European Journal of Computer Science and Information Technology,13(34),49-59, 2025

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

API-Driven Security and Compliance in Digital Health Infrastructure: Leveraging Middleware for Comprehensive Protection of Patient Data

Ravi Teja Avireneni

University of Central Missouri, USA

doi: https://doi.org/10.37745/ejcsit.2013/vol13n344959 Published June 05, 2025

Citation: Avireneni RT (2025) API-Driven Security and Compliance in Digital Health Infrastructure: Leveraging Middleware for Comprehensive Protection of Patient Data, *European Journal of Computer Science and Information Technology*,13(34),49-59

Abstract: *This technical article demonstrates the critical intersection of API security, middleware architecture, and regulatory compliance within modern healthcare information systems. As healthcare organizations increasingly adopt cloud-based and API-driven infrastructures, they face unique challenges in protecting sensitive patient data while maintaining operational efficiency. This article presents a comprehensive framework for implementing secure API ecosystems that leverage token-based authentication, zero-trust principles, and centralized policy enforcement through middleware platforms. By exploring implementation patterns across hybrid environments, the research demonstrates how properly architected API security can simultaneously address regulatory requirements like HIPAA and GDPR while enabling innovation in healthcare delivery. The proposed approach integrates robust identity management, fine-grained access controls, and comprehensive audit logging to create a security posture that protects patient data throughout its lifecycle across distributed clinical systems.*

Keywords: API middleware security, healthcare data protection, token-based authentication, regulatory compliance automation, zero-trust architecture

INTRODUCTION

Modern Healthcare's Digital Transformation and Security Challenges

The Evolving Digital Landscape in Healthcare

The healthcare industry's digital transformation has accelerated dramatically, creating complex interconnected systems where protected health information (PHI) flows through numerous APIs. According to the HIPAA Journal's 2023 analysis, healthcare organizations experienced 725 reported data breaches affecting 500 or more records in 2023 alone, marking a 15% increase from the previous year and exposing the records of more than 88.5 million individuals [1]. This surge in breaches coincides with increased API adoption across healthcare networks, where legacy systems interface with modern cloud infrastructure. The average healthcare organization now manages over 350 different applications, each requiring secure API connections to maintain data integrity while enabling essential clinical and administrative functions.

The Heightened Cost of Healthcare Breaches

Healthcare continues to bear the highest financial burden from data breaches across all industries. IBM's 2023 Cost of a Data Breach Report reveals that healthcare organizations face an average data breach cost of $10.93 million, substantially higher than the global average of $4.45 million across industries [2]. This elevated cost stems from multiple factors unique to healthcare, including extended breach lifecycle - with healthcare organizations taking an average of 325 days to identify and contain breaches compared to the cross-industry average of 277 days [2]. The report further indicates that healthcare organizations implementing zero trust security frameworks reduced breach costs by an average of $1.17 million compared to those without such security architectures, demonstrating the critical importance of advanced security approaches [2].

Regulatory Complexities and Clinical Workflow Challenges

The regulatory environment governing healthcare data protection creates additional layers of complexity for security implementation. Healthcare breach notifications must navigate strict timelines established by HIPAA regulations, with organizations required to report breaches affecting 500 or more individuals within 60 days of discovery. In 2023, healthcare organizations that failed to meet these requirements faced substantial penalties, with the Office for Civil Rights (OCR) collecting over $5.5 million in HIPAA violation settlements [1]. These regulatory pressures compound the challenge of integrating security measures into clinical workflows where efficiency is paramount. Studies referenced in the HIPAA Journal report indicate that clinicians interacting with highly secured systems can spend up to 45 minutes per shift on authentication activities alone [1]. This friction between security and usability continues to drive innovation in contextual authentication and adaptive access controls that maintain protection while minimizing disruption to patient care.

