IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 23 August 2024, accepted 18 September 2024, date of publication 27 September 2024, date of current version 21 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3469215

TOPICAL REVIEW

Security and Privacy in E-Health Systems: A Review of AI and Machine Learning Techniques

MARY NANKYA[1], (Member, IEEE), ALLAN MUGISA[2], YUSUF USMAN[3], (Member, IEEE), AADESH UPADHYAY[4], AND ROBIN CHATAUT[5], (Senior Member, IEEE)

[1]Department of Computer Science, Fitchburg State University, Fitchburg, MA 01420, USA
[2]School of Business, Fitchburg State University, Fitchburg, MA 01420, USA
[3]School of Computing and Engineering, Quinnipiac University, Hamden, CT 06514, USA
[4]Department of Computer Science and Engineering, University of North Texas, Denton, TX 76207, USA
[5]College of Science and Engineering, Texas Christian University, Fort Worth, TX 76109, USA

Corresponding author: Mary Nankya (mnankya@fitchburgstate.edu)

ABSTRACT The adoption of electronic health (e-health) systems has transformed healthcare delivery by harnessing digital technologies to enhance patient care, optimize operations, and improve health outcomes. This paper provides a comprehensive overview of the current state of e-health systems, tracing their evolution from traditional paper-based records to advanced Electronic Health Record Systems(EHRs) and examining the diverse components and applications that support healthcare providers and patients. A key focus is on the emerging trends in AI-driven cybersecurity for e-health, which are essential for protecting sensitive health data. AI's capabilities in continuous monitoring, advanced pattern recognition, real-time threat response, predictive analytics, and scalability fundamentally change the security landscape of e-health systems. The paper discusses how AI strengthens data security through techniques like anomaly detection, automated countermeasures, and adaptive learning algorithms, enhancing the efficiency and accuracy of threat detection and response. Furthermore, the paper delves into future directions and research opportunities in AI-driven cybersecurity for e-health. These include the development of advanced threat detection systems that adapt through continuous learning, quantum-resistant encryption to safeguard against future threats, and privacy-preserving AI techniques that protect patient confidentiality while ensuring data remains useful for analysis. The importance of automating regulatory compliance, securing data interoperability via blockchain, and prioritizing ethical AI development are also highlighted as critical research areas. By emphasizing innovative security solutions, collaborative efforts, ongoing research, and ethical practices, the e-health sector can build resilient and secure healthcare infrastructures, ultimately enhancing patient care and health outcomes.

INDEX TERMS Data security, electronic health records, machine learning, predictive analytics, privacy, quantum-resistant encryption, telemedicine, threat detection.

I. INTRODUCTION

e-health systems are comprehensive frameworks that leverage electronic and information technologies to revolutionize healthcare delivery, management, and accessibility. These systems integrate various digital components, applications, and services designed to support healthcare providers, patients, and other stakeholders within the healthcare ecosystem [1]. By utilizing technologies such as the web, personal digital assistants (PDAs), interactive television, voice response systems, and computer kiosks, e-health systems aim to enhance healthcare services' quality, efficiency, and reach. E-health systems transcend conventional healthcare boundaries, offering a diverse array of capabilities that

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Alawneh.

enhance patient care quality and overall health results. These systems enable the efficient management and exchange of health information, support clinical decision-making, and promote patient engagement in their healthcare journey. E-health systems also play a crucial role in streamlining administrative processes, reducing healthcare costs, and enhancing the overall efficiency of healthcare organizations. One of the key advantages of e-health systems is their ability to break down geographical barriers and expand healthcare access to remote or underserved populations [2]. By integrating high-quality network services, these systems enable telemedicine, remote monitoring, and virtual consultations, making healthcare services more accessible to individuals who may otherwise face challenges in receiving timely care. This aspect of e-health systems contributes significantly to promoting healthcare equity and improving population health outcomes. Furthermore, e-health systems embody a patient-centric approach to healthcare delivery. Through the utilization of cutting-edge information and communication technologies, these platforms facilitate tailored treatment strategies, prompt medical actions, and enhanced interaction between individuals receiving care and their healthcare professionals [3]. This strategy not only elevates the standard of care provided but also encourages patients to become more engaged and proactive in their own health management journey. Additionally, the data-driven nature of e-health systems supports evidence-based practices, facilitates medical research, and contributes to the continuous improvement of healthcare delivery models.

A. EVOLUTION OF E-HEALTH

Healthcare documentation initially relied entirely on paper records. Healthcare providers manually recorded patient information, treatment histories, prescriptions, and test results. These paper-based systems were cumbersome, prone to errors, and difficult to manage, primarily as patient volumes and the complexity of medical care increased. The transition from paper-based records to EHRs began in the late 20th century. The goal was to improve the accuracy, accessibility, and efficiency of health information management. Early EHR systems were primarily used for administrative tasks like patient registration, scheduling, and billing. They were often standalone systems with limited interoperability. In the 1990s, health information systems (HIS) were developed to integrate various aspects of healthcare management, such as patient management, laboratory information, and pharmacy information systems. These systems aimed to create a more cohesive and streamlined workflow within healthcare institutions, improving data management and reducing redundancies, focusing on digitizing health records and administrative processes. The rapid advancement of information and communication technologies (ICT) during this period enabled the development of more sophisticated and capable EHR systems. Increased computing power and the proliferation of the internet significantly enhanced the capabilities of these systems. The spending has consistently increased, reflecting the growing need for robust cybersecurity measures in the healthcare industry due to rising cyber threats. Projected values for 2024, 2025, and 2026 indicate continued growth at a compound annual growth rate of 14.1%, reaching over 27 billion USD by 2026 [4]. Figure 1 illustrates the global spending on cybersecurity in the healthcare sector from 2019 to 2026 [5].

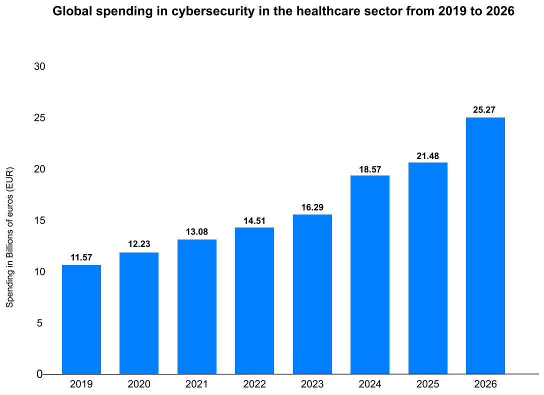

FIGURE 1. Global spending on cybersecurity in the healthcare sector.

B. IMPORTANCE AND BENEFITS OF E-HEALTH

E-health significantly improves access to healthcare by facilitating remote consultations, reducing the need for travel, and making medical services accessible to individuals in rural and underserved areas. Through telehealth services, patients can connect with specialists via video conferencing and other communication tools, receiving timely medical advice without the constraints of distance [6]. With the capability to collect and analyze detailed patient data, these technologies facilitate the development of personalized and highly effective treatment plans tailored to individual needs. Additionally, wearable devices and remote monitoring tools enable continuous tracking of health metrics, allowing for the early identification of health concerns and management of improving patient outcomes and overall well-being.

E-health initiatives contribute to cost efficiency in healthcare through various means. Firstly, by facilitating remote care and continuous monitoring, e-health initiatives reduce the necessity for frequent hospital visits, thereby cutting healthcare expenses for both patients and healthcare systems. Additionally, the automation of administrative tasks and the electronic management of health records streamline operations, reducing paperwork and administrative burdens. This enhanced efficiency offers time savings and optimum resource utilization, ultimately leading to significant cost savings across the healthcare ecosystem.

E-health platforms empower patients by granting them access to their health records, educational resources, and tools to manage their health effectively. This access enables patients to actively participate in their healthcare decisions, leading to better-informed choices and improved health outcomes. Additionally, enhanced communication features allow patients to easily interact with healthcare providers, schedule appointments, and receive timely reminders, fostering a collaborative relationship between patients and providers and improving the overall healthcare experience.

E-health systems revolutionize health information management by prioritizing secure data storage and seamless data sharing. Through robust encryption and authentication measures, these systems ensure that health data is stored securely, minimizing the risk of unauthorized access and data breaches. Authorized personnel can easily retrieve patient information when needed, streamlining data management and reducing errors. Moreover, health information exchange systems facilitate seamless patient data exchange among healthcare providers, promoting more coordinated and comprehensive care delivery. This interoperability enhances provider communication, reduces duplicate testing, and improves patient outcomes.

E-health technologies offer significant public health benefits through disease surveillance and health education initiatives. By facilitating large-scale health data collection and analysis, these tools aid in disease surveillance, allowing for the early detection of outbreaks and informing effective public health planning and response strategies. Additionally, online platforms and mobile apps serve as powerful tools for health education, delivering accessible and personalized information to the public. Through educational resources, interactive content, and lifestyle tracking features, e-health promotes healthy behaviors, empowers individuals to take control of their health, and contributes to disease prevention efforts on a community-wide scale. Table 1 below shows the benefits of e-health systems.

C. MAJOR COMPONENTS OF E-HEALTH SYSTEMS

- EHRs and Electronic Medical Records (EMRs): These digital repositories store patients' health information, including medications, allergies, radiology images, medical history, diagnoses, treatment plans, and lab test outcomes [7].
- Telemedicine and Tele-health Platforms: These platforms enable healthcare service delivery through virtual consultations, remote monitoring of patient's health status, telemedicine visits, and tele-education for healthcare professionals [8].
- Health Information Exchange (HIE) Networks: HIE networks facilitate the secure sharing of patients' health information among healthcare providers and organizations, allowing for seamless electronic health data exchange across different healthcare settings [9].
- Clinical Decision Support Systems (CDSS): CDSS provides healthcare providers with evidence-based clinical guidelines, recommendations, and alerts to assist in clinical decision-making at the point of care.
- Health Monitoring Devices and Wearables: These devices enable the collection of real-time health data, such as activity levels, vital signs, and biometric measurements, from patients, enabling remote monitoring of patient's health status and early detection of health issues.
- Patient Portals and Personal Health Records (PHRs): Patient portals and PHRs empower patients to access their health information, communicate with healthcare providers, schedule appointments, refill prescriptions, and engage in self-management activities.
- Health Analytics and Population Health Management Tools: These tools analyze large volumes of healthcare data to identify trends, patterns, and insights related to population health, disease management, and healthcare utilization, helping organizations optimize resource allocation and improve care quality [10], [11].
- Mobile Health (mHealth) Applications: These applications leverage mobile devices, including smartphones and tablets, to support health-related activities and services, including fitness tracking, medication adherence, chronic disease management, and remote monitoring [12].
- Regulatory and Policy Frameworks: These frameworks establish standards, guidelines, and regulations for the development, implementation, and use of e-health systems, ensuring data privacy, security, interoperability, and compliance with legal and ethical requirements [13].

Figure 2 below shows the major components of e-health systems.

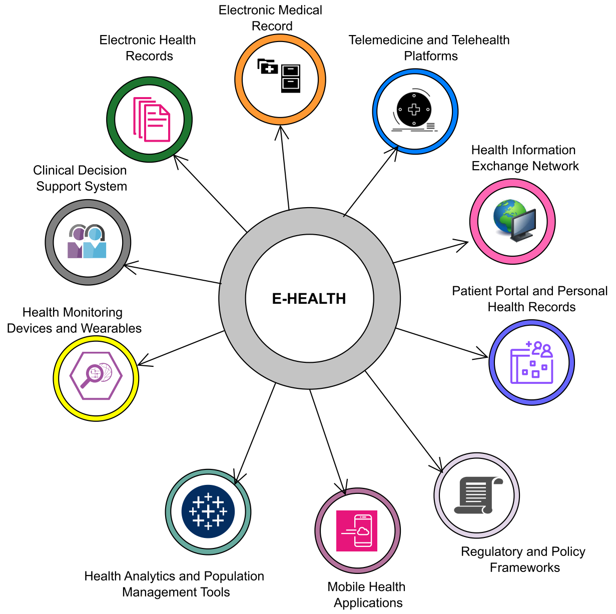
Electronic Medical Record
Electronic Health Records
Telemedicine and Telehealth Platforms
Health Information Exchange Network
Clinical Decision Support System
E-HEALTH
Patient Portal and Personal Health Records
Health Monitoring Devices and Wearables
Regulatory and Policy Frameworks
Health Analytics and Population Management Tools
Mobile Health Applications

FIGURE 2. The major components of e-health systems.

In the subsequent sections of this article, we explore various aspects of e-health cybersecurity. Section II addresses evolving threats in healthcare data security, discussing the dynamic nature of cyber risks targeting sensitive health information. Section III analyzes vulnerabilities in e-health

TABLE 1. Benefits of e-health systems.

