Journal of Digital Media & Interaction
ISSN 2184-3120
Vol. 8, No. 19, (2025), pp. 46-65
DOI: 10.34624/jdmi.v8i19.40187

Threat Modeling a Health Web3 DApp

Ricardo Gomes
School of Technology and Management, Polytechnic of Leiria, Portugal
ricardo.p.gomes@ipleiria.pt
0000-0002-0438-9119

Daniela Dinis
School of Technology and Management, Polytechnic of Leiria, Portugal
daniela.o.dinis@ipleiria.pt
0009-0004-2541-2463

João Oliveira
School of Technology and Management, Polytechnic of Leiria, Portugal
joao.a.oliveira@ipleiria.pt
0009-0005-9903-5223

Marisa Maximiano
School of Technology and Management, Polytechnic of Leiria; CIIC, Portugal
marisa.maximiano@ipleiria.pt
0000-0002-1212-7864

Vítor Távora
School of Technology and Management, Polytechnic of Leiria, Portugal
vitor.tavora@ipleiria.pt
0009-0004-0404-9378

Carlos Machado Antunes
School of Technology and Management, Polytechnic of Leiria, Portugal
carlos.machado@ipleiria.pt
0009-0005-7010-4328

Manuel Dias
BioGHP, Portugal
manuel@bioghp.com
0009-0000-1830-6479

Ricardo Correia Bezerra
BioGHP, Portugal
ricardo@bioghp.com
0009-0005-1237-6632

Received: 6 June 2025
Accepted: 24 November 2025

Abstract
The healthcare sector increasingly explores Distributed Ledger Technology (DLT) and Health Web 3.0 Decentralized Applications (DApps) as promising solutions for patient-centric data management, data sovereignty, and privacy-preserving systems. Despite significant research at the intersection of blockchain and healthcare, current efforts predominantly address isolated technical challenges—focusing narrowly on specific mechanisms such as confidentiality, privacy, or individual smart contract vulnerabilities. Even cybersecurity assessments typically examine discrete attack vectors rather than comprehensive threat landscapes. This fragmented approach limits our ability to build trustworthy systems and delays real-world adoption, as stakeholders lack frameworks to holistically evaluate security posture.
This study addresses this gap by conducting a comprehensive threat modeling analysis of Health Web 3.0 DApps, taking into account the complex and interconnected security challenges inherent in blockchain-based healthcare systems. We employ a multi-framework approach integrating LINDDUN threat modeling methodology, OWASP Top 10 Smart Contract Vulnerabilities catalog, and Threat Dragon analytical tool to systematically identify, categorize, and evaluate security risks across the entire application stack. Our analysis maps threats spanning smart contract design flaws, cross-chain interaction vulnerabilities, decentralized identity management weaknesses, unauthorized data access risks, and denial-of-service attack vectors.
The primary contribution of this work is demonstrating the critical importance and practical value of holistic threat modeling in blockchain healthcare systems. Our findings reveal interdependencies between seemingly isolated vulnerabilities and show how comprehensive security assessment enhances data privacy protection, smart contract integrity, and overall application resilience. This research provides stakeholders with a systematic methodology for deriving trust in blockchain healthcare solutions, advancing both regulatory compliance and user confidence in decentralized medical data management systems.

Keywords *Blockchain, Healthcare, Threat Modeling*

© 2025 Ricardo Gomes, Daniela Dinis, João Oliveira, Marisa Maximiano, Vítor Távora, Carlos Machado Antunes, Manuel Dias, Ricardo Correia Bezerra
This is an open access article under the CC BY-NC-ND license.

1. Introduction

The modern healthcare landscape is experiencing unprecedented digital transformation, driven by the exponential growth of health data generation and the increasing demand for patient-centric care models. Electronic Health Records (EHRs), Internet of Medical Things (IoMT) devices, genomic sequencing, and telemedicine platforms collectively generate vast amounts of sensitive health information that require sophisticated management approaches. However, traditional centralized data management systems face significant challenges in addressing contemporary healthcare requirements, particularly concerning data sovereignty, interoperability, patient privacy, and regulatory compliance (Austin et al., 2024; Limna, 2023).

Current healthcare data infrastructure is characterized by fragmented systems, proprietary databases, and centralized architectures that create data silos and limit patient control over personal health information. These limitations become increasingly problematic as healthcare providers, researchers, and patients demand seamless data sharing capabilities while maintaining stringent privacy and security standards. The growing emphasis on patient empowerment and the shift toward value-based care models further amplifies the need for innovative data management solutions that can provide transparency, auditability, and patient ownership of health data (Shen et al., 2025).

Distributed Ledger Technology (DLT), particularly Blockchain technology, has emerged as a transformative paradigm that addresses many fundamental limitations of traditional healthcare data management systems, with a focus on the primary components shown in Figure 1. The inherent characteristics of DLT - including immutability, transparency, decentralization, and cryptographic security - align closely with healthcare requirements for secure, auditable, and patient-controlled data management. Blockchain technology enables the creation of tamper-resistant health records, facilitates secure data sharing among authorized stakeholders, and provides patients with unprecedented control over their personal health information (Agbo et al., 2019; Xia et al., 2024).

Figure 1. Main components of a Health Web 3 Ecosystem

The application of DLT in healthcare extends beyond simple data storage to encompass complex workflows, including clinical trial management, pharmaceutical supply chain tracking, insurance claim processing, and medical research collaboration. Smart contracts, self-executing programs with terms directly written into code, enable automated and trustless execution of healthcare agreements, reducing administrative overhead and eliminating intermediaries. These capabilities position DLT as a

foundational technology for next-generation healthcare systems that prioritize patient autonomy, data integrity, and system interoperability (Agbo et al., 2019).

The evolution toward Health Web 3.0 represents a paradigm shift from centralized, institution-controlled health data systems to decentralized, patient-centric ecosystems. Health Web 3.0 leverages blockchain technology, decentralized storage systems, and cryptographic protocols to create an internet of health data where patients maintain sovereignty over their information while enabling authorized access for healthcare delivery and research purposes. This ecosystem is primarily realized through Decentralized Applications (DApps) that operate on blockchain networks and provide user interfaces for interacting with decentralized health data systems (Narayan et al., 2024).