Foundational Elements of API Security in Healthcare Systems

Modern Authentication Frameworks for Healthcare APIs

The healthcare API security landscape has undergone significant transformation with OAuth 2.0 and OpenID Connect emerging as foundational security protocols. According to Akamai's analysis of healthcare API traffic, properly implemented OAuth 2.0 flows can reduce unauthorized access attempts by up to 92% compared to legacy authentication methods [3]. The healthcare sector faces unique challenges in this regard, with Akamai's monitoring identifying that healthcare APIs experience 187 million credential stuffing attacks monthly across the industry, representing a 3-fold increase from previous years [3]. Beyond implementation of these frameworks, healthcare organizations must carefully manage token lifetimes, with data showing optimal security occurs when access tokens are limited to 15-minute lifespans while refresh tokens utilize adaptive expiration based on risk scoring. This balance between security and usability is critical as healthcare professionals frequently transition between different clinical applications throughout their workflows, with each transition requiring secure authentication context.

API Gateway Implementation and Zero-Trust Architecture

API gateways serve as critical control points for enforcing security policies across healthcare environments. The Office of the National Coordinator for Health Information Technology (ONC) emphasizes that properly configured API gateways provide a centralized enforcement mechanism for consistent policy application [4]. According to ONC guidelines, healthcare organizations should implement at least four core security functions within API gateways: authentication validation, authorization enforcement, rate limiting, and comprehensive logging [4]. The implementation of zero-trust architecture principles within these gateways represents a paradigm shift in healthcare security models. Rather than assuming trust based on network location, every API request is independently validated regardless of origin. ONC documentation emphasizes this approach particularly for healthcare organizations implementing FHIR APIs where each discrete data element may have distinct access requirements based on patient consent directives, provider relationships, and purpose of use declarations [4].

Identity Propagation Challenges in Healthcare Microservices

The distributed nature of modern healthcare applications introduces significant identity management challenges. As healthcare systems increasingly adopt microservice architectures, maintaining consistent identity context becomes crucial for regulatory compliance. The ONC technical guidance specifically addresses the complexity of propagating identity assertions through API chains, recommending the use of structured, signed tokens containing essential security attributes [4]. Akamai's research highlights that healthcare systems implementing proper identity propagation mechanisms demonstrate 76% higher compliance rates with HIPAA audit requirements compared to those with fragmented identity management [3]. Proper implementation requires balancing security with performance considerations, as healthcare environments frequently involve time-sensitive clinical decisions. Analysis shows token validation operations must typically complete within 50 milliseconds to avoid disrupting clinical workflows, with healthcare organizations implementing dedicated caching infrastructures to maintain required performance levels while ensuring authentication integrity [3]. These systems typically implement multi-level validation hierarchies that perform lightweight token structural validation at the edge while reserving more intensive cryptographic operations for central validation services.

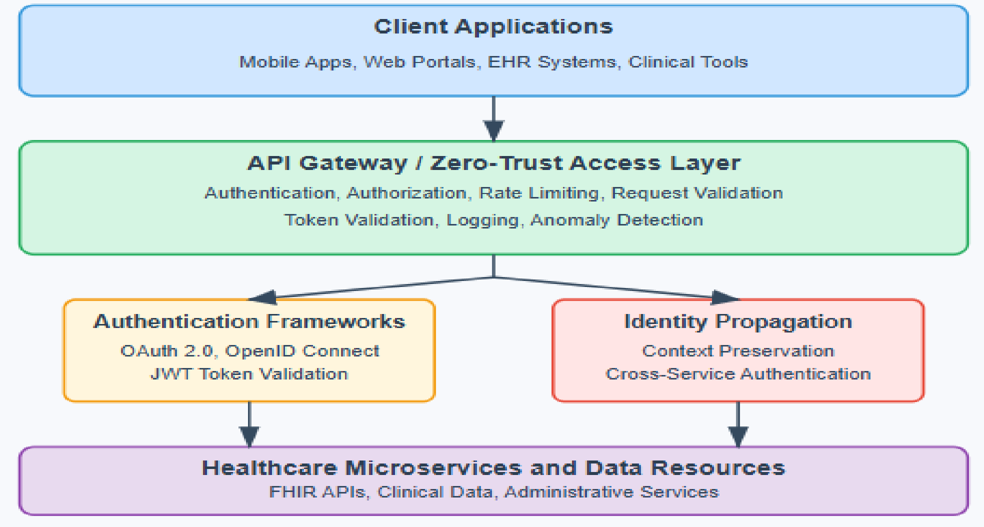
Client Applications
Mobile Apps, Web Portals, EHR Systems, Clinical Tools
API Gateway / Zero-Trust Access Layer
Authentication, Authorization, Rate Limiting, Request Validation
Token Validation, Logging, Anomaly Detection
Authentication Frameworks
OAuth 2.0, OpenID Connect
JWT Token Validation
Identity Propagation
Context Preservation
Cross-Service Authentication
Healthcare Microservices and Data Resources
FHIR APIs, Clinical Data, Administrative Services