Benefit	Description
Improved Access to Healthcare	Remote consultations and telehealth services improve healthcare access, especially in rural areas, enabling patients to consult with specialists remotely via video conferencing. This timely access to medical advice fosters better healthcare outcomes and patient satisfaction.
Enhanced Quality of Care	Personalized Medicine uses detailed patient data for tailored treatment plans, while continuous monitoring employs wearable devices for early health issue detection and proactive management.
Cost Efficiency	Remote care and monitoring cut hospital visits and save costs. Automation and electronic records streamline operations, boosting efficiency and cutting paperwork.
Patient Empowerment	Access to health information empowers patients with records and resources for active participation in care, while enhanced communication streamlines interaction with healthcare providers, improving the overall healthcare experience.
Better Health Information Management	Secure data storage ensures health data is safely stored and retrievable, reducing errors and improving data management. Data sharing facilitates seamless exchange among providers, enhancing care coordination and comprehensiveness.
Public Health Benefits	Disease Surveillance aids in early outbreak detection and effective public health planning by facilitating large-scale data collection and analysis. Health education offers accessible online platforms and mobile apps to promote healthy lifestyles and disease prevention.

system infrastructure, detailing weaknesses that attackers could exploit. Section IV delves into the role of human factors in e-health security and their impact on AI - Driven Cybersecurity. Section V highlights AI-driven threat detection and prevention techniques, examining how AI can create new risks and offer protective solutions. Section VI focuses on privacy-preserving AI techniques in e-health, emphasizing the protection of sensitive information while still enabling valuable insights. Section VII explores secure model deployment and management, stressing the importance of safeguarding AI and ML models from tampering and unauthorized access. Section VIII covers ethical and regulatory considerations for the cybersecurity of e-health systems, exploring frameworks and ethical implications of AI in this domain. Section IX delves into the frameworks for automating Regulatory Compliance in e-health systems. Section X investigates blockchain for data security, presenting novel technologies for securing and sharing health data. Section XI provides a practical look at real-world applications of AI and ML-driven security in e-health systems, showcasing how these technologies protect patient data. Section XII discusses large language models in e-health systems, evaluating their potential benefits and associated security concerns. Section XIII outlines emerging trends in AI-driven cybersecurity, identifying cutting-edge developments shaping the future of e-health security. Section XIV proposes future directions and research opportunities for improving e-health cybersecurity. Finally, Section XV summarizes the key points discussed and reaffirms the critical importance of robust cybersecurity measures in the evolving e-health landscape. Figure 3 below shows the organizational structure for this paper.

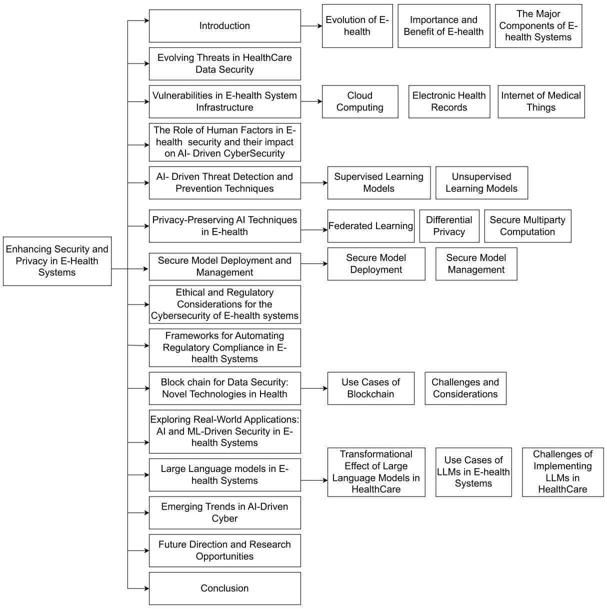
Enhancing Security and Privacy in E-Health Systems
Introduction
Evolution of E-health
Importance and Benefit of E-health
The Major Components of E-health Systems
Evolving Threats in HealthCare Data Security
Vulnerabilities in E-health System Infrastructure
Cloud Computing
Electronic Health Records
Internet of Medical Things
The Role of Human Factors in E-health security and their impact on AI- Driven CyberSecurity
AI- Driven Threat Detection and Prevention Techniques
Supervised Learning Models
Unsupervised Learning Models
Privacy-Preserving AI Techniques in E-health
Federated Learning
Differential Privacy
Secure Multiparty Computation
Secure Model Deployment and Management
Secure Model Deployment
Secure Model Management
Ethical and Regulatory Considerations for the Cybersecurity of E-health systems
Frameworks for Automating Regulatory Compliance in E-health Systems
Block chain for Data Security: Novel Technologies in Health
Use Cases of Blockchain
Challenges and Considerations
Exploring Real-World Applications: AI and ML-Driven Security in E-health Systems
Large Language models in E-health Systems
Transformational Effect of Large Language Models in HealthCare
Use Cases of LLMs in E-health Systems
Challenges of Implementing LLMs in HealthCare
Emerging Trends in AI-Driven Cyber
Future Direction and Research Opportunities
Conclusion

FIGURE 3. Organizational structure of the paper.

II. EVOLVING THREATS IN HEALTHCARE DATA SECURITY

Healthcare data breaches have significantly increased over the past 14 years, with a notable surge in recent years. From October 2009 to December 2023, 5,887 breaches involving 500 or more records were reported to the Office for Civil Rights (OCR), exposing over 519 million records. In 2023 alone, 725 breaches were reported, impacting over 133 million records, the highest on record. Hacking and ransomware attacks have become the primary causes, with hacking incidents rising by 239% and ransomware by 278% between 2018 and 2023. Major breaches include the 2015 Anthem Inc. breach affecting 78.8 million individuals and the 2024 Change Healthcare ransomware attack, potentially affecting up to one-third of Americans. Due to chronic underfunding, the OCR continues to need help with a backlog of investigations. The shift from theft or loss of records to hacking incidents highlights the evolving nature of cyber threats in healthcare [14].

In 2023, the OCR reported a staggering 239% increase in hacking-related breaches and a 278% rise in ransomware attacks between January 1, 2018, and September 30, 2023. Hacking accounted for 49% of breaches in 2019, escalating to 79.7% in 2023. Not only are the numbers of breaches increasing, but their severity is also intensifying. In 2021, breaches compromised 45.9 million records, worsening to 51.9 million in 2022 and reaching an unprecedented high of 133 million in 2023. This alarming total includes 26 breaches exceeding 1 million records and four breaches surpassing 8 million, with the most significant breach affecting 11,270,000 individuals marking it as the second-largest healthcare data breach in history [15].

Security and privacy are critical pillars within the e-health systems' framework, primarily due to their pivotal role in managing highly sensitive personal health data [16]. The importance of these aspects is immense, given that any security compromise can result in severe privacy breaches, limited data access, compromised data integrity, and the potential for significant harm to individuals [17]. Ensuring the security and privacy of e-health systems is crucial for maintaining patient trust, which is fundamental for successfully adopting and utilizing these technologies. Without robust security measures and privacy protections, some patients may be reluctant to share their health information, hindering the potential benefits of e-health initiatives [18]. Moreover, compliance with legal and regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, necessitates stringent security and privacy controls to protect patient information and avoid legal penalties [19]. Comprehensive measures, including technical safeguards, secure authentication, access controls, regular audits, user education, and privacy by design in e-health system development, are crucial to effectively addressing security and privacy concerns [20]. Prioritizing security and privacy in healthcare and e-health development ensures regulatory compliance and cultivates a healthcare environment where patients trust that their health data is handled responsibly and respectfully.

The integration of advanced technologies such as AI and ML further enhances the capabilities of e-health systems, particularly in the areas of security and privacy [21]. AI/ML algorithms can process vast amounts of healthcare data to identify patterns, detect anomalies, and predict potential security threats, thereby bolstering the defenses against cyberattacks and safeguarding sensitive patient information [22]. Additionally, AI/ML-driven techniques can optimize access controls, encryption methods, and authentication mechanisms to ensure robust security measures while maintaining user privacy [23]. By leveraging AI/ML technologies, e-health systems can achieve greater resilience against cybersecurity risks and instill confidence in patients regarding protecting their health data [24].

Figure 4 shows the healthcare industry cyber-attacks by the number of patients affected for the year 2022-2023 [25].

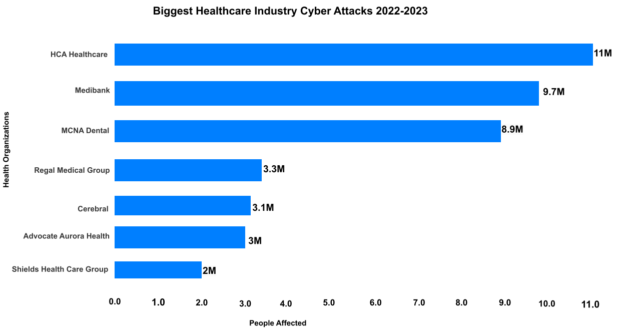

FIGURE 4. Biggest healthcare industry cyber attacks 2022-2023.

III. VULNERABILITIES IN E-HEALTH SYSTEM INFRASTRUCTURE

The rapid advancement and adoption of e-health systems have revolutionized healthcare delivery by integrating many digital technologies [26]. However, this evolution also brings numerous vulnerabilities within the e-health infrastructure. Compliance challenges also arise in the cloud environment, as healthcare providers must navigate complex regulations such as HIPAA to ensure that patient data is handled securely and per legal requirements [27]. This section delves into the specific security challenges posed by the core components of e-health systems, including cloud computing platforms, the Internet of Medical Things (IoMT), mobile health (mHealth) applications, and electronic health records (EHRs) [28].

A. CLOUD COMPUTING PLATFORMS

Cloud computing platforms provide scalable, flexible resources essential for managing healthcare data and performing complex analytics [29]. Despite their benefits, they introduce several vulnerabilities, as mentioned below:

Data Breaches: Cloud services can suffer from data breaches, where sensitive patient information is exposed [30]. These breaches are often a result of poor security practices, such as weak passwords or lack of multi-factor authentication.

Unauthorized Access: Misconfigured cloud services and weak authentication protocols can lead to unauthorized access to stored data [31]. Cybercriminals exploit these weaknesses using techniques such as:

- *Phishing*: Phishing attacks are characterized by sending bogus emails or messages that appear authentic [32]. These emails aim to deceive users into disclosing their login credentials on counterfeit websites or through other methods.
- *Keylogging*: Keyloggers are malicious software or hardware designed to record keystrokes entered by users, thereby capturing sensitive information like usernames and passwords [33].

- *Person-in-the-Middle (PITM) Attacks*: In PITM attacks, hackers intercept communication between two parties, capturing login credentials exchanged during the authentication process [34].
- *Brute Force Attacks*: In brute force attacks, attackers methodically attempt numerous combinations of usernames and passwords to access a system or account [35].
- *Credential Stuffing*: Attackers leverage credentials obtained from prior breaches to illicitly access additional accounts, exploiting instances where users have reused identical usernames and passwords [36].

Compliance Challenges: Navigating regulatory compliance in cloud environments is complex. Healthcare providers should verify that their cloud service providers comply with HIPAA laws, which mandate stringent data protection standards [37]. Inadequate compliance with these standards can cause significant legal repercussions and diminished trust [38].

B. ELECTRONIC HEALTH RECORDS (EHRS)

Electronic Health Records (EHRs) have become an integral part of the modern healthcare ecosystem, with their adoption reaching near-universal levels in many advanced nations [39], [40]. By 2024, the United States has achieved over 95% EHR implementation in non-federal acute care hospitals, exemplifying this trend. This widespread adoption has yielded significant benefits, including better coordination of care, fewer medical errors, and improved clinical decision-making support. However, the rapid shift towards digital health information has concurrently intensified security concerns associated with these systems. A primary challenge in EHR security is the escalating complexity of cyber threats [41]. Electronic Health Record (EHR) systems face other significant security challenges due to software vulnerabilities, phishing attacks, and insufficient access controls [42]. Many EHR systems operate on outdated software without current security patches, making them susceptible to exploitation [43]. Healthcare staff are often targeted by phishing attacks that trick them into revealing login credentials or installing malicious software, leading to data breaches [44]. Poorly implemented access controls can also allow unauthorized individuals to access sensitive patient information [45]. To maintain the security of EHR data, it is essential to regularly update software, enforce strict access policies, and conduct frequent audits. Healthcare institutions have experienced a notable increase in cyber-attacks, with cybercriminals targeting the vital nature of medical data for substantial financial gain. These breaches jeopardize patient confidentiality and can interrupt essential care services, potentially endangering lives. Furthermore, the advent of AI-enhanced hacking tools has simplified the process for malicious entities to detect and exploit EHR system vulnerabilities, necessitating the development of more sophisticated cybersecurity strategies. The quest for seamless data sharing across various healthcare systems and organizations introduces additional security risks for EHRs through interoperability challenges. As the network of data exchange points expands, so does the potential attack surface, requiring the implementation of strong encryption and secure data transmission protocols. Additionally, the growing emphasis on patient empowerment through access to their health records via online portals and mobile apps presents new security hurdles, as these access points must be safeguarded against unauthorized entry while maintaining user-friendliness.

