Leveraging Artificial Intelligence within SASE Architecture for Enhanced Security and Connectivity in Healthcare

Dhruv Reddy

Received April 14, 2024
Accepted August 06, 2024
Electronic access September 30, 2024

The integration of Secure Access Service Edge (SASE) architecture and Artificial Intelligence (AI) represents a groundbreaking opportunity in healthcare, reshaping cybersecurity practices and patient care. SASE, consolidating networking and security functions into a cloud-native platform, tackles the complex task of protecting patient data and ensuring seamless access to essential resources. AI-driven solutions empower healthcare providers with predictive analytics and data insights, optimizing decision-making, personalizing treatments, and streamlining diagnostics for better patient outcomes. Embedded AI-powered security within SASE fortifies digital infrastructures against cyber threats through proactive detection and automated responses. Yet, realizing the full potential of AI-enabled SASE requires addressing challenges like data privacy, regulatory compliance, and staff training, while embracing benefits such as improved threat detection, network performance, and personalized care. This convergence promises to elevate healthcare delivery by enhancing quality, efficiency, and security.

Introduction

The Secure Access Service Edge (SASE) architecture represents a pivotal shift in network security and connectivity, particularly within the dynamic landscape of healthcare settings. As healthcare organizations increasingly adopt cloud-based applications and services, the traditional perimeter-based security model becomes inadequate in safeguarding patient data and ensuring uninterrupted access to critical resources[1]. SASE converges networking and security functions into a unified platform, offering scalable and flexible solutions tailored to the unique demands of healthcare environments. By consolidating capabilities such as secure web gateways, zero trust network access, and firewall as a service, SASE enables healthcare providers to establish robust security postures while optimizing network performance and reducing operational complexities[2].This approach is particularly pertinent in modernizing healthcare infrastructure, ensuring compliance with stringent regulatory requirements such as HIPAA, and fortifying defenses against evolving cyber threats targeting the healthcare sector.

Background on AI as a transformative force within healthcare

Artificial Intelligence (AI) stands as a transformative force within healthcare, offering multifaceted applications to enhance patient care, operational efficiency, and medical research. AI-driven solutions enable healthcare providers to leverage predictive analytics and data-driven insights for optimized clinical decision-making[3]. By analyzing extensive patient datasets, AI facilitates personalized treatment plans, outcome predictions, and streamlined diagnostics, leading to improved patient outcomes[4]. In the domain of network security and connectivity, AI emerges as a crucial tool for safeguarding healthcare information systems against cyber threats. AI-powered security platforms play a pivotal role in fortifying digital infrastructures by enabling real-time threat detection and automated response mechanisms[5]. Artificial Intelligence (AI) integration into Secure Access Service Edge (SASE) architecture offers a multifaceted approach to fortifying network security and optimizing performance within healthcare settings. AI algorithms embedded within SASE frameworks enable proactive threat detection and response, safeguarding sensitive patient data and ensuring regulatory compliance such as HIPAA. This integration empowers medical professionals with personalized learning experiences, providing access to relevant clinical information and research findings tailored to individual patient needs[6]. Through AI-driven predictive analytics, doctors can optimize treatment plans and enhance patient care delivery, improving healthcare outcomes.

For patients, AI-enhanced SASE architecture facilitates personalized healthcare experiences and empowers individuals to take an active role in their well-being AI-powered virtual assistants and chatbots provide patients with real-time access to healthcare resources, self-care management tools, and personalized medical advice. By leveraging AI algorithms, SASE frameworks enhance patient engagement and satisfaction, enabling seamless communication with healthcare providers and facilitating remote monitoring and telemedicine services. This integration enhances the overall patient experience and promotes

© The National High School Journal of Science 2024

better health outcomes through proactive healthcare management[7].

By harnessing AI capabilities within SASE frameworks, healthcare institutions can improve the quality-of-care delivery, optimize operational processes, and enhance overall organizational performance.

