IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 May 2024, accepted 29 May 2024, date of publication 5 June 2024, date of current version 21 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3410035

SURVEY

Digital Privacy in Healthcare: State-of-the-Art and Future Vision

SHALAKA S. MAHADIK[1], (Student Member, IEEE), PRANAV M. PAWAR[1], (Member, IEEE), RAJA MUTHALAGU[1], NEELI RASHMI PRASAD[2], (Senior Member, IEEE), SIN-KUEN HAWKINS[3], (Senior Member, IEEE), DIMITRIS STRIPELIS[4], (Member, IEEE), SREEDHAR RAO[5], (Senior Member, IEEE), PETER EJIM[6], AND BRUCE HECHT[7], (Senior Member, IEEE)

[1]Birla Institute of Technology and Science Pilani, Dubai Campus, Dubai, United Arab Emirates
[2]SmartAvatar, 1101 CB Amsterdam, The Netherlands
[3]Future Directions, IEEE Technical Activities, Piscataway, NJ 08854, USA
[4]FedML Inc., Sunnyvale, CA 94085, USA
[5]Snowflake Inc., Seattle, WA 94117, USA
[6]Reda Consulting LLC, Manasquan, NJ 08736, USA
[7]VG2PLAY, Brookline, MA 02142, USA

Corresponding author: Pranav M. Pawar (pranav@dubai.bits-pilani.ac.in)

ABSTRACT The article draws inspiration from IEEE Digital Privacy, which explores attaining privacy goals for individuals in the digital realm. Privacy is an umbrella term that equates to respect for an individual's dignity. When it integrates with digital technology, it alludes to individuals' right and authority to control the flow of their personally identifiable information (PII) on the digital platform. Adopting digital technology in healthcare is not novel, but the COVID-19 outbreak has accelerated its incorporation into healthcare. Digital technology perks a wide range of healthcare professions, including biomedicine, diagnostic imaging, and remote patient monitoring, to mention a few, through facilitating accurate and effective health-related decisions. Thanks to technological advancements, healthcare professionals and other medical personnel are now quickly accessing and retaining patient information, which aids in scouring for optimal and swiftly acted-upon medications. While the technology's inception is positive, it raised privacy issues for patients' PII and other sensitive health data that remain intact. The review article addresses the key challenges in digital privacy for healthcare while also reviewing the state-of-the-art work by investigating data encryption techniques, access control mechanisms, and risk assessment techniques with digital privacy as a primary concern. Every country has enacted resilient laws and regulations to protect digital privacy in healthcare, which are briefed in the article. Artificial intelligence (AI) has proven valuable in cybersecurity and healthcare technology growth. As a result, the article delves into the hurdles of employing AI for healthcare digital privacy and cutting-edge work in healthcare digital privacy using AI. Finally, the article concludes with a future vision of data privacy in healthcare.

INDEX TERMS Digital privacy, healthcare, artificial intelligence, challenges, data privacy.

I. INTRODUCTION

A. ABOUT PRIVACY AND ITS IMPORTANCE

The liberty and willingness to regulate the exposure of personally identifiable information (PII), such as name, phone number, email address, date of birth, bank details, etc., are enshrined in the scope of *privacy*. The term additionally alludes to the individual's authority to control when, how, and why outsiders use their PII. Nowadays, personal information is regularly collected surreptitiously, automatically, and remotely without consent. Attorneys and individuals sometimes fail to clarify the importance of privacy. They perceive privacy breaches as annoyances, whereas privacy is significantly more critical. Because invading an individual's

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

privacy can result in reputational harm, humiliation, mental suffering, fake identities, monetary loss, and other negative consequences. Privacy protection is vital to preserving human dignity, safety, and independence. It allows individuals to develop their distinctive traits independently [1], [2], [3], [4]. Failure to respect the right to privacy may have societal ramifications as well. It can erode an individual's confidence and lead to a lack of motivation to cooperate with the government. For government entities, this might include failures of programs, projects, and operations and the public objectives they aspire to achieve [5]. According to The New York Times, Cambridge Analytica, a political firm, utilized people's private information for political campaigns, which violates their privacy without their knowledge [6]. There is no ideal solution that addresses the privacy concern. It is a fluid scenario that will fluctuate with individual feelings. Everyone strives for a certain degree of privacy, confidentiality, and isolation. Nobody wants their passwords, family money, personal relationship details, medical history, location, purchases, or private chats made public [7]. Many countries have essential legislation to safeguard the privacy of individuals and data, such as the California Privacy Rights Act (CPRA), China's Personal Information Protection Law (PIPL), the Swiss Revised Federal Act on Data Protection (FADP), and the Australian Privacy Act 1988. However, reassuring individuals that their information and privacy are trustworthy is still challenging.

B. DIGITAL PRIVACY AND ITS TYPES

Digital privacy resembles ensuring the confidentiality and privacy of individuals' PII while using digital devices, technologies, and online services. Digital technologies like the internet-of-things (IoT), eShoping, eTradings, eBanking, eEducation, and eSocial-media, to name a few, are developing to help the community whereas, on the other hand, such development leads to *ePrivacy*, also referred as *digital privacy* as one of the primary concern. In today's digitized world, most people don't realize how much data their digital apps and devices gather, analyze, or trade, infringing on digital privacy [8]. Every individual's actions and judgment significantly impact the digital landscape. Their digital fingerprints are witnessed everywhere they explore and visit by revealing their location, latest updates, and likes or dislikes. Every click they make, every file, application, and device they use generates it. When such data is aggregated, it can yield incredibly significant insights about them or the community. If such digital information is exposed, it creates a new goldmine for the black-digital market, sparking a destructive struggle that puts the privacy of digital information at risk. In short, tracking, hacking, and trading are among the top three privacy issues presented in Fig. 1. Additionally, Fig. 1 highlighted three types of digital privacy, including information privacy, individual privacy, and communication privacy [9]. The digital privacy types and issues are interrelated terms that eventually influence

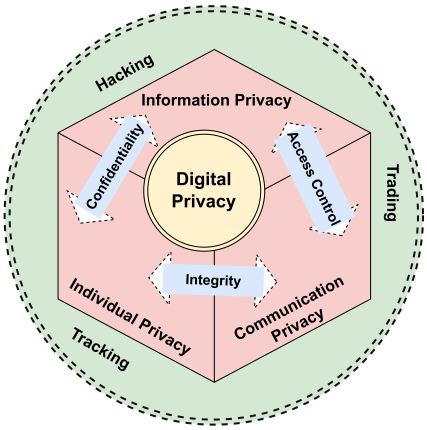

FIGURE 1. Digital privacy types and issues.

confidentiality, integrity, and access control, i.e., CIA, which are the main pillars of digital privacy and are addressed more below.

- *Information privacy* refers to a person's ability to manage how their digital information, specifically PII, is accessed and utilized. Countries like the European Union (EU) have a wide range of privacy regulations that control how each organization or corporation legally collects and uses personal data online without violating people's privacy. Some countries oblige organizations and websites to provide individuals with notice and consent before collecting their PII. However, these policies are not always effectively supervised, allowing websites to deceive users and violate their digital privacy rights. E.g., TikTok, a social networking app, collects user data without the user's awareness, raising concerns about the application being used by the government to snoop on its citizens and therefore highlighting the issue of digital privacy [10], [11].
- *Communication privacy* refers to the right to secure digital communication, which includes texts, emails, and video calls, and ensures that communications are only exposed to the sender's intended recipient. However, in the digital era, hacking techniques can intercept or send communications to unintended recipients without the sender's knowledge. This notion necessitates consideration of technological methods, their effectiveness, and the creation of new technologies, including laws and regulations, to assure digital communication preservation [9], [12].
- *Individual privacy* in the context of digital privacy refers to the freedom to exist freely on the internet, to choose information exposure, and to avoid unwelcome disruptions. When people receive unwelcome adverts, emails, or malware, they are allowing their privacy to be infringed upon by raising the question of digital privacy [9].

In reality, privacy is restricted in the digital age, but individuals can proactively preserve it by being aware of the most recent technological developments, adhering to

ethical standards, and being alert. To maintain an individual's digital privacy, various precautions need to be taken, such as using strong passwords, two-way authentication, data encryption, and exercising vigilance while disclosing PII online. Many corporations, including Facebook, Google, and Amazon, protect PII held in their systems with various levels of privacy protection. Moreover, a person's right to privacy in the digital realm can also be protected by adhering to relevant regulations and standards. Privacy legislation, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) of 2018, assists organizations in treating digital privacy with care by explicitly outlining their privacy practices and how they maintain information [13]. This legislation ensures people have the right to review, update, or have their data erased from any databases an organization may maintain on them.

C. DIGITAL PRIVACY MODEL

Professionals in technology and privacy need simple and reliable mechanisms by which individuals may articulate clear objectives toward their privacy expectations in any given setting. The IEEE Digital Privacy Model (DPM) is an evolving visual representation of the many shifting aspects of digital privacy. The approach centers on the user, their expectations for privacy, and the factors that affect online privacy regardless of location. By utilizing Confidentiality & Integrity, as well as Access & Observability of individuals' Identities, Behaviors, Inferences, and Transactions in any digital ecosystem to represent digital privacy for individuals, this evolving model shows how Technical, Regulatory, Economic, Legislative, Legal, Individual, Societal & Cultural influences on individuals' expectations of privacy are more attainable. The DPM creates a secure digital privacy structure/system by combining six privacy expectations and seven significant impacts, as shown in Fig. 2. Businesses, government agencies, and other interested parties can use it to identify areas of weakness and develop strategies to address them all, without regard to the industry or country in which they operate. The framework promotes communication and collaboration across departments to create a secure digital environment [14]. As stated in DPM and illustrated in Fig. 2, the six characteristics of privacy expectations are:

- *Identities*: All distinguishing characteristics unique to specific persons.
- *Behaviors*: Sequences of actions exhibited by individuals within economic or social contexts.
- *Inferences*: Inferences attributed to individuals by human or AI/ML algorithms.
- *Transactions*: Individual exchanges in physical or virtual contexts, spanning any social or economic situation.
- *Confidentiality and Integrity*: Protecting the privacy and trustworthiness of individual transactions, identities, behaviors, and inferences.
- *Access and observation*: Encouraging individuals to access and observe the identities, behaviors, inferences, and transactions about themselves.

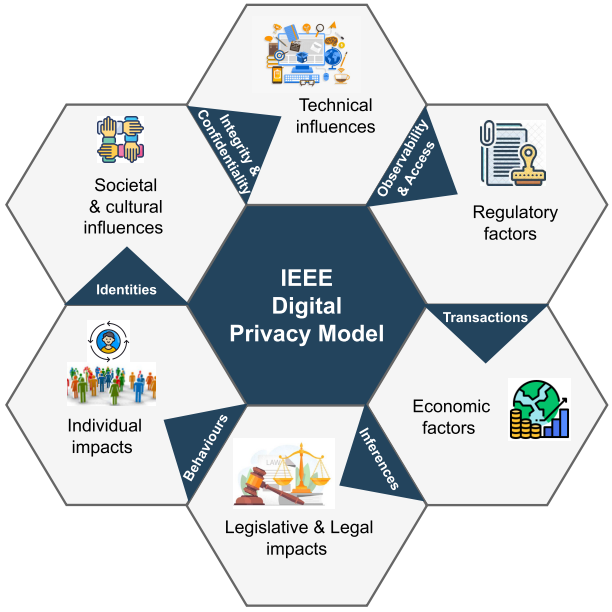

FIGURE 2. IEEE digital privacy model [14].

