European Journal of Computer Science and Information Technology,13(20),56-68, 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

Enhancing Cybersecurity for Society through Automated Cloud Defenses – Implementation and Application in Healthcare

Srinivas Pagadala Sekar
Anna University, India

doi: https://doi.org/10.37745/ejcsit.2013/vol13n205668 Published May 17, 2025

Citation: Sekar S.P. (2025) Enhancing Cybersecurity for Society through Automated Cloud Defenses – Implementation and Application in Healthcare, *European Journal of Computer Science and Information Technology*,13(20),56-68

Abstract: *Automated cloud defenses offer a transformative solution to cybersecurity challenges in today's healthcare landscape, where sensitive patient data protection is critical. This article examines key strategies for implementing automated security in cloud environments, presenting a structured implementation framework adapted for healthcare contexts. It explores specific applications including patient data protection, HIPAA compliance enforcement, advanced threat detection, and service availability maintenance. Through detailed case studies of both large hospital networks and regional healthcare providers, the article demonstrates how organizations successfully implement zero-trust architectures and secure legacy systems during cloud transitions, achieving measurable improvements in security posture and operational efficiency. While automated cloud defenses deliver substantial benefits—enhanced security, cost efficiency, scalability, improved compliance, operational resilience, and accelerated innovation—healthcare organizations must navigate challenges including legacy system integration, complex vendor ecosystems, skills gaps, budget constraints, and potential clinical workflow disruption. The article provides practical approaches to overcoming these obstacles while maximizing security effectiveness in protecting sensitive healthcare information.*

Keywords: Cloud security automation, healthcare cybersecurity, HIPAA compliance, threat mitigation, patient data protection

INTRODUCTION

In today's rapidly evolving digital landscape, organizations across all sectors are increasingly migrating their critical infrastructure, applications, and data to cloud environments. According to Gartner's research, worldwide end-user spending on public cloud services is forecast to grow 20.7% to total $591.8 billion in 2023, up from $490.3 billion in 2022, with Infrastructure-as-a-Service (IaaS) projected as the highest-

growth segment at 29.8% [1]. This transition, while offering unprecedented scalability,cost-efficiency, and flexibility, also introduces significant cybersecurity challenges. As cloud adoption accelerates, the attack surface expands, making traditional manual security approaches insufficient to address the complex threat landscape.

The healthcare sector faces particularly acute challenges, with electronic health records (EHRs) becoming increasingly vulnerable to cyberattacks. A comprehensive analysis of healthcare cybersecurity reveals that 94% of healthcare organizations have experienced at least one cybersecurity incident, with compromised cloud servers accounting for a significant portion of these breaches [2]. The integration of Internet of Medical Things (IoMT) devices further complicates security postures, with an average hospital now managing thousands of connected devices across hybrid environments.

This article examines how automated cloud defenses provide a proactive, efficient solution to protect sensitive information, ensure compliance, and maintain operational integrity in the face of evolving cyber threats. By developing an actionable framework for implementing these automated defenses, we can address the pressing security needs of various industries, with particular focus on healthcare—a sector where secure handling of sensitive patient data is not just good practice, but a regulatory mandate with life-critical implications.

The Evolving Landscape of Cloud Security Threats

The migration to cloud environments has fundamentally altered the cybersecurity paradigm. Unlike traditional on-premises infrastructure, cloud environments feature distributed architectures, shared responsibility models, and dynamic resource allocation. According to IBM's Cost of a Data Breach Report, organizations experiencing breaches in public cloud environments face an average cost of $4.99 million per incident, with breaches taking approximately 237 days to identify and an additional 84 days to contain [3]. This lengthy detection and response window illustrates the complexity inherent in securing modern cloud infrastructures.

The distributed nature of cloud computing creates an expanded attack surface where multi-tenant environments and API-driven architectures multiply potential entry points for attackers. This expansion is compounded by identity and access management challenges, as organizations struggle to implement appropriate permission controls across distributed resources. The research report indicates that compromised credentials were responsible for 19% of breaches, making them the most common initial attack vector in cloud environments [3].

Data sovereignty concerns present another significant challenge as organizations must navigate varying jurisdictional requirements for data storage and processing. The cross-border nature of cloud computing often means that data traverses multiple regulatory domains, each with distinct compliance requirements that must be simultaneously satisfied. Supply chain vulnerabilities further complicate cloud security, as

dependencies on third-party services introduce additional risk vectors that may be outside an organization's direct control.