Health Web 3.0 DApps encompass a diverse range of applications, including decentralized health record management systems, peer-to-peer telemedicine platforms, decentralized clinical trial coordination tools, and blockchain-based health insurance solutions. These applications leverage various blockchain architectures, including public blockchains like Ethereum, private consortium chains, and hybrid solutions that balance transparency with regulatory compliance requirements. The integration of additional Web 3.0 technologies, such as decentralized identity (DID) systems, InterPlanetary File System (IPFS) for distributed storage, and cross-chain interoperability protocols, create sophisticated ecosystems that require comprehensive security considerations (Song et al., 2024).

Despite the promising potential of Health Web 3.0 DApps, their adoption in healthcare environments introduces complex security challenges that significantly differ from traditional web application security concerns (Jeršič et al., 2024). The decentralized nature of these systems, combined with the immutable characteristics of blockchain technology, creates unique attack vectors and vulnerability patterns that require specialized security assessment methodologies. Smart contracts, which serve as the core logic layer for many Health Web 3.0 DApps, are particularly susceptible to design flaws, coding errors, and economic attacks that can result in catastrophic failures (Alotaibi, 2025).

The multi-layered architecture of Health Web 3.0 DApps, spanning user interfaces, smart contract layers, blockchain networks, and external data sources, creates complex interaction patterns that can introduce systemic vulnerabilities. Cross-chain interactions, decentralized identity management systems, and integration with legacy healthcare infrastructure further complicate the security landscape. Additionally, the regulatory requirements for healthcare data protection, including Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and emerging blockchain-specific regulations, necessitate (Alotaibi, 2025).

Current literature on blockchain security primarily focuses on general smart contract vulnerabilities and cryptocurrency-related attacks (Gharavi et al., 2024), with limited attention to healthcare-specific security requirements and the unique characteristics of health data management applications. The

intersection of healthcare regulatory compliance, patient privacy requirements, and blockchain security represents a significant research gap that requires comprehensive investigation and specialized threat modeling approaches.

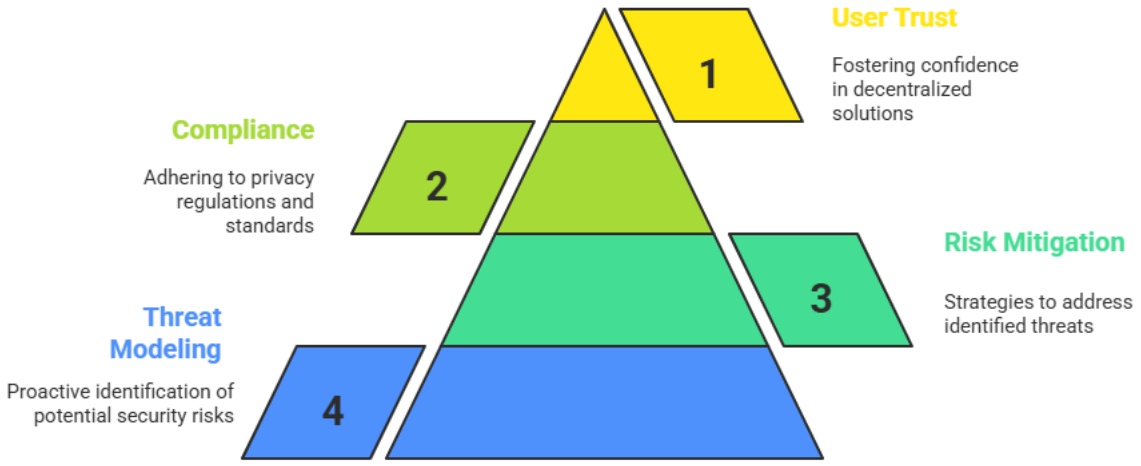

Figure 2. Proposed Hierarchical Security Framework for Blockchain Healthcare Systems.

Our research motivation is grounded in addressing a critical gap in blockchain healthcare security: while existing research predominantly examines isolated technical challenges—individual smart contract vulnerabilities, specific privacy mechanisms, or discrete attack vectors—the complex, interconnected nature of Health Web 3.0 ecosystems demands comprehensive security assessment. As illustrated in our research framework (depicted in Figure 2), we propose a hierarchical security model where holistic threat modeling (4) serves as the foundational layer upon which all other security considerations are built. Without systematic identification of potential security risks across the entire application stack and their interdependencies, it becomes impossible to develop effective risk mitigation (3) strategies, achieve meaningful compliance with healthcare privacy regulations (2), or ultimately foster the user trust (1) necessary for widespread adoption of decentralized healthcare solutions.

The pyramid structure of our approach emphasizes that user trust, the ultimate goal for any healthcare technology, cannot be achieved through fragmented security assessments that address only individual components. Healthcare stakeholders, including patients, providers, and regulatory entities, require demonstrable evidence that Health Web 3.0 DApps can meet stringent security and privacy standards through comprehensive rather than piecemeal evaluation. By establishing holistic threat modeling practices as the cornerstone of our security framework, we bridge the gap between current narrow-focus research and the integrated security perspective required for real-world healthcare implementation.

The key contributions of this study are: (1) demonstrating the critical importance and practical value of comprehensive threat modeling in blockchain healthcare systems by revealing interdependencies

between seemingly isolated vulnerabilities; (2) providing a replicable multi-framework methodology for holistic security assessment of Health Web 3.0 DApps.

The remainder of this paper is organized as follows: Section 2 presents the necessary related concepts of existing research on blockchain security, healthcare data protection, and threat modeling methodologies. Section 3 describes the architecture of our target Health Web3 DApp, and application of the threat modeling exercise. Section 4 details the methodology employed in our threat modeling exercise. Section 5 presents our findings, including identified threats, vulnerability categories, and risk assessments specific to Health Web 3.0 DApps. Finally, Section 5 concludes the paper with a summary of the key contributions and directions for future research in Health Web 3.0 security.

2. Related Concepts

This section establishes the foundational concepts required for understanding the security challenges inherent in Health Web 3.0 DApps. We examine four interconnected domains: distributed ledger technologies that enable decentralized healthcare applications, digital healthcare management solutions that define the application context, cybersecurity principles specific to healthcare environments, and threat modeling methodologies that provide systematic frameworks for security assessment. Understanding these concepts is essential for comprehending the multi-dimensional security challenges addressed in our research and the rationale behind our chosen threat modeling approach.