Furthermore, any actor engaged in managing the digital privacy expectations of an individual must take into account:

- *Technical* factors, that are the foundation for establishing technical and business standards for solutions that fulfill privacy demands.
- *Regulatory* factors that dictate business rules, government supervision, and compliance with privacy regulations.
- *Economic* factors that influence enterprise and individual decisions to attain optimal digital privacy outcomes.
- *Legislative* actions that aid in identifying concerns and codifying laws affecting privacy concerns.
- *Legal* actions that establish legal rules for checks and balances to maintain privacy demands.
- *Individuals* and their actions that set privacy limits, since they are the primary subjects of data and metadata in every digital ecosystem.
- *Societal and cultural* factors that influence beliefs that acknowledge and shape an individuals privacy expectations.

Although the IEEE DPM put forward a secure framework for digital privacy with explicit expectations and influential elements, digital privacy faces certain hurdles in the context of digital ecosystems. Next, the segment looks into the challenges of digital privacy.

D. CHALLENGES IN DIGITAL PRIVACY

It's becoming increasingly apparent that the right to privacy is at odds with the ability to collect massive amounts of information through various forms of digital media. More and more business, government, and societal & cultural activities are occurring online, heightening the significance of PII and related data. Over time, governments and multinational corporations have amassed a wealth of data about our daily

activities for research purposes [15]. According to Forbes, until 2020, every individual generated 1.7 gigabytes of new data each second through the digital world, but in the future year, it is expected to rise from 4.4 zettabytes to 44 zettabytes, or 44 trillion gigabytes [16]. Such `Big data` poses challenges like data storage, data management, and data security [17] while preserving the digital privacy of individuals. The responsible organization or entity must face colossal revenue loss if such data is breached. Hence, the maintenance cost of such digital data is also high and becoming a rising concern. Individuals' fictitious authority over PII limits privacy as sovereignty. Profitable companies frequently exploit large volumes of sensitive information without authorization. This information can be used in many ways, some of which are good and some of which are detrimental to individuals, too, not just the community. Sometimes, more explicit national or international regulation is required to establish what types of uses of PII are legal and appropriate and obliging organizations to obtain authorization.

Smartwatches, connected cars, and automated farms are just a few examples of how the Internet of Things (IoT) has improved people's daily lives and made them more sustainable. However, IoT devices are more vulnerable to security threats, and manufacturers are also not releasing their vulnerability updates rapidly, posing another barrier to the CIA and, ultimately, to the digital privacy context [18].

As mentioned by [19], Poor handling of information (a.k.a., information privacy), intercepting (a.k.a., individual privacy), and location tracking (a.k.a., communication privacy) are some ways in which individuals' privacy is compromised digitally. Many people now regularly use social media platforms, including Facebook, Instagram, LinkedIn, Snapchat, and TikTok. They are very comfortable with sharing their precise location with friends and family. It's lovely to tell loved ones about important moments in your life, but this may bring in additional viewers. Information gathered in this way is persistently stored by social media analytics. Apps like Google Maps that constantly pry into individuals' `location information` pose privacy risks and must be used with prudence [20]. An Austrian law student seeking personal information on one social network received 1224 pages of images, texts, and publications he thought erased. The site collected more PII than expected and stored unnecessary and deleted data as well [19]. Such cases make it even more challenging to enact rules and regulations that effectively tackle such social media platforms, ultimately risking digital privacy.

`Web cookies` [21], which are utilized by web servers, can store PII such as credit card numbers and names, posing another difficulty threatening individuals' online privacy by making it digitally vulnerable. Web bugs [21] are small transparent image files placed on web pages and used to track users' online activities. It is possible to couple web bugs' information with cookies' information to identify individuals' profiles. The conveyance of PII on a global scale is another source of concern that pulls digital privacy into question. In May 2023, EU officials fined Meta $1.3 billion for disobeying EU digital privacy norms by preserving and exporting Facebook users' PII to the U.S [11]. Individuals' Sensitive information gets leaked even if privacy measures are in place. The preceding discussion shows that, despite rigorous laws and regulations such as GDPR, digital privacy requires more stringent `compliance with regulations`. Fig. 3 depicts the challenges to digital privacy outlined in this subsection.

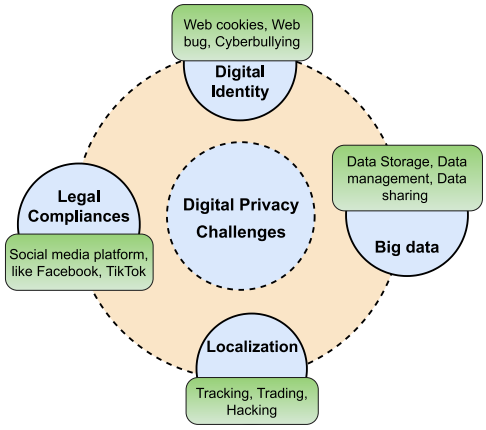

FIGURE 3. Challenges in digital privacy.

E. DIGITAL PRIVACY IN HEALTHCARE AND ITS IMPORTANCE

"Shifting physical hospital buildings to wherever patients are…" Gains in technological innovation have created new options to boost existing healthcare infrastructure by serving more significant portions of the world's population. The COVID-19 pandemic has significantly impacted individuals' perceptions of their health. The COVID-19 outbreak accelerated the introduction of digital innovations in healthcare. Digital technology helps the healthcare sector by providing services like online patient monitoring, teleconference clinics, and vaccination booths. These services help in maintaining social distancing and reducing infectious spread [22], [24].

Healthcare organizations investigated novel approaches toward patient care and safety. The healthcare industry, encompassing various sectors such as mHealth (mobile health), the wearable device market, telemedicine, telehealth services, health information technology, and customized healthcare, has increasingly relied on technological advancements to transition from focusing on emergency treatment to a preventive medicine approach. Significant transformation marks the forthcoming year, as multiple developments are expected. There has been a noticeable rise in the prevalence of innovative technologies and healthcare solutions.

The Internet of Medical Things (IoMT) is an ideal instance of a fast-growing technology that has enabled the development of a wide variety of innovative digital health applications, including but not limited to heart monitoring,

TABLE 1. Examples of recent security breaches within the healthcare sector [25].

Year	Name of the Organization	Number of Impacted data	Brief about commonly breach information or patients' sensitive data	Reason for privacy breaches
May-20	Trinity Health	3.3 million	-Patients PII like name, social security numbers,	- Ransomware attack on data store on third party server
Mar-22	Shields Healthcare Group	2 million	Birth data, including health data like Medial record numbers,	- Network server attack
Jan-22	Broward Health	1.3 million	Patient IDs, lab reports, Diagnosis Information,	- Third-party service provider, lack of Multi-factor authentication
Feb-22	Morley Companies	521,046	medical insurance details, doctors details	- Ransomware attack on data store on third party server
Mar-22	L'Assurance Maladie	510,000		- Attackers used pharmacist accounts through their credentials
Jul-22	OneTouchPoint	2.6 million		- Attacker succeed to decrypt Third-party service providers system

cardiac alarm systems, fitness trackers, and others. IoMT gadgets share real-time health information between healthcare professionals and patients. It includes PII, medical history, names of previous healthcare providers and facilities, and monitoring information. The sheer quantity of data in the healthcare sector is experiencing rapid growth and is being evaluated in real time. The healthcare industry is responsible for generating around 30% of the total worldwide data, and it is projected to experience an annual growth rate of 36% by 2025 [26]. Nevertheless, the enactment of the IoMT and the digitalization process have been reported to be related to incidences of data breaches. Table 1 presents a few examples of recent security breaches within the digital healthcare sector. The table underscores the significant impact of privacy breaches on each patient's PII, including health-related data like medical insurance details (policy number, insurance provider, insurance amount, etc.), patients' diagnostics reports (AIDS, cancer, infertility), etc. The exposure of medical insurance details causes unauthorized access while sharing patients' diagnostics reports without their consent, resulting in harassment or discrimination. As a result, exploiting personal health-related data has an immediate impact on patients' digital privacy and requires vigilance. The primary contributors of privacy breaches typically involve the compromise of a third-party server, the absence of multi-factor authentication measures, and network server attacks that put patients' privacy in danger. Preventing such events and security breaches is the paramount concern in today's digital healthcare industry.

F. MOTIVATION AND OBJECTIVE

The deliberation mentioned above, which began with privacy and progressed to digital privacy, including its concerns, challenges, and frameworks such as DPM, motivates the article to explore digital privacy in healthcare more. In the age of information technology's relentless march, the healthcare industry finds itself at a critical crossroads, where the ethical and legal dimensions of digital privacy converge to shape the foundation of patient trust, data security, and the future of healthcare delivery. As digital transformation revolutionizes healthcare, the delicate balance between harnessing the power of data for improved patient outcomes and safeguarding individual privacy rights has never been more precarious nor more essential.

This article aims to comprehensively understand health privacy policy and contribute to the ongoing discourse. It offers insights that can shape the way forward as healthcare and technology converge. In doing so, the intent is to foster a future in which the concepts of privacy, ethics, and innovation come together to fuel a healthcare system that not only heals but also respects and empowers individuals on their healthcare journeys. Thus, the article's main objective is to study the current state-of-the-art work and future vision of data privacy in the digital healthcare ecosystem. The article's detailed contribution is given in the next segment.

G. CONTRIBUTION

One of the most contentious issues in today's world is how digital technology challenges healthcare data privacy. After thoroughly evaluating both the role and significance of digital privacy in the healthcare sector, the following key contributions are made:

- The article discusses the impact of technological advances on digital privacy, focusing on the healthcare sector. It begins by stating that people have a right to privacy, dignity, freedom, and autonomy.
- The article underlines the importance of digital privacy regulations such as GDPR and HIPPA in the healthcare context worldwide. The regulations attempt to preserve patient privacy by defining criteria for gathering, using, and sharing health data while honoring patients' dignity. As a result, this article investigates digital privacy standards in the healthcare sector.
- Further, the review article looks at essential challenges in digital privacy by assessing relevant state-of-the-art work from the same era, i.e., healthcare. The review article reviews different data encryption systems, access control mechanisms, and risk assessment approaches.
- Artificial intelligence (AI) has grown in popularity in various fields over the last few decades, including speech

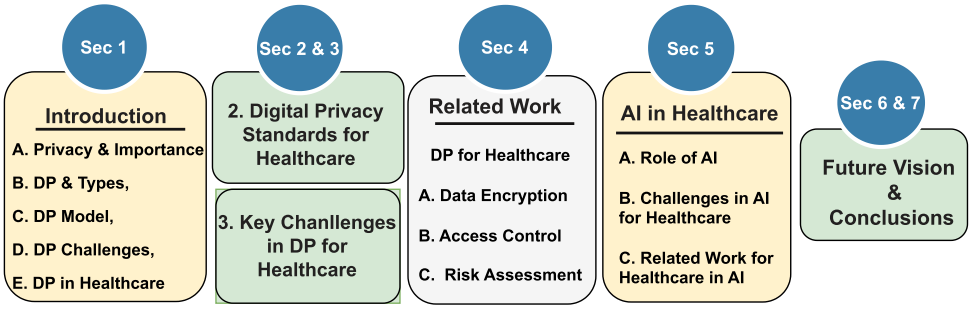

FIGURE 4. Organization of article.

recognition, natural language processing, and computer vision, to mention a few. It has also demonstrated its importance in the healthcare industry by developing various applications such as telemedicine, nanomedicine, wearable devices, etc. The review article discusses AI's significance in healthcare digital privacy by examining essential obstacles such as data breaches, AI model extraction, and heterogeneous data. The article also features cutting-edge AI development in healthcare, focusing on digital privacy.