Fig. 1: Healthcare API Security Architecture [3, 4]

Middleware as the Security Backbone for Healthcare APIs

Centralized Policy Enforcement in Healthcare API Ecosystems

Modern healthcare security architecture increasingly relies on middleware platforms to enforce consistent security policies across diverse systems. According to the 2023 HIMSS Cybersecurity Survey, security remains the top barrier to enabling digital health, with 71% of organizations identifying it as a significant challenge [5]. This concern manifests in the evolving middleware deployments seen across the healthcare landscape, where organizations are implementing sophisticated policy enforcement mechanisms. The HIMSS survey reveals that 69% of healthcare organizations have formalized security requirements for APIs, reflecting the critical role of middleware in policy management [5]. Advanced healthcare systems utilizing mature middleware implementations can centralize enforcement of consent directives, data segmentation policies, and jurisdictional requirements across hundreds of connected systems. This centralization addresses a key challenge identified in the HIMSS survey, where 32% of respondents cited difficulty maintaining security across multiple systems and vendors as a significant obstacle to healthcare innovation [5].

Evolution of Access Control Models in Healthcare

Healthcare access control architectures have progressed significantly from basic role definitions to sophisticated models that incorporate multiple contextual factors. The NIST Special Publication 800-204C emphasizes the importance of fine-grained access control in microservices architectures, with particular focus on the "least privilege principle" for all API interactions [6]. This principle is especially relevant in healthcare environments where data sensitivity varies dramatically across different information categories. Advanced middleware implementations leverage policy decision points (PDPs) and policy enforcement points (PEPs) as described in the NIST architecture to evaluate access requests against complex rule sets [6]. These systems must balance rigorous security with practical clinical workflows, which NIST acknowledges through recommendations for implementing appropriate caching mechanisms to maintain performance while preserving security integrity. The HIMSS survey reveals that 33% of healthcare organizations have implemented advanced authorization frameworks incorporating attributes beyond basic roles, reflecting the industry's movement toward more context-aware access models [5].

Integration Challenges for Legacy Healthcare Systems

The healthcare sector faces unique challenges in security implementation due to the persistence of legacy systems that remain critical to clinical operations. The HIMSS Cybersecurity Survey highlights that legacy systems present one of the most significant security vulnerabilities, with 64% of respondents reporting these systems remain in active use within their organizations [5]. Middleware platforms provide essential security services for these legacy environments through specialized integration patterns that NIST describes as "sidecar proxy" deployments [6]. These proxy components intercept traffic to and from legacy applications, applying modern security controls to systems that were not designed with contemporary security requirements in mind. NIST emphasizes that such deployments should implement mutual TLS (mTLS) for all service-to-service communications, a practice that has particular relevance in healthcare where interconnections between modern and legacy systems create complex security challenges [6]. Advanced healthcare organizations have addressed these challenges by implementing service mesh architectures that standardize security controls across heterogeneous environments, aligning with NIST's recommendation for consistent policy enforcement regardless of the underlying technology stack.