2.1. Blockchain and Distributed Ledger Technology

Blockchain technology represents a fundamental shift from traditional centralized data management systems to distributed, cryptographically secured networks. At its core, a blockchain is a distributed ledger that maintains a list of records, called blocks, which are linked and secured using cryptographic principles. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, creating an immutable chain of information that is resistant to modification (Gorkhali et al., 2020).

Distributed Ledger Technology (DLT) encompasses blockchain and other distributed database technologies that enable multiple parties to maintain synchronized copies of a shared database without requiring a central authority or intermediary (Somma et al., 2024). The key characteristics of DLT include: decentralization, where no single entity controls the network; immutability, where recorded data cannot be easily altered or deleted; transparency, where all participants can verify transactions; and consensus mechanisms that ensure all network participants agree on the validity of transactions.

Smart contracts (Alaba et al., 2024) are self-executing programs with contract terms directly written into code that automatically execute when predetermined conditions are met. These programmable contracts eliminate the need for intermediaries and enable complex business logic to be implemented directly on the blockchain. In healthcare contexts, smart contracts can automate processes such as

insurance claim processing, clinical trial protocols, and patient consent management while ensuring transparency and reducing administrative overhead.

Different blockchain architectures serve various use cases: public blockchains offer maximum transparency and decentralization but may raise privacy concerns for sensitive healthcare data; private blockchains provide greater control and privacy but sacrifice some benefits of decentralization; and consortium or hybrid blockchains attempt to balance transparency with privacy requirements, making them particularly suitable for healthcare applications where multiple trusted organizations need to collaborate while maintaining regulatory compliance (Abrar & Sheikh, 2024).

In blockchain-enabled healthcare systems, it is crucial to differentiate between on-chain and off-chain data storage mechanisms. On-chain data encompasses information permanently recorded within the blockchain ledger, such as transactions, smart contract parameters, and cryptographic hashes. While this method guarantees immutability and transparency, it is limited by block size constraints and high transaction fees, rendering it unsuitable for storing large-scale medical datasets (e.g., imaging records). Conversely, off-chain storage refers to data maintained outside the blockchain, with the ledger retaining only cryptographic proofs or reference pointers. By combining these approaches, healthcare applications can achieve both scalability and cost efficiency while maintaining verifiable integrity and authenticity of sensitive medical information (Hepp et al., 2018).

2.2. Digital Solutions for Healthcare Management

The healthcare industry has undergone significant digital transformation (Shen et al., 2025), with technology solutions addressing various aspects of medical care delivery, administration, and research. Electronic Health Records (EHRs) serve as the foundation of modern healthcare information systems, digitizing patient medical histories, treatment plans, and clinical outcomes. However, traditional EHR systems often operate in silos, limiting interoperability and patient control over personal health information.

Telemedicine platforms have revolutionized healthcare delivery by enabling remote consultations, monitoring, and treatment, particularly gaining prominence during the COVID-19 pandemic. These systems rely on secure communication technologies, digital identity verification, and remote monitoring devices to provide healthcare services across geographical boundaries. The Internet of Medical Things (IoMT) encompasses connected medical devices, wearable sensors, and smart healthcare equipment that continuously collect patient data and enable real-time health monitoring (El-Saleh et al., 2024).

Health Information Exchanges (HIEs) facilitate the secure electronic movement of health-related information among healthcare organizations, enabling coordinated care and reducing duplicate testing. However, current HIE systems face challenges related to data standardization, privacy protection, and patient consent management. Clinical Decision Support Systems (CDSS) leverage artificial intelligence and machine learning to assist healthcare providers in making informed treatment

decisions by analyzing patient data and providing evidence-based recommendations (Shojaei et al., 2024).

Digital health solutions also encompass pharmaceutical supply chain management systems that track medications from manufacturing to patient delivery, ensuring authenticity and preventing counterfeit drugs. Research platforms facilitate clinical trial management, patient recruitment, and data collection while ensuring regulatory compliance and participant privacy. The integration of these various digital solutions creates complex healthcare ecosystems that require sophisticated security and privacy protection mechanisms (Dhingra et al., 2024).

2.3. Cybersecurity

Healthcare cybersecurity presents unique challenges due to the sensitive nature of medical data, the critical importance of system availability for patient safety, and the complex regulatory environment governing health information protection. Healthcare organizations face a diverse threat landscape that includes ransomware attacks targeting hospital systems, data breaches exposing patient records, insider threats from employees with privileged access, and sophisticated advanced persistent threats seeking valuable health information.

The Health Insurance Portability and Accountability Act (HIPAA) in the United States (United States, 1996) establishes comprehensive privacy and security requirements for protected health information, mandating specific safeguards for electronic health data. The General Data Protection Regulation (GDPR) in Europe (European Parliament & European Council, 2016) provides additional privacy protection for health data, requiring explicit consent for data processing and establishing strict breach notification requirements. These regulatory frameworks create complex compliance requirements that healthcare organizations must navigate while implementing cybersecurity measures.

Healthcare cybersecurity challenges are compounded by the proliferation of connected medical devices, many of which were not designed with security as a primary consideration. Legacy medical equipment often lacks security features such as encryption, authentication, and updating mechanisms, creating potential entry points for attackers. The critical nature of healthcare services means that security measures must be implemented without disrupting patient care or clinical workflows (Dobrovolska et al., 2024).

Traditional cybersecurity approaches in healthcare focus on perimeter defense, access controls, and monitoring systems to protect centralized databases and networks (Rahim et al., 2024). However, the shift toward decentralized health data management introduces new security paradigms that require an understanding of cryptographic protocols, consensus mechanisms, and distributed system vulnerabilities. The integration of blockchain technology with healthcare systems creates hybrid environments that require security expertise spanning both traditional IT security and distributed ledger technologies.

2.4. Threat Modeling

Threat modeling is a systematic approach to identifying, quantifying, and addressing security threats in software systems and IT infrastructure. This proactive security methodology enables organizations to understand potential attack vectors, assess risk levels, and implement appropriate countermeasures before systems are deployed, or attacks occur. Threat modeling typically involves defining system boundaries, identifying assets and data flows, enumerating potential threats, and evaluating the likelihood and impact of successful attacks (Hammami, 2024).