- Finally, the article envisions the future of data privacy in the healthcare industry.

H. ORGANIZATION OF PAPER

The article's organization is presented in Figure 4. The paper is organized as follows: section I is an introduction, sections II and III discuss digital privacy (DP) standards and challenges in healthcare, section IV presents related work addressing digital privacy in healthcare, section V discusses the importance of AI for healthcare digital privacy as well as its challenges and related work, section VI discusses the future vision of data privacy in healthcare, and finally section VII conclude the paper.

II. DIGITAL PRIVACY STANDARDS (REGULATIONS) FOR HEALTHCARE

This section provides information about multiple countries' digital privacy standards for the healthcare sector. The adoption of digital healthcare systems has been pervasive among a significant proportion of the population, highlighting data privacy's emergence as a prominent concern in recent times. There is a growing awareness among individuals that corporations can gather personal data without their explicit consent and afterward exploit this information for financial gain through its sale to third parties. Countries have expressed concern for protecting individuals' privacy by enacting international data privacy legislation. There are a variety of data privacy laws in effect around the world, each with its own set of restrictions on what data can be collected and how it can be used.

In the US, due to the sensitive nature of personal information stored in electronic health records (EHR), several security and privacy safeguards have been introduced in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These safeguards promote the confidentiality, integrity, and availability of protected health information (PHI). HIPAA lists 18 categories of protected health information that must be removed before health data is released to a third party.

The EU's General Data Protection Regulation (GDPR) covers all personal data, including sensitive health data that reflects individuals' health conditions. GDPR necessitates data permission and breach reporting, and it includes several essential regulations, such as the right to access, the right to be discarded, and portability. According to GDPR, healthcare organizations must obtain explicit permission from people who provide data, and individuals have the right to control data processing.

In addition, it is worth noting that China lacks explicit regulations on protecting health data privacy. However, certain limitations on the disclosure of private information can be identified within the legal framework, namely the China Civil Code (CCC), the Medical Practitioners Act of the People's Republic of China (MPAPRC), and the Regulations on Medical Records Management in Medical Institutions (RMRMMMI). These regulations apply to individuals, medical practitioners, and healthcare facilities.

In 2017, the National Institute of Standards and Technology (NIST) of the United States released a security standard for implantable medical devices (IMDs). The Food and Drug Administration (FDA) also provided guidance by issuing two advisory articles to assist healthcare device manufacturers. Several industry groups, including Technical Information Report 57 (TIR57) and UL 2900 series standards, have established and published standards about the security administration for active healthcare devices [27].

Table 2 overviews the extant and prospective privacy regulations [28], [29], [32]. The table displays several countries' digital data privacy laws and regulations used for maintaining digital privacy in the healthcare sector.

III. KEY CHALLENGES IN DIGITAL PRIVACY FOR HEALTHCARE

The preceding section elaborated on the significance of digital privacy in the healthcare sector. This section discusses

TABLE 2. Worldwide data privacy laws and regulations.

Country	Laws and regulations	Effective Date	Brief descriptions
USA	California Privacy Rights Act (CPRA) California Consumer Privacy Act (CCPA) Virginia's Consumer Data Protection Act (VCDPA) Colorado's Privacy Act (CPA), Utah Consumer Privacy Act (UCPA), Wisconsin(Adopted in January 2024 if approved)	Jan-23 Jan-20 Jan-23 Jul-23 Dec-23 —	Laws impose tighter confidentiality obligations on corporations and expand consumer liberties while managing their personal data
EMEA	Ohio: HB 376 (Ohio's House Bill 376	Dec-21	It is a personal privacy act that offers people control over how their data is gathered, maintained, and used. The law urges enterprises to adopt a data privacy policy based on the NIST Privacy Framework.
China	Personal Information Protection Law (PIPL) Data Security Law (DSL)	Nov-21 Sep-21	The PIPL governs Chinese organizations that process and analyze personal information, establishing stringent requirements and granting significant rights, whereas the DSL governs data processing activities, data risk management and risk assessments, cross-border data transfers, and data export regulations within and outside the country. It additionally fosters safe technological development and the digitization of the Chinese economy.
New Zealand	New Zealand's Privacy Act (NZPA)	Dec-20	It is a revised version of the previous legislation that includes data breach notification, including the duty to inform privacy breaches caused by any outsourced third-party, as well as other data protection duties.
Saudi Arabia	Personal Data Protection Law (PDPL)	Mar-23	The PDPL strives to protect individuals' data privacy and to govern organizations' collection, storage, processing, disclosure of data. The law applies to entities within and outside Saudi Arabia that process personal information about Saudi residents.
South Africa	Protection of Personal Information Act (POPIA)	Jul-21	It establishes eight standards that organizations must follow while processing individual information. For specific contrary actions, offenders may be fined up to ZAR10 million or punished with up to ten years in prison.
India	Digital Personal Data Protection Act (DPDP)	Aug-23	The Act intends to preserve individuals' rights to privacy by enacting strict restrictions for the collection, storage, and sharing of patients' personal sensitive data [30].
UAE	Federal Law No 2 of 2019 (Health Data Law)	Feb-19	It governs the use of information technology and communications (ITC) in the healthcare sector. It is the federal legislation in the UAE that specifically addresses data protection issues. [31].

the most pressing concerns surrounding patient data privacy in the digital age.

The digital technology benefits the healthcare sector in different subdomains such as biomedicine, diagnostics, remote patient monitoring, and many others. Biomedicine impacts and advances digital healthcare by providing the scientific foundation and medical knowledge required to develop and deploy novel technologies and solutions. To solve health concerns such as genetic diseases and cancer, multidisciplinary teams of researchers, doctors, and data analysts work together. The team uses new research studies, clinical trials, and data-sharing programs to improve patient care [8]. The remote monitoring system is helpful for post-operative treatment and chronic illness management, such as diabetes. Digital technology assists the system in continuous monitoring and active treatment of health conditions, resulting in improved patient outcomes, cheaper healthcare expenditures, and superior treatment quality [33]. Thus, healthcare professionals can quickly access patient information and write an evidence-based prescription based on each patient's needs and medical conditions. It enables medical providers to improve treatment efficacy, safety, and patient satisfaction.

The burgeoning interconnected ecosystem of electronic health records, telemedicine, wearable health devices, and data analytics offers unparalleled opportunities to enhance medical care and research. Simultaneously, it raises serious concerns regarding the confidentiality of personal health information and the ethical implications of its use. As mentioned in [34], *Openness* (individuals are unaware that they are being monitored), *discrepancies* (flawed data), *endurance* (data never expire), *connectivity* (data is commonly purchased and sold, i.e., trading of individuals data), and *identity* (individuals may be easily re-identified)

are main key challenges occurred in digital privacy in the healthcare sector. Even though HIPPA [35] clearly states in its regulations that no patient's data should be accessed without their permission, one of the healthcare professionals at UCLA Hospital accessed patients' data, highlighting *access control* as another challenging issue in digital privacy. Healthcare often uses a third-party service provider to handle patient's medical insurance or EHR. It raises concerns about protecting patient confidentiality and access control [25]. It is challenging to maintain track of third parties and ensure that they adhere to standard compliances and regulations. Therefore, the evolving character of today's technologies calls for more stringent *compliance with regulatory frameworks* to oversee digital privacy, particularly in the healthcare sector.

Healthcare data, in general, exhibit a high degree of structure and encompass several data forms, including textual information, picture data (such as x-rays and heart graphs), and video data. Managing and handling this type of data within healthcare facilities and nationwide is an additional problem in healthcare organizations, namely in terms of *standards* and *interoperability*. Moreover, fast healthcare interoperability resources (FHIR) is a standard developed by health level seven international (HL7) organizations to exchange health data digitally. The healthcare sector's integration of digital technologies necessitates the adoption of FHIR to provide the utmost security and privacy of healthcare data [36]. However, FHIR utilizes Representational State Transfer (REST) APIs and JavaScript Object Notation (JSON) for data exchange, offering a simple and uncomplicated implementation process. Using an open design and relying on web technologies beneath the standard may render it more susceptible to security breaches, eliciting apprehension. So, FHIR must still be fully compatible with the appropriate handling of interoperability standards in the healthcare industry.

Several cybersecurity risks might arise as healthcare products become more interconnected with hospital networks and the global web. The invaders deploy eavesdropping and man-in-the-middle attacks to intercept healthcare equipment communications. Wearable devices or wireless body area networks are resource-constrained devices used in remote monitoring systems. The constrained nature of such devices presents challenges while implementing security mechanisms. Another security threat, such as a distributed denial of service attack, renders health-related services unavailable. Such a cyber threat damages the reputation of a specific healthcare organization [37]. Cybercriminals and national governments have shown interest in the healthcare industry, with the former being primarily motivated by their potential for enormous financial advantages. It covers things like the illegal trade of patients' precious medical records and the deployment of ransomware against expensive or essential healthcare gadgets. There is a rising tide of obsolete, unpatched devices with clarified vulnerabilities that hackers can easily exploit. Updating device software and guaranteeing security in medical device firms are complex tasks due to two main factors. First, the timely upgrade of device software is hampered by stringent guidelines that require significant time and effort to comply with. Second, many parties involved, such as healthcare product manufacturers, regulatory agencies, healthcare providers, and patients, need to recognize the situation's gravity and invest adequately in safety protocols [38].

Technology-based psychotherapy is increasingly prevalent in mental healthcare, enabling professionals to interact, save data, and use digital software. However, this can impact digital privacy and increase clients' risk of confidentiality breaches. The paper mentioned above [39] emphasizes the utilization of email, text messaging, televideo appointments, and numerous healthcare apps inside the mental healthcare system as a significant worry for preserving digital privacy. It demands encrypted email, two-way authentications to text messages, and secure network connectivity for live video appointments or discussions, which is a concern in the healthcare industry. However, the healthcare industry confronts issues ensuring secure network connectivity for live video visits or talks and implementing encrypted systems for email and text communication authentication and authorization techniques.

Medical records are essential in patient care since they contain a range of PII. The maintenance of data privacy in electronic medical records is a critical concern [40]. Furthermore, several countries have urged the adoption of a centralized record system in the medical and healthcare industries. Even though the EU is actively involved in measures to ensure the continuous interoperability of such infrastructures, it remains an issue for digital privacy in healthcare. The EU's varied legislative environment makes it difficult to ensure uniform and strong privacy protections for healthcare data. While the EU has adopted legislation (GDPR) to protect personal data, disparities in national laws and interpretations result in inconsistencies and gaps in protection, particularly when it comes to international data exchange [41].