The shared responsibility model fundamentally redefines security obligations in cloud environments. As noted by cloud security experts, this model clearly delineates which security tasks belong to the cloud service provider versus the customer, but the boundaries are often misunderstood [4]. While providers secure the underlying infrastructure, customers remain responsible for protecting their data, managing access controls, and ensuring application security. This division of responsibilities creates potential security gaps, with 82% of cloud breaches occurring due to misconfigured security controls, inadequate change control procedures, or unsecured access points that fall within the customer's security domain [4].

Zero-day exploits represent another critical threat vector, with previously unknown vulnerabilities that can be rapidly weaponized against cloud infrastructure. The dynamic nature of cloud environments often means that traditional security approaches cannot detect or mitigate these emerging threats quickly enough.These challenges are further complicated by the severe shortage of cybersecurity professionals, with an estimated global gap of over 3.5 million unfilled positions. This skills shortage makes automated defenses not just advantageous but necessary for maintaining adequate security postures, as human security teams cannot scale to meet the complexity and volume of threats targeting modern cloud environments.

Table 1: Key Metrics in Cloud Cybersecurity Landscape 2023 [3, 4]

Metric	Value
Average cost of public cloud breach	$4.99 million
Average breach identification time	237 days
Average breach containment time	84 days
Total breach lifecycle	321 days
Percentage of breaches caused by compromised credentials	19%
Percentage of cloud breaches due to misconfigured security controls	82%
Estimated global cybersecurity professional shortage	3.5 million

European Journal of Computer Science and Information Technology,13(20),56-68, 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

Key Strategies for Automated Cloud Defenses

Vital Role of Automation

Automated cloud defenses serve as the foundation for proactive and efficient cybersecurity in modern environments. According to the Ponemon Sullivan Report, organizations implementing preventive security automation experience an average cost savings of 61% compared to detection-only approaches, with prevention measures costing approximately $22 per endpoint versus $103 for detection and response [5]. This economic advantage stems from automation's ability to deploy continuous monitoring systems that detect anomalies in real-time, implement security controls consistently across distributed resources, and respond to incidents with predetermined playbooks. Organizations leveraging automated security solutions can effectively scale operations without proportionally increasing security staff—a critical advantage when considering the cybersecurity workforce gap. Additionally, automated systems maintain accurate inventories of cloud assets and their security states, supporting comprehensive risk management in complex environments. These capabilities have become essential for protecting societies increasingly reliant on cloud services, from financial systems to healthcare delivery platforms.

Deployment Automation Benefits

The automation of security deployment processes offers significant advantages in maintaining robust cloud defenses. Research indicates that following the four-step process toward cloud security automation—analyzing current security operations, identifying automation opportunities, implementing security-as-code, and continually refining the approach—can reduce security incident response times by up to 80% [6]. Infrastructure-as-Code (IaC) approaches ensure configuration consistency, with security templates that can be version-controlled and tested before deployment. Automated scanning and remediation minimize the exposure window for known vulnerabilities, while replacing manual processes with automated workflows significantly reduces configuration mistakes—one of the leading causes of security breaches. Organizations implementing automated patch management deploy critical security updates up to 30 times faster than manual processes, with automation enabling rapid deployment at scale with minimal delay [6]. Furthermore, automated processes create comprehensive audit trails that strengthen compliance verification and simplify forensic analysis. By streamlining implementation and management of cloud defenses, organizations maintain a stronger security posture while optimizing resource utilization.

Modernizing Applications

Legacy applications present significant security challenges when migrated to cloud environments. The Ponemon Sullivan Report indicates that security modernization efforts focused on prevention yield a 47% higher return on investment compared to approaches that primarily emphasize detection and response [5]. Modernization strategies like containerization encapsulate applications to enhance security isolation, while microservices architecture breaks monolithic applications into secure, independently deployable components. Organizations implementing API security gateways establish centralized control and monitoring of application interfaces, significantly reducing unauthorized access attempts. Runtime

application self-protection (RASP) embeds security monitoring directly within applications, enabling immediate threat response without human intervention. DevSecOps integration incorporates security throughout the development lifecycle, with automated testing reducing the cost to fix vulnerabilities by up to 72% when identified during development rather than in production [5]. These approaches are critical to secure legacy systems and strengthen defenses within cloud environments, particularly for sectors with substantial technical debt like healthcare.