Several established threat modeling frameworks provide structured approaches to security assessment. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) focuses on categorizing threats based on the type of security violation (Van Landuyt & Joosen, 2022). PASTA (Process for Attack Simulation and Threat Analysis) emphasizes business impact and risk assessment throughout the threat modeling process (Wolf et al., 2020). LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) specifically addresses privacy threats and is particularly relevant for healthcare applications handling sensitive personal data (Nweke et al., 2022).

In the context of blockchain and smart contract security, specialized threat modeling approaches have emerged to address unique vulnerabilities such as reentrancy attacks, integer overflow, access control flaws, and economic manipulation attacks. The OWASP (Open Web Application Security Project) Smart Contract Top 10 (OWASP, 2025a) provides a comprehensive catalog of the most critical smart contract vulnerabilities, serving as a foundation for blockchain-specific threat assessment.

Threat modeling tools such as Threat Dragon (OWASP, 2025b), Microsoft Threat Modeling Tool (Microsoft, 2022), and CAIRIS (CAIRIS, 2025) provide automated support for the threat modeling process, enabling systematic documentation of system architecture, threat identification, and mitigation planning. These tools facilitate collaboration among development teams, security professionals, and stakeholders while maintaining comprehensive documentation of security assessments.

The application of threat modeling to Health Web 3.0 DApps requires integration of traditional application security concerns with blockchain-specific vulnerabilities and healthcare privacy requirements. This multi-dimensional approach must consider technical vulnerabilities in smart contracts, privacy threats related to health data exposure, regulatory compliance requirements, and the complex interaction patterns between decentralized components and traditional healthcare infrastructure.

3. Architecture

This section presents our threat modeling architecture, for analyzing Health Web 3.0 DApps. Our approach recognizes that effective security assessment of decentralized healthcare applications requires a multi-layered methodology that addresses the distinct components of DApp infrastructure

while leveraging specialized frameworks and tools designed for privacy and smart contract security analysis. Figure 3 depicts the landscape or our research efforts, showing the conceptual abstractions of the target health care application and our main components for the threat modeling exercise, both detailed in the following sub-sections.

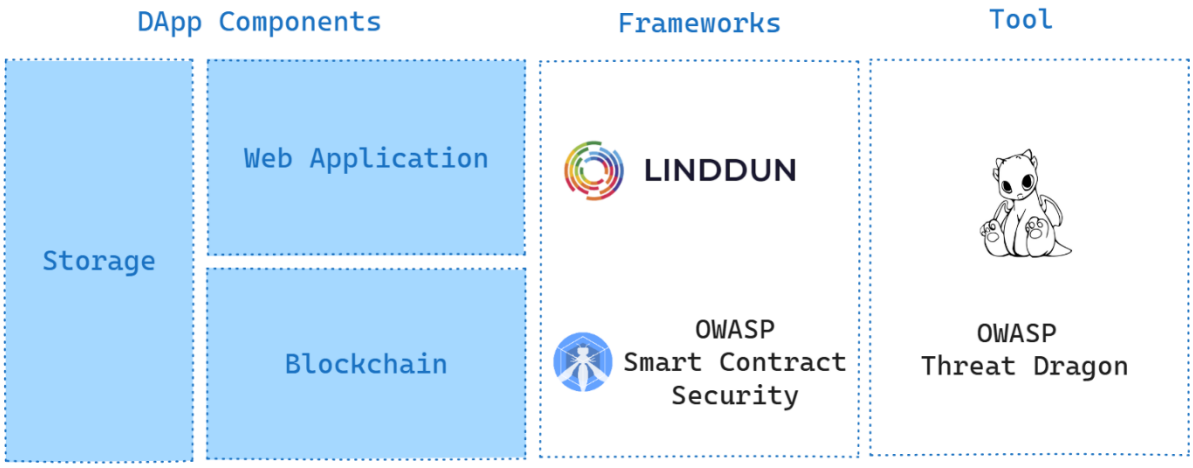

Figure 3 - Threat Modeling Landscape

3.1. DApp Component Analysis Framework

Our threat modeling analysis focuses on a Health Web 3.0 DApp currently being developed by a parallel research team, examining its abstracted architectural design rather than implementation-level code. This approach deliberately leverages the application's development status as an advantage: threat modeling frameworks are most effective when integrated throughout the software development lifecycle rather than applied retrospectively to completed systems. By conducting our security assessment during the active development phase, we demonstrate the practical value of proactive threat identification—enabling developers to address vulnerabilities during design and implementation rather than after deployment.

Health Web 3.0 DApps consist of three fundamental architectural layers, each presenting unique security challenges that require targeted assessment approaches. Our analysis framework systematically examines each component at the architectural level to ensure comprehensive threat identification across the entire application stack, providing actionable security insights that can inform ongoing development decisions.

3.1.1. Storage Layer

The storage component encompasses both on-chain and off-chain data management systems used by Health Web 3.0 DApps. On-chain storage includes data directly recorded on the blockchain, such as transaction records, smart contract state variables, and cryptographic hashes of medical documents. Off-chain storage systems, including decentralized storage networks like IPFS (InterPlanetary File System) (Daniel & Tschorsch, 2022) and traditional cloud storage solutions, handle larger data files such as medical images, detailed patient records, and clinical documentation.

Security considerations for the storage layer include data encryption mechanisms, access control implementations, data integrity verification, and compliance with healthcare data protection regulations. The immutable nature of blockchain storage creates unique challenges for data correction and patient privacy rights, while off-chain storage systems introduce additional attack vectors related to data availability and unauthorized access.

3.1.2. Web Application Layer

The web application layer represents the user interface and client-side logic that enables healthcare stakeholders to interact with the underlying blockchain infrastructure. This component includes web browsers, mobile applications, and specialized healthcare software interfaces that provide functionality for patient data management, clinical workflow automation, and healthcare service delivery.

The web application layer faces traditional web security threats such as cross-site scripting (XSS), SQL injection, and authentication vulnerabilities, while also introducing DApp-specific concerns related to wallet integration, transaction signing, and blockchain communication protocols. The integration of healthcare-specific requirements, including patient identity verification and clinical workflow support, creates additional complexity in the user interface layer (Al-Kahla et al., 2021).

