for securing controlled drug prescriptions in India. *2024 6th International Conference on Blockchain Computing and Applications (BCCA).* IEEE, pp. 513-518. doi:10.1109/bcca62388.2024.10844414

Truong, W. R. & Yamaki, J. (2018). The Hospital Antimicrobial Use Process: From Beginning to End. *Open Forum Infectious Diseases,* Vol. 5, No. 6, ofy098. US: Oxford University Press. doi:10.1093/ofid/ofy098

Wu, W., Huang, J. & Xu, Z. (2024). Antibiotic influx and efflux in Pseudomonas aeruginosa: Regulation and therapeutic implications. *Microbial biotechnology*, Vol. 17, No. 5, e14487. doi:10.1111/1751-7915.14487

Wu, C. et al. (2024). Healthcare 5.0: A secure and distributed network for system informatics in medical surgery. *International journal of medical informatics*, Vol. 186, 105415. doi:10.1016/j.ijmedinf.2024.105415. 380