C. INTERNET OF MEDICAL THINGS (IOMT)

The IoMT connects various medical devices and applications, enhancing patient care through real-time data collection and monitoring. However, it also introduces several security risks:

Device Vulnerabilities: Many IoMT devices are vulnerable to cyber attacks due to insufficient security protocols. For example, a compromised pacemaker or insulin pump can lead to dire consequences, potentially endangering patients' lives.

Data Interception: The wireless communication between IoMT devices and healthcare systems can be intercepted if not properly encrypted. Unauthorized interception of this data can lead to privacy breaches and manipulation of critical health information

Remote Attacks: IoMT devices, often lacking robust security features, can be susceptible to remote attacks. These attacks can disrupt the functionality of medical devices, potentially causing harm to patients who rely on them for critical health monitoring and treatment [46].

IV. THE ROLE OF HUMAN FACTORS IN E-HEALTH SECURITY AND THEIR IMPACT ON AI-DRIVEN CYBERSECURITY

Human factors in e-health security refer to the various human elements that influence the effectiveness of security measures, including user behavior, skills, decision-making, and the overall interaction between humans and technology. These factors play a critical role in determining the success or failure of cybersecurity efforts. In e-health systems, human factors encompass the actions and awareness of healthcare professionals, patients, and cybersecurity operators in maintaining security protocols, managing sensitive data, and responding to potential threats. The significance of human factors lies in their direct impact on the resilience of security systems. While advanced technologies like AI and automated tools help safeguard digital health systems, human behavior and decision-making often introduce vulnerabilities. Human vulnerabilities arise from user mistakes, exposing networks, hardware, and sensitive information to malicious threats. They constitute the most significant danger, mainly because of the increasing number of remote and mobile workers. Examples of human weaknesses in security involve opening email attachments laced with malware or failing to apply software updates on mobile devices. Another scenario is when sophisticated defenses are in place; a user's mistake, such as clicking on a phishing link or failing to update a password, can expose sensitive information. Hence, user skills, awareness, and the ability to make informed security decisions are crucial in defending against cyberattacks.

In crisis management, human factors are particularly critical. Cybersecurity professionals handle technical challenges and face immense psychological stress from continuous cyber threats. Their decision-making under pressure, ability to quickly adapt to new security threats, and understanding of AI-driven tools for incident management all play a vital role in maintaining the integrity of e-health systems. Ensuring that professionals are equipped with technical expertise and psychological resilience is critical to addressing the growing number of cyberattacks in healthcare environments.

Motivation, ability, and triggers influence behavior, making it crucial to foster strong cybersecurity habits among healthcare workers. Organizations can enhance cybersecurity by providing adequate training, tools, and prompts to guide behavior, improving resilience against cyber threats. This holistic approach to e-health security addresses the technical and human aspects necessary to secure modern healthcare systems. Some other cybersecurity challenges of the health sector are remote work security assurance, endpoint device management, human errors, the lack of security awareness, inadequate senior-level security risk assessment, inadequate business continuity plans, the lack of coordinated incident response, constraints on budget and resources, and vulnerability of medical systems. To address the challenges of human factors in e-health security, enhancing education and employee awareness is critical. A foundational step involves introducing essential cybersecurity awareness early in the educational system, with expert-led lectures, workshops, and academic collaborations to foster industry-relevant skills. Exposing students to real-world practices through internships can provide valuable, hands-on experience with security challenges. For healthcare employees, regular training sessions emphasizing best practices, such as recognizing phishing attacks and following company protocols, are essential. Organizations should introduce mandatory e-learning courses focused on security awareness, and advanced security policies should be implemented to ensure compliance and safeguard systems from evolving threats. These united efforts target creating a workforce attuned to security and capable of mitigating risks in the e-health environment through knowledge and skill. As healthcare systems increasingly adopt artificial intelligence and machine learning for sophisticated analytics and personalized medical treatments, new security paradigms become essential. These emerging frameworks must protect the sensitive underlying data. Moreover, complex algorithms and models process and interpret this vital health information.

V. AI-DRIVEN TECHNIQUES FOR THREAT DETECTION AND PREVENTION: SUPERVISED VS. UNSUPERVISED LEARNING

A. SUPERVISED LEARNING MODELS

In AI-driven threat detection and prevention, various models and techniques utilize machine learning and artificial intelligence to bolster security measures across various applications. Supervised learning models leverage labeled datasets to identify and categorize threats accurately. Techniques such as Machine Learning Classification, Signature-Based Detection, Behavioral Analysis, Deep Learning, Support Vector Machines (SVM), Random Forests, Logistic Regression, and Neural Networks are designed to detect known and evolving threats by learning from historical data and adapting to new patterns. These models excel in providing accurate threat detection and response by utilizing pre-labeled examples to train and refine their algorithms [47]. Table 2 below shows a Comparison of Supervised Learning Techniques in Threat Detection and Prevention.

Table 2 below shows a Comparison of Supervised Learning Techniques in Threat Detection and Prevention.

B. UNSUPERVISED LEARNING MODELS

On the other hand, unsupervised learning techniques operate without predefined labels, focusing on discovering hidden patterns and anomalies within datasets. Methods such as Anomaly Detection, Clustering, Dimensionality Reduction, Association Rule Learning, and User Behavior Analytics using k-nearest Neighbors (k-NN) are particularly valuable for identifying novel or unknown threats. By analyzing deviations from typical behavior, these techniques can uncover new and previously unknown security issues that might not be detectable using traditional methods. Together, these AI-driven approaches provide a robust framework for safeguarding systems against cyber threats, including phishing, malware, network intrusions, and insider attacks.

Table 3 below shows a Comparison of Unsupervised Learning Techniques in Threat Detection and Prevention.

VI. PRIVACY-PRESERVING AI TECHNIQUES IN E-HEALTH:

Privacy-preserving AI techniques are essential for protecting sensitive health data in e-health systems, ensuring confidentiality and security. Fundamental approaches, including federated learning (FL), differential privacy (DP), Data Anonymization (DA), Homomorphic Encryption (HE) and secure multiparty computation (SMPC), are recognized as practical solutions for maintaining data privacy while allowing for the analysis and sharing of medical information. These techniques are vital in healthcare, where regulations like GDPR and HIPAA prioritize patient data protection. This evaluation reviews the strengths and limitations of these methods and explores their potential applications in e-health systems [58].

A. FEDERATED LEARNING

Federated Learning (FL) permits multiple institutions, including hospitals and clinics, to train a machine learning model without transferring raw data. Instead, they share model updates, like gradients and weights, aggregated to improve the global model [59].

The FL process begins with initialization. A central server initializes the global model and distributes it to local clients,

TABLE 2. Comparison of supervised learning techniques in threat detection and prevention.

Technique	Description	Strengths	Weaknesses	Accuracy	Precision	Recall	F1-Score	False Positive Rate	Training Time	Memory Usage
Machine Learning Classification	Uses labeled data to train models that classify activities or data.	High accuracy with sufficient labeled data; can be very precise [48].	Requires large amounts of labeled training data; can be overfitted.	High (85-95%)	High (80-90%)	High (85-95%)	High (85-90%)	Low (5-10%)	Long	High
Signature-Based Detection	Relies on predefined patterns (signatures) of known threats [49].	Effective against known threats; low false positive rate.	Limited to known threats; requires constant updates.	Medium (70-80%)	High (80-90%)	Low (60-70%)	Medium (65-75%)	Very Low (<5%)	Short	Low
Behavioral Analysis	Trains models to recognize normal behavior patterns and flag deviations.	Can detect complex threats when trained properly; context-aware.	Requires substantial labeled behavior data; may have high computational needs.	High (85-95%)	High (80-90%)	Medium (70-80%)	High (80-85%)	Medium (10-15%)	Medium	Medium to High
Deep Learning	Uses labeled data to train neural networks for complex pattern recognition [50].	Can capture intricate patterns with high accuracy; scalable.	Computationally intensive; needs large amounts of training data.	Very High (90-99%)	Very High (90-95%)	Very High (90-95%)	Very High (90-95%)	Medium (5-10%)	Very Long	Very High
Anomaly Detection Using Support Vector Machines (SVM)	Classifies data as normal or abnormal based on features extracted from network traffic, user behavior, or system logs [51].	Effective for detecting anomalies in complex datasets; clear decision boundaries.	Requires a labeled dataset; might be sensitive to noisy data.	High (80-90%)	Medium (70-80%)	High (80-90%)	High (80-85%)	Medium (10-15%)	Long	High
Intrusion Detection Using Random Forests	Uses an ensemble of decision trees to classify network traffic or user activities as benign or malicious [52].	Aggregates multiple decision trees for robust detection; handles large datasets well.	Can be complex to interpret; model size can be large.	High (85-95%)	High (80-90%)	High (85-90%)	High (85-90%)	Low (5-10%)	Medium	Medium
Phishing Detection Using Logistic Regression	Analyzes email content, URLs, and metadata to classify messages as legitimate or phishing.	Simple and interpretable model; effective with good feature selection [53].	Limited by feature quality; may need to handle novel phishing tactics better.	Medium (70-80%)	High (80-90%)	Medium (70-80%)	Medium (70-75%)	Medium (10-15%)	Short	Low
Malware Detection Using Neural Networks	Uses deep learning models to detect malware by learning intricate patterns in system behaviors and file characteristics [54].	Captures complex patterns and behaviors; highly adaptable with large datasets.	Computationally intensive; requires substantial data and training time.	Very High (90-99%)	Very High (90-95%)	Very High (90-95%)	Very High (90-95%)	Medium (5-10%)	Very Long	Very High

such as hospitals. Each client then engages in local training, where the model is trained on its local dataset, and model updates are computed. These local updates are subsequently sent back to the central server for aggregation, typically using techniques like Federated Averaging. The central server incorporates the aggregated information into the global model. This iterative process continues for several rounds until the model converges.

FL offers several benefits. Keeping raw data localized reduces the risk of data breaches. The approach is well-suited for large datasets distributed across multiple locations and helps comply with data protection regulations like GDPR and HIPAA. However, there are challenges associated with FL. The frequent transmission of model updates can be bandwidth-intensive. Variability in data distribution and quality across clients can affect model performance.

TABLE 3. Comparison of unsupervised learning techniques in threat detection and prevention.

Technique	Description	Strengths	Weaknesses	Accuracy	Precision	Recall	F1-Score	False Positive Rate	Training Time	Memory Usage
Anomaly Detection	Identifies deviations from normal behavior without labeled data.	Can detect unknown threats; adaptive to new patterns.	May generate false positives; requires a baseline.	High (80-90%)	Medium (70-80%)	High (80-90%)	High (80-85%)	Medium (10-15%)	Medium	Medium
Clustering	Aggregates similar data points to uncover patterns and outliers [55].	Can discover hidden patterns; doesn't require labeled data.	May require tuning of parameters; may not always be intuitive.	Medium (70-85%)	Medium (75-85%)	Medium (70-80%)	Medium (75-80%)	Medium (10-20%)	Medium	Low to Medium
Dimensionality Reduction	Lowers feature count while preserving key information.	Reduces computational complexity; helps visualize and simplify data.	Can lead to loss of important information; requires careful interpretation.	Medium to High (75-90%)	Medium to High (75-90%)	Medium (70-85%)	Medium (80%)	Medium (15-20%)	Short	Low
Association Rule Learning	Finds relationships or associations between features.	Useful for discovering hidden patterns and correlations [56].	May produce too many rules; only some are actionable.	Medium (70-80%)	Medium (70-85%)	Medium (70-85%)	Medium (75%)	Medium (10-20%)	Short	Low
User Behavior Analytics Using k-NN	Monitors user activities and compares them with known patterns of normal and suspicious behavior using k-NN [57].	Simple to implement; effective with well-defined behavior patterns.	Requires labeled dataset for training; may struggle with high-dimensional data.	Medium to High (75-85%)	Medium to High (70-85%)	High (75-90%)	High (80-85%)	Medium (10-15%)	Long	High

Additionally, potential vulnerabilities in model updates could leak information if not properly secured.

B. DIFFERENTIAL PRIVACY:

Differential Privacy (DP) provides a mathematical framework to quantify and control the privacy risk of individuals when analyzing aggregate data [60]. It ensures that the output of a computation does not significantly change when any individual's data is added or removed. DP follows the below process:

Injecting random noise into the data or computation results, typically calibrated to the desired privacy level epsilon (ϵ). Carefully manages the privacy budget by ensuring that data analysis provides valuable insights while still protecting the privacy of individuals in the dataset. Algorithms such as the Laplace Mechanism (for numerical data) or the Exponential Mechanism (for categorical data) are used to add noise.

DP presents the following benefits:

Quantifiable Privacy: Provides a clear metric (ϵ) to balance privacy and data utility.

Strong Guarantees: Ensures that outputs do not reveal significant information about any individual.