3.1.3. Blockchain Layer

The blockchain component forms the core infrastructure that enables decentralized functionality, including smart contract execution, consensus mechanisms, and network communication protocols. This layer encompasses the underlying blockchain network (such as Ethereum or Hyperledger), smart contract implementations, and cross-chain interoperability protocols.

Security analysis of the blockchain layer focuses on smart contract vulnerabilities, consensus mechanism attacks, network-level threats, and economic manipulation attempts. The programmable nature of smart contracts introduces unique vulnerabilities that differ significantly from traditional software security concerns, requiring specialized assessment of methodologies and tools.

3.2. Multi-Framework Assessment Approach

Our threat modeling methodology integrates two complementary frameworks that address different aspects of Health Web 3.0 DApp security. This multi-framework approach ensures comprehensive coverage of both privacy-specific threats relevant to healthcare data and technical vulnerabilities inherent in smart contract implementations.

3.2.1. LINDDUN Framework for Privacy Threat Analysis

LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) (LINDDUN, 2025) provides a systematic approach to identifying privacy threats in healthcare applications. This framework is particularly relevant for Health Web 3.0 DApps due to the sensitive nature of medical data and stringent regulatory requirements for patient privacy protection.

The LINDDUN methodology enables systematic evaluation of how patient data flows through DApp components, identification of potential privacy breaches, and assessment of compliance with healthcare privacy regulations such as HIPAA and GDPR. By applying LINDDUN principles to each DApp component, we can identify privacy risks that might not be apparent through traditional security assessment approaches.

3.2.2. OWASP Smart Contract Security Framework

The OWASP Smart Contract Top 10 (OWASP, 2025a) provides a comprehensive catalog of the most critical vulnerabilities affecting smart contract implementations. This framework addresses technical security concerns specific to blockchain-based applications, including coding errors, design flaws, and economic attack vectors that can compromise smart contract functionality.

Our application of the OWASP framework focuses on evaluating smart contracts used in Health Web 3.0 DApps, including patient consent management contracts, clinical trial automation logic, and healthcare payment processing systems. This analysis identifies potential vulnerabilities that could lead to unauthorized access to patient data, manipulation of clinical records, or disruption of healthcare services.

3.3. OWASP Threat Dragon

OWASP Threat Dragon (OWASP, 2025b) serves as our primary implementation tool for conducting systematic threat modeling across DApp components and frameworks. Threat Dragon provides a collaborative platform for documenting system architecture, identifying potential threats, and developing mitigation strategies while maintaining comprehensive documentation of the threat modeling process.

The tool's visual modeling capabilities enable clear representation of data flows between DApp components, identification of trust boundaries, and systematic enumeration of potential attack vectors. Threat Dragon's integration with established threat modeling methodologies supports consistent application of both LINDDUN and OWASP frameworks while providing structured documentation of findings and recommendations.

Our use of Threat Dragon facilitates collaborative analysis among security researchers, healthcare domain experts, and blockchain developers, ensuring that threat identification incorporates both technical security expertise and healthcare-specific knowledge. The tool's reporting capabilities support the development of actionable mitigation strategies and compliance documentation required for healthcare technology implementations.

3.4. Integrated Analysis Methodology

The integration of DApp component analysis, multi-framework assessment, and Threat Dragon implementation creates a comprehensive methodology for Health Web 3.0 DApp security evaluation. This approach ensures that threat identification spans technical vulnerabilities, privacy concerns, and healthcare-specific requirements while providing systematic documentation and mitigation planning.

Our methodology recognizes that effective security assessment of Health Web 3.0 DApps requires understanding of the complex interactions between traditional web application security, blockchain-specific vulnerabilities, and healthcare privacy requirements. By combining established threat modeling frameworks with specialized tools and systematic component analysis, we aim to provide comprehensive security guidance for developers and healthcare organizations implementing decentralized healthcare solutions.

The architectural framework presented in this section forms the foundation for our empirical analysis and findings, which will be detailed in subsequent sections of this paper. This methodology represents an initial step toward developing standardized approaches for Health Web 3.0 DApp security assessment, with future research building upon these foundational principles to address emerging threats and evolving regulatory requirements.

4. Threat Modeling Exercise Methodology

This study presents a preliminary threat modeling assessment of a Health Web 3.0 DApp currently undergoing active development by a parallel research team. The preliminary nature of this exercise is both intentional and methodologically advantageous, as threat modeling frameworks are designed to function as iterative security practices integrated throughout the software development lifecycle. By conducting our assessment during the design and development phases, we enable early identification and mitigation of vulnerabilities before they manifest in production systems. Our primary objective is to identify potential threats to patient confidentiality and privacy—the paramount security concerns in healthcare applications—while establishing a systematic framework that can be refined and expanded as the underlying application evolves.

We employed a multi-framework approach that integrates two complementary security methodologies to ensure comprehensive threat coverage. Our core methodology utilizes the LINDDUN framework (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance), a privacy-centric threat modeling approach that aligns directly with our focus on patient confidentiality and data protection. LINDDUN provides systematic categories for identifying privacy risks across data flows, storage mechanisms, and user interactions within decentralized architectures, making it particularly well-suited for healthcare applications where protecting sensitive medical information is critical. To address blockchain-specific vulnerabilities, we integrated the OWASP Smart Contract Security Guidelines as a complementary knowledge base. Smart contracts serve as the trust and access control layer in Health Web 3.0 DApps, and the OWASP guidelines provide a structured catalog of common vulnerabilities, that could compromise patient data confidentiality or enable unauthorized access to medical records.

Our threat modeling exercise focused on the abstracted architectural design of the Health Web 3.0 DApp rather than implementation-level code. This abstraction approach serves dual strategic purposes: it enables threat identification during the design phase when vulnerabilities are less costly to address, and it produces generalizable security insights applicable to similar blockchain healthcare

applications beyond this specific implementation. Working with the development team's architectural documentation, we decomposed the application into three fundamental components. The Web Application component represents the user-facing interface where patients, healthcare providers, and administrators interact with the system, handling authentication, data input, and results presentation. The Blockchain component serves as the notarization layer where health data integrity is verified, and access permissions are managed through smart contracts, ensuring tamper-proof audit trails without storing sensitive information on-chain. The Storage component encompasses off-chain decentralized storage solutions where actual private patient data, like medical records, diagnostic images, and personal health information, resides, separated from the public blockchain to maintain confidentiality while leveraging blockchain-based access control.