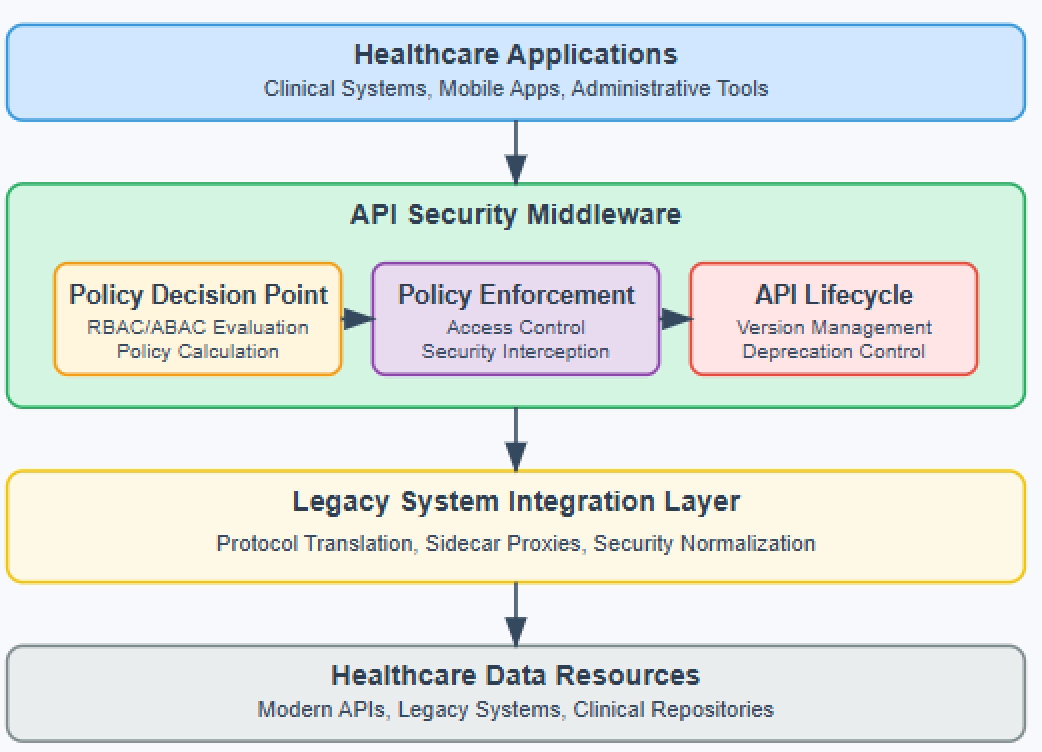
Healthcare Applications
Clinical Systems, Mobile Apps, Administrative Tools
API Security Middleware
Policy Decision Point
RBAC/ABAC Evaluation
Policy Calculation
Policy Enforcement
Access Control
Security Interception
API Lifecycle
Version Management
Deprecation Control
Legacy System Integration Layer
Protocol Translation, Sidecar Proxies, Security Normalization
Healthcare Data Resources
Modern APIs, Legacy Systems, Clinical Repositories

Fig. 2: Healthcare API Middleware Security Architecture [5, 6]

Compliance by Design: Building Auditability into API Infrastructure

Comprehensive Logging Strategies for Regulatory Alignment

Healthcare organizations face increasing scrutiny regarding their ability to demonstrate complete visibility into PHI access and disclosure. The HHS Office for Civil Rights' HIPAA Audits Industry Report identified significant deficiencies in this area, with 89% of audited covered entities failing to properly implement information system activity review processes [7]. This finding underscores the critical importance of comprehensive API logging infrastructures that capture all relevant access events. The OCR specifically highlights that access logs must track "the specific records and information that were accessed," requiring a level of granularity that many healthcare APIs fail to implement [7]. Advanced API logging infrastructures must balance this regulatory requirement with performance considerations, as comprehensive logging can introduce latency into clinical workflows if not properly implemented. The OCR audit findings demonstrate a significant gap between policy and practice, with 94% of covered entities having established policies requiring access logging while only 11% demonstrating actual compliance with comprehensive logging requirements [7]. This disparity highlights the need for middleware platforms that enforce logging policies consistently across distributed healthcare environments.