Flexibility: Applicable to various data analysis tasks, including statistical analysis, machine learning, and data publishing. There are some challenges associated with DP, as seen below: High privacy levels can reduce the accuracy and utility of the data. Requires careful design to ensure appropriate noise addition. Effective utilization of the privacy budget is critical to maintaining utility over multiple queries.

C. SECURE MULTIPARTY COMPUTATION (SMPC)

Secure Multiparty Computation (SMPC) allows multiple parties to compute a function collaboratively while ensuring the privacy of their inputs. Each party only knows their input and the final output, with intermediate computations kept confidential [61].

The SMPC process begins with input sharing, where each party divides its input into multiple shares and distributes them to other parties. During joint computation, parties collaboratively perform calculations on the shared inputs without revealing their actual values. Techniques like secret sharing and homomorphic encryption are often used. Finally, the parties combine their shares of the result to reconstruct the final output in result reconstruction.

SMPC offers several benefits. It ensures privacy preservation by keeping individual data confidential throughout the computation. It guarantees against adversaries, as no single party can infer the complete input. SMPC applies to collaborative tasks like joint disease modeling, multi-center clinical studies, and shared data analysis.

However, there are challenges associated with SMPC. It can be resource-intensive, requiring significant computational power and time. Implementing SMPC protocols can be technically complex and requires careful coordination. Managing the computation and communication overhead can be challenging with many participants.

D. HOMOMORPHIC ENCRYPTION (HE)

Homomorphic Encryption enables calculations to be done on encrypted data without revealing its underlying content. This technique is beneficial in e-health systems, where sensitive patient data must often be processed on cloud-based AI systems. Homomorphic encryption safeguards data privacy by allowing computations to be performed directly on encrypted data. Even if an unauthorized party intercepts the encrypted data, it cannot extract any meaningful information without the decryption key. This approach provides a strong layer of privacy protection, particularly in environments where data is transmitted to third-party servers for processing. Data Anonymization techniques are commonly used to protect privacy in e-health systems by removing or obscuring personally identifiable information (PII) from patient datasets before they are used for AI training. This technique masks or removes sensitive personal details from datasets, making identifying the individuals associated with the information harder. Although data anonymization is not foolproof, especially when combined with other datasets, it remains a widely used method for mitigating privacy risks in AI systems. When paired with advanced methods like differential privacy or homomorphic encryption, anonymization can further enhance privacy protections in e-health applications.

E. DATA ANONYMIZATION (DA)

Data Anonymization involves removing or obscuring personally identifiable information (PII) from patient datasets before they are used in AI training, reducing the risk of identifying individuals. This process ensures that sensitive details, such as names, addresses, or medical IDs, are removed or altered. While anonymization is not foolproof, especially when data is combined with other datasets, it is widely used to mitigate privacy risks. Combined with techniques like Differential Privacy or Homomorphic Encryption, anonymization enhances privacy in e-health applications.

VII. SECURE MODEL DEPLOYMENT AND MANAGEMENT

Deploying and managing AI and machine learning models in e-health systems is crucial for safeguarding the security and privacy of sensitive health data [62]. Effective strategies in these areas can help mitigate potential risks and enhance the overall robustness of e-health systems. Here's an in-depth discussion on secure model deployment and management:

A. SECURE MODEL DEPLOYMENT

1) Environment Isolation:
   - Containerization and Virtualization: Use containerization (e.g., Docker) and virtualization (e.g., Kubernetes) to isolate models from other system components. This strategy minimizes the risk of security breaches spreading across different system parts.
   - Sandboxing: Deploy models in sandboxed environments to test their behavior in a controlled setting before full-scale deployment. This measure helps identify and mitigate any security vulnerabilities.
2) Access Controls:
   - Role-Based Access Control (RBAC): Implement RBAC to restrict access to the model and its data based on the user's role. This approach limits the accessibility to sensitive data and model modifications to authorized personnel only
   - Multi-Factor Authentication (MFA): Use MFA for accessing model deployment environments to add an extra layer of security.
3) Secure Communication:
   - Encryption: Use encryption (e.g., TLS/SSL) for data in transit to protect against interception and unauthorized access. Encrypt data at rest to ensure its confidentiality even if the storage medium is compromised.
   - API Security: Secure APIs through authentication mechanisms (e.g., OAuth) and ensure they are resilient to attacks, including SQL injection and cross-site scripting (XSS).
4) Compliance and Governance
   - Regulatory Compliance: Ensure model deployment adheres to healthcare regulations such as HIPAA, GDPR, and other relevant standards. This strategy includes maintaining data privacy and security and ensuring patient confidentiality.
   - Audit Trails: Maintain comprehensive logs of model access, changes, and usage to provide an audit trail for compliance and forensic analysis during a security incident.

B. SECURE MODEL MANAGEMENT

1) Model Integrity:
   - Version Control: Implement robust version control for models to track changes and roll back to previous versions if necessary [63]. This approach helps maintain model integrity and facilitates recovery in case of corruption or tampering.
   - Checksums and Digital Signatures: Use checksums and digital signatures to verify the integrity of models during deployment and updates, ensuring that they have not been altered maliciously.
2) Monitoring and Logging:
   - Continuous Monitoring: Monitor model performance and behavior in real-time to detect anomalies that may indicate security breaches or data corruption. Use automated tools to alert administrators of suspicious activities.
   - Detailed Logging: Maintain detailed logs of model predictions, inputs, and outputs to enable forensic

TABLE 4. The comparison of federated learning, differential privacy, secure multiparty computation, homomorphic encryption, and data anonymization.

Technique	Focus	Benefits	Challenges
Federated Learning	Privacy-preserving machine learning	Data Privacy, Collaboration, Privacy Preservation	Communication Overhead, Heterogeneous Data, Security Risks
Differential Privacy	Quantifying privacy risk in data analysis	Quantifiable Privacy, Strong Guarantees, Flexibility	Data Analysis Limitations, Utility vs. Privacy Trade-offs
Secure Multiparty Computation	Joint computation on private data	Privacy Preservation, Strong Guarantees, Applicability	Computational Overhead, Complex Protocols, Scalability
Homomorphic Encryption	Secure computations on encrypted data	Strong Privacy, Enables Computation on Encrypted Data	High Computational Costs, Performance Limitations
Data Anonymization	Removing identifiable information from data	Privacy Protection, Compliance with Data Regulations	Risk of Re-Identification, Reduced Data Utility

analysis and troubleshooting in the event of an issue.

3) Patch Management:
   - Regular Updates: Keep models and their deployment environments updated with the latest security patches and updates to protect against newly discovered vulnerabilities.
   - Automated Patching: Implement automated patch management tools to apply security updates without manual involvement quickly.
4) Data Privacy and Anonymization:
   - Data Minimization: Collect and use only the minimum data necessary for the model's purpose to reduce the potential impact of data breaches.
   - Anonymization and Pseudonymization: Apply techniques to anonymize or pseudonymize data before using it for model training and inference to protect patient identities.
5) Robust Testing:
   - Adversarial Testing: Conduct adversarial testing to evaluate and mitigate potential model vulnerabilities under various attack scenarios, such as adversarial examples or poisoning attacks.
   - Penetration Testing: Regularly perform penetration testing on the model deployment infrastructure to uncover security weaknesses and address them proactively.

VIII. ETHICAL AND REGULATORY CONSIDERATIONS FOR THE CYBERSECURITY OF E-HEALTH SYSTEMS:

The ethical principles of beneficence, non-maleficence, autonomy, and justice, which serve as cornerstones for ethical decision-making in healthcare, are equally applicable and essential in the realm of cybersecurity for e-health systems, where they can inform and guide the development of secure, patient-centered, and equitable digital health infrastructures [64]. Beneficence involves acting in the best interest of patients by ensuring their data is secure from breaches and cyber threats [65]. The principle of non-maleficence, which dictates the avoidance of harm, necessitates the implementation of rigorous cybersecurity measures to prevent data breaches and ensure the confidentiality, integrity, and availability of sensitive healthcare information, thereby safeguarding patients from potential harm and upholding the ethical obligations of healthcare providers in the digital era [66]. Autonomy respects patients' rights to make informed decisions by ensuring they know how their data is used and secured. Finally, justice promotes fairness and equity in healthcare by ensuring all patients receive equal data protection. Patient privacy and data security are crucial aspects of AI-driven healthcare, which relies on vast amounts of sensitive patient data, including EHRs, medical imaging, genetic information, and wearable device data. Ensuring the confidentiality, integrity, and availability of patient data is paramount. It can be achieved through comprehensive measures, including encrypting data both in transit and at rest, implementing role-based access controls to restrict sensitive information to authorized personnel, and conducting periodic security audits to identify and remediate vulnerabilities. These measures are essential for maintaining patient trust, upholding ethical standards, and adhering to regulatory requirements such as HIPAA [67].

AI algorithms in healthcare must be transparent and free from bias to ensure fairness and trust. Bias in algorithms can arise from imbalanced training data or flawed design. Addressing algorithm bias requires using diverse datasets to train AI models, regularly auditing algorithms for bias, and making algorithmic decisions understandable and explainable to patients and healthcare providers [68].

Informed consent is a fundamental principle in AI-driven healthcare. Patients have the right to be fully informed about the potential risks and benefits, enabling them to make educated decisions regarding their care. Also, healthcare professionals should inform patients about the limitations of AI technologies and be able to opt in or out of AI-driven interventions, which involves providing clear and comprehensive information about the AI technologies used in their care and establishing robust processes for obtaining and documenting informed consent [69].

AI-driven healthcare has the potential to exacerbate existing disparities in access to care. Ensuring equity involves identifying and addressing barriers to technology adoption among underserved populations, educating patients and healthcare providers about AI technologies, and designing AI solutions that are accessible to diverse patient populations.

The development and deployment of AI in healthcare necessitates the establishment of rigorous guidelines and standards to ensure adherence to ethical principles, privacy regulations, and existing healthcare laws. Moreover, robust accountability mechanisms must be instituted to hold developers and healthcare providers responsible for the ethical application of AI technologies, thereby promoting transparency, trust, and responsible innovation in the field.

Healthcare professionals require comprehensive training and education on AI-driven healthcare ethics, encompassing data privacy, algorithm bias, and patient consent, through integrated ethics education in healthcare curricula and targeted continuous professional development programs.

Fostering transparency, trust, and accountability in AI-driven healthcare requires inclusive engagement with patients, caregivers, advocacy groups, and other stakeholders through diverse representation in AI solution development and implementation, as well as open public discourse on the ethical considerations of AI in healthcare.

Maintaining patient confidentiality is fundamental to building trust in healthcare. Integrating e-health technologies introduces challenges in safeguarding patient information. Addressing these issues involves ensuring private settings for telehealth consultations, using up-to-date technology to minimize the risk of unauthorized access, and understanding and effectively addressing patient concerns through surveys.

Privacy breaches in e-health systems trigger regulatory responses and obligations. HIPAA imposes strict regulations to ensure the confidentiality and security of patient information, with non-compliance potentially incurring hefty penalties and irreparable harm to an organization's reputation. Ethical obligations include taking swift action in response to breaches, which may involve mandatory retraining and adhering to HIPAA's breach notification requirements.

Healthcare organizations must navigate an intricate regulatory environment to protect sensitive health information, adhering to stringent guidelines such as HIPAA and the HITECH Act, which mandate implementing cutting-edge cybersecurity measures and routine risk assessments to ensure compliance. It is also crucial to continuously update security practices and policies to address new threats and educate staff on their roles in protecting health information and meeting compliance requirements.