For each architectural component, we systematically applied LINDDUN privacy threat categories to identify potential risks to patient confidentiality, examining how data flows between components, where trust boundaries exist, and which interaction points could expose sensitive information. Concurrently, we cross-referenced potential attack vectors documented in OWASP smart contract security guidelines, focusing particularly on vulnerabilities in the Blockchain component that could lead to unauthorized data access or compromise the integrity of access control mechanisms. This layered analysis approach ensures comprehensive threat identification across user-facing interfaces, blockchain transaction logic governing data permissions, and storage mechanisms handling sensitive medical records. Identified threats were then prioritized based on their potential impact on patient confidentiality, data privacy, and regulatory compliance requirements under frameworks such as GDPR. This preliminary assessment establishes a baseline threat landscape that demonstrates the practical value of integrating holistic security assessment throughout the software development lifecycle, with findings that will inform ongoing development decisions and can be iteratively refined as the application architecture matures.

5. Discussion

This section presents our preliminary findings and insights gained from the initial phases of our Health Web 3.0 DApp threat modeling research. As an introductory study, our work has focused on establishing the foundational framework and conducting preliminary analysis across representative Health Web 3.0 applications. The insights presented here reflect our current understanding of the security landscape and provide direction for comprehensive threat assessment in decentralized healthcare systems.

5.1. Research Overview and Current Progress

Our research has progressed through several key phases, beginning with the systematic identification and categorization of Health Web 3.0 DApp components across multiple healthcare use cases. We have examined representative applications including decentralized patient record management systems, blockchain-based clinical trial coordination platforms, and peer-to-peer

telemedicine DApps. This analysis has provided valuable insights into the architectural patterns and security challenges common across different types of healthcare decentralized applications.

The application of our multi-framework approach—integrating LINDDUN privacy threat modeling, OWASP smart contract vulnerability assessment, and Threat Dragon systematic analysis—has revealed the complexity of security considerations in Health Web 3.0 environments. Our preliminary findings indicate that traditional cybersecurity frameworks, while necessary, are insufficient for addressing the unique challenges posed by the intersection of healthcare privacy requirements and blockchain technology constraints.

Through our systematic component analysis, we have identified recurring patterns in how Health Web 3.0 DApps handle sensitive health data, implement patient consent mechanisms, and manage cross-system interoperability. These patterns suggest both common vulnerabilities that span multiple applications and specialized threats that emerge from specific healthcare workflow implementations.

5.2. Key Insights from Privacy Threat Analysis

The application of LINDDUN methodology to Health Web 3.0 DApps has yielded significant insights into privacy-specific threats that differ substantially from general blockchain privacy concerns. Our analysis reveals that healthcare DApps face unique challenges in balancing the transparency inherent in blockchain technology with the stringent privacy requirements mandated by healthcare regulations, namely:

- **Linkability and Identifiability Concerns**: Our preliminary findings indicate that even when patient data is pseudonymized or encrypted, the immutable and transparent nature of blockchain transactions can create linkability patterns that potentially compromise patient privacy. The correlation of transaction patterns with external healthcare data sources presents risks that traditional privacy impact assessments may not adequately address.
- **Detectability and Disclosure Challenges**: Health Web 3.0 DApps often require complex data sharing scenarios involving multiple healthcare stakeholders. Our analysis suggests that current implementations may inadvertently create data disclosure pathways that violate healthcare privacy principles. The challenge lies in maintaining necessary clinical data accessibility while preventing unauthorized detectability of patient health status.
- **Regulatory Compliance Complexity**: The intersection of blockchain immutability with healthcare regulations requiring data correction and deletion rights (such as GDPR's "right to be forgotten") presents fundamental architectural challenges. Our research indicates that current Health Web 3.0 DApp designs often lack robust mechanisms for addressing these regulatory requirements without compromising system integrity.

5.3. Smart Contract Vulnerability Patterns

Our application of OWASP smart contract security analysis to healthcare DApps has revealed concerning patterns of vulnerabilities that are amplified in healthcare contexts due to the critical nature of medical data and processes. The economic incentives and attack motivations in healthcare applications differ significantly from traditional cryptocurrency applications, creating unique threat vectors. These are the main patterns:

- **Access Control Vulnerabilities**: Healthcare smart contracts typically implement complex access control mechanisms to manage different stakeholder roles (patients, healthcare providers, researchers, regulators). Our preliminary analysis suggests that many implementations suffer from inadequate access control validation, potentially allowing unauthorized parties to access or modify sensitive health information.
- **Business Logic Flaws**: The translation of complex healthcare workflows into smart contract logic introduces opportunities for business logic vulnerabilities. Our research indicates that clinical decision support contracts and automated treatment protocols may contain logic flaws that could lead to incorrect medical recommendations or treatment decisions.
- **Integration Security Issues**: Health Web 3.0 DApps frequently integrate with external healthcare systems and oracles providing real-world medical data. Our analysis reveals that these integration points often represent significant security vulnerabilities, particularly regarding data validation and source authentication.

5.4. Systemic Security Challenges

Beyond component-specific vulnerabilities, our research has identified systemic security challenges that emerge from the complex interactions between DApp layers and the healthcare ecosystem:

- **Cross-Chain Security Implications**: Many Health Web 3.0 applications use cross-chain protocols to achieve interoperability with different blockchain networks and healthcare systems. Our preliminary findings suggest that these cross-chain implementations introduce additional attack vectors related to bridge security, consensus validation, and data integrity across networks.
- **Legacy System Integration**: The integration of blockchain-based Health Web 3.0 DApps with existing healthcare infrastructure creates hybrid environments with complex security dependencies. Our analysis indicates that security vulnerabilities in legacy systems can potentially compromise the security assumptions of blockchain components, creating systemic risks.
- **Scalability and Security Trade-offs**: Healthcare applications require high throughput and low latency to support clinical workflows. Our research suggests that performance optimizations in Health Web 3.0 DApps often involve security trade-offs that may not be apparent to healthcare stakeholders but could significantly impact system security.

These challenges require holistic security approaches that consider the entire healthcare technology stack.