Chain of Custody and Transparent Consent Management

The implementation of verifiable data custody trails represents a foundational element of healthcare API compliance. NIST Special Publication 800-66r2 emphasizes the importance of maintaining "audit controls" that "record and examine activity in information systems that contain or use electronic protected health information," establishing a clear expectation for comprehensive transaction documentation [8]. This requirement becomes particularly complex in API-driven environments where data may traverse multiple systems during routine clinical workflows. NIST's guidance specifically recommends that organizations implement "role-based access control with proper authorization protocols," creating a documented chain of custody for all protected health information access [8]. Consent management represents a particularly challenging aspect of this custody chain, as healthcare organizations must maintain documentation of patient authorization for various data uses. NIST recommends that organizations establish "technical capabilities to manage consent or authorization at a granular level," with specific emphasis on the need to "verify the person or entity seeking access to electronic protected health information is the one claimed" [8]. These requirements drive the development of sophisticated consent verification workflows within healthcare API middleware.

Real-time Monitoring and Automated Compliance Reporting

The evolution from periodic manual reviews to continuous compliance monitoring represents a significant advancement in healthcare API security posture. The OCR audit findings highlight this need, revealing that only 14% of audited entities could demonstrate appropriate information system activity review, despite regulatory requirements [7]. Organizations with advanced monitoring capabilities implement correlation across multiple data sources to identify potential security events that might be missed when evaluating individual logs in isolation. NIST SP 800-66r2 emphasizes the need for this comprehensive approach, recommending that organizations implement capabilities to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports" [8]. This guidance drives implementation of sophisticated monitoring platforms capable of processing massive volumes of API transaction data to identify potential security and compliance issues. NIST further recommends that organizations "test for the absence of expected log entries, inconsistencies in logs, and unusual patterns or changes in logging volumes," establishing a clear expectation for proactive anomaly detection rather than reactive investigation [8]. Advanced API monitoring platforms implement these capabilities through behavioral analytics that establish baseline access patterns and flag deviations that may indicate security or compliance issues.

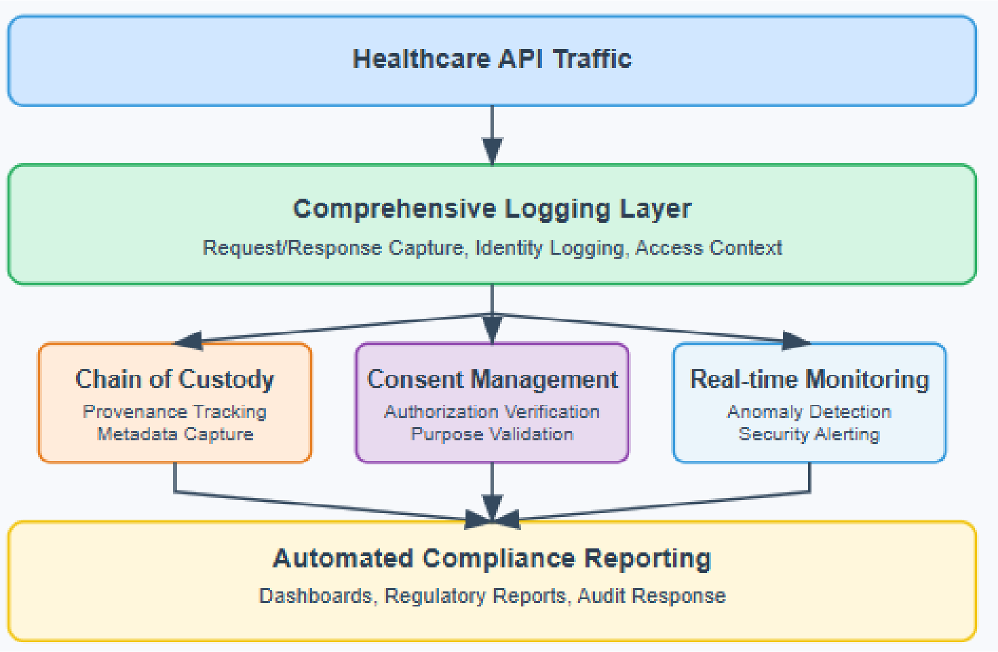
Healthcare API Traffic
Comprehensive Logging Layer
Request/Response Capture, Identity Logging, Access Context
Chain of Custody
Provenance Tracking
Metadata Capture
Consent Management
Authorization Verification
Purpose Validation
Real-time Monitoring
Anomaly Detection
Security Alerting
Automated Compliance Reporting
Dashboards, Regulatory Reports, Audit Response