IX. FRAMEWORKS FOR AUTOMATING REGULATORY COMPLIANCE IN E-HEALTH SYSTEMS

Adherence to healthcare regulations is essential for safeguarding patient privacy and ensuring the ethical provision of care. However, maintaining compliance with continuously evolving regulations can be challenging. Non-compliance may result in severe penalties and reputational damage for healthcare providers. Artificial intelligence (AI) facilitates compliance by automating monitoring and reporting processes. Advanced algorithms can continuously analyze records and activities to ensure compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA). AI systems can identify anomalies and potential breaches in real-time, promptly notifying healthcare providers to implement corrective measures. The advantages of AI in compliance are substantial. Automated systems mitigate the risk of human error, ensure consistent adherence to regulations, and provide comprehensive audit trails. Healthcare organizations can avoid costly penalties and maintain patient trust by ensuring their operations consistently comply with regulations. Implementing a HIPAA-compliant audit trail system necessitates ongoing efforts, including continuous monitoring and regular reviews, to maintain compliance and enhance security measures. Automated alerts should be configured to detect suspicious or unauthorized activities, enabling immediate responses and investigations. Regular audits of audit trail data are crucial to identifying patterns or anomalies that could indicate a breach or non-compliance. It is imperative to keep audit trail policies and procedures updated to align with changes in technology, regulations, and organizational structure. Furthermore, organizations should periodically conduct incident response exercises to evaluate their ability to detect and address security incidents based on audit trail data. Implementing automated compliance training is another effective method for automating regulatory compliance in e-health systems. This approach utilizes technology to manage, monitor, and report employee training programs, ensuring staff remain current on regulations and complete necessary training. These systems streamline report generation, reminders, and progress tracking, reducing human error and conserving time. By automating compliance training, organizations can achieve consistent and efficient instruction, ensuring all employees receive uniform information while reducing costs associated with in-person training. Real-time tracking and reporting features also enhance compliance monitoring, allowing administrators to track progress and address gaps in understanding. Organizations should conduct a thorough needs analysis to implement automated compliance training effectively, select a scalable and user-friendly platform, create engaging training materials, and secure management support. Regular performance analysis and employee feedback collection ensure the program remains effective and can be improved over time. There are numerous advantages to automated compliance training, including improved scalability, cost savings, and compliance monitoring. Organizations can develop a comprehensive and efficient compliance training program that fulfills requirements and promotes long-term success by adhering to best practices and utilizing technology. The transformative potential of artificial intelligence (AI) in healthcare documentation and compliance is significant. AI is reshaping the healthcare landscape by enhancing accuracy and efficiency, streamlining compliance processes, optimizing revenue cycle management, and improving data security. As healthcare organizations continue to adopt AI, they can anticipate substantial improvements in operational efficiency, patient care, and regulatory adherence. The healthcare documentation and compliance future appear promising, with AI driving innovation and excellence. Healthcare providers should explore AI solutions, such as those offered by Thoughtful, to leverage these benefits fully. Embracing AI ensures improved outcomes and positions healthcare organizations at the forefront of technological advancement.

X. BLOCKCHAIN FOR DATA SECURITY: NOVEL TECHNOLOGIES IN E-HEALTH

Blockchain is a decentralized, distributed ledger technology that utilizes a cryptographically secure, transparent, immutable record-keeping system. It comprises a sequential series of blocks, each containing a validated list of transactions linked together through a unique digital fingerprint, creating a permanent and unalterable chain of data. The primary features of blockchain technology include decentralization, immutability, transparency and traceability, and security. In contrast to conventional databases that rely on a centralized authority for management and control, blockchain technology employs a decentralized architecture, wherein a distributed network of nodes collectively validates and confirms transactions, ensuring a secure, transparent, and consensus-driven process for data management and exchange. Data recorded on a blockchain is immutable, meaning that once it is written, it becomes a permanent and unalterable record, resistant to modification or deletion, ensuring the long-term integrity and authenticity of the information. Each block incorporates a unique digital signature, known as a cryptographic hash, of the preceding block, thereby establishing a secure and immutable link between consecutive blocks, which ensures the integrity and chronology of the entire blockchain. All transactions are visible to all participants in the network, ensuring transparency. This feature also allows for easy traceability of records. Blockchain uses cryptographic techniques and consensus algorithms to ensure data integrity and prevent unauthorized access [70].

A. USE CASES OF BLOCKCHAIN IN E-HEALTH

Blockchain technology has several applications in the healthcare sector, particularly in enhancing data security, interoperability, patient control, operational efficiency, and research capabilities. It addresses key challenges in securing health data through cryptographic security, decentralization, an immutable ledger, and fine-grained access control.

From a data security perspective, the immutable ledger inherent to blockchain technology guarantees that patient data, once recorded, becomes irreversibly fixed, rendering it impervious to tampering, alteration, or manipulation, thereby ensuring the integrity, confidentiality, and trustworthiness of sensitive healthcare information. Each health record is hashed and linked to the previous record, ensuring that any alteration would be immediately detectable. Blockchain uses advanced cryptographic techniques to protect data, with each block containing a cryptographic hash of the previous block, ensuring data integrity.

Blockchain technology enables the secure, interoperable, and efficient exchange of healthcare data across disparate systems, bridging the gaps in fragmented healthcare information and facilitating a unified, coordinated, and patient-centric approach to care. Authorized healthcare providers and patients can access health records stored on the blockchain, regardless of their systems, enhancing care coordination and reducing administrative burdens.

Another critical application is inpatient control. Through blockchain technology, patients are empowered to assume ownership and mastery over their personal health information, granting them the authority to selectively share or withhold access to their data, thereby fostering a secure, autonomous, and privacy-preserving environment for managing their sensitive medical records. Through self-sovereign identity solutions, patients can securely manage their health records and consent to data sharing. Blockchain allows for fine-grained access control, enabling patients and healthcare providers to manage permissions to access sensitive data.

Blockchain can also improve operational efficiency by automating various healthcare processes, reducing overhead, and improving accuracy. Smart contracts can automate insurance claims processing, supply chain management, and clinical trials [71]. For example, a smart contract can trigger a payment once a claim is verified, reducing processing time and errors.

Regarding research capabilities, blockchain can securely aggregate and anonymize health data from multiple sources, providing valuable insights. Blockchain-based data marketplaces can incentivize patients to share their data for research while maintaining their privacy and ownership rights. This aggregated data can be used to study disease patterns and treatment outcomes, informing public health strategies.

Decentralization is another benefit of blockchain in healthcare. Blockchain's decentralized architecture, which disperses data across many nodes, enhances its robustness and resistance to attacks by eliminating a single vulnerable point of failure, thereby providing a more secure and fault-tolerant system. Furthermore, the immutable characteristic of blockchain technology ensures that once data is recorded, it becomes tamper-proof and irreversible, thereby providing a secure, transparent, and indelible audit trail that maintains the integrity and authenticity of the recorded information [72]. Blockchain enables seamless exchange of healthcare information across different platforms by creating a standardized, decentralized infrastructure. This guarantees that patient data remains consistent and accessible across multiple systems, reducing fragmentation. Providers can securely share and retrieve accurate information in real time, enhancing care coordination without compromising data integrity. Blockchain reduces vulnerability to attacks by removing centralized points of failure and provides traceable, auditable records of access and transactions, enhancing both privacy and transparency in e-health systems.

AI significantly enhances blockchain's potential in healthcare by automating data analysis, predicting trends, and optimizing blockchain operations. For example, AI-driven algorithms can monitor healthcare data in real time, identifying potential security breaches or anomalies. AI can also help automate smart contracts, allowing healthcare transactions like insurance claims or data-sharing agreements to be processed more efficiently. Additionally, AI and machine learning can improve the scalability of blockchain by dynamically optimizing the network's performance, making it more adaptable to the large-scale data needs of healthcare systems. By integrating AI with blockchain, healthcare systems gain the ability to process vast amounts of data securely and efficiently while enhancing decision-making and predictive capabilities.

B. CHALLENGES AND CONSIDERATIONS

Despite its potential, integrating blockchain into e-health systems presents several challenges.

One of the primary issues is scalability. Blockchain networks can become slow and inefficient as the number of transactions increases. Sharding and off-chain transactions offer solutions to this issue.

Regulatory compliance is another significant challenge. Healthcare data is subject to strict regulations like HIPAA. Ensuring blockchain solutions comply with these regulations is critical to their successful implementation.

It is necessary to establish interoperability standards across different blockchain systems and existing healthcare IT systems for widespread adoption. Without these standards, seamless integration and communication between systems can be problematic [73].

Data privacy remains a concern. While blockchain ensures data integrity and security, maintaining patient privacy within a transparent ledger can be challenging. Zero-knowledge proofs and private blockchains provide solutions to this concern.

Finally, robust cybersecurity measures are required to protect blockchain networks from attacks such as 51% attacks and phishing. Maintaining the security and integrity of blockchain networks is crucial to upholding the trust, reliability, and confidentiality of healthcare solutions that leverage this technology, as any compromise could have significant consequences for patient data and the overall healthcare ecosystem.

XI. EXPLORING REAL-WORLD APPLICATIONS: AI AND ML-DRIVEN SECURITY IN E-HEALTH SYSTEMS

- AI-Assisted Robotic Surgery: Da Vinci Surgical System: The incorporation of AI-powered robotic systems in surgical procedures necessitates the implementation of comprehensive cybersecurity safeguards to safeguard sensitive patient information and maintain the integrity and security of surgical operations, thereby preventing potential disruptions or compromises. Data from pre-operative records and real-time surgical data are encrypted to avoid unauthorized access [74]. Implementing strict access controls ensures that only authorized personnel can operate or access the robotic systems. One of the primary cybersecurity challenges is network security. Ensuring secure network connections is crucial to prevent cyber-attacks during surgeries. Protecting robotic systems from malware and other cyber threats that could disrupt surgical procedures is essential to maintaining system integrity. Lessons learned from these challenges highlight the importance of continuous security monitoring. Implementing AI-driven security tools that utilize anomaly detection algorithms to continuously monitor the network and robotic systems for vulnerabilities and potential threats is crucial to identify activities that may indicate a security breach. Automated penetration testing is another key lesson. Utilizing AI to conduct regular automated penetration testing can uncover and address security weaknesses in robotic systems. Training and awareness are also critical. Developing AI-based training programs that simulate cyber-attacks and teach healthcare professionals about best cybersecurity practices can enhance their preparedness and response to potential threats.
- Nursing Assistants: Care Angel's Virtual Nurse Assistant Virtual nursing assistants rely on continuous data exchange between patients and healthcare systems, necessitating robust data protection mechanisms. All communications between patients and virtual assistants are encrypted to protect sensitive health information. Multi-factor authentication (MFA) provides an additional layer of security, ensuring that only verified and authorized individuals can gain access to the virtual assistant services. The cyber security challenges for the above case study include ensuring patient trust by safeguarding personal health information (PHI) from breaches and protecting the system from denial-of-service (DoS) attacks that could disrupt patient care. The lessons learned from the above challenges include utilizing advanced encryption standards (AES) to secure data transmission and storage and Keeping the virtual assistant software and security protocols updated to defend against emerging threats.
- AI in Clinical Judgment and Diagnosis: Stanford University's AI Algorithm for Skin Cancer Detection. AI algorithms for clinical diagnosis handle vast amounts of patient data, requiring comprehensive cybersecurity measures to ensure data integrity and confidentiality and implementing secure data storage solutions to protect sensitive diagnostic information. Using cryptographic hash functions to ensure the integrity of diagnostic data. The cyber security challenges for the above case study lack ways to prevent unauthorized access to sensitive patient information used for AI training and diagnosis and protect AI models from adversarial attacks that could compromise diagnostic accuracy. The lessons

learned from the above challenges include anonymizing patient data before using it for AI training to protect privacy, implementing secure access protocols, and monitoring for unusual access patterns to detect potential breaches [75].

- Workflow and Administrative Tasks: Cleveland Clinic and IBM Watson Partnership: AI-driven automation of administrative tasks involves handling patient records and other sensitive information, necessitating robust cybersecurity measures. This consists of encrypting administrative data to protect it from unauthorized access during processing and implementing role-based access controls (RBAC) to limit access to authorized personnel. The cyber security challenges for the above case study involve ensuring compliance with data privacy regulations such as HIPAA and ensuring that AI systems are resilient against cyber threats that could disrupt administrative functions. Key takeaways from the challenges mentioned above include the importance of continuous monitoring, adherence to data privacy regulations, and developing and implementing strong incident response plans to swiftly address any security breaches [76].
- Analysis in MIT's Machine-Learning Algorithm for 3D Scans AI-driven image analysis processes large volumes of medical imaging data, requiring comprehensive cybersecurity measures to protect data integrity and confidentiality [77]. This case study involved anonymizing imaging data before analysis to protect patient privacy and ensure secure transmission of imaging data between systems. The cyber security challenges for the above case study involved ensuring that imaging data is not altered or tampered with during analysis and implementing continuous monitoring and real-time alert systems to detect and respond to security threats. Lessons learned from the MIT Machine-Learning Algorithm for 3D Scans include the critical importance of anonymizing imaging data to protect patient privacy and ensure secure transmission between systems. The case study also highlights the need for continuous monitoring and real-time alerts to detect and address any potential tampering during analysis. These insights emphasize the necessity of robust cybersecurity measures to maintain data integrity and confidentiality in AI-driven image analysis.

XII. LARGE LANGUAGE MODELS IN HEALTHCARE

Over the past year, large language models (LLMs) have attracted considerable attention. As interest in generative artificial intelligence (AI) and LLMs grows, healthcare software providers are exploring how to integrate this technology into their clinical applications. Large language models (LLMs) utilize advanced computational artificial intelligence (AI) algorithms to generate text that mimics human language. Trained on extensive text data from sources like the internet, these models can answer questions, provide summaries, and offer translations [78].

LLMs hold significant potential in various areas of medicine due to their ability to process complex concepts and respond to diverse prompts. However, these models also present challenges, including misinformation, privacy concerns, biases in training data, and potential misuse. As we delve deeper into the role of Large Language Models (LLMs) in healthcare, it is crucial to understand their transformative impact on the industry. The advent of healthcare LLMs has propelled us beyond simple data analysis, ushering in an era where AI can generate human-like text based on the information it has been trained on.