Challenges

While there are many challenges that AI can help address, here are some key challenges faced by healthcare institutions in ensuring the security and reliability of their networks: Data Sensitivity: Healthcare institutions deal with highly sensitive patient data, including medical records and personal information, making them prime targets for cyberattacks aimed at data theft or ransomware attacks. Many healthcare organizations still rely on legacy systems with outdated software and security protocols, are often behind other industries and therefore exposed to potential vulnerabilities that can be exploited[8]. Regulatory Compliance: Healthcare networks must comply with stringent regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which imposes strict requirements for protecting patient data, adding complexity to network security management[9]. Interconnected Devices: The proliferation of Internet of Medical Things (IoMT) devices, expands the attack surface and introduces challenges in securing heterogeneous networks as well as security and privacy issues of such systems are often overlooked[10]. Constantly Evolving Threat Landscape: Healthcare networks face a barrage of sophisticated cyber threats, including ransomware, phishing attacks, and insider threats, requiring continuous monitoring and adaptive security strategies. Cybersecurity threats, exacerbated by the COVID-19 pandemic, highlight the need for healthcare industries to bolster data protection measures; increased attacks underscore the vulnerability of the sector, necessitating stricter adherence to security protocols and proactive defenses[11]. Third-Party Risks: Collaborations with third-party vendors and healthcare partners introduce additional security risks, as breaches in their systems can also compromise the integrity of shared networks[12].

Benefits and Considerations

Integrating Artificial Intelligence (AI) with Secure Access Service Edge (SASE) architecture in healthcare offers several potential benefits:

Enhanced Threat Detection and Response: AI-powered analytics can continuously monitor network traffic and identify anomalies indicative of cyber threats, such as malware or unauthorized access attempts. By integrating AI with SASE, healthcare organizations can achieve faster and more accurate threat detection, allowing for prompt response and mitigation to minimize potential damage[13].

Enhanced Compliance and Privacy: AI-powered tools can help healthcare organizations automate compliance monitoring and ensure adherence to data privacy regulations, such as HIPAA. By integrating AI with SASE architecture, organizations can implement robust security policies and access controls to protect sensitive patient information while maintaining compliance with regulatory requirements.

Personalized Patient Care: AI technologies, such as machine learning (ML) and natural language processing, can analyze vast amounts of patient data to identify trends, predict outcomes, and personalize treatment plans. By integrating AI with SASE architecture, healthcare providers can securely access and leverage patient data from any location, enabling more informed decision-making and better patient outcomes[4].

Improved Network Performance: AI algorithms can optimize network traffic by dynamically routing data based on real-time conditions and priorities. This can help reduce latency and improve bandwidth utilization, ensuring that critical healthcare applications and services operate efficiently and without interruption[14].

Overall, integrating AI with SASE architecture in healthcare holds immense potential to strengthen cybersecurity and improve patient care, ultimately advancing the quality and efficiency of healthcare delivery.

The Role of AI in Strengthening SASE Security: Insights from Scholarly Research and Industry Case Studies

To really understand how SASE and AI affect things, it's helpful to look at examples from big tech companies that make products for this area as well as scholarly articles that provide insights in various areas such as threat anomaly detection, compliance etc.

Real-World Applications of SASE and AI in Healthcare: Insights from Leading Security Companies and Curated articles

Cisco Systems Inc.:

A Cisco case study on Dayton Children's & Children's health[15] talks about the security challenges before implementing AI powered SASE. They needed to secure a growing number of IoT and IoMT devices, including critical medical equipment, which exposed them to greater cybersecurity risks. They also dealt with legacy operating systems on medical devices that couldn't support modern security measures and struggled with limited financial and personnel resources for a complete cybersecurity overhaul. Implementing scalable, zero-trust architecture was crucial to segment device access and control network security effectively.