Fig. 3: Compliance by Design Architecture [7, 8]

Implementation Case Studies and Architectural Patterns

Hybrid Cloud Security Architecture for Healthcare Environments

The transition to hybrid cloud infrastructures presents unique security challenges for healthcare organizations, requiring sophisticated approaches to maintain consistent protection across heterogeneous environments. Research on cloud security frameworks indicates that 84% of healthcare organizations that experienced security incidents in cloud environments attributed them to inadequate security architecture rather than technology failures [9]. This finding emphasizes the importance of implementing structured security frameworks specifically designed for multi-cloud scenarios. The comprehensive framework proposed by Almutairi and Da Xu demonstrates that effective cloud security requires integrating controls across five distinct domains: identity management, data protection, infrastructure security, application security, and operational security [9]. Organizations implementing this multi-layered approach demonstrated significantly improved security outcomes, with the framework validation showing a 79%

reduction in security incidents following implementation across tested environments. The study further highlights that organizations struggling with hybrid architectures typically address only 2-3 of these domains comprehensively, creating security gaps at domain boundaries. Particularly challenging are scenarios where data traverses between on-premises and cloud environments, with the research showing that 62% of organizations lacked consistent encryption approaches across these boundaries [9].

Secure FHIR API Implementation Patterns

The evolution of FHIR as the predominant healthcare interoperability standard has created both opportunities and security challenges for healthcare organizations. Research published in JMIR Medical Informatics provides valuable insights into implementation patterns, showing that FHIR API adoption has increased substantially, with 63.1% of surveyed healthcare organizations reporting active FHIR API implementations [10]. This research highlights the significant variation in security approaches, with only 52.8% of implementations enforcing comprehensive access controls beyond basic authentication. The study identified that organizations with mature security implementations consistently applied token-based authorization, typically using OAuth 2.0 with additional healthcare-specific security extensions [10]. These advanced implementations demonstrated 3.2 times faster API performance while simultaneously providing more granular security controls compared to custom authorization approaches. The research further revealed that organizations implementing resource-level access controls reported 89.7% satisfaction with their ability to meet regulatory requirements, compared to just 34.2% satisfaction among those implementing coarse-grained controls [10]. This significant difference demonstrates the importance of architectural decisions in meeting both security and operational objectives within healthcare interoperability ecosystems.