A. TRANSFORMATIONAL EFFECT OF LARGE LANGUAGE MODELS IN HEALTHCARE

Large Language Models (LLMs) and generative AI hold transformative potential for healthcare and medical practices. Technologies like reinforcement learning from human feedback (RLFH), few-shot learning, and chain-of-thought reasoning offer significant advancements. A PubMed study emphasizes the need for guidance on integrating these technologies into healthcare.

For example, LLMs can enhance clinical note summarization, achieving higher accuracy and enabling healthcare professionals to review and understand complex clinical documents efficiently. These capabilities elevate AI's utility over traditional rule-based systems, fostering collaboration among clinicians, patients, and other stakeholders [79].

Several prominent large language models (LLMs) are widely recognized for their advanced capabilities in natural language processing. Among these, GPT-4 by OpenAI stands out for its impressive text generation and comprehension abilities. Google's contributions include Gemma, Gemini 1.5 Pro, PaLM, and BERT, each excelling in various applications such as translation, summarization, and question-answering. Anthropic's Claude v1 offers robust performance in understanding and generating human-like text. Meta's Llama 2 is another notable model for its efficiency and accuracy. Stability.ai has developed Stable LM 2, which generates stable and coherent text outputs. Lastly, Mistral AI's Mistral 7B is recognized for its scalability and precision in handling large datasets. These LLMs represent the forefront of AI technology, driving innovation and enhancing various applications across industries.

Innovation in data acquisition, fine-tuning LLMs, prompt engineering, LLM evaluation, and system implementation are essential to harness the full benefits of these technologies. Proactive engagement with LLMs can improve healthcare service quality, patient safety, and efficiency while adhering to ethical and legal guidelines.

B. USE CASES OF LLMS IN E HEALTHCARE SYSTEMS

LLMs play a crucial role in various healthcare tasks, including clinical documentation, medical research, and patient care, as seen below [80]:

Virtual Medical Assistants: LLM-powered AI assistants enhance telemedicine by understanding patient queries, providing medication reminders, offering health information, and answering medical questions, thereby improving patient engagement.

Clinical Documentation and Electronic Health Records: LLMs efficiently summarize extensive patient notes and medical histories, saving time and enhancing accuracy. This allows healthcare providers to focus more on personalized patient care. Large language models can also be privately trained on a facility's structured data to achieve higher accuracy.

Adverse-Event Detection: LLMs can automate the detection of adverse events from electronic health record data, supporting drug safety surveillance in the post-marketing setting.

Automated Drafting and Response Suggestion: LLMs assist in drafting medical emails by providing content suggestions, formatting help, and generating text, saving time and improving the quality of written communications. They also suggest short responses or actions for incoming emails, enhancing communication efficiency within healthcare teams.

Brainstorming and Idea Generation: LLMs facilitate brainstorming sessions by offering creative ideas and generating new concepts based on input, providing diverse perspectives, and aiding in evaluating new healthcare strategies and solutions.

Translation and Localization: LLMs translate medical documents and text from one language to another, breaking down language barriers and facilitating global collaboration in healthcare operations and patient care.

Content Creation: LLMs quickly create engaging healthcare-related blog articles by understanding the context, style, and tone of the desired content, helping to disseminate medical information and updates efficiently.

C. CHALLENGES OF IMPLEMENTING LLMS IN HEALTHCARE

High Cost and Resource Consumption: The development and maintenance of LLMs entail substantial financial and logistical investments. These models are costly, requiring significant computational resources and advanced hardware. The training process can span several months, placing a heavy burden on healthcare facilities. Despite these expenses, the versatility of LLMs, which allows them to be repurposed for various tasks, offers a valuable return on investment. The advantages of these models must be balanced against their significant expenses and substantial resource requirements.

Bias and Ethical Concerns: LLMs have the potential to inadvertently propagate biases embedded in their training data, including those related to race, gender, and religion. In healthcare settings, fairness and accuracy are paramount; such biases can lead to unjust or incorrect outcomes. Addressing these ethical concerns requires a meticulous approach during the training and deployment phases. Continuous monitoring and intervention are necessary to identify and mitigate potential harms, ensuring that AI systems contribute positively to patient care [81].

Importance of Rigorous Testing: Thorough evaluation of LLMs is essential to guarantee their safe and reliable operation, enabling the detection and mitigation of potential weaknesses and biases. Adversarial testing involves challenging models with complex or misleading data and helps uncover weaknesses and guide improvements. This proactive approach is crucial for revealing current failures and informing strategies such as fine-tuning, implementing model safeguards, or applying filters. By addressing these vulnerabilities, healthcare systems can enhance the reliability and performance of AI-driven applications.

Privacy and Data Security: The deployment of LLMs in healthcare raises significant concerns regarding privacy and data security. Handling sensitive patient information demands robust data-sharing protocols to protect individual privacy and comply with regulations such as HIPAA and GDPR. Additionally, implementing explainable AI techniques is critical to maintaining transparency and trust in AI-driven healthcare solutions. Building trust in AI technologies requires secure patient data management and transparent AI systems, fostering confidence in their use.

Over-Reliance on AI: While AI technologies can significantly enhance decision-making processes, over-reliance on these tools can have adverse effects. AI outputs may occasionally need to be more accurate, and uncritical acceptance of these results could negatively impact patient care. Maintaining the human element in patient care is vital, with AI serving as a supportive tool rather than a replacement for professional judgment. Ensuring that healthcare professionals retain ultimate responsibility for patient decisions is essential for maintaining high standards of care [82].

XIII. EMERGING TRENDS IN AI-DRIVEN CYBERSECURITY FOR E-HEALTH

The e-health sector is transforming through AI-powered cybersecurity, bolstering data protection, elevating patient care, and safeguarding the reliability of health information systems. The integration of AI in e-health cybersecurity is accelerating, giving rise to innovative trends redefining the digital healthcare security landscape.

One of the most impactful trends is continuous monitoring, where AI systems are utilized to provide 24/7 threat detection by analyzing network traffic and system logs for anomalies. This constant vigilance is exemplified by anomaly detection using machine learning algorithms, which enables real-time identification and response to potential threats, thereby enhancing the security posture of e-health systems [83].

Advanced pattern recognition is another critical development, with AI demonstrating the ability to identify complex patterns that traditional rule-based systems might miss. Techniques like intrusion detection using Random Forests and phishing detection with Logistic Regression showcase

AI's advanced pattern recognition capabilities, leading to earlier and more accurate threat detection.

The ability to offer real-time threat response is a significant strength of AI systems. These systems can analyze and respond to threats immediately, reducing the window of vulnerability. Automated countermeasures triggered by anomaly detection illustrate this strength, allowing for swift defensive actions that mitigate potential damage.

Predictive analytics represents another emerging trend: AI analyzes past data to predict future threats. This proactive approach enables healthcare organizations to anticipate attack patterns and vulnerabilities, allowing for implementing preventative measures that enhance cyber resilience and maintain operational continuity even during an attack.

Increased Efficiency and Improved Accuracy are achieved through machine learning algorithms that continuously learn and refine their threat detection capabilities over time. Automated anomaly classification, response actions, and constantly updated detection models exemplify this efficiency and accuracy, leading to more streamlined and reliable threat management.

The scalability of AI systems is crucial for efficiently handling extensive data volumes, making AI particularly suitable for complex healthcare networks. This scalability allows for the practical analysis of vast network traffic and system logs, ensuring that AI systems can manage and process data regardless of size.

Flexibility in AI techniques further enhances their application in cybersecurity. AI's adaptability allows for using different algorithms tailored to various threats, such as network intrusion detection, phishing, and malware detection. This versatility is essential for addressing a wide range of cybersecurity challenges.

AI's capacity to adaptively learn and detect novel patterns transforms how security threats are identified and managed in e-health systems. AI enhances cybersecurity threat detection, containment, and response by constantly adapting to new data, streamlining the workload of Security Operations Center (SOC) analysts, and enabling them to concentrate on higher-level responsibilities [84].

The global market for AI-driven cybersecurity tools is expected to grow significantly, reflecting increasing recognition of AI's potential to enhance security measures. This growth, with projections indicating an increase of $19 billion between 2021 and 2025, underscores the importance of AI in the healthcare sector.

Regulatory developments, such as the NIS 2 Directive proposal, are set to impact the healthcare sector by mandating comprehensive security measures [85]. This regulatory push will likely drive further adoption of AI-driven cybersecurity solutions to ensure compliance and enhance security infrastructure.

Mobile technology and smart devices are increasingly integrated into healthcare, presenting opportunities and challenges. Emerging applications include skin disease detection through mobile apps, diabetes management, fall detection in the elderly, and fitness tracking. These innovations highlight the need for robust policies and regulations to guide their use and ensure equitable access.

AI is also making strides in medical imaging and diagnostics, which is crucial for cybersecurity, given the sensitivity of patient data. AI algorithms enhance image analysis for early disease detection and support remote monitoring in areas with limited healthcare access. Additionally, deep learning and predictive analytics are transforming disease detection and treatment, with AI models improving cancer detection and cardiovascular and pulmonary health through advanced data analysis.

In conclusion, AI-driven cybersecurity is poised to significantly enhance the e-health sector by improving data security, patient care, and operational efficiency. As these technologies evolve, they will play an increasingly vital role in safeguarding healthcare systems and ensuring the integrity of sensitive health information.

XIV. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES IN AI-DRIVEN CYBERSECURITY FOR E-HEALTH

The fusion of AI and e-health cybersecurity is an emerging and dynamic domain, holding vast promise for groundbreaking advancements and enhancements. Future research and development in this area can focus on several key areas to enhance healthcare systems' security, efficiency, and resilience.

Advanced threat detection and response systems are at the forefront of this evolution. Designing algorithms that can evolve through continuous learning is essential, allowing them to stay ahead of emerging threats and adjust to new attack strategies, thereby maintaining effective cybersecurity measures. Another vital aspect is behavioral analysis, where AI systems analyze user behavior to identify real-time anomalies and potential security breaches. Creating automated incident response systems that autonomously mitigate threats is also essential for minimizing the impact of cyber attacks. Additionally, dynamic security protocols that adapt to new threats and vulnerabilities, using AI to update security measures continuously, are vital for maintaining robust defenses.

Quantum-resistant encryption is a promising research area, focusing on AI-based methods to protect patient data against future quantum computing threats. Innovations in data anonymization techniques are also important; AI algorithms that anonymize patient data in real time can ensure privacy while preserving data utility for research and analysis.

In privacy-preserving AI techniques, federated learning approaches allow AI models to learn from decentralized data without compromising patient privacy. Integrating differential privacy mechanisms ensures that individual patient data cannot be reverse-engineered from AI models. Exploring homomorphic encryption can enable computations on encrypted data, maintaining confidentiality throughout the process.

AI for regulatory compliance is another critical area. Automated compliance monitoring systems can continuously track adherence to regulatory standards such as HIPAA, GDPR, and the NIS 2 Directive. Policy-adaptive systems that adjust to changes in regulatory policies without manual intervention and risk assessment models to evaluate and mitigate compliance risks are essential for ensuring ongoing adherence to regulations.

Secure data interoperability is fundamental for effective e-health systems. Investigating blockchain integration for immutable records of data transactions can enhance data integrity and traceability. Developing standardization protocols for consistent data formats ensures seamless interoperability between different healthcare systems. Implementing AI techniques for data anonymization enables secure data sharing for research while preserving patient privacy.

Ethical AI development must be prioritized to ensure the responsible use of AI in healthcare. Research on bias mitigation methods will help address and reduce biases in AI models, promoting equitable treatment across diverse patient populations. Developing transparent AI systems that offer clear insights into decision-making processes can foster trust and accountability. Establishing comprehensive ethical guidelines will be essential for ensuring patient safety, privacy, and informed consent.

Collaborative research initiatives are vital for addressing complex challenges. Promoting interdisciplinary collaboration among healthcare professionals, AI researchers, cybersecurity experts, and policymakers can drive innovative solutions. Encouraging public-private partnerships can leverage shared expertise and resources, while global cooperation will help develop international standards and share best practices in AI-driven e-health cybersecurity.

AI in telemedicine and remote care presents unique opportunities and challenges. Designing secure telehealth platforms with AI-driven security measures will protect patient-provider interactions. Developing AI systems for secure remote monitoring of patients using wearable devices and IoT technologies can enhance data collection and analysis. Implementing AI tools for emergency response in remote care settings can improve patient safety and outcomes.

Education and workforce development are crucial for successfully integrating AI into e-health cybersecurity. Creating specialized cybersecurity training programs for healthcare professionals will enhance their understanding of AI-driven tools and practices. Promoting AI literacy among providers will enable informed decision-making and effective use of AI technologies. Research fellowships and grants can support innovative projects and drive further advancements.

Finally, evaluation and benchmarking are essential for assessing the effectiveness of AI-driven cybersecurity solutions. Developing standardized performance metrics and conducting benchmarking studies will help identify best practices. Performing longitudinal studies to evaluate the long-term impact of AI-driven measures on healthcare delivery and patient outcomes will provide valuable insights into their effectiveness.