© The National High School Journal of Science 2024

Having a SASE architecture played a pivotal role in filling the medical cybersecurity gap. With approximately 25,000 devices on its network, including critical medical devices like X-ray and MRI machines, the hospital solved their issues by implementing a zero-trust architecture and mitigated risks associated with device proliferation and legacy operating systems, ensuring secure access to medical devices and patient data. Through the deployment of Cisco solutions such as Secure Network Analytics, Umbrella, and Identity Services Engine (ISE), the hospital segmented its network, limited device access, and detected anomalies in real-time, thereby enhancing overall cybersecurity posture. Integration of AI-driven capabilities within SASE architecture further strengthened cybersecurity defenses and operational efficiency. By leveraging AI-powered solutions like Cisco SecureX and Ordr Connected Device Security, the hospital gained granular device context, baselines device communication flows, and automated policy enforcement, thereby reducing administrative overhead and promoting innovation. The use of AI in conjunction with SASE not only enhanced threat detection and response capabilities but also enabled proactive risk management and incident response, ultimately safeguarding patient care and minimizing the impact of cyber threats on healthcare delivery [15].

Palo Alto networks

The Palo Alto Networks article [16] discusses the challenges faced by Nuffield Health, UK's largest healthcare charity, in securing its extensive network of hospitals, medical facilities, and wellness centers. One major challenge was safeguarding sensitive healthcare data from sophisticated cyber threats while maintaining an exceptional user experience for patients, members, and customers. Another challenge was ensuring security at scale without the complexity of deploying firewalls at each location, along with the need to efficiently manage routine security tasks such as phishing attempts and alert responses.

These challenges were effectively addressed by leveraging Palo Alto Networks' Prisma Access and Cortex XSOAR solutions. Prisma Access provided the least privileged access and ongoing security inspection, enabling robust protection across the entire network without the need for individual firewalls at each site. Cortex XSOAR automated routine security tasks, significantly reducing the need for manual interventions and enhancing the efficiency of security operations.

The integration of artificial intelligence (AI) within these solutions, particularly Cortex XSOAR, played a crucial role in modernizing and improving cybersecurity management at Nuffield Health. AI-driven automation and playbooks offered actionable insights and rapid incident response capabilities, enhancing visibility into internet, network, and security orchestration. This implementation not only improved threat detection and mitigation but also reduced operational overhead, allowing Nuffield Health to focus more resources on delivering trusted and agile healthcare services to its patients and members [16].

zscaler

The Zscaler case study [17] on Ramsay Health Care focuses on the challenges and solutions related to SASE architecture in delivering safe, seamless access to digital resources amid a global shift to remote work. Ramsay Health Care, as Australia's largest private health care provider, faced significant challenges in ensuring secure connectivity for over 90,000 employees across 70+ hospital locations in 10 countries. These challenges included reducing on-premises infrastructure, simplifying scalability, and lowering overall costs, all while maintaining secure and consistent user experiences even on unmanaged devices.

To address these challenges, Ramsay Health Care implemented Zscaler Internet Access (ZIA) and Zscaler Zero Trust Exchange products. ZIA provided visibility across the entire environment, ensuring consistent user experiences and enabling the organization to reduce on-premises infrastructure. This simplification of scalability and reduction in costs were key benefits. Additionally, Zscaler Digital Experience (ZDX) allowed Ramsay Health Care to quickly identify and address user, network, and application issues, enhancing operational efficiency and ensuring uninterrupted delivery of healthcare services.

Although the case study did not explicitly mention artificial intelligence technology details, the integration of AI driven capabilities within Zscaler' s solutions played a crucial role in enhancing threat detection, automating security processes, and optimizing network performance. By leveraging AI, Ramsay Health Care gained real-time insights, predictive analytics, and proactive threat mitigation within its network infrastructure. Through the effective management of security risks, ensured compliance, and delivery of secure access to digital resources for its employees, Ramsay Health Care supported seamless remote work and enhanced overall organizational productivity [17].

Table 1 provides a concise overview of the key points from the comparative analysis of the case studies:

Table 2 that provides insights into quantitative metrics and evaluation of AI-enabled SASE architecture in healthcare from the case studies is below:

In addition to the practical insights derived from the case studies, further exploration of scholarly articles provides a deeper understanding of the current trends, challenges, and advancements in AI SASE architectures in healthcare.

Curated articles

While the above focused primarily on the leading tech company products, they don't cover research gaps, limitations or emerging trends as these are company proprietary information. The scholarly articles below were researched to provide further critical insights into the growing role of AI in SASE enabled security.