Facial recognition is a viable solution, allowing people to access their health records and handheld gadgets securely. However, pandemics such as COVID-19 make it difficult due to the use of face masks and the demand to articulate new prominent solutions that will preserve the privacy of health data. From the privacy standpoint, another significant area for improvement in the healthcare industry is the cost of managing information technology. The Fig. 5 presents significant challenges discussed in the section. In light of the preceding debate, the following section delves more into cutting-edge related work, significantly emphasizing healthcare digital privacy.

IV. STATE-OF-THE-ART REVIEW OF KEY CONSIDERATION HEALTHCARE DIGITAL PRIVACY

To ensure digital privacy inside the healthcare system, it is imperative to establish and maintain confidentiality, integrity, and availability of healthcare data. Therefore, this section

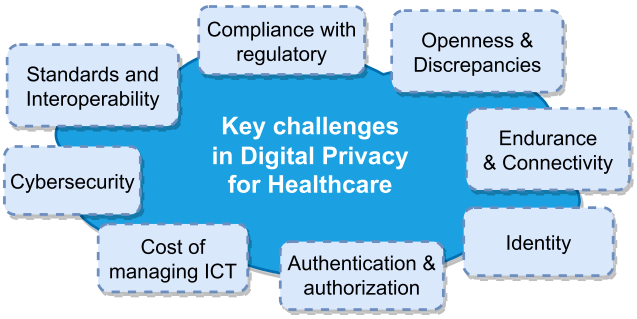

FIGURE 5. Challenges in digital privacy for healthcare.

will examine specific tactics for data encryption, access management, and risk assessment. Access management and risk assessment help digital healthcare systems to maintain privacy. Risk assessment can identify system vulnerabilities and design measures to minimize them, while access control restricts sensitive information to authorized users. Data encryption techniques assist in securing PII and other sensitive information, even if it enters into the hands of unauthorized individuals.

A. DATA ENCRYPTION

Cloud computing for digital health record (DHR) storage is becoming commonplace. However, while data is uploaded to the cloud, it can be viewed illegally. That leads to disclosing individuals' PII, including health-related sensitive data, raising concerns about data privacy. It challenges healthcare firms to mitigate this risk by encrypting data at the user end and transferring it to the cloud. Author [33] proposed the privacy-preserving priority classification (PPC) approach, which respects the privacy of users' personal information and the confidentiality of disease prediction models used by remote healthcare centers. The proposed encryption approach is resistant to cipher and known plaintext attacks. The method is effective in terms of both computation and communication.

Patients' main barriers to accessing DHRs across healthcare institutions are privacy and record sensitivity. Data sharing via fax or mail is widely used due to a need for more systematic infrastructure support for secure, trustworthy health data transmission. It can result in significant delays in receiving medical treatment. Also, the present framework must have a standard architecture, making it impossible to maintain adequate patient confidentiality (C) and access control (AC) after data is delivered. So, the study [42] looks at how blockchain technology can resolve this issue and securely share digital health records with health care services across numerous medical centers and hospitals. The study [43] offered a ground-breaking solution to healthcare organizations' challenges while keeping and distributing digital health records. To maintain data confidentiality alongside access control, the proposed approach employs authorization-based blockchains and attribute encryption while protecting individual patient privacy.

Patients who visit multiple hospitals can save money by not having to repeat medical tests and procedures. The patient-driven access approach additionally permits individuals to serve as digital guardians of their health data, providing doctors and hospitals with on-demand access and removing it after a predetermined period. As a result, the study [44] proposed a blockchain-based system that uses two-factor authentication and multi-factor authentication to access control of health data. Any nefarious manipulation of digital health records could lead to inaccurate health decisions; ensuring that accurate data is available to cloud service providers is essential. To address the preceding challenge, the study [45] proposed an incremental proxy re-encryption scheme for secure data sharing with cloud technology.

Table 3 summed up the recently discussed data encryption techniques in terms of the type of encryption, decryption algorithm used, the proposed approach protects what kind of data, the proposed solution uses blockchain technology or cloud computing, and the kinds of data they shield alongside the security triad achieved.

B. ACCESS CONTROLS

Protecting private data from prying eyes is the job of access control systems. An authorized user can jeopardize a person's privacy and lead to identity revelation when sharing sensitive information without a confidentiality protection policy [46]. Some of the access control strategies are role-based access control, fine-grained access controls, and user authentication, among others. User authentication methods such as single-sign-on, multi-factor authentication, and regular audit trails aid in the management of unauthorized access [51]. Role-based access control mechanisms grant access to certain data depending on predefined roles [49], [73]. For example, doctors will have access to medical treatment information and lab reports, whereas nurses will only have access to records of patients' visits. Fine-grained access policies, such as context-aware policies, enable precise control over the access of patient data based on factors such as durations, devices, or specific locations [51]. These strategies aid healthcare organizations in upholding the security and privacy of patient data.

Applications like SecureDoc [47] provide access control from unauthorized users when physical devices like data storage systems are stolen or lost. It also handles the keys smartly by allowing multiple users to log on to a single device and access it securely and efficiently. It will give authorized and concerned persons access to particular data only. This approach is time efficient as it will only decrypt some of the file systems.

It intends to address the growing issue of patient privacy infringement in intelligent healthcare management. The study [48] examines significant indications influencing privacy disclosure and develops a fuzzy theory-based risk access control mechanism. The model accurately analyzes

TABLE 3. State-of-the-art review of recent data encryption techniques.

Year	Data encryption algorithm	Brief discussion	Type of data collected & protected	Data storage domain	Security triad
2019	ECIES, Paillier encryption system	Proposed approach encrypt and decrypt medical data packets using pailier and ECIES algorithm while medical center uses standard encryption techniques for disease model [33].	Wearable devices data (WBAN)	Cloud computing	C
2019	Ciphertext-based attribute encryption, trapdoor function	Permissioned chains are used to achieve secure keyword search and encrypted EHR exchange [43].	Medical centers data (DHR)	Blockchain	C & AC
2019	Elliptic curve cryptography, certificateless cryptography, proxy re-encryption	Proposed approach employs a pairing-free technique without certificates to avoid certificate maintenance and key-escrow concern [45].	Wearable devices data (DHR)	Cloud computing	C & I
2020	PKI-based asymmetric encryption, digital signatures	Proposed approach provides fast and secure access to EHR [42].	Cancer care related data (DHR)	Blockchain	C & AC
2022	AES-128, RSA-4096, Digital signatures	Proposed patient-driven, secure and unbreakable data storage approach which is comparatively faster [44].	Medical centers data (DHR)	Blockchain	C & AC

safety concerns and forecasts various risk factors. Another study [49] presents a triple subject purpose-based access control model for IoMT scenarios, utilizing blockchain-enabled trustworthy networks and designing privacy-preserving mechanisms for individual users.

The study [50] presents a hybrid computing approach that integrates cloud-edge computing to benefit from both (edge and cloud computing) and develop the fortified-chain framework. The proposed model maintains a public ledger for each medical record and critical event to provide traceability. The study [51] proposes a cloud-enabled framework for industry-IoT healthcare systems that allows patients and healthcare professionals to specify their access strategy to encrypted data so only authorized peers can access health data.

Many individuals experience negative emotions while discussing their mental health or weight-related concerns. Teenagers experience fear of being stigmatized or subjected to differential treatment if such information is not managed carefully. It is crucial to address these concerns in order to enhance youngsters' attitudes and confidence in healthcare systems. The study [23] underlines the importance of addressing teenagers' anxieties around digital privacy, security, and control in patient-accessible electronic health data (PAEHR). It is crucial for fostering confidence, interaction, and participation in healthcare environments. According to the study, most teenagers demand more access control over who can view their health records. Next, the study [24] proposed a blockchain-based access control architecture for the privacy preservation of remote healthcare data. The proposed architecture includes access control methods such as policy transactions, access policies recorded in blockchain, data owner authorization, and patient-centric access restrictions. These policies ensure that only authorized personnel can access and interact with personal health data. The proposed architecture considers a clustering strategy to maintain data integrity and network overload.

Table 4 exhibits recent state-of-the-art work addressing access control issues in the healthcare sector. The table provides insights, including access control techniques proposed by various researchers, algorithms, or key indicators used to address privacy issues if the proposed method is centralized or distributed manner and application domain.

C. RISK ASSESSMENT

Risk analysis is critical but needs to be identified through an adequate risk management procedure. It should be prioritized and treated promptly. Also, Table 1 evidence the importance of risk analysis in healthcare for privacy protection. The study [52] suggested various risk assessment techniques for safeguarding the digital privacy of data. De-identification techniques can be used to remove or conceal PII from health-related data, which is one of the approaches. Another tactic is to use access restrictions and authentication systems to restrict who can access and utilize health-related data. The study also explores approaches for lessening the possibility of privacy exposure, like suppression, generalization, randomization, and synthetization.

Healthcare organizations must develop a practical approach to IoMT security risk management, which includes identifying healthcare gadgets and associated risks and assessing, prioritizing, formulating, implementing, monitoring, reviewing, and constantly improving a security risk management model for healthcare practice. The study [53] offers best practices for dealing with risk vulnerabilities in healthcare gadgets. It focuses on key areas of concern, including data privacy, manipulated data, location privacy, and the absence of robust authentication mechanisms concerning healthcare gadgets. The proposed method used COBIT5, an IT governance and management framework that

TABLE 4. State-of-the-art review of recent access control techniques.

Year	Access control techniques	Brief discussion	Algorithm/key indicators for privacy disclosure	Limitations or issues	Domain
2019	Fuzzy theory-based technique	Access behavior sensitivity, Past access risk, network environment at the time of request access, resource sensitivity, threat of patient privacy data disclosure [48].	Centralized using cloud environment	Proposed approach didn't consider dynamic nature while accessing the risk is not suitable for all kind of healthcare scenario	Smart healthcare management
2021	Selective ring-based AC (SRAC) and device authorization	SRAC selectively shares file access credentials with authorized devices and individuals, also allow to deny access to data at any time [50].	Hybrid using blockchain technique	Proposed approach is not suitable for applications that need high-speed data processing, not scalable, need high computing power so not ideal for battery-operated and resource-constraint devices	IoMT
2022	Purpose-based AC (PBAC), local differential privacy (LDP), and role-based AC (RBAC) techniques	PBAC ensure only authorized users with specific purposes will get data access, LDAP ensures sensitive information is protected locally, and RBAC determines role-based rules [49].	Distributed using blockchain technique	PBAC may fail if the data requester's purpose is unclear, also may not prevent authorized user exploitation.	IoT
2022	Privacy-Preserving Bilateral Fine-Grained AC (PPBFG-AC)	PPBFG-AC creates a bilateral smooth access control method using attribute-based and privacy-preserving pairing encryption [51].	Centralized using cloud computing	The applicability and feasibility of PPBFG-AC in real-world scenarios may depend on resources, healthcare system complexity, and participant adoption.	IIoT healthcare
2023	Blockchain-based AC architecture	Proposed architecture uses clustering and data disturbance strategy to enhance data security, privacy, and access control policies [24].	Integration of cloud and blockchain approach	Proposed approach does not provide differential privacy, may fail against future quantum attacks.	Remote healthcare

TABLE 5. State-of-the-art review of recent risk assessment techniques.