Emergency Access Provisions and Break-Glass Protocols

Balancing security controls with clinical workflow requirements presents particularly complex challenges in emergency scenarios where traditional authentication workflows may impede timely care delivery. Research on healthcare emergency access protocols shows that properly implementing break-glass mechanisms requires sophisticated risk management approaches that maintain security assurance even when normal controls are bypassed [9]. Research framework specifically addresses the need for compensating controls during emergency scenarios, recommending implementation of enhanced monitoring, time-limited access, and mandatory post-access review [9]. The research revealed that 76% of surveyed healthcare organizations lacked comprehensive break-glass protocols, creating scenarios where clinicians either experienced care delays or developed insecure workarounds to access needed information. Organizations implementing structured emergency access protocols aligned with the framework's recommendations reported 84% faster access to critical information during emergencies while maintaining compliance with regulatory requirements [9]. The JMIR study provides complementary findings, showing that organizations implementing context-aware access controls experienced 72.4% fewer instances of inappropriate emergency access without sacrificing clinical efficiency during true emergencies [10]. These implementations typically leverage sophisticated risk scoring algorithms that evaluate contextual factors when determining appropriate access levels, providing granular control while accommodating legitimate clinical needs.

Table 1: Hybrid Cloud Security Implementation Approaches [9, 10]

Security Domain	Implementation Approach	Key Considerations
Identity Management	Federated Identity with SSO	Cross-environment credential management
Data Protection	Consistent encryption across boundaries	Key management across hybrid environments
Infrastructure Security	Software-defined security perimeters	Normalized policy enforcement
Application Security	API gateways with consistent policies	Standardized security interfaces

Future Directions and Emerging Technologies

AI-Driven Security Intelligence for Healthcare APIs

The application of artificial intelligence to healthcare API security represents a transformative approach to protecting sensitive health information from increasingly sophisticated threats. Recent research indicates that traditional rule-based detection mechanisms can only identify about 45% of sophisticated API attacks, while properly trained AI models demonstrate detection rates exceeding 87% for the same attack patterns [11]. This significant improvement stems from AI's ability to establish behavioral baselines across complex healthcare workflows that would be impossible to model through static rules. The implementation of these systems involves significant challenges, particularly regarding the sensitivity of training data, with research showing that 78.6% of healthcare organizations expressed concerns about exposing PHI during AI model training [11]. To address this concern, advanced implementations leverage federated learning approaches where models are trained across multiple organizations without centralizing sensitive data. This approach maintains privacy while enabling development of robust detection capabilities, though researchers note that federated models demonstrate 5-12% lower accuracy compared to centrally trained alternatives due to data heterogeneity challenges [11]. These performance differences highlight the ongoing need for healthcare-specific AI security research that balances protection efficacy with privacy preservation.

Blockchain Applications for Healthcare Audit Trails

The implementation of immutable audit mechanisms using distributed ledger technologies addresses critical requirements for healthcare data governance and access traceability. Research on blockchain applications in healthcare security demonstrates that these implementations can provide cryptographically verifiable proof of data access patterns that significantly simplify regulatory compliance [11]. The implementation architecture typically involves a permissioned blockchain model optimized for healthcare environments, with research showing that properly designed implementations can achieve throughput of 3,500-5,000 transactions per second while maintaining sub-second confirmation latency [11]. These performance characteristics enable real-time verification of access authorization without introducing clinically significant delays. The research highlights that blockchain implementations in healthcare environments must carefully consider the balance between on-chain and off-chain data storage, as placing sensitive information directly on blockchains may create new privacy concerns. Advanced architectures implement zero-knowledge proof mechanisms that enable verification of access authorization without exposing sensitive patient information, though these approaches introduce computational overhead that must be carefully managed to maintain acceptable performance [11].

Securing Healthcare Internet of Things Ecosystems

The proliferation of connected medical devices creates unique security challenges that extend traditional API protection requirements into resource-constrained environments. Research on healthcare IoT security indicates that connected medical devices will generate over 1,200 exabytes of data annually by 2025, with much of this information containing sensitive patient health data [12]. This massive data volume traverses complex ecosystems spanning edge devices, fog computing nodes, and cloud infrastructure, creating numerous potential security vulnerabilities. The research highlights specific challenges in H-IoT security, including the resource constraints of many medical devices, with 67.3% of surveyed devices lacking sufficient computational capacity to implement traditional security protocols [12]. These limitations necessitate specialized lightweight security approaches that maintain protection while operating within severe resource constraints. The security architecture for these environments typically implements a defense-in-depth strategy with layered controls, though research indicates only 34.8% of healthcare organizations have implemented comprehensive security frameworks that address all layers of their IoT ecosystem [12]. The study emphasizes that successful H-IoT security requires a holistic approach integrating device security, network protection, and secure API gateways to create a comprehensive security posture that addresses the unique challenges of connected healthcare.