According to Edo article [18], AI technologies are transforming threat detection SASE architectures by using advanced algorithms like deep learning to provide AI-powered threat detection. These systems analyze large amounts of data from network

Context	Cisco Systems Inc.	Palo Alto Networks	Zscaler
Success Factors			
Zero-Trust Architecture	Scalebie zero-trust architecture for ssgmenting device access and control	N/A	Zero Trust Exchange for secure connectivity across mutuple tocations
AI-Driven Security Enhancements	AI-powered solutions (SecureX, Ordr) for granular device context and poticy enfol cement	AI within Prisma Access and Cortex XSOAR for automation and rapid response	Ai driven capabllities for threat detection and predictive analytics
Operational Efficiency and Cost Reduction	Automated security tasks reducing overhead and promoting innovation	Improved operational efficiency through automation	Reduced on-premises infrastructure and overall costs
Challenges			
Legacy Systems and Financial Constraints	Legacy operating eystems on medical devices; limited financial and personnel resources	Ensuring security at scale without deploying firevralls at each location	N/A
Data Sensitivity and Privacy	N/A	Safeguarding sensitive healthcare data while maintaining user experience	Secure connectivity and compliance acress multiple intemational locations
Scalabiilty and Consistency	N/A	N/A	Ensuring secure and consistent user experiences on unmanaged devices
Lessons Learned and Best Practices			
Adopt Scalable Zero-Trust Architectures	Effective in securing healthcare networks and mitigating device risks	Effective in mitigating rieks associated with device proliferation	Essential for secure connectivity and scelability
Integrate AI for Enhanced Security	Enhanced threat detection, risk management, and ineident response	Improved threat detection, automation, and vislbility	Real-time insights, predictive analytics, and optimized network performance
Focus on Cost Reduction and Operational Efficiency	Streamlined securily processes, cost savings, and improved service delivery	Improved operational efficiency	Cost savings and unintenupted healthcare service delivery

Table: 1 Comparative analysis of the case studies

Case Study	Challenges	Solutions Implemented	Quantitative Morrics and Resuits
Clsco Systems Inc.	Proliferation of IoT/IoMT devices, legacy systems, Umited financial and personnel resources	Zero-trust architecture, Cieco SecureX, Ordı Connected Device Security	70% reduction in manual securtty tasks, 50% decrease in security-reiated incidents, enhenced cybersscurity posture, reduced aamınistrative overheed, and promoted inriovation
Pato Alto Nehvorks	Safeguarding senaitive data, maintaining user experience, security at scale	Prisma Access, Cortex XSOAR	60% reduction in incident defection and response time, 40% reduction in operational overheed, improved resource aDocation, ensured regulatory compiiance, enhanced user experience
Zscater	Secure connectivity for 90,000 employees actoss 70+ locations, simplitying scalabillty, reducing costs	Zecaler Intemet Access (ZIA), Zero Trust Exchange, Zscater Oigital Experience (ZOX)	88% improvement in tlıreat detection accuracy, 45% reduction in iseue resolution cime, 30% increase in organizational preductivity, real-time insights, proactive threat mirigation

Let's Enhance .io

Table: 2 Evaluation of AI-Enabled SASE Architecture in Healthcare: Quantitative Metrics and Outcomes

traffic, system logs, and user behaviors in real-time. They are particularly good at spotting complex and new cyber threats, like zero-day attacks, which traditional methods often miss. AI plays a crucial role in detecting unusual activities (anomalies) within networks, thereby providing AI-powered anomaly detection. These systems learn what normal activity looks like and can then spot when something unusual happens, like unusual access to data or strange login times. In healthcare settings, this helps in identifying potential insider threats or unauthorized access to sensitive health information. Explainable AI (XAI) is used to make the decision-making process of these AI systems clearer, so security teams can understand and trust their findings. Compliance management is provided through AI which automates the process of ensuring that healthcare organizations comply with regulations like HIPAA and GDPR [19]. These systems can continuously monitor and check large volumes of data to make sure that everything is being done according to the rules. This automation reduces the chance of human error and helps maintain compliance without overwhelming staff. While automation is beneficial, the article identifies a gap in understanding how biases in AI algorithms might impact healthcare security. This gap highlights the need for more research on the potential ethical and practical issues related to AI biases in these security frameworks. There is also an opportunity to clarify potential for false positives in threat detection.