Year	Risk assessment for various devices	Methodology used	Methodology working / Criteria utilized
2019	IoT devices in healthcare	Control Objectives for Information and related Technology (COBIT5) [53]	Healthcare IoT Risk Management, Hospital Performance Indicator for Accountability (HPIA), and COBIT5.
2020	MIDs (X-ray radiography, CT, MRI, ultrasound)	Threat identification, ontology-based Likelihood, severity Decomposition, and Risk integration (TLDR) [38]	Identifying vulnerable components of medical devices by creating Attack Flow Diagrams (AFDs), Mapping, estimating and computing overall risk.
2020	Medical devices (Infusion pump)	Integrated Safety, Security, and Privacy (ISSP) Risk Assessment Framework [55]	The Bayesian theorem calculates the probability of hazard, the Common Weakness Enumeration (CWE) database estimates vulnerability likelihood, the CVSS score estimates vulnerability impact, and the Boolean expression estimates privacy risk.
2020	Nano-Biomaterials (NBM)	BIOmaterials Risk Management (BIORIMA) framework [56]	Patient safety risks, occupational risks for healthcare workers, and environmental risks.
2020	Biomedical engineering devices	Medical equipment management programs (MEMP) approach [57]	Functionality based-function, connection, data type, Threat modeling, threat incidence, and threat success possibility.
2021	Digital healthcare devices	Privacy Policy Risk Assessment tool [58]	Reviewing privacy policies, doing risk assessments, interacting with consumers, developing trust, communicating privacy policies, and knowing legal requirements and best practices promote safe use.

assists organizations in managing risk associated with IT use. The study [27] addresses the potential risks related to the increased usage of software-dependent implantable medical devices and the need for privacy protections that safeguard patients.

The study [38] proposes a novel methodology for assessing the digital security risk of healthcare equipment. The TLDR methodology identifies potentially vulnerable medical instruments, maps possible breaches into a known attack, estimates the probability of attacks with the assistance of senior

healthcare Information Security Experts, and computes the overall risk. Existing risk assessment techniques regarding privacy are associated with the traditional approach. They didn't consider heterogeneity or scalability provision of the IoT technology. Hence, the study [54] talks about possible privacy risks in IoT remote healthcare systems, such as reply and snooping attacks, weak security measures, and social engineering attacks, among others. Another study [55] proposed a framework to determine the risk level of medical equipment and required security measures based on software and hardware weaknesses. The framework considers the cumulative impact of safety and privacy threats on patient well-being. The study [56] considers not only the risk evaluation of patient data but also medical instruments and advanced therapeutic medicinal items based on genes, somatic cells, and tissue engineering. The proposed model uses a life cycle approach to assess the human health and environmental risks of NBMs, considering EU legislation and modern nanomaterial safety evaluation methods. These strategies aid stakeholders in defining and implementing relevant methodologies and instruments for risk assessment.

The study [57] provides a multicriteria decision-making model that prioritizes medical equipment by expanding the Fennigkoh and Smith model, which enables the construction of greater security, including privacy risk evaluations. Using the proposed method, the author also investigates the threat incidence and threat success possibility for medical equipment. A biological engineering team can use the proposed approach for risk evaluation and management of medical equipment. The paper [58] underlines the importance of privacy rules for health professionals and suppliers of services to provide proper data privacy and security measures when using healthcare information systems (HITs). It emphasizes that most HITs comply with the Privacy Act of 1988.

Table 5 illustrates the state-of-the-art recent risk management framework to maintain privacy in the healthcare industry. The table describes the risk assessment framework for the recommended healthcare equipment, the techniques employed by the various authors, i.e., the methodology used and the criteria used for the proposed method.

The techniques mentioned in the segments, such as data encryption, access control, and risk assessment, not only aid in the preservation of digital privacy in healthcare but also improve overall security. These techniques can help in device-level and system-level vulnerability analysis in the healthcare context. Medical devices with IoT integration are more vulnerable to device capture, eavesdropping, phishing, and denial of service (DoS) attacks, to mention a few. Regularly updating such device's firmware and software with security patches is essential. Healthcare businesses can set up ways to check the compatibility of patches, see how they affect systems, and quickly deploy updates to fix known vulnerabilities. Further, healthcare entities can conduct frequent audits to assess risks. It will help to determine the possible impact of device flaws on patient safety and data security. Healthcare organizations can employ intrusion detection systems (IDS) and conduct penetration testing to assess system-level vulnerabilities. They can also create and implement security policies and procedures that regulate access, data management, incident response, and security standards. Security risks can be reduced by educating employees about security and making sure they follow organizational regulations and industry standards.

V. ROLE OF AI IN HEALTHCARE DIGITAL PRIVACY

This segment delves into the relevance of AI in healthcare and digital privacy, as well as critical challenges and state-of-the-art work. Figure 6 clearly shows the current trend of the use of AI techniques, digital privacy, and digital health transformation, which has been gaining a peak in the past five years (2018-2023).

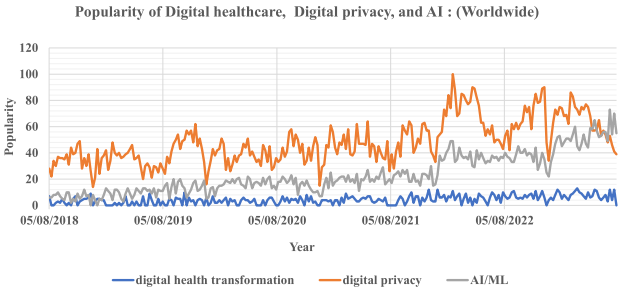

FIGURE 6. Growth of AI in digital privacy for healthcare (Google trend).

A. ROLE OF AI

Machine learning (ML) and deep learning (DL) algorithms, which are integral parts of Artificial Intelligence (AI), are increasingly being employed in the field of digital healthcare. These technologies assist healthcare professionals in making reliable forecasts and delivering accurate medical interventions. As physicians can quickly track their patients', tailored care is possible. AI techniques also contribute to predictive analysis, which proves to be beneficial in the context of remote medical diagnostics. The utilization of AI in TeleTech services is experiencing a notable expansion. The global AI sector is currently estimated to be worth $11 billion in 2021, with projections indicating a substantial increase to $37 billion by the year 2030. AI can beat the shortage of medical professionals in rural areas. AI can decrease the clinical decision-making time and resources needed to diagnose and assess patients. This advancement can significantly enhance the efficiency of medical practitioners, enabling them to respond promptly and effectively, ultimately resulting in a higher number of lives saved. AI algorithms have demonstrated higher accuracy in identifying potential diseases than conventional methodologies [59].

AI-based large language models (LLMs) are becoming more popular in the healthcare sector to improve privacy

and security. Federated learning, differential privacy, and secure multi-party computation are among the strategies used by LLMs with healthcare data to ensure patient privacy. These methods enable models to be trained on decentralized data sources while retaining sensitive information, hence improving privacy in healthcare environments. The study [61] uses a BERT, a pre-trained language model from Hugging Face, to predict mental health disorders in social networks. Nowadays, social media possesses a vast quantity of data, and LLMs use these data to diagnose behavioral illnesses like depression and self-harm. It is highly beneficial to healthcare practitioners to identify risks in patients by monitoring social media and making treatment easier [60].

The following are a few pertinent AI achievements in healthcare. The World Health Organization (WHO) has officially launched Florence 2.0, an AI-based chatbot designed to function as a digital healthcare expert, providing advice on healthcare lifestyle [62]. An additional illustration of AI can be observed in the deployment of a defibrillator drone, which effectively transported a defibrillator to rescue a 71-year-old individual experiencing a cardiac arrest [63]. Alivecors' Kardia, an FDA-approved electrocardiogram (ECG) recorder, is a notable illustration of AI [64]. Virtual reality (VR) and augmented reality (AR) exemplify AI applications that enhance medical training by enabling trainers to see critical procedures with enhanced precision. AI-enabled telemedicine services enhance patient accessibility to healthcare by allowing remote consultations and diagnostic procedures. Various healthcare providers, including hospitals and polyclinics, deploy LLM-integrated chatbots or virtual assistants to improve patient engagement, support, and access to healthcare services [65]. BioBERT, ClinicalBERT, and BlueBERT are a few examples of LLMs that are actively used in the healthcare sectors [65], [66], [67]. Fig. 7 summarizes the various healthcare sectors in which AI plays an integral role.

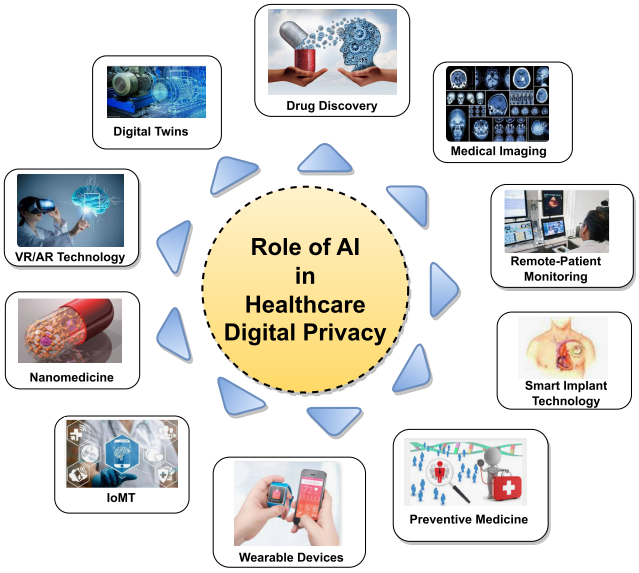

FIGURE 7. Role of AI in digital healthcare.

B. KEY CHALLENGES IN APPLYING AI FOR HEALTHCARE DIGITAL PRIVACY

AI can effectively fulfill privacy objectives through its ability to de-identify and suppress health data while safeguarding the data's integrity. AI can potentially develop ML and DL models that can autonomously detect and eliminate PII from health-related data [52]. In addition, AI can create models that provide artificially generated data substantially comparable to actual data. This approach holds potential for constructing ML/DL models or other uses that need substantial data volumes, all while ensuring the confidentiality of patients.

However, *data breaches* pose a severe risk of applying AI in the healthcare industry. The healthcare sector generates, receives, stores, and transfers large amounts of PII and health-related data, making them potential targets for hackers. Threat actors can and will take advantage of AI data pipeline flaws at any stage. There's also the possibility that AI models could be vulnerable to things like *membership inference attack*, *attribute inference attacks*, *data poising*, and *model extraction*, all of which violate users' privacy in novel ways.

Because of its sensitivity, there are stringent rules regarding using and disclosing healthcare information. Therefore, it is challenging to construct any ML or DL model while protecting PII and health-related data. DL models are often considered extensive computational calculations to classify or predict any problem accurately. It's only sometimes evident how the model came up with its forecasts or decisions. In healthcare, however, understanding the reasoning behind a model's predictions is essential for validating its accuracy and relevance to real-world scenarios. This results in a lack of *openness* in AI models, which creates a new challenge. Some research suggests that DL models trained on a single dataset don't transfer well to others. It could restrict the model's usability to actual healthcare environments [68]. *Poor*, *insufficient*, and *erroneous data* quality is another issue in the healthcare business and can have a detrimental impact on ML and DL model outputs [69].