Addressing Integration Challenges

Organizations implementing automated cloud defenses frequently encounter integration complexities across their environments. TechTarget research indicates that successful cloud security automation requires addressing four key challenges: managing heterogeneous cloud platforms, controlling tool proliferation, standardizing security data, and harmonizing authentication across environments [6]. Enterprise environments typically involve multiple cloud providers alongside on-premises systems, creating significant integration hurdles. Many organizations struggle with tool proliferation, with security teams managing an average of 25-49 different security tools, each generating its own alerts and using proprietary formats. Standardizing security telemetry across these diverse sources remains a major challenge, with many security teams spending over 50% of their time normalizing data before analysis can begin [6]. Authentication harmonization and policy synchronization across environments present ongoing difficulties, with inconsistencies creating security gaps. Practical solutions include implementing security orchestration platforms that centralize management, adopting open standards for interoperability, developing comprehensive API strategies, and creating unified security data repositories—all essential components for ensuring a secure and manageable digital future.

Table 2: Automated Cloud Defense Metrics and ROI Analysis [5, 6]

Metric	Value
Cost savings with preventive security automation	61%
Cost per endpoint for prevention measures	$22
Cost per endpoint for detection and response	$103
Security incident response time reduction with automation	80%
ROI improvement with prevention-focused security modernization	47%
Vulnerability fix cost reduction with automated testing	72%
Security patch deployment speed improvement with automation	30x
Average number of security tools managed by organizations	25-49
Percentage of time security teams spend normalizing data	>50%

Technical Implementation Framework

A comprehensive automated cloud defense implementation requires a structured approach that systematically addresses the evolving security requirements of modern cloud environments. According to Gartner's Innovation Insight for Cloud-Native Application Protection Platforms, organizations implementing integrated security approaches experience significantly fewer successful attacks compared to those using disparate point solutions [7]. This structured framework consists of five essential phases that guide implementation.

The assessment and planning phase begins with comprehensive inventory of cloud assets and data classification, establishing the foundation for effective security controls. Threat modeling specific to cloud architecture identifies unique vulnerabilities in distributed environments, while regulatory compliance mapping ensures adherence to relevant standards like HIPAA for healthcare organizations. Security gap identification completes this phase by prioritizing vulnerabilities based on risk assessment methodologies.

Architecture design focuses on implementing zero-trust principles, which according to Scott Rose et al., treats all users as potential threats and prevents access to data and resources until the user is authenticated and authorized [8]. This approach significantly reduces the attack surface by removing implicit trust from network architecture. Defense-in-depth strategies layer security controls to protect sensitive data, while secure CI/CD pipelines and API security frameworks ensure that security is embedded throughout the development lifecycle.

Technology selection involves evaluating cloud-native security platforms that provide integrated protection across infrastructure, workloads, and containers. As Gartner notes, Cloud-Native Application Protection Platforms (CNAPPs) that combine multiple capabilities perform better than siloed tools by providing unified visibility [7]. SIEM/SOAR solutions enable automated incident detection and response, while container security and identity management tools address specific protection requirements.The implementation phase executes security controls in a structured sequence, beginning with core infrastructure hardening based on industry benchmarks. Continuous monitoring deployment provides real-time security visibility, while automated response mechanisms, as emphasized in research zero-trust architecture, ensure immediate action against detected threats [8]. Security policy-as-code implementation ensures consistent application of controls across dynamic cloud environments.

Validation and optimization establish ongoing security assurance through penetration testing and red team exercises that simulate real-world attacks. Security metrics development enables quantitative evaluation of defense effectiveness, while performance impact assessment ensures security controls don't compromise operational efficiency. Continuous improvement processes complete the framework by establishing mechanisms for ongoing adaptation to evolving threats.This systematic approach provides organizations with a comprehensive methodology for implementing automated cloud defenses that can be adapted to various industry contexts and security maturity levels.

Industry Application: Healthcare

The healthcare industry serves as a compelling example of where automated cloud defenses can have a transformative impact. With the shift toward cloud-based electronic health records (EHRs), telehealth platforms, and data analytics, healthcare providers manage vast amounts of personal health information (PHI) that require stringent protection. According to research healthcare cybersecurity benchmarks, 83% of healthcare institutions experienced at least one cyberattack in the past year, with 30% reporting patient safety impacts resulting from these incidents [9].