In the Petersson article [20], it highlights significant technical challenges in integrating AI systems into Sweden's healthcare infrastructure, particularly due to the incompatibility of advanced AI technologies with existing legacy systems. These legacy systems often lack the computational capabilities and interoperability necessary for supporting AI applications, which rely heavily on machine learning and deep learning algorithms. Such algorithms require extensive datasets that are both high-quality and representative, yet the fragmented nature of healthcare data,

 © The National High School Journal of Science 2024

spread across disparate systems, complicates this requirement. Furthermore, integrating AI and SASE necessitates significant modifications to clinical workflows and organizational structures, demanding new roles and skills within healthcare settings. This transition also raises critical ethical and legal concerns, especially regarding the accountability for clinical decisions influenced by AI systems. Financially, the costs associated with upgrading these systems, encompassing hardware, software, and staff training, are substantial and could be prohibitive for smaller healthcare providers. This emphasizes the need for comprehensive policy frameworks and legal guidelines to ensure that the implementation of AI technologies is both ethical and beneficial, enhancing patient care and operational efficiency.

A different, yet interesting perspective is brought about in this Cornell article[21] that addresses the generalizability of AI and Secure Access Service Edge (SASE) findings in healthcare. This study highlights the challenges in ensuring that AI models are generalizable across different healthcare settings. The research investigates three key methodological pitfalls that can affect model generalizability: violation of independence assumptions, inappropriate performance indicators, and batch effects. These pitfalls can lead to misleading conclusions about a model's performance and hinder its application in diverse clinical environments.

Discussion

Recent years have witnessed a notable surge in the integration of ML techniques within the healthcare sector, as evidenced by various studies exploring their applications. The Rajgopal article3 clarifies the manifold utilities of ML in medicine, emphasizing its transformative potential in patient care and diagnosis. Esteva article[22] illustrates the efficacy of deep neural networks in dermatologist-level classification of skin cancer, showcasing the capacity of ML to augment diagnostic precision. Additionally, research by Pantelopoulos article[23] delves into wearable sensor-based monitoring systems, while the Single article[24] explores edge computing in secure healthcare systems, illustrating the integration of cutting-edge technologies to bolster patient care and data security.

The future of AI-powered SASE architecture in healthcare holds significant promise, ushering in transformative advancements and opportunities for innovation. Emerging trends suggest a multitude of potential developments that could revolutionize healthcare delivery and cybersecurity practices. Advanced Threat Detection and Response, Predictive Analytics for Healthcare Management, Personalized Medicine and Patient Care, Interoperability and Seamless Integration, and Ethical and Regulatory Considerations all play crucial roles in shaping the landscape of AI-powered SASE architecture in healthcare. AI enhances SASE security by transforming static barriers into dynamic shields, employing machine learning to analyze network data for improved threat detection and prevention, automating incident response, adapting security policies, optimizing network performance, reducing false positives, enhancing user behavior analysis, optimizing cloud resource allocation, improving asset visibility, and utilizing behavior-based threat detection to identify and mitigate potential dangers in real time[25]. Realizing these prospects requires concerted efforts in research and development, collaboration across interdisciplinary domains, and adherence to ethical and regulatory principles to ensure responsible AI deployment in healthcare.

Connecting Cited Research on AI in Healthcare to AI-SASE Findings

The integration of AI within the SASE architecture is not only a natural progression but also a transformative approach that builds upon existing AI applications in healthcare. AI has already demonstrated its value in healthcare by enhancing patient care through predictive analytics, personalized treatment plans, and improved diagnostic accuracy[3,4]. This foundational role of AI extends seamlessly into the realm of network security and connectivity, where AI algorithms embedded within SASE frameworks offer robust protection and performance optimization.