By focusing on these emerging trends and research opportunities, AI-driven cybersecurity for e-health can continue evolving, improving healthcare systems' security and resilience worldwide.

XV. CONCLUSION

Integrating AI into the security of e-health systems presents transformative potential for enhancing the protection of sensitive health data and ensuring the resilience of healthcare infrastructures. The discussion highlighted several key areas where innovation, collaboration, and advancement can significantly impact e-health cybersecurity.

Innovative AI-driven security solutions can revolutionize threat detection and response, providing real-time protection and adaptive security protocols. These advancements will reduce response times and mitigate damage from cyber threats, ensuring that healthcare providers can maintain secure environments for patient data.

Collaboration across sectors is essential for successfully implementing AI in e-health cybersecurity. Public-private partnerships, interdisciplinary cooperation, and international collaboration will facilitate sharing best practices, threat intelligence, and the development of global security standards. This collective effort will strengthen the cybersecurity posture of healthcare systems worldwide.

Research and development in AI and cybersecurity education, ethical AI development, and scalable security solutions will advance secure e-health systems. Regular training and adherence to ethical standards will ensure that AI technologies are developed and utilized in a way that prioritizes responsibility, addresses potential biases, and maintains the highest level of patient privacy. New business models and services such as Security-as-a-Service (SaaS) and patient-centric security solutions will make advanced cybersecurity accessible to all healthcare providers and empower patients to manage their health data security. These innovations will create more efficient and effective care delivery models, enhancing overall health outcomes. Regulatory compliance and policy development will be crucial in maintaining the integrity of e-health systems. Automated compliance checks and policy-adaptive AI systems will reduce administrative burdens and ensure continuous adherence to evolving regulations. Engaging with policymakers to advocate for supportive regulations will further promote the safe and ethical use of AI in healthcare.

REFERENCES

[1] D. K. Ahern, J. M. Kreslake, J. M. Phalen, and B. Bock, "What is eHealth (6): Perspectives on the evolution of eHealth research," *J. Med. Internet Res.*, vol. 8, no. 1, p. e4, Mar. 2006.

[2] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Telemedicine for healthcare: Capabilities, features, barriers, and applications," *Sensors Int.*, vol. 2, Jul. 2021, Art. no. 100117.

[3] C. O. Alenoghena, A. J. Onumanyi, H. O. Ohize, A. O. Adejo, M. Oligbi, S. I. Ali, and S. A. Okoh, "EHealth: A survey of architectures, developments in mHealth, security concerns and solutions," *Int. J. Environ. Res. Public Health*, vol. 19, no. 20, p. 13071, Oct. 2022.

[4] A. Borgeaud, "CAGR on cybersecurity spending globally 2019–2026, by industry," *Statista*, vol. 1, pp. 1–18, Apr. 6, 2019.

[5] J. Yang. *Healthcare Cybersecurity Spending Globally 2023*. Accessed: Aug. 08, 2024. [Online]. Available: https://www.statista.com/statistics/1359081/cybersecurity-spending-in-healthcare-sector-worldwide

[6] *Telehealth and Health Information Technology in Rural Healthcare Overview*. Accessed: Aug. 01, 2024. [Online]. Available: https://www.ruralhealthinfo.org/topics/telehealth-health-it

[7] M. D. Iturry, S. N. Alves-Souza, M. Ito, and S. A. da Silva, "Data quality in health records: A literature review," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Chaves, Portugal, Jun. 2021, pp. 1–6, doi: 10.23919/CISTI52073.2021.9476536.

[8] S. Colantonio, D. Conforti, M. Martinelli, D. Moroni, F. Perticone, O. Salvetti, and A. Sciacqua, "An intelligent and integrated platform for supporting the management of chronic heart failure patients," in *Proc. Comput. Cardiol.*, vol. 4594, Sep. 2008, pp. 897–900, doi: 10.1109/CIC.2008.4749187.

[9] S. Adibi, "The mPOC framework: An autonomous outbreak prediction and monitoring platform based on wearable IoMT approach," *Future Internet*, vol. 15, no. 8, p. 257, Jul. 2023.

[10] E. N. Volkov and A. N. Averkin, "Explainable artificial intelligence in clinical decision support systems," in *Proc. IV Int. Conf. Neural Netw. Neurotechnologies (NeuroNT)*, Jun. 2023, pp. 3–6.

[11] S. Mohammed, T.-H. Kim, R.-S. Chang, and C. Ramos, "Guest editorial: Data analytics for public health care," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 4, pp. 1409–1410, Apr. 2022, doi: 10.1109/JBHI.2022.3159347.

[12] V. Sandulescu, S. Pucoci, M. Petre, M. Dumitrache, V. Bota, and A. Garlea, "MHealth application for remote health monitoring useful during the COVID 19 pandemic," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Lausanne, Switzerland, Jun. 2021, pp. 1–6.

[13] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical dilemmas and privacy issues in emerging technologies: A review," *Sensors*, vol. 23, no. 3, p. 1151, Jan. 2023, doi: 10.3390/s23031151.

[14] *Healthcare Data Breach Statistics*. Accessed: Jul. 28, 2024. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[15] Assistant Secretary for Public Affairs (ASPA). (2023). *HHS' Office for Civil Rights Settles Ransomware Cyber-attack Investigation*. Accessed: Jul. 28, 2024. [Online]. Available: https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html

[16] R. Chataut, Y. Usman, and F. Scholl. (2024). *Unveiling Cyber Threats: A Comprehensive Analysis of Connecticut Data Breaches Paper*.

[17] D. R. Farringer, "Maybe if we turn it off and then turn it back on again? Exploring health care reform as a means to curb cyber attacks," *J. Law, Med. Ethics*, vol. 47, no. S4, pp. 91–102, Dec. 2019, doi: 10.1177/1073110519898046.

[18] R. Ong, "Factors affecting patient and public perceptions of the adoption of electronic health record sharing: A Hong Kong study," *Int. J. Med. Informat.*, vol. 178, Oct. 2023, Art. no. 105193, doi: 10.1016/j.ijmedinf.2023.105193.

[19] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-Healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2018, doi: 10.1109/ACCESS.2017.2767561.

[20] (2022). *Summary of the HIPAA Privacy Rule*. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[21] J. Bajwa, U. Munir, A. Nori, and B. Williams, "Artificial intelligence in healthcare: Transforming the practice of medicine," *Future Healthcare J.*, vol. 8, no. 2, pp. e188–e194, Jul. 2021, doi: 10.7861/fhj.2021-0095.

[22] S. A. Alowais, S. S. Alghamdi, N. Alsuhebany, T. Alqahtani, A. I. Alshaya, S. N. Almohareb, A. Aldairem, M. Alrashed, K. B. Saleh, H. A. Badreldin, M. S. A. Yami, S. A. Harbi, and A. M. Albekairy, "Revolutionizing healthcare: The role of artificial intelligence in clinical practice," *BMC Med. Educ.*, vol. 23, no. 1, p. 689, Sep. 2023, doi: 10.1186/s12909-023-04698-z.

[23] M. Nankya, R. Chataut, and R. Akl, "Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies," *Sensors*, vol. 23, no. 21, p. 8840, Oct. 2023, doi: 10.3390/s23218840.

[24] (2024). *Leveraging AI and Machine Learning for Robust Cybersecurity in Healthcare*. Accessed: Apr. 19, 2024. [Online]. Available: https://emag.medicalexpo.com/leveraging-ai-and-machine-learning-for-robust-cybersecurity-in-healthcare/

[25] A. Wolf. (2024). *Biggest Healthcare Industry Cyber Attacks*. Accessed: Aug. 08, 2024. [Online]. Available: https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/

[26] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," *ICT Exp.*, vol. 9, no. 4, pp. 571–588, Aug. 2023, doi: 10.1016/j.icte.2023.02.007.

[27] (20, 2022). *Summary of the HIPAA Security Rule*. Accessed: May 23, 2024. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[28] P. Mishra and G. Singh, "Internet of Medical things healthcare for sustainable smart cities: Current status and future prospects," *Appl. Sci.*, vol. 13, no. 15, p. 8869, Aug. 2023, doi: 10.3390/app13158869.

[29] S. Sachdeva, "Unraveling the role of cloud computing in the health care system and biomedical sciences," *Heliyon*, vol. 10, no. 7, pp. 1–24, 2024.

[30] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-Health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[31] R. Chataut, Y. Usman, and F. Scholl. (2024). *Unveiling Cyber Threats: A Comprehensive Analysis of Connecticut Data Breaches*. [Online]. Available: https://peer.asee.org/unveiling-cyber-threats-a-comprehensive-analysis-of-connecticut-data-breaches

[32] A. Alhammad, M. M. Yusof, and D. I. Jambari, "A review of cyber threats to medical devices integration with electronic medical records," in *Proc. Int. Conf. Cyber Resilience (ICCR)*, vol. 13089, Dubai, United Arab Emirates, Oct. 2022, pp. 1–6, doi: 10.1109/iccr56254.2022.9995984.

[33] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. Ahmad Khan, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[34] A. Guerra. (2023). *HC3 Breaks Down Types of Actors Threatening Healthcare*. Accessed: May 23, 2024. [Online]. Available: https://healthsystemcio.com/2023/06/09/hc3-breaks-down-types-of-actors-threatening-healthcare/

[35] K. Taylor, A. Smith, A. Zimmel, K. Alcantara, and Y. Wang, "Medical device security regulations and assessment case studies," in *Proc. IEEE 19th Int. Conf. Mobile Ad Hoc Smart Syst. (MASS)*, Denver, CO, USA, Oct. 2022, pp. 742–747, doi: 10.1109/MASS56207.2022.00116.

[36] *Credential Stuffing Attack Exposed United Healthcare Member Data*. [Online]. Available: https://www.hipaajournal.com/credential-stuffing-attack-exposed-united-healthcare-member-data/

[37] (2023). *HIPAA Network Compliance and Security Requirements Explained*. Accessed: May 23, 2024. [Online]. Available: https://www.algosec.com/resources/hipaa-compliance/

[38] (2019). *What is an Electronic Health Record (EHR)?*. Accessed: May 23, 2024. [Online]. Available: https://www.healthit.gov/faq/what-electronic-health-record-ehr

[39] A. Alanazi. (2023). *Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats*.

[40] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Digital healthcare–cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations," *IEEE Access*, vol. 10, pp. 12345–12364, 2022, doi: 10.1109/ACCESS.2022.3145372.

[41] *The Impact of Social Engineering on Healthcare*. Accessed: May 23, 2024. [Online]. Available: https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf

[42] S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)—An overview," in *Proc. 5th Int. Conf. Devices, Circuits Syst. (ICDCS)*, Mar. 2020, pp. 101–104, doi: 10.1109/ICDCS48716.2020.243558.

[43] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and cloud–fog–edge architectures," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100887, doi: 10.1016/j.iot.2023.100887.

[44] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Prospect of Internet of Medical things: A review on security requirements and solutions," *Sensors*, vol. 22, no. 15, p. 5517, Jul. 2022, doi: 10.3390/s22155517.

[45] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informat. J.*, vol. 22, no. 2, pp. 177–183, Jul. 2021, doi: 10.1016/j.eij.2020.07.003.

[46] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[47] V. Gupta, V. K. Mishra, P. Singhal, and A. Kumar, "An overview of supervised machine learning algorithm," in *Proc. 11th Int. Conf. Syst. Model. Advancement Res. Trends (SMART)*, Moradabad, India, Dec. 2022, pp. 87–92, doi: 10.1109/SMART55829.2022.10047618.

[48] D. Savchuk and A. Doroshenko, "Investigation of machine learning classification methods effectiveness," in *Proc. IEEE 16th Int. Conf. Comput. Sci. Inf. Technol. (CSIT)*, vol. 1, Sep. 2021, pp. 33–37, doi: 10.1109/CSIT52700.2021.9648582.

[49] H. Holm, "Signature based intrusion detection for zero-day attacks: (Not) a closed chapter?" in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 4895–4904, doi: 10.1109/HICSS.2014.600.

[50] H. Shahinzadeh, A. Mahmoudi, A. Asilian, H. Sadrarhami, M. Hemmati, and Y. Saberi, "Deep learning: A overview of theory and architectures," in *Proc. 20th CSI Int. Symp. Artif. Intell. Signal Process. (AISP)*, Feb. 2024, pp. 1–11, doi: 10.1109/aisp61396.2024.10475265.

[51] K. Tscharke, S. Issel, and P. Debus, "Semisupervised anomaly detection using support vector regression with quantum kernel," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, vol. 3, Bellevue, WA, USA, Sep. 2023, pp. 611–620, doi: 10.1109/qce57702.2023.00075.

[52] M. Choubisa, R. Doshi, N. Khatri, and K. Kant Hiran, "A simple and robust approach of random forest for intrusion detection system in cyber security," in *Proc. Int. Conf. IoT Blockchain Technol. (ICIBT)*, Ranchi, India, May 2022, pp. 1–5, doi: 10.1109/ICIBT52874.2022.9807766.