Protecting Patient Data

Patient data protection represents the foremost priority for healthcare cybersecurity. Automated encryption ensures PHI is secured at rest and in transit, significantly reducing breach risks. Contextual access controls restrict data visibility to authorized personnel only, with automation revoking permissions instantly upon role changes or detected threats. Research reports that healthcare organizations implementing contextual

access controls experience 43% fewer unauthorized access incidents compared to those using static permission models [9]. Data loss prevention systems automatically identify and protect sensitive information from exfiltration, while tokenization replaces sensitive identifiers with non-sensitive equivalents in non-production environments. Blockchain-based audit trails create immutable records of data access and modifications, enhancing forensic capabilities during breach investigations. These automated mechanisms provide multi-layered protection for patient information throughout the healthcare data lifecycle.

Ensuring Compliance with HIPAA

Regulatory compliance remains a critical concern for healthcare organizations. According to research published in the ACM Digital Library, healthcare institutions implementing automated compliance solutions reduce their risk of HIPAA violations by 67% while decreasing compliance management costs by 41% [10]. Automated policy enforcement verifies adherence to HIPAA requirements through continuous compliance checks that monitor configurations against regulatory frameworks in real-time. Automated documentation generates necessary artifacts for audits, while regular automated audits produce comprehensive reports for regulatory bodies. The study demonstrated that compliance drift detection, which identifies and remediates deviations from approved configurations, reduces the mean time to resolve compliance issues from 24 days to just 3 days—an 87.5% improvement [10]. These capabilities significantly reduce the compliance burden while improving overall security posture.

Detecting and Mitigating Threats

The unique threat landscape facing healthcare organizations requires sophisticated detection and response capabilities. Research benchmarks reveal that healthcare organizations experience an average of 109 days of EHR downtime per year due to cybersecurity incidents, with potential annual revenue losses exceeding $30 million for larger providers [9]. AI-driven monitoring identifies unusual access patterns or ransomware indicators, triggering immediate alerts. Behavioral analytics establish baselines for normal activities, while automated incident responses prevent attack proliferation. Research shows that healthcare organizations implementing automated threat response reduce mean time to contain (MTTC) by 72% compared to manual approaches [10]. Threat intelligence integration and deception technology further enhance detection capabilities. These automated tools enable healthcare organizations to identify and contain threats before they impact patient care.

Maintaining Service Availability

Continuous operation of healthcare systems is critical for patient safety. According to research, 67% of healthcare providers have experienced patient care impacts due to cyberattacks, with 15% reporting direct patient safety incidents [9]. Automated resource scaling ensures systems remain operational during usage spikes, while failover mechanisms automatically redirect traffic when primary systems are compromised. DDoS protection, self-healing infrastructure, and backup automation provide additional resilience. Research indicates that healthcare organizations with fully automated recovery processes reduce recovery

time objectives (RTOs) by 83% and achieve 96% success rates during recovery exercises compared to 61% for organizations with primarily manual recovery procedures [10]. This resilience is vital for patient care continuity, especially in emergencies when manual intervention may be delayed.

Benefits and Challenges

The adoption of automated cloud defenses in healthcare yields significant benefits while presenting implementation challenges that require strategic solutions.

Benefits

Enhanced security posture stands as a primary advantage, with proactive threat detection and response significantly reducing data breach risks. According to IBM's Cost of a Data Breach Report, healthcare continues to have the highest breach costs of any industry for the 13th consecutive year, reaching $10.93 million per incident in 2023—65% higher than the global average of $4.45 million [11]. Organizations implementing security automation experience substantially lower breach costs, with companies deploying comprehensive security automation saving an average of $3.05 million per breach compared to those with no automation.

Cost efficiency represents another significant benefit, as automation minimizes the need for extensive manual oversight while optimizing resource utilization. The research report indicates that organizations with fully deployed security automation experience breach lifecycle durations 95 days shorter than those without automation—a 28% reduction that directly translates to lower operational costs [11]. Scalability enables healthcare organizations to adapt security controls to growing data volumes without proportionally increasing security staffing, particularly valuable in an industry facing persistent talent shortages.Improved compliance results from automated controls and documentation that reduce regulatory penalties and streamline audit processes. Operational resilience allows healthcare organizations to maintain critical services during security incidents, with automated detection and response minimizing service disruptions. Accelerated innovation completes the benefit profile, as secure-by-design automated environments enable faster deployment of new healthcare technologies without compromising security.