5.5. Implications for Healthcare Web3 Technology Adoption

Our preliminary findings have important implications for the adoption of Health Web 3.0 technologies in healthcare environments. The security challenges identified through our research suggest that current DApp implementations may not meet the stringent security and privacy requirements necessary for widespread healthcare adoption.

Healthcare organizations considering Health Web 3.0 DApp adoption face significant challenges in conducting appropriate risk assessments due to the novel nature of these technologies and the limited availability of healthcare-specific security guidance. Our research indicates that traditional healthcare technology risk assessment frameworks require substantial adaptation to address blockchain-specific threats.

The regulatory landscape for Health Web 3.0 applications remains largely undefined, creating challenges for healthcare organizations seeking to ensure compliance. Our analysis suggests that current DApp implementations may struggle to demonstrate compliance with existing healthcare regulations, potentially limiting adoption in regulated healthcare environments.

The deployment and maintenance of secure Health Web 3.0 DApps requires specialized expertise spanning healthcare domain knowledge, blockchain technology, and cybersecurity. Our findings indicate that the current shortage of professionals with this interdisciplinary expertise represents a significant barrier to secure implementation.

6. Conclusion

This paper presents a foundational investigation into the security challenges of Health Web 3.0 Decentralized Applications (DApps), establishing a comprehensive threat modeling framework specifically designed for healthcare blockchain environments. Our research addresses a critical gap in the current understanding of security risks associated with decentralized healthcare systems by integrating established privacy and smart contract security methodologies with healthcare-specific requirements.

Our primary contribution lies in the development of a multi-layered threat modeling architecture that systematically addresses the three fundamental components of Health Web 3.0 DApps: storage systems, web applications, and blockchain infrastructure. By integrating LINDDUN privacy threat modeling with OWASP smart contract security analysis and implementing this approach through Threat Dragon, we have established a comprehensive methodology for identifying and evaluating security risks unique to decentralized healthcare applications.

The research demonstrates that traditional cybersecurity frameworks, while necessary, are insufficient for addressing the complex security landscape of Health Web 3.0 environments. Our analysis reveals that the intersection of healthcare privacy requirements, regulatory compliance

mandates, and blockchain technology constraints creates novel security challenges that require specialized assessment approaches. Through our systematic component analysis, we have identified recurring security patterns across different types of healthcare DApps, including decentralized patient record management systems, blockchain-based clinical trial platforms, and peer-to-peer telemedicine applications.

Our preliminary analysis has yielded several critical insights that advance the understanding of Health Web 3.0 security challenges. The application of privacy-focused threat modeling reveals fundamental tensions between blockchain transparency and healthcare privacy requirements, particularly regarding patient data linkability and regulatory compliance with data protection laws. The smart contract security analysis highlights patterns of vulnerabilities that are amplified in healthcare contexts due to the critical nature of medical data and processes, including access control vulnerabilities, business logic flaws, and integration security issues that could compromise patient safety and data integrity.

The findings have significant implications for healthcare organizations considering the adoption of Health Web 3.0 technologies. The security challenges identified suggest that current DApp implementations may not meet the stringent requirements necessary for deployment in regulated healthcare environments. Healthcare technology stakeholders must carefully evaluate these risks and implement comprehensive security frameworks before adopting decentralized healthcare solutions.

The preliminary nature of this research opens several critical avenues for future investigation that are essential for advancing the security and adoption of Health Web 3.0 technologies. The development of standardized security assessment frameworks specifically designed for Health Web 3.0 applications represents the highest priority research direction, requiring purpose-built assessment methodologies that integrate healthcare regulatory requirements, blockchain security considerations, and privacy protection mechanisms. Future research should also investigate novel privacy-preserving technologies, including zero-knowledge proofs and homomorphic encryption, for healthcare blockchain applications while conducting comprehensive threat modeling to identify potential vulnerabilities.

Additionally, the development of comprehensive economic security models that account for the unique incentive structures and attack motivations present in healthcare environments requires significant research attention. Traditional blockchain economic security models may not adequately address the non-financial motivations and regulatory constraints that characterize healthcare applications. The evolving regulatory landscape for Health Web 3.0 applications also requires ongoing research to understand compliance requirements and develop practical implementation guidance.

Despite the significant contributions of this study, it is essential to acknowledge certain limitations. First, the analysis remains primarily conceptual, supported by structured threat modeling but lacking empirical validation through a real-world deployment or large-scale case study. Although the integration of LINDDUN with established knowledge bases offers a comprehensive theoretical

foundation, the effectiveness of the proposed mitigations remains untested in operational healthcare environments.

Second, the architecture presented constrained the scope of the threat modeling exercise. These omissions may underestimate systemic vulnerabilities that emerge in more heterogeneous Health Web 3.0 ecosystems.

Third, the study focused primarily on privacy-related threats (linkability, identifiability, unawareness, and non-compliance) identified via LINDDUN but did not equally explore adversarial dynamics such as advanced persistent threats, insider misuse, or emerging AI-driven attack strategies.

Future work could complement this privacy-centric approach with broader resilience assessments using STRIDE, DREAD, or hybrid models. Looking ahead, several avenues for further research are evident. Empirical validation through prototyping and penetration testing of a functional Health Web 3.0 DApp would provide secure evidence of the practicality of the mitigations proposed.

This research establishes a foundational understanding of the security challenges inherent in Health Web 3.0 DApps and provides a systematic approach for identifying and evaluating these risks. While our findings reveal significant security challenges that must be addressed before widespread healthcare adoption, they also demonstrate the potential for developing secure and privacy-preserving decentralized healthcare solutions through careful design and comprehensive security assessment. The complexity of Health Web 3.0 security requires sustained research effort and collaboration among healthcare professionals, blockchain developers, security experts, and regulatory authorities. The threat modeling framework and preliminary findings presented in this work provide a starting point for this collaborative effort, establishing the foundation for developing more secure and trustworthy decentralized healthcare systems.