[53] V. Vajrobol, B. B. Gupta, and A. Gaurav, "Mutual information based logistic regression for phishing URL detection," *Cyber Secur. Appl.*, vol. 2, Jun. 2024, Art. no. 100044.

[54] S. Shinde, A. Dhotarkar, D. Pajankar, K. Dhone, and S. Babar, "Malware detection using efficientnet," in *Proc. Int. Conf. Emerg. Smart Comput. Informat. (ESCI)*, Mar. 2023, pp. 1–6, doi: 10.1109/ESCI56872.2023.10099693.

[55] E. Abdelfattah and S. Joshi, "Comparison of machine learning classification and clustering algorithms for TV commercials detection," *IEEE Access*, vol. 11, pp. 116741–116751, 2023, doi: 10.1109/access.2023.3325888.

[56] O. Sharma, K. Mehta, and R. Sharma, "Significant support (SISU): A new interest measure in association rule mining," in *Proc. Int. Conf. Comput. Perform. Eval. (ComPE)*, Dec. 2021, pp. 153–156, doi: 10.1109/ComPE53109.2021.9752100.

[57] M. H. Shaikh, K. J. Ho, and F. Mustafa, "K-nearest neighbor based association data mining in healthcare correlated data systems," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1119–1122, doi: 10.1109/ICTC55196.2022.9952466.

[58] R. Torkzadehmahani, R. Nasirigerdeh, D. B. Blumenthal, T. Kacprowski, M. List, J. Matschinske, J. Spaeth, N. K. Wenke, and J. Baumbach, "Privacy-preserving artificial intelligence techniques in biomedicine," *Methods Inf. Med.*, vol. 61, no. S 01, pp. e12–e27, Jun. 2022, doi: 10.1055/s-0041-1740630.

[59] X. Gu, F. Sabrina, Z. Fan, and S. Sohail, "A review of privacy enhancement methods for federated learning in healthcare systems," *Int. J. Environ. Res. Public Health*, vol. 20, no. 15, p. 6539, Aug. 2023, doi: 10.3390/ijerph20156539.

[60] A. Nguyen. (2024). *Understanding Differential Privacy*. [Online]. Available: https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a

[61] (2024). *Leverage Secure Multi-Party Computation (SMPC) for Machine Learning Inference in RS-FMRI Datasets*. Accessed: Jun. 2, 2024. [Online]. Available: https://techcommunity.microsoft.com/t5/healthcare-and-life-sciences/leverage-secure-multi-party-computatin-smpc-for-machine/ba-p/4057703

[62] E. Zvorni. (2023). *How To Version Control Data in ML for Various Data Sources*. [Online]. Available: https://neptune.ai/blog/data-versioning-control-for-various-data-sources

[63] N. Narendra. *Version Control for Machine Learning*. [Online]. Available: https://dagshub.com/blog/version-control/

[64] L. Weidener and M. Fischer, "Proposing a principle-based approach for teaching AI ethics in medical education," *JMIR Med. Educ.*, vol. 10, Feb. 2024, Art. no. e55368, doi: 10.2196/55368.

[65] F. Li, N. Ruijs, and Y. Lu, "Ethics & AI: A systematic review on ethical concerns and related strategies for designing with AI in healthcare," *AI*, vol. 4, pp. 28–53, Dec. 2023.

[66] C. Hine, R. Nilforooshan, and P. Barnaghi, "Ethical considerations in design and implementation of home-based smart care for dementia," *Nursing Ethics*, vol. 29, no. 4, pp. 1035–1046, Jun. 2022, doi: 10.1177/09697330211062980.

[67] R. Nowrozy, K. Ahmed, A. S. M. Kayes, H. Wang, and T. R. McIntosh, "Privacy preservation of electronic health records in the modern era: A systematic survey," *ACM Comput. Surveys*, vol. 56, no. 8, pp. 1–37, Aug. 2024.

[68] C. Elendu, D. C. Amaechi, T. C. Elendu, K. A. Jingwa, O. K. Okoye, M. J. Okah, J. A. Ladele, A. H. Farah, and H. A. Alimi, "Ethical implications of AI and robotics in healthcare: A review," *Medicine*, vol. 102, no. 50, Dec. 2023, Art. no. e36671, doi: 10.1097/md.0000000000036671.

[69] K. Astromske, E. Peicius, and P. Astromskis, "Ethical and legal challenges of informed consent applying artificial intelligence in medical diagnostic consultations," *AI Soc.*, vol. 36, no. 2, pp. 509–520, Jun. 2021, doi: 10.1007/s00146-020-01008-9.

[70] A. A. Mamun, S. Azam, and C. Gritti, "Blockchain-based electronic health records management: A comprehensive review and future research direction," *IEEE Access*, vol. 10, pp. 5768–5789, 2022, doi: 10.1109/ACCESS.2022.3141079.

[71] C. A. F. B. Triana, E. P. Guillén, and W. M. R. Reales, "Smart contracts on the management of EHR: Review, challenges, and future directions," in *Proc. 6th Int. Conf. Syst. Rel. Saf. (ICSRS)*, Venice, Italy, Nov. 2022, pp. 318–323, doi: 10.1109/ICSRS56243.2022.10067426.

[72] M. Prokofieva and S. J. Miah, "Blockchain in healthcare," *Australas. J. Inf. Syst.*, vol. 23, pp. 1–24, Jul. 2019.

[73] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *Int. J. Healthcare Manage.*, vol. 15, no. 1, pp. 70–83, Jan. 2022, doi: 10.1080/20479700.2020.1843887.

[74] K. Reddy, P. Gharde, H. Tayade, M. Patil, L. S. Reddy, and D. Surya, "Advancements in robotic surgery: A comprehensive overview of current utilizations and upcoming frontiers," *Cureus*, vol. 1, p. 21, Dec. 2023.

[75] (2024). *AI Improves the Accuracy of Skin Cancer Diagnoses in Stanford Medicine-led Study*. [Online]. Available: https://med.stanford.edu/news/all-news/2024/04/ai-skin-diagnosis.html

[76] *Cleveland Clinic and IBM Unveil Landmark 10-Year Partnership To Accelerate Discovery in Healthcare and Life Sciences*. Accessed: Aug. 1, 2024. [Online]. Available: https://newsroom.ibm.com/2021-03-30-Cleveland-Clinic-and-IBM-Unveil-Landmark-10-Year-Partnership-to-Accelerate-Discovery-in-Healthcare-and-Life-Sciences

[77] R. Matheson. (2018). *Faster Analysis of Medical Images*. Accessed: Aug. 1, 2024. [Online]. Available: https://news.mit.edu/2018/faster-analysis-of-medical-images-0618

[78] X. Yang, A. Chen, N. PourNejatian, H. C. Shin, K. E. Smith, C. Parisien, C. Compas, C. Martin, A. B. Costa, M. G. Flores, Y. Zhang, T. Magoc, C. A. Harle, G. Lipori, D. A. Mitchell, W. R. Hogan, E. A. Shenkman, J. Bian, and Y. Wu, "A large language model for electronic health records," *Npj Digit. Med.*, vol. 5, no. 1, p. 194, Dec. 2022.

[79] H. Ali, J. Qadir, Z. Shah, T. Alam, and M. Househ, "ChatGPT and large language models (LLMs) in healthcare: Opportunities and risks," *TechRxiv*, vol. 1, pp. 1–14, Jul. 2023.

[80] S. Sai, A. Gaur, R. Sai, V. Chamola, M. Guizani, and J. J. P. C. Rodrigues, "Generative AI for transformative healthcare: A comprehensive study of emerging models, applications, case studies, and limitations," *IEEE Access*, vol. 12, pp. 31078–31106, 2024, doi: 10.1109/access.2024.3367715.

[81] *Ethical and Regulatory Challenges of Large Language Models*. Accessed: Aug. 1, 2024. [Online]. Available: https://www.thelancet.com/journals/landig/article/PIIS2589-7500

[82] *AI Overreliance is a Problem. Are Explanations a Solution?*. Accessed: Aug. 1, 2024. [Online]. Available: https://hai.stanford.edu/news/ai-overreliance-problem-are-explanations-solution

[83] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," *Cogent Eng.*, vol. 10, no. 2, pp. 1–24, Dec. 2023, doi: 10.1080/23311916.2023.2272358.

[84] G. Author. (15, 2024). *The Role of AI in Healthcare Cybersecurity: Enhancing Threat Detection*. Accessed: Aug. 1, 2024. [Online]. Available: https://www.healthcareittoday.com/2024/02/14/the-role-of-ai-in-healthcare-cybersecurity-enhancing-threat-detection/

[85] E. Biasin and E. Kamenjasevic, "Cybersecurity of medical devices: New challenges arising from the AI act and NIS 2 directive proposals," *Int. Cybersecurity Law Rev.*, vol. 3, no. 1, pp. 163–180, Jun. 2022, doi: 10.1365/s43439-022-00054-x.

MARY NANKYA (Member, IEEE) received the Bachelor of Science degree in computer science from Makerere University, Uganda, in 2016, the Master of Science degree in computer science from Fitchburg State University, USA, in 2023. Currently, she is a Visiting Professor with the Computer Science Department, Fitchburg State University, where she is teaching courses, such as computer science II (CSC 1550) and advanced programming (CSC 7131). In addition to her academic role, she is the Data and Evaluation Manager with Hearth Inc. Her research interests include AI, 6G network evolution, machine learning, cyber defense mechanisms, industrial control systems, threat incidents, and vulnerabilities. She holds a membership at the Greater Boston Evaluation Network and American Association of University Women with a commitment to empowering women in technology. Her dedication and accomplishments in the field were recognized when she received the National Conference for College Women Student Leader Scholarship in 2023. Her passion for technology and community impact led her to be honored with the Grace Hopper Women in Computing Scholarship in Houston, TX, USA, in 2015. She was awarded the AnitaB.org Advancing Inclusion Faculty Scholarship, in April 2023. Furthermore, she received the Silver Award from Orange Community Innovations Awards, Uganda, in 2015, for her notable contributions to innovation.

ALLAN MUGISA received the bachelor's and M.B.A. degrees from Salem State University, MA, USA, and the Ph.D. degree in business administration (technology entrepreneurship) from Walden University. He is currently a seasoned Financial Planning Analyst with Maine General Health. As a Senior Financial Planning Analyst, he is instrumental in conducting financial analysis and planning activities that bolster the organization's financial well-being and advance its strategic initiatives. His expertise is enhanced by his Six Sigma Yellow Belt Certification, which underscores his commitment to process improvement and operational efficiency. His research interests include diverse and encompassing foreign trade, supply chain management, business process improvement, and enterprise solutions. He is particularly focused on harnessing the power of artificial intelligence (AI) and machine learning (ML) technologies within these domains. Additionally, he is deeply interested in emerging technologies, such as blockchain and their potential applications across various industries and business contexts. He is a member of HFMA.

YUSUF USMAN (Member, IEEE) received the B.Sc. degree in computer science from ESGT University, Benin. He is currently pursuing the master's degree in cybersecurity with Quinnipiac University, Hamden, CT, USA. He was a Cyber Security Analyst with the National Assembly of Nigeria and an IT Support Specialist/Sales Representative with Lamido-Tex NIG Ltd., Nigeria. These diverse roles have solidified his foundation in networking, cloud network design, operating system security, and business. He is a Graduate Research Assistant of cybersecurity with Quinnipiac University. His research interests include cybersecurity, exploring ML and AI techniques for phishing detection, automated attack and defense strategies, malware detection, and autonomous vehicle security. He has authored and co-authored several research articles on these topics. As an Active Member of ASEE, IEEE, and BSides CT, he brings diverse experience from business and security roles, pioneering AI-driven security solutions. He holds professional certifications, such as AWS Certified Security—Specialty, CompTIA CASP+, and PenTest+.

AADESH UPADHYAY received the Bachelor of Engineering degree in electrical and electronics engineering from the Sri Krishna College of Engineering and Technology, Coimbatore, India. He is currently pursuing the Master of Science degree in computer science with the University of North Texas, TX, USA. He is a Graduate Research Assistant with the University of North Texas. His research interests include machine learning and large language models for cybersecurity applications, particularly in developing detection mechanisms for cybercrimes, like phishing and spam. Additionally, he is actively engaged in exploring the potential of generative AI models for proactive defense strategies against emerging cyber threats.

ROBIN CHATAUT (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the University of North Texas. He is currently an Assistant Professor of computer science with the College of Science and Engineering, Texas Christian University. His research interests include a wide spectrum of topics, with a primary focus on cybersecurity, network security, wireless communication and networks, and emerging technologies, such as 5G, 6G, and beyond networks. In addition to these areas, he is deeply passionate about the application of machine learning (ML) and artificial intelligence (AI) techniques in cybersecurity and network optimization.