C. STATE-OF-THE-ART WORK HEALTHCARE DIGITAL PRIVACY USING AI

This segment presents an overview of the current advancements achieved through utilizing AI in healthcare, specifically focusing on digital privacy.

Digital health records frequently get compromised while uploading to the public cloud, which faces privacy and security issues in the healthcare domain. However, AI techniques can be combined with encryption algorithms like AES and DES to enhance health data privacy. Therefore, the study [74] focuses on five ML techniques and encryption algorithms to safeguard data storage from unauthorized use. The study [70] presented a secure privacy digital risk assessment system for medical data distributed across many hospitals. All medical data obtained from various hospitals is first preprocessed into a standard format and then encrypted. Such data is then used for model training, classification, and prediction. The

TABLE 6. State-of-the-art review AI in healthcare digital privacy.

Year	AI techniques (ML/DL)	Brief discussion	Data storage techniques	Security measures address	Dataset	Application domain
2021	DL: LSTM, ring learning with errors (R-LWE)	Proposed approach store and analyze EHR efficiently and securely while respecting healthcare users' privacy and trust [68].	Blockchain (Distributed approach)	Access control	SemVal 2013 task 9.2 dataset	Healthcare 4.0
2022	ML: SVM, MNB, DT, RF, GB, KNN and AES-GCM	Combine ML techniques with encryption algorithm for privacy protection to blood bank data [74].	Pubilc Cloud (Centralized approach)	Data encryption	KSM Blood bank	Blood bank sector
2022	ML: NB classification, AES-256, HMAC-SHA1	Naıve Bayesian algorithm is applied on encrypted medical data, an authorized user can decrypt the data [70].	Distributed approach	Risk assessment	BCW and synthetic	Online disease risk assessment service
2023	DL: Contractive deep AE, Quantum DNN	IDS includes differential privacy and content-driven filtering for privacy preservation [71].	Private cloud (Distributed approach)	Risk assessment	WUSTL-EHMS-2020, ICU dataset	IoMT
2023	DL: BiLSTM	Proposed approach utilized blockchain and FL to ensure privacy [72].	Blockchain and FL (Distributed approach)	–	Generated from glucose-insulin simulator	IoMT

SVM: Support vector machine, MNB: Multinomial Naive Bayes, DT: Decision tree, RF: Random forest, GB: Gradient boosting, KNN: K-Nearest Neighbour, AES-GCM: Advanced Encryption Standard-Galois Counter Mode, LSTM: Long-short term memory, BiLSTM: Bidirectional LSTM, AE: Auto-encoder, DNN: Deep neural network, FL: Federated learning

proposed method achieves authorization by utilizing keys distributed by a trusted authority.

The study [71] focuses on cyberattacks on IoMT devices and systems that put patients' safety in jeopardy. IoMT devices that have been compromised can leak patient data and disrupt critical services like ventilation and intensive care unit medical devices. Malicious attackers often exploit IoMT devices because they lack security standards and authentication methods. As a result, attackers can quickly access these devices and move laterally across networks or introduce malware to harm patients. The study [71] proposed an intrusion detection system based on QDNN and CDAE approaches. QDNN is utilized for attack detection and classification, and CDAE is used for data fusion that helps to maintain the privacy of IoMT devices and patients during the learning process.

Another study [68] proposed approach employed lattice cryptography technique for data encryption and authentication, whereas the DL technique is used for disease prediction. The study [72] proposed a lightweight DL approach that leverages blockchain and federated learning for privacy preservation in IoMT. The study [73] presented a multi-agent system employing deep learning techniques to solve privacy concerns in e-healthcare applications. The proposed system incorporates homomorphic security, differential privacy, and federated learning techniques to protect patient data privacy.

Table 6 presents current state-of-the-art work using AI in healthcare digital privacy. The table explicitly highlights the ML and DL algorithms used, a brief discussion about the proposed methodology, healthcare-related data storage techniques utilized to maintain data privacy, the dataset used, and the key challenges the proposed methodology addresses.

VI. FUTURE VISION OF DIGITAL PRIVACY IN HEALTHCARE

This section addresses the future vision of digital privacy in healthcare, which will be more prominent in the upcoming year. An explicit and identifiable solution has yet to be immediately evident in healthcare privacy issues. Ensuring the preservation of individuals' privacy rights while also catering to the collective welfare of the community is a crucial aspect for any healthcare sector [76].

- **Federated learning**: As digital privacy has become a critical societal issue, federated learning (FL) has emerged as a hot research area for enabling shared training of AI models across various connected devices while adhering to privacy constraints. This technique allows AI models to be trained on independent datasets spread across different devices or parties without sharing the original data. Researchers can construct models without disclosing patients' vital information; they share the model parameters. This strategy can aid in the preservation of local data privacy [52] as well. It is a significant technique for developing innovative healthcare based on sensitive and confidential medical information in remote medical institutions and hospitals.

However, FL is only sometimes private and secure out-of-the-box. FL may be susceptible to different types of attacks, such as white-box, model, and data poisoning attacks [78], an active research area. With the advent of 6G technology, FL with quantum computing in healthcare is yet another dynamic field that academics can explore.

- Encryption techniques: Proper integration of AI and encryption techniques is one of the solutions to mitigate digital privacy issues in healthcare. Recently, various encryption techniques have evolved to achieve this goal. However, an encryption algorithm must provide maximum security with minimum computation and communication cost [74]. The issue of secure access to shared devices is a significant concern for numerous firms as they endeavor to enhance their full disk encryption (FDE) solution to safeguard digital privacy. IoMT technology, which promotes data sharing across individuals, poses a substantial barrier to developing such solutions and requires the researchers' undivided focus.
- Blockchain technology: The preceding section's discussion exhibits the growing use of blockchain technology and AI techniques to preserve digital privacy in healthcare. Blockchain techniques have shown prominent results in data encryption and access control challenges. Moreover, the state-of-the-art study [42] proposed a patient-oriented blockchain technique that is secure and maintains the confidentiality of the patient's data by making it available anytime. However, the proposed approach fails to give healthcare professionals access in an emergency. So, researchers and academics can concentrate on such situations and propose more robust solutions. Some studies [43] presented a scheme based on the permission blockchain concept that might be used in any healthcare organization that wants to safely and efficiently store and transfer digital health records. However, the offered methodologies have limitations, such as needing to be more scalable for massive datasets and requiring considerable processing resources. Researchers can delve deeper into this gap and give marginal remedies. The researchers can pay attention to the combination of federated learning and blockchain technology to address scalability, trust, and privacy concerns.
- Compliance with regulations: It is anticipated that numerous nations must carefully adopt relevant policies to handle privacy obstacles in their healthcare sector. As healthcare organizations endeavor to implement digital privacy policies, they grapple with challenges beyond legal Compliance to encompass the fabric of healthcare delivery and innovation. Emerging technologies like AI and IoT can potentially revolutionize healthcare while simultaneously posing new ethical dilemmas that need attention. Additionally, as long as the medical IoTs and other mobile health application tools are integrated into a healthcare system, the medical IoT or mobile health application vendor does not have to meet HIPAA or HITECH guidelines. It leads to a critical privacy protection gap where consumers need more understanding and control over how health data is stored, accessed, and utilized.

VII. DISCUSSION AND CONCLUSION

With the swift development of digital technology, preserving privacy is becoming more challenging. There is continuous research and debate on how to handle the privacy of individuals or a community while adopting digital technologies. According to several research articles, there is no one-stop solution to this issue; instead, a balance must be maintained between technology innovation and privacy. The IEEE DPM encourages privacy solutions that start with the individuals and their healthcare information. Healthcare is a prized industry, and the COVID-19 pandemic evidence its utmost importance worldwide. Digital technology accelerated its significance in the healthcare industry during this pandemic. Technology assists healthcare professionals in working efficiently and accurately by bringing medical facilities to our doorstep and saving lives. It provides a facility for the healthcare industry to maintain patients' digital health records. Whenever healthcare professionals are in need, they can use it to make precise diagnoses of the root cause and offer adequate service to patients. However, while technology enhancement in the healthcare industry benefits everyone, it also opens the door to hackers who steal patients' PII, including sensitive health-related information. Such information is platinum within the black-digital market since it can be used to sell or destroy the industry's reputation. According to literature, distributed denial of service, ransomware, phishing attacks, insider threats, and other incidents resulting in the illegal exposure of patient information, data theft, and violations of privacy legislation. Healthcare organizations face reputational damage, legal liabilities, and financial penalties, resulting in a loss of patient trust and business.

The article dives deep into finding the challenges in digital privacy for healthcare, like scalability, maintenance of big data, adaptability, data accuracy, ethical and legal compliance, etc. The article also delves into the role of encryption techniques, access control mechanisms, and risk assessment models that assist in maintaining healthcare digital privacy. Encryption techniques assist in maintaining the confidentiality of the health data. At the same time, the access control mechanism ensures that only authorized and authenticated persons will get access to PII and health-related data. The risk assessment model assists in understanding the risks of data explosion and ensuring that healthcare professionals are always up to date on cyber threats and how to deal with them.

The different novel instances of AI in healthcare are early diagnosis of fatal blood diseases, accurate cancer diagnosis,

digital therapeutics, vocal biomarkers, dotplot-breast cancer detectors, and many more. AI with ML and DL algorithms can actively detect cyber threats, and many researchers and cybersecurity professionals are constantly working on it, with notable outcomes. The results will be astounding if healthcare and AI technologies can be combined to protect patient data. So, the article looks into the key challenges in adapting AI for healthcare digital privacy and explores how various encryption techniques and access control mechanisms can be employed with ML and DL algorithms to maintain digital privacy. FL is a good solution for digital privacy, while blockchain technology attracts many researchers to develop a privacy protection framework. FL enables the training of ML/AI models across geographically distributed data sources by pushing the computation of the ML/DL model down to each source and sharing only the locally trained model parameters. This data movement restriction benefits FL by complying with different data regulatory frameworks and ensuring local data privacy. However, blockchain technology is not scalable, and FL faces model poising attacks and independent and identically distributed (IID) and non-IID dataset issues that necessitate further investigation. Lastly, the article highlights future trends such as federated learning, blockchain technology, computationally lightweight encryption techniques, differential privacy, and secure multi-party computation.

The fundamental underpinning of most regulations relating to data protection is to protect consumers' privacy and provide security by enforcing attributes such as CIA. It has been argued that legal compliance may become the most important non-functional requirement (NFR) for many software systems. Government and state regulations are mandatory; however, compliance with these regulations remains a significant challenge plaguing entities to whom these laws apply. HIPAA was designed basically to protect the privacy of personal information. However, the mechanism or framework to protect the CIA from this information is not captured in HIPAA. Thus, the use of the Internet and other medical IoTs are governed by guidelines or standards developed by bodies such as ISO and NIST, whose enforcement falls outside the purview of the Department of Human and Health Services, the regulatory body for HIPAA. Moreover, wearable devices and mHealth apps represent a new digital privacy issue that HIPAA does not address. Unfortunately, neither the Department of Health and Human Services nor the Office of Civil Rights (OCR) can oversee consumer health data breaches relating to these products. Due to the intricacy of most tech health products and IoTs, most consumers must know that their information has been breached, shared, or sold to a third party due to a lack of robust breach disclosure legislation.