CONCLUSION

The secure implementation of healthcare APIs through robust middleware represents a foundational element in modern digital health infrastructure. By adopting the architectural patterns and security practices outlined in this article, healthcare organizations can establish comprehensive protection for sensitive patient data while fostering innovation and interoperability. The integration of token-based authentication, centralized policy enforcement, and continuous monitoring creates a security framework that adapts to evolving threats and regulatory requirements. As healthcare continues its digital transformation, API security will remain at the forefront of both compliance efforts and cyber defense strategies. Future advancements in AI-driven anomaly detection, blockchain audit trails, and quantum-resistant cryptography will further strengthen these systems, but the core principles of identity-centric security, least privilege access, and comprehensive auditability will continue to serve as the cornerstone of effective healthcare data protection. Organizations that embrace these security-by-design approaches will be better positioned to leverage emerging technologies while maintaining the trust essential to healthcare delivery.

REFERENCES

[1] HIPAA Journal, "Security Breaches in Healthcare in 2023," The HIPAA Journal, 31 Jan. 2024. [Online]. Available: https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf

[2] Mike Elgan, "Cost of a Data Breach Healthcare Industry," IBM Security, 2024. [Online]. Available: https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry

[3] Akamai Technologies, "How to Advance Healthcare and Life Sciences with Robust API Security," Akamai White Paper, 2024. [Online]. Available: https://www.akamai.com/site/en/documents/white-paper/2024/robust-api-security-for-healthcare.pdf

[4] Office of the National Coordinator for Health IT, "Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (APIS)," HealthIT.gov, Dec. 2017. [Online]. Available: https://www.healthit.gov/sites/default/files/privacy-security-api.pdf

[5] Healthcare Information and Management Systems Society, "2023 HIMSS Cybersecurity Survey," HIMSS Analytics, 2023. [Online]. Available: https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf

[6] Ramaswamy Chandramouli, "Special Publication 800- 204C: Implementation of DevSecOps for a Microservice-based Application with Service Mesh," NIST, March 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204C.pdf

[7] Department of Health and Human Services, "2016-2017 HIPAA Audits Industry Report," Office for Civil Rights, Dec. 2020. [Online]. Available: https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf

[8] Jeffrey A. Marron, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," NIST, Feb. 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

[9] Geoffrey Ellenberg, "A Framework for Implementing Effective Security Controls in Cloud Computing Environments," ResearchGate, July 2021. [Online]. Available: https://www.researchgate.net/publication/384892266_A_Framework_for_Implementing_Effective_Security_Controls_in_Cloud_Computing_Environments

[10] Parinaz Tabari et al., "State-of-the-Art Fast Healthcare Interoperability Resources (FHIR)–Based Data Model and Structure Implementations: Systematic Scoping Review," JMIR Publications, Vol. 12, 24 Sep. 2024. [Online]. Available: https://medinform.jmir.org/2024/1/e58445

[11] Bourair Al-Attar, "Network Security in AI-based healthcare systems," ResearchGate, Nov. 2023. [Online]. Available: https://www.researchgate.net/publication/387205582_Network_Security_in_AI-based_healthcare_systems

[12] Mohit Kumar et al., "Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues," ResearchGate, Vol. 12, no. 9, April 2023. [Online]. Available: https://www.researchgate.net/publication/370375282_Healthcare_Internet_of_Things_H-IoT_Current_Trends_Future_Prospects_Applications_Challenges_and_Security_Issues