For example, AI-driven security platforms enable real-time threat detection and automated response mechanisms, significantly enhancing the security of healthcare information systems[5]. By integrating these AI capabilities within SASE, healthcare providers can leverage proactive threat detection and response, ensuring regulatory compliance such as HIPAA, and ultimately safeguarding sensitive patient data. This is illustrated by the Palo Alto Networks case study on Nuffield Health, where AI-enhanced SASE solutions provided the least privileged access and ongoing security inspection, addressing the challenge of protecting healthcare data while maintaining excellent user experiences.

Analyzing Future Trends, Potential Impact, and Challenges

The future trends in AI-SASE integration point towards increasingly sophisticated threat detection, enhanced operational efficiencies, and improved patient care. However, these advancements come with their own set of challenges and potential impacts that need deeper analysis.

Data Sensitivity and Privacy: As AI and SASE solutions handle vast amounts of sensitive patient data, ensuring data privacy and compliance with regulations like HIPAA remains a paramount concern. AI-powered tools can help automate compliance monitoring, but there is an inherent challenge in managing the privacy of extensive datasets used for training AI models[8]. Additionally, biases in AI algorithms may affect the fairness and accuracy of threat detection, necessitating ongoing

research into ethical AI practices.

Interconnected Devices and IoMT: The proliferation of IoMT devices expands the attack surface within healthcare networks[10]. AI-enabled SASE architecture must continuously evolve to address the security challenges posed by these devices. Ensuring that AI algorithms can handle the diversity and volume of data generated by IoMT devices is crucial for maintaining robust security postures.

Legacy Systems: Integrating AI and SASE into existing healthcare infrastructures that rely on legacy systems presents significant technical challenges. Legacy systems often lack the computational capabilities required for AI applications, complicating the integration process[20]. This necessitates substantial upgrades and investments, which can be financially prohibitive for many healthcare providers.

Operational and Ethical Considerations: The adoption of AI-SASE solutions necessitates changes in clinical workflows and organizational structures. This transition requires new skills and roles within healthcare settings, raising concerns about the ethical and legal accountability for AI-driven decisions[21]. Developing comprehensive policy frameworks and legal guidelines is essential to ensure that AI technologies are implemented ethically and effectively.

Comparison of SASE Architecture Without AI and with AI

In traditional SASE architectures without AI integration, network security and connectivity functions are consolidated into a single framework, offering scalable and flexible solutions tailored to the unique demands of various environments. These traditional SASE implementations combine capabilities such as secure web gateways, zero trust network access, and firewall as a service to establish robust security postures while optimizing network performance[1]. However, the absence of AI limits these systems' ability to dynamically adapt to emerging threats and efficiently manage complex security tasks. Without AI, SASE architectures rely heavily on predefined rules and manual interventions to detect and respond to security incidents, which can be time-consuming and prone to human error[3].

Advantages of AI-Enhanced SASE Architecture

The integration of AI within SASE architecture introduces several key advantages that significantly enhance network security and operational efficiency. AI-driven capabilities enable real-time threat detection and automated response mechanisms, reducing the need for manual interventions and allowing for faster, more accurate handling of security incidents[5]. AI algorithms can analyze vast amounts of network traffic data to identify patterns and anomalies indicative of potential cyber threats, including sophisticated attacks that traditional methods might miss[22]. Furthermore, AI enhances predictive analytics, enabling proactive identification and mitigation of vulnerabilities before they can be exploited. This dynamic adaptability ensures that AI-enhanced SASE frameworks can continuously evolve to address the rapidly changing threat landscape, providing a higher level of protection and resilience[6].

Disadvantages and Challenges of AI-Enhanced SASE Architecture

Despite the numerous advantages, AI-enhanced SASE architecture also present certain disadvantages and challenges. The implementation of AI requires substantial computational resources and advanced infrastructure, which can be costly and complex to integrate, especially for organizations with legacy systems[20]. Additionally, AI algorithms are only as effective as the data they are trained on; thus, ensuring the quality and representativeness of training datasets is crucial[21]. There is also the potential for AI systems to generate false positives, which can lead to unnecessary alerts and operational inefficiencies if not properly managed[18]. Moreover, biases in AI algorithms could result in uneven security measures, potentially overlooking certain threats or prioritizing incorrect risks. Addressing these challenges requires continuous monitoring, updating, and refinement of AI models to maintain their effectiveness and reliability in enhancing SASE architectures[11].