Acknowledgments

This work was financially supported by Project BlockchainPT – Decentralize Portugal with Blockchain Agenda, WP 2: Health and Wellbeing, 02/C05-i01.01/2022.PC644918095-00000033, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

Abrar, I., & Sheikh, J. A. (2024). Current trends of blockchain technology: architecture, applications, challenges, and opportunities. *Discover Internet of Things*, *4*(1), 1–17. https://doi.org/10.1007/S43926-024-00058-5/TABLES/3

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare 2019, Vol. 7, Page 56*, *7*(2), 56. https://doi.org/10.3390/HEALTHCARE7020056

Alaba, F. A., Sulaimon, H. A., Marisa, M. I., & Najeem, O. (2024). Smart Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science*, *5*, 15–41. https://doi.org/10.37256/CCDS.5120243271

Al-Kahla, W., Shatnawi, A. S., & Taqieddin, E. (2021). A Taxonomy of Web Security Vulnerabilities. *2021 12th International Conference on Information and Communication Systems, ICICS 2021*, 424–429. https://doi.org/10.1109/ICICS52457.2021.9464576

Alotaibi, B. (2025). Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. *Sensors 2025, Vol. 25, Page 342*, *25*(2), 342. https://doi.org/10.3390/S25020342

Austin, J. A., Lobo, E. H., Samadbeik, M., Engstrom, T., Philip, R., Pole, J. D., & Sullivan, C. M. (2024). Decades in the Making: The Evolution of Digital Health Research Infrastructure Through Synthetic Data, Common Data Models, and Federated Learning. *J Med Internet Res 2024;26:E58637 Https://Www.Jmir.Org/2024/1/E58637*, *26*(1), e58637. https://doi.org/10.2196/58637

CAIRIS. (2025). *Threat Modelling, Documentation and More*. https://cairis.org/cairis/tmdocsmore/

Daniel, E., & Tschorsch, F. (2022). IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks. *IEEE Communications Surveys and Tutorials*, *24*(1), 31–52. https://doi.org/10.1109/COMST.2022.3143147

Dhingra, S., Raut, R., Naik, K., & Muduli, K. (2024). Blockchain Technology Applications in Healthcare Supply Chains - A Review. *IEEE Access*, *12*, 11230–11257. https://doi.org/10.1109/ACCESS.2023.3348813

Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024). Health Security and Cybersecurity: Analysis of Interdependencies. *Health Economics and Management Review*, *5*(2), 84–103. https://doi.org/10.21272/HEM.2024.2-06

El-Saleh, A. A., Sheikh, A. M., Albreem, M. A. M., & Honnurvali, M. S. (2024). The Internet of Medical Things (IoMT): opportunities and challenges. *Wireless Networks*, *31*(1), 327–344. https://doi.org/10.1007/S11276-024-03764-8/FIGURES/14

European Parliament, & European Council. (2016). *Regulation - 2016/679 - EN - gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. *IEEE Communications Surveys and Tutorials*, *26*(3), 1748–1774. https://doi.org/10.1109/COMST.2024.3355222

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, *7*(3), 321–343. https://doi.org/10.1080/23270012.2020.1801529;WGROUP:STRING:PUBLICATION

Hammami, A. (2024). The Art of Threat Modeling. *Journal of Computer Sciences and Informatics*, *1*(1), 1. https://doi.org/10.5455/JCSI.20240710052550

Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., & Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *IT - Information Technology*, *60*(5–6), 283–291. https://doi.org/10.1515/itit-2018-0019

Limna, P. (2023). The Digital Transformation of Healthcare in The Digital Economy: A Systematic Review. *International Journal of Advanced Health Science and Technology*, *3*(2), 127–132. https://doi.org/10.35882/IJAHST.V3I2.244

LINDDUN. (2025). *linddun.org | Privacy Engineering*. https://linddun.org/

Microsoft. (2022). *Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Narayan, A., Weng, K., & Shah, N. (2024). Decentralizing Health Care: History and Opportunities of Web3. *JMIR Formative Research*, *8*(1), e52740. https://doi.org/10.2196/52740

Nweke, L. O., Abomhara, M., Yayilgan, S. Y., Comparin, D., Heurtier, O., & Bunney, C. (2022). A LINDDUN-Based Privacy Threat Modelling for National Identification Systems. *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*. https://doi.org/10.1109/NIGERCON54645.2022.9803177

OWASP. (2025a). *OWASP Smart Contract Top 10 | OWASP Foundation*. https://owasp.org/www-

project-smart-contract-top-10/

OWASP. (2025b). *OWASP Threat Dragon | OWASP Foundation*. https://owasp.org/www-project-threat-dragon/

Rahim, J., Ihsan, M., Rahim, I., Afroz, A., & Akinola, O. (2024). Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *6*(1), 438–462. https://doi.org/10.60087/JAIGS.V6I1.268

Shen, Y., Yu, J., Zhou, J., & Hu, G. (2025). Twenty-Five Years of Evolution and Hurdles in Electronic Health Records and Interoperability in Medical Research: Comprehensive Review. *J Med Internet Res 2025;27:E59024 Https://Www.Jmir.Org/2025/1/E59024*, *27*(1), e59024. https://doi.org/10.2196/59024

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers 2024, Vol. 13, Page 41*, *13*(2), 41. https://doi.org/10.3390/COMPUTERS13020041

Somma, A., De Benedictis, A., Esposito, C., & Mazzocca, N. (2024). The convergence of Digital Twins and Distributed Ledger Technologies: A systematic literature review and an architectural proposal. *Journal of Network and Computer Applications*, *225*, 103857. https://doi.org/10.1016/J.JNCA.2024.103857

Song, X., Xu, G., Huang, Y., & Dong, J. (2024). DID-HVC-based Web3 healthcare data security and privacy protection scheme. *Future Generation Computer Systems*, *158*, 267–276. https://doi.org/10.1016/J.FUTURE.2024.04.015

United States. (1996). *Health Insurance Portability and Accountability Act of 1996*. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

Van Landuyt, D., & Joosen, W. (2022). A descriptive study of assumptions in STRIDE security threat modeling. *Software and Systems Modeling*, *21*(6), 2311–2328. https://doi.org/10.1007/S10270-021-00941-7/FIGURES/10

Wolf, A., Simopoulos, D., D'Avino, L., & Schwaiger, P. (2020). The PASTA threat model implementation in the IoT development life cycle. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-307*, 1195–1204. https://doi.org/10.18420/INF2020_111

Xia, L., Cao, Z., & Zhao, Y. (2024). Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows. *Risk Management and Healthcare Policy*, *17*, 3291. https://doi.org/10.2147/RMHP.S450082