With proactive adaptation and innovation, a healthcare ecosystem that balances data utility and patient privacy can be achieved. This would ensure that the benefits of digital transformation are accessible to all while respecting the sanctity of individual health information.

REFERENCES

[1] *Importance of Privacy*. Accessed: May 2023. [Online]. Available: https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-importance-of-privacy/

[2] *Privacy & Security*. Accessed: Feb. 2022. [Online]. Available: https://digitalprivacywise.com/what-is-difference-between-privacy-security/

[3] *Internet Privacy Issues*. Accessed: May 2023. [Online]. Available: https://www.globalbrandsmagazine.com/internet-privacy-issues-tracking-hacking-and-trading/

[4] X. Fang and M. Li, "Privacy-preserving process mining: A blockchain-based privacy-aware reversible shared image approach," *Artif. Intell.*, vol. 38, no. 1, 2024, Art. no. 2321556.

[5] D. Solove. *Reasons Why Privacy Matters*. Accessed: Jan. 2014. [Online]. Available: https://teachprivacy.com/10-reasons-privacy-matters/

[6] K. Granville. *Facebook and Cambridge Analytica*. Accessed: Mar. 2018. [Online]. Available: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[7] M. Rosenquist. *Privacy*. Accessed: Jul. 2020. [Online]. Available: https://www.helpnetsecurity.com/2020/07/28/what-is-privacy-and-why-does-it-matter/

[8] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Comput. Biol. Med.*, vol. 158, May 2023, Art. no. 106848.

[9] H. Hung and Y. H. Wong, "Information transparency and digital privacy protection: Are they mutually exclusive in the provision of e-services?" *J. Services Marketing*, vol. 23, no. 3, pp. 154–164, May 2009.

[10] R. Touma. *TikTok*. Accessed: Jul. 2022. [Online]. Available: https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

[11] A. Hetler. *Social Media Privacy Issues*. Accessed: Jan. 2023. [Online]. Available: https://ts2.space/en/the-impact-of-fhir-on-healthcare-data-security-and-privacy/

[12] *Privacy*. Accessed: May 2023. [Online]. Available: https://privacy.ucsd.edu/privacy/index.html

[13] O. Husain. *Digital Privacy & Digital Safety*. Accessed: Mar. 2023. [Online]. Available: https://www.enzuzo.com/blog/digital-privacy-definition

[14] *IEEE Digital Privacy Model*. Accessed: Jul. 2023. [Online]. Available: https://digitalprivacy.ieee.org/about/digital-privacy-model

[15] T. S. Altshuler. *Privacy in a Digital World*. Accessed: Sep. 2019. [Online]. Available: https://ts2.space/en/the-impact-of-fhir-on-healthcare-data-security-and-privacy/

[16] B. Marr. *Big Data*. Accessed: Sep. 2015. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/?sh=2492dde417b1

[17] *Challenges in Global Data Privacy and Protection*. Accessed: May 2023. [Online]. Available: https://cipher.com/blog/the-5-biggest-challenges-in-global-data-privacy-and-protection/

[18] S. Mahadik, P. M. Pawar, and R. Muthalagu, "Efficient intelligent intrusion detection system for heterogeneous Internet of Things (HetIoT)," *J. Netw. Syst. Manage.*, vol. 31, no. 1, p. 2, Jan. 2023.

[19] S. Alexandra. *Major Internet Privacy Issues*. Accessed: Sep. 2019. [Online]. Available: https://securitytoday.com/articles/2019/09/03/3-major-internet-privacy-issues-and-how-to-avoid-them.aspx

[20] R. P. Romansky and I. S. Noninska, "Challenges of the digital age for privacy and personal data protection," *Math. Biosci. Eng.*, vol. 17, no. 5, pp. 5288–5303, 2020.

[21] *Cookies and Web Bugs*. Accessed: Sep. 2004. [Online]. Available: https://ts2.space/en/the-impact-of-fhir-on-healthcare-data-security-and-privacy/

[22] C. Dhasarathan, M. K. Hasan, S. Islam, S. Abdullah, U. A. Mokhtar, A. R. Javed, and S. Goundar, "COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach," *Comput. Commun.*, vol. 199, pp. 87–97, Feb. 2023.

[23] J. Hagström, R.-M. Åhlfeldt, C. Blease, Å. Cajander, H. Rexhepi, J. Moll, B. Kane, I. Scandurra, and M. Hägglund, "Security and privacy of online record access: A survey of adolescents' views and experiences in Sweden," *J. Adolescent Health*, pp. 1–7, Feb. 2024.

[24] H. N. Alsuqaih, W. Hamdan, H. Elmessiry, and H. Abulkasim, "An efficient privacy-preserving control mechanism based on blockchain for e-health applications," *Alexandria Eng. J.*, vol. 73, pp. 159–172, Jul. 2023.

[25] E. Kost. *Healthcare Data Breaches (Updated 2023)*. Accessed: Jul. 2023. [Online]. Available: https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

[26] C. Hogan. *Privacy Considerations in the Advancement of Digital Healthcare*. Accessed: May 2023. [Online]. Available: https://www.bsigroup.com/en-GB/blog/Digital-trust-blog/2022/privacy-considerations-in-the-advancement-of-digital-healthcare/

[27] V. Hassija, V. Chamola, B. C. Bajpai, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?" *Sustain. Cities Soc.*, vol. 66, no. 2021, Mar. 2021, Art. no. 102552.

[28] (2023). *Guide to Data Privacy Laws by Country*. Accessed: Jun. 2023. [Online]. Available: https://www.caseiq.com/resources/a-practical-guide-to-data-privacy-laws-by-country/

[29] *Global Comprehensive Privacy Law Mapping Chart*. Accessed: Apr. 2022. [Online]. Available: https://iapp.org/media/pdf/resource_centerglobal_comprehensive_privacy_law_mapping.pd

[30] (2023). *Digital Personal Data Protection Act*. Accessed: Oct. 2023. [Online]. Available: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

[31] *Federal Law No 2*. Accessed: Jul. 2023. [Online]. Available: https://mohap.gov.ae/app_content/legislations/php-law-en-77/mobile/index.html

[32] (2023). *Data Privacy Laws and Regulations Around the World*. Accessed: Jul. 2023. [Online]. Available: https://securiti.ai/data-privacy-laws/

[33] G. Wang, R. Lu, and Y. L. Guan, "Achieve privacy-preserving priority classification on patient health data in remote eHealthcare system," *IEEE Access*, vol. 7, pp. 33565–33576, 2019.

[34] D. Grande, X. Luna Marti, R. Feuerstein-Simon, R. M. Merchant, D. A. Asch, A. Lewson, and C. C. Cannuscio, "Health policy and privacy challenges associated with digital technology," *J. Amer. Med. Assoc. Netw. Open*, vol. 3, no. 7, Jul. 2020, Art. no. e208285.

[35] *Ten Most Common HIPAA Violations*. Accessed: Jun. 2023. [Online]. Available: https://www.hipaajournal.com/common-hipaa-violations/

[36] M. Frackiewicz. *Impact of FHIR on Healthcare Data Security and Privacy*. Accessed: Jun. 2023. [Online]. Available: https://ts2.space/en/the-impact-of-fhir-on-healthcare-data-security-and-privacy/

[37] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Heterogeneous IoT (HetIoT) security: Techniques, challenges and open issues," *Multimedia Tools Appl.*, vol. 83, no. 12, pp. 35371–35412, Sep. 2023.

[38] T. Mahler, Y. Elovici, and Y. Shahar, "A new methodology for information security risk assessment for medical devices and its evaluation," 2020, *arXiv:2002.06938*.

[39] S. D. Lustgarten, Y. L. Garrison, M. T. Sinnard, and A. W. Flynn, "Digital privacy in mental healthcare: Current issues and recommendations for technology use," *Current Opinion Psychol.*, vol. 36, pp. 25–31, Dec. 2020.

[40] I. A. Moonesar, F. M. AlMarzooqi, and J. Sarabdeen, "Before and after: Healthcare users and professionals perceptions on implementation of eHealth privacy protection laws in United Arab Emirates," *J. Arch. Nursing Care*, vol. 2, no. 4, pp. 1–2, 2019.

[41] A. L. Martínez, M. G. Pérez, and A. Ruiz-Martínez, "A comprehensive review of the state-of-the-art on security and privacy issues in healthcare," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, Dec. 2023.

[42] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e13598.

[43] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic health record sharing scheme with searchable attribute-based encryption on blockchain," *IEEE Access*, vol. 8, pp. 7195–7204, 2020.

[44] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022.

[45] T. Bhatia, A. K. Verma, and G. Sharma, "Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," *Concurrency Comput., Pract. Exp.*, vol. 32, no. 5, Mar. 2020, Art. no. e5520.

[46] Z. Pervaiz, W. G. Aref, A. Ghafoor, and N. Prabhu, "Accuracy-constrained privacy-preserving access control mechanism for relational data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 4, pp. 795–807, Apr. 2014.

[47] *SecureDoc*. Accessed: Jun. 2023. [Online]. Available: https://cybersecurity-excellence-awards.com/candidates/securedoc/

[48] M. Shi, R. Jiang, X. Hu, and J. Shang, "A privacy protection method for health care big data management based on risk access control," *Health Care Manage. Sci.*, vol. 23, no. 3, pp. 427–442, Sep. 2020.

[49] G. Wu, S. Wang, Z. Ning, and J. L. records, "Blockchain-enabled privacy-preserving access control for data publishing and sharing in the Internet of Medical Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8091–8104, Jun. 2022.

[50] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, Jul. 2021.

[51] J. Sun, Y. Yuan, M. Tang, X. Cheng, X. Nie, and M. U. Aftab, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6483–6493, Sep. 2022.

[52] D. Xiang and W. Cai, "Privacy protection and secondary use of health data: Strategies and methods," *BioMed Res. Int.*, vol. 2021, pp. 1–11, Oct. 2021.

[53] H. Zakaria, N. A. A. Bakar, N. H. Hassan, and S. Yaacob, "IoT security risk management model for secured practice in healthcare environment," *Proc. Comput. Sci.*, vol. 161, pp. 1241–1248, Jan. 2019.

[54] M. Elkhodr, B. Alsinglawi, and M. Alshehri, "A privacy risk assessment for the Internet of Things in healthcare," *Appl. Intell. Technol. Healthcare*, pp. 47–54, 2019.

[55] T. Yaqoob, H. Abbas, and N. Shafqat, "Integrated security, safety, and privacy risk assessment framework for medical devices," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 6, pp. 1752–1761, Jun. 2020.

[56] E. Giubilato et al., "Risk management framework for nano-biomaterials used in medical devices and advanced therapy medicinal products," *Materials*, vol. 13, no. 20, p. 4532, Oct. 2020.

[57] D.-W. Kim, J.-Y. Choi, and K.-H. Han, "Medical device safety management using cybersecurity risk analysis," *IEEE Access*, vol. 8, pp. 115370–115382, 2020.