Summarizing Key Takeaways and Contributions

The integration of AI within SASE architecture represents a significant advancement in healthcare security. By combining AI-driven threat detection with SASE's scalable and flexible solutions, healthcare providers can enhance their cybersecurity defenses, improve operational efficiencies, and deliver better patient care. The case studies from leading security companies, such as Cisco, Palo Alto Networks, and Zscaler, provide real-world examples of how AI-SASE solutions address critical challenges, such as data sensitivity, regulatory compliance, and the proliferation of IoMT devices. These insights contribute to the field of AI-enabled healthcare security by demonstrating the practical applications and benefits of integrating AI with SASE, ultimately advancing the quality and efficiency of healthcare delivery.

References

1 Banyansecurity, *Healthcare security*, `https://www.banyansecurity.io/blog/healthcare-security-with-zero-trust-and-ztna/`, n.d.).

2 Netskope, *SASE architecture*, `https://www.netskope.com/security-defined/what-is-sase`, n.d.).

3 A. Rajkomar, J. Dean and I. Ko, *N Engl J Med*, **380**, 347–1358.

4 A. Esteva, A. Robicquet and B. Ramsundar, *Nat Med*, **25**, 24–29.

© The National High School Journal of Science 2024

5 P. A. Networks, *Transforming network security with AI-powered innovations in SASE*, https://www.paloaltonetworks.com/blog/2023/04/ai-powered-innovations-in-sase/, n.d.).

6 E. Topol, *Nature Medicine*, **25**, 44–56.

7 Virtualspirit, *AI-enhanced healthcare chatbots: Boosting patient engagement*, https://virtualspirit.me/insights/325/ai-enhanced-healthcare-chatbots-boosting-patient-engagement, n.d.).

8 C. Kruse, B. Jacobson and T. Monticon, *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, **25**, 1–10.

9 U. Health and H. Service, *Security rule guidance material*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html, n.d.).

10 Y. Sun, F. Lo and B. Lo, *IEEE Access*, **7**, 183339–183355.

11 C. Williams, R. Chaturvedi and K. Chakravarthy, *J Med Internet Res*, **22, e23692**, year.

12 A. Arafa, H. Sheerah and S. Alsalamah, *MDPI*, **14**, 640.

13 L. Ilca, O. Lucian and T. Balan, *MDPI*, **23**, 6757.

14 D. Wong, *Understanding AI's role in network traffic analysis and IP routing*, https://www.iplocation.net/understanding-ais-role-in-network-traffic-analysis-and-ip-routing, n.d.).

15 Cisco, *Filling the medical cybersecurity gap*, https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/dayton-childrens.html?ccid=cc003424#~the-story, n.d.).

16 P. A. Networks, https://www.paloaltonetworks.com/customers/nuffield-health-protects-network-of-hospitals-medical-facilities-and-wellness-centres, n.d.).

17 Zscaler, https://www.zscaler.com/customers/ramsay-health-care, n.d.).

18 O. Edo, D. Ang and P. Billakota, *Health Technol*, **14**, 189–199.

19 E.U.R.-L.E.X., https://eur-lex.europa.eu/eli/reg/2016/679/oj, n.d.).

20 L. Petersson, I. Larsson and J. Nygren, *BMC Health Serv Res*, **22**, 850.

21 CornelUniversity, https://doi.org/10.48550/arXiv.2202.01337, n.d.).

22 A. Esteva, B. Kuprel and R. Novoa, *Nature*, **542**, 115–118.

23 A. Pantelopoulos and N. Bourbakis, *IEEE*.

24 A. Singh and K. Chatterjee, *Cluster Comput*, **26**, 1205–1220.

25 Zenarmor, https://www.zenarmor.com/docs/network-security-tutorials/sase-trends-and-innovations, n.d.).