Challenges

Despite these benefits, healthcare organizations face substantial implementation hurdles. Legacy system integration presents significant difficulties, with research indicating that many healthcare institutions maintain clinical systems that are 15-20 years old and were not designed with modern security capabilities [12]. Complex vendor ecosystems further complicate security automation, as healthcare environments typically incorporate multiple technology providers with varying security standards and integration capabilities.

The skills gap represents a critical challenge, with research showing a significant shortage of healthcare IT professionals possessing both clinical workflow understanding and cybersecurity expertise. A study of

healthcare IT teams found that 83% report difficulty recruiting and retaining security specialists with healthcare-specific knowledge [12]. Budget constraints affect security initiatives across the sector, with smaller healthcare organizations particularly struggling to allocate sufficient resources for comprehensive security automation.

Clinical workflow disruption remains a paramount concern, as security controls perceived as hindering healthcare delivery face significant resistance. Research shows that security measures that add more than 30 seconds to clinical workflows experience adoption rates below 50% [12]. These challenges can be addressed through phased migrations that prioritize critical systems, hybrid cloud strategies bridging legacy and modern environments, managed security service providers filling expertise gaps, and comprehensive staff training ensuring smooth adoption while maintaining clinical efficiency.

Table 3: Financial Impact and Implementation Barriers for Healthcare Cloud Security Automation [11, 12]

Metric	Value
Average healthcare data breach cost (2023)	$10.93 million
Global average data breach cost (2023)	$4.45 million
Healthcare cost premium compared to global average	65%
Average savings with comprehensive security automation	$3.05 million per breach
Breach lifecycle reduction with automation	95 days
Percentage reduction in breach lifecycle	28%
Age of legacy healthcare systems	15-20 years
Percentage of IT teams reporting difficulty recruiting security specialists with healthcare knowledge	83%
Adoption rate for security measures adding >30 seconds to clinical workflows	<50%

Case Studies in Healthcare Security Automation

Large Hospital Network Case Study

MedStar Health, a leading hospital network operating across multiple facilities, successfully addressed complex security challenges by implementing zero-trust architecture with AI-powered automated defenses. Their implementation leveraged machine learning algorithms capable of analyzing up to 50 terabytes of sensitive patient data daily while continuously monitoring for suspicious access patterns [13]. According to Johnson & Johnson's healthcare technology analysis, this approach reduced unauthorized access attempts by 89% within six months while simultaneously decreasing authentication time for legitimate users by 62%, demonstrating that security improvements need not compromise efficiency [13].

The hospital network integrated continuous security validation capabilities that automatically tested defenses against 1,200 different attack scenarios daily, prioritizing remediation based on clinical impact assessment. This proactive approach led to a remarkable 76% improvement in security incident investigation rates and reduced average threat detection time from 8 days to just 37 minutes. Perhaps most significantly, their post-implementation survey revealed that 87% of physicians reported no negative impact on patient care activities, supporting the notion that properly designed automation enhances rather than hinders clinical workflows [13].

Regional Healthcare Provider Case Study

Valley Health System, a mid-sized regional provider, successfully addressed the challenge of securing legacy systems during their cloud transition through carefully orchestrated automation solutions. According to the Information Security Forum's Annual Report, the provider implemented a coordinated approach to legacy system protection that reduced security incidents by 64% while maintaining operational continuity for critical clinical applications ranging from 8-15 years in age [14].

Their strategy centered on deploying API security gateways that enabled secure communication between legacy systems and modern cloud services, coupled with virtual patching that protected outdated components that couldn't be directly updated. The implementation of security orchestration reduced their vulnerability exposure window from an average of 102 days to just 4 days, while automated continuous compliance monitoring decreased manual compliance reporting time by 94% with a 78% improvement in reporting accuracy [14]. The ISF report specifically highlighted Valley Health's approach as exemplary for smaller healthcare organizations, noting that their carefully phased implementation achieved a 71% reduction in compliance-related audit findings while allowing for gradual migration that minimized clinical disruption [14].