[58] H. M. LaMonica, A. E. Roberts, G. Y. Lee, T. A. Davenport, and I. B. Hickie, "Privacy practices of health information technologies: Privacy policy risk assessment study and proposed guidelines," *J. Med. Internet Res.*, vol. 23, no. 9, Sep. 2021, Art. no. e26317.

[59] K. Syama, J. A. A. Jothi, and N. Khanna, "Automatic disease prediction from human gut metagenomic data using boosting GraphSAGE," *BMC Bioinf.*, vol. 24, no. 1, p. 126, Mar. 2023.

[60] R. Safa, S. A. Edalatpanah, and A. Sorourkhah, "Predicting mental health using social media: A roadmap for future development," in *Deep Learning in Personalized Healthcare and Decision Support*. New York, NY, USA: Academic, 2023, pp. 285–303.

[61] A. Pourkeyvan, R. Safa, and A. Sorourkhah, "Harnessing the power of hugging face transformers for predicting mental health disorders in social networks," *IEEE Access*, vol. 12, pp. 28025–28035, 2024.

[62] *Florence 2.0*. Accessed: Jun. 2023. [Online]. Available: https://www.who.int/campaigns/Florence

[63] B. Sharma. *Drone Defibrillator Saves Heart Attack Faster Than Ambulance*. Accessed: Jan. 2024. [Online]. Available: https://www.indiatimes.com/technology/news/drone-defibrillator-heart-attack-safety-558638.html

[64] *Personal EKG*. Accessed: Jan. 2024. [Online]. Available: https://www.kardia.com/

[65] C. Dilmegani. *Large Language Models in Healthcare*. Accessed: Jan. 2024. [Online]. Available: https://research.aimultiple.com/large-language-models-in-healthcare/

[66] E. Kim, Y. Jeong, and M.-S. Choi, "MediBioDeBERTa: Biomedical language model with continuous learning and intermediate fine-tuning," *IEEE Access*, vol. 11, pp. 141036–141044, 2023.

[67] M. A. K. Raiaan, M. S. H. Mukta, K. Fatema, N. M. Fahad, S. Sakib, M. M. J. Mim, J. Ahmad, M. E. Ali, and S. Azam, "A review on large language models: Architectures, applications, taxonomies, open issues and challenges," *IEEE Access*, vol. 12, pp. 26839–26874, 2024.

[68] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[69] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and robust machine learning for healthcare: A survey," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 156–180, 2021.

[70] F. Wang, H. Zhu, R. Lu, Y. Zheng, and H. Li, "Achieve efficient and privacy-preserving disease risk assessment over multi-outsourced vertical datasets," *IEEE Trans. Depend. Sec. Comput.*, vol. 19, no. 3, pp. 1492–1504, May 2022.
[71] M. Al-Hawawreh and M. S. Hossain, "A privacy-aware framework for detecting cyber attacks on Internet of Medical Things systems using data fusion and quantum deep learning," *Inf. Fusion*, vol. 99, Nov. 2023, Art. no. 101889.
[72] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 710–721, Feb. 2023.
[73] C. Dhasarathan, M. Shanmugam, M. Kumar, D. Tripathi, S. Khapre, and A. Shankar, "A nomadic multi-agent based privacy metrics for e-health care: A deep learning approach," *Multimedia Tools Appl.*, vol. 83, no. 3, pp. 7249–7272, Jan. 2024.
[74] K. Shankar Komathi Maathavan and S. Venkatraman, "A secure encrypted classified electronic healthcare data for public cloud environment," *Intell. Autom. Soft Comput.*, vol. 32, no. 2, pp. 765–779, 2022.
[75] M. Z. Gunja, E. D. Gumas, R. D. Williams. *U.S. Health Care From a Global Perspective*. Accessed: Jan. 2023. [Online]. Available: https://www.commonwealthfund.org/publications/issue-briefs/2023/jan/us-health-care-global-perspective-2022
[76] C. M. L. Zegers, A. Witteveen, M. H. J. Schulte, J. F. Henrich, A. Vermeij, B. Klever, and A. Dekker, "Mind your data: Privacy and legal matters in eHealth," *JMIR Formative Res.*, vol. 5, no. 3, Mar. 2021, Art. no. e17456.
[77] *Website and Internet Privacy Policies*. Accessed: Jun. 2023. [Online]. Available: https://ehealthtechnologies.com/wp-content/uploads/2020/12/Internet-Privacy-Policy-2021Jun1.pdf
[78] N. Rodríguez-Barroso, D. Jiménez-López, M. V. Luzón, F. Herrera, and E. Martínez-Cámara, "Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges," *Inf. Fusion*, vol. 90, pp. 148–173, Feb. 2023.

SHALAKA S. MAHADIK (Student Member, IEEE) received the B.E. and M.E. degrees in computer engineering from Mumbai University, India, in 2005 and 2011, respectively. She is currently a Ph.D. Researcher with BITS Pilani, Dubai Campus, United Arab Emirates. Her research interests include networks & security, the Internet of Things (IoT), federated learning, and artificial intelligence. She was a Lecturer, from 2005 to 2011, and as an Assistant Professor, from 2011 to 2014. She has participated in and coordinated various workshops and national conferences. Her research is currently based on security and privacy in heterogeneous IoT (HetIoT). She has published her research work in well-known, reputed conferences and journals like IEEE, Springer, and Elsevier. She also received honors for Best Paper Presentation, in 2022, at the BITS Pilani Dubai Campus and Best Research Proposal, in 2023, at the University of Sharjah, United Arab Emirates.

PRANAV M. PAWAR (Member, IEEE) received the Graduate degree in computer engineering from Dr. Babasaheb Ambedkar Technological University, Maharashtra, India, in 2005, the master's degree in computer engineering from Pune University, in 2007, and the Ph.D. degree in wireless communication from Aalborg University, Denmark, in 2016. His Ph.D. thesis received a nomination for Best Thesis Award from Aalborg University. Currently, he is an Assistant Professor with the Department of Computer Science, Birla Institute of Technology and Science, Dubai, before BITS, he was a Postdoctoral Fellow with Bar-Ilan University, Israel, from March 2019 to October 2020, in the area of wireless communication and deep leaning. He was a recipient of an Outstanding Postdoctoral Fellowship from the Israel Planning and Budgeting Committee. He was an Associate Professor with MIT ADT University, Pune, from 2018 to 2019, and also as an Associate Professor with the Department of Information Technology, STES's Smt. Kashibai Navale College of Engineering, Pune, from 2008 to 2018. From 2006 to 2007, he was a System Executive with POS-IPC, Pune, India. He received Recognition from Infosys Technologies Ltd., for his contribution to the Campus Connect Program and also received different funding for research and attending conferences at the international level. He has published more than 40 articles at the national and international levels. He is an IBM DB2 and IBM RAD Certified Professional and completed NPTEL certification in different subjects. His research interests include security and privacy, machine and deep learning applications, reinforcement learning, the Internet of Things, and bioinformatics.

RAJA MUTHALAGU is currently an Associate Professor with the Birla Institute of Technology and Science, Pilani, Dubai Campus, Dubai, United Arab Emirates. He was a Postdoctoral Research Fellow with the Air Traffic Management Research Institute, Nanyang Technological University, Singapore, from 2014 to 2015. His research interests include wireless communication, signal processing, aeronautical communication, and cyber security. He was a recipient of Canadian Commonwealth Scholarship Award 2010 for the Graduate Student Exchange Program in the Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, Canada.

NEELI RASHMI PRASAD (Senior Member, IEEE) is currently a Visionary CEO and the Co-Founder of SmartAvatar B.V., The Netherlands, and the Technology Thought Leader with a proven track record of driving strategic growth and global expansion initiatives. With deep expertise in telecommunications, cyber security, and wireless technology, she has positioned herself as a driving force in shaping the future of technology and communications. As a Cyber-Security and Wireless Technology Expert, she has spent her career driving business and technology innovation, from incubation to prototyping to validation. Her leadership and industry knowledge have helped organizations achieve success and growth and her contributions have been recognized by industry giants, such as CISCO, HUAWEI, and Nokia-Siemens. She is also an Elected Member and a VP Membership of the IEEE VTS Board of Governors and IEEE WIE Treasurer. She is also a Trailblazer in her field, championing diversity, equity, and inclusion (DEI) initiatives and paving the way for future generations of women in technology. She is a Sought-After Speaker and the Thought Leader, frequently invited to share her insights and expertise at industry conferences and events. Under her visionary leadership, organizations have achieved unprecedented success and growth, and her contributions have helped shape the future of technology and communications. Her dedication to innovation, coupled with her commitment to DEI initiatives, has made her a role model for women in technology and a respected figure in the industry.

SIN-KUEN HAWKINS (Senior Member, IEEE) received the B.S. degree in electrical engineering from Cornell University and the M.S. degree from the Information Networking Institute, Carnegie Mellon University. She is currently the Program Director of IEEE Future Directions, supporting new and emerging initiatives, including digital and data privacy, metaverse, brain and neurotechnology, and life sciences. Prior to joining IEEE, she served as an engineering consultant on projects for the U.S. Department of Defense and the U.S. Army. She also has 18 years of experience with Bell Communications Research and Telcordia Technologies, as a member of Technical Staff and most recently was the Director of Network Engineering and Design leading the development of number portability, lawful surveillance capabilities, and emergency services.

DIMITRIS STRIPELIS (Member, IEEE) received the B.Sc. degree in computer science from the Athens University of Economics and Business and the M.Sc. and Ph.D. degrees in computer science from USC. He is currently a Research Scientist with FedML Inc. Previously, he was a Research Scientist with the University of Southern California, Information Sciences Institute (USC/ISI). His research focused on federated machine learning and federated neuroscience with USC. His research interests include federated and distributed machine learning, machine learning systems, data integration, and data management systems.

SREEDHAR RAO (Senior Member, IEEE) received the master's degree in cybersecurity policy and compliance from George Washington University, Washington, DC, USA, and the master's degree in telecommunications from the Asian Institute of Technology, Bangkok, Thailand. He has over 20 years of experience in designing and implementing carrier-grade solutions covering the telecom core network elements and their business/operations support systems (BSS/OSS). His areas of expertise include the evolution of telecom BSS/OSS architectures, monetization of emerging 5G/private 5G/industrial 4.0 use cases, public/private/hybrid cloud technology implementations for enterprise/government agencies, and cybersecurity best practices for the communications industry. He is passionate about bringing an individuals' perspective to the conversation on privacy in physical and virtual environments. As a Lead Volunteer of the IEEE Digital Privacy Initiative, he is working on multiple projects, including the creation of the IEEE Digital Privacy Model. His current research interests include understanding individuals' expectations of privacy across regional and cultural boundaries, emerging privacy-preserving technologies, digital privacy legislations for emerging 5G/6G use cases, and generative AI technologies.

PETER EJIM received the Master of Law degree from the UNH Franklin Pierce School of Law, USA. He is currently a Privacy/Compliance Officer Reda Consulting LLC, NJ, USA. His current research interests include data protection compliances and data privacy regulations.

BRUCE HECHT (Senior Member, IEEE) is currently the CEO/CTO of VG2PLAY, Cambridge, MA, USA, to create and advance the enterprise architecture for virtual games learning. He is also the Leader of Sensors, Systems, Circuits and Biomedical Engineering. He has vast experience of more than 30 years in different area of engineering and management.