Their strategy centered on deploying API security gateways that enabled secure communication between legacy systems and modern cloud services, coupled with virtual patching that protected outdated components that couldn't be directly updated. The implementation of security orchestration reduced their

vulnerability exposure window from an average of 102 days to just 4 days, while automated continuous compliance monitoring decreased manual compliance reporting time by 94% with a 78% improvement in reporting accuracy [14]. The ISF report specifically highlighted Valley Health's approach as exemplary for smaller healthcare organizations, noting that their carefully phased implementation achieved a 71% reduction in compliance-related audit findings while allowing for gradual migration that minimized clinical disruption [14].

CONCLUSION

As healthcare continues its digital transformation journey, automated cloud defenses have evolved from advantageous to essential. The structured approach presented provides healthcare organizations with a roadmap for implementing robust security measures tailored to their unique requirements while addressing the cybersecurity skills shortage. The case studies demonstrate that organizations of varying sizes can successfully implement automated defenses, achieving tangible improvements in security posture, operational efficiency, and compliance management. The large hospital network's success with zero-trust architecture and the regional provider's effective securing of legacy systems during cloud transition offer practical templates that can be adapted across the healthcare sector. Although implementation challenges exist, particularly around legacy system integration and specialized expertise, these can be overcome through careful planning, phased approaches, and strategic partnerships. The continued evolution of cloud-native security technologies, artificial intelligence, and security orchestration will further enhance automated defense capabilities, positioning healthcare organizations to better protect digital assets, maintain compliance with evolving regulations, and ensure operational continuity. For healthcare specifically, this translates to better protection of patient privacy, improved clinical service reliability, and ultimately enhanced patient care and safety in our increasingly connected world.

REFERENCE

1. Mao E. et al.(2024) , "Forecast: Public Cloud Services, Worldwide, 2022-2028, 2Q24 Update," Gartner, [Online] Available: https://www.gartner.com/en/documents/5541595
2. She A.H. et al. (2022) , "Healthcare Data Breaches: Insights and Implications," healthcare MPDI [Online] Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636/,
3. IBM Security, (2024) "Cost of a Data Breach Report 2024," IBM Security, [Online]. Available: https://www.ibm.com/reports/data-breach
4. Cohen J. (2025), "The Shared Responsibility Model in Cloud Security: Who Owns What?," Upwind Solutions [Online]. Available: https://www.upwind.io/glossary/what-is-the-shared-responsibility-model
5. BobSulli, (2022) "The economic value of prevention in the cybersecurity lifecycle," Ponemon Sullivan privacy report . [Online]. Available: https://ponemonsullivanreport.com/2020/04/the-economic-value-of-prevention-in-the-cybersecurity-lifecycle/

6. Shackleford D. (2024) , "Cloud security automation: Benefits and best practices," TechTarget, . [Online]. Available: https://www.techtarget.com/searchsecurity/tip/4-steps-toward-cloud-security-automation
7. MacDonald N., and Croll T.(2021) , "Market Guide for Cloud Workload Protection Platforms," Gartner, [Online]. Available: https://www.gartner.com/en/documents/4003465
8. Rose S. et al. (2020), "Zero Trust Architecture," NIST Special Publication 800-207. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
9. Censinet (2024) , "Strengthen cyber maturity and resiliency with Peer Benchmarking," Censinet . [Online]. Available: https://www.censinet.com/provider-solutions/cybersecurity-benchmarks
10. Silva R.(2024) , Andrey Brito and Jan Paulo de Lima Filho, "Automation of Security Controls for Continuous Compliance in Vulnerability Management," ACM Digital Library, [Online]. Available: https://dl.acm.org/doi/10.1145/3697090.3697107
11. Elgan M. (2024) , "Cost of a data breach: The healthcare industry," IBM, 2024. [Online]. Available: https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry
12. Rahim M.J. et al. (2024) , "Cybersecurity Threats in Healthcare IT Challenges, Risks, and Mitigation Strategies," ResearchGate, . [Online]. Available: https://www.researchgate.net/publication/388792390_Cybersecurity_Threats_in_Healthcare_IT_Challenges_Risks_and_Mitigation_Strategies
13. Johnson and Johnson (2024) , "6 ways Johnson & Johnson is using AI to help advance healthcare," J&J.com, . [Online]. Available: https://www.jnj.com/innovation/artificial-intelligence-in-healthcare
14. Information Security Forum (2024) "ISF Annual Report 2023," Information Security Forum, . [Online]. Available: https://www.securityforum.org/wp-content/uploads/2024/04/ISF-Annual-Report-2023-2.pdf.