Recent Advances in a Medical Domain Metaverse: Status, Challenges, and Perspective

Jose M. Ruiz Mejia and Danda B. Rawat
Department of Electrical Engineering and Computer Science
Howard University, Washington, D.C., USA
jose.mejia@bison.howard.edu, db.rawat@ieee.org

***Abstract*—The Meta-verse is the new, innovative platform in which is being investigated by every industry. The thought of simulating reality in a digital platform was never inconceivable but seemed distant. Now, it is taking over every industry like wildfire and the possibilities seem endless. Recently, the healthcare industry is looking into implementing the qualities of the metaverse within specialties and practices of medical professionals. This space encompasses a variety of factors such as virtual reality, augmented reality, and secured spaces for communication and processes. The healthcare industry has been looking into methods to increase patient experience and broadening the accessibility of medical care. Although the concept of the metaverse is not new, the uses are still unexplored and has to many unknowns. In an industry where patient data is critical and remains at the upmost level of privacy, it is unsure that it will remain with its integrity still intact. This paper is aiming to explore the use of the meta-verse in the healthcare industry along with the current status, challenges, and perspective of applicable technology and practices. To be more specific, we focused on the outpatient telemedicine practice experience using body sensor networks and the challenges of maintaining privacy in a healthcare metaverse space.**

***Index Terms*—metaverse, healthcare, vulnerabilities, privacy**

I. Introduction

Many industries are looking into the digital space to create a more unified environment in a simulated manner. The Metaverse is a digital platform that allows for a multi-use environment that is suppose to simulate reality. Many of the industries are looking for cost-effective methods by investing in the metaverse to carry out their business agenda and reducing cost in order to focus on what really matters. In addition, the revolution of remote work brings more attention to using a metaverse platform in order to give a sense of normalcy and moral boost for remote workers. One industry in particular is looking to expand its future with the metaverse, healthcare. The healthcare industry is looking to provide feasible and accessible medical care to the most remote of places in the world. Their main focus is to optimize the concept of telemedicine with healthcare based metaverse. This can come in a variety of forms but the most invested is augmented reality and virtual reality within the industry. These aspects are able to provide medical professionals a virtual design of the patient without being physically present. The use of body sensor networks can provide an enhancement for range of motion and details of the physiology of the patient that can support decision making procedures. Virtual reality has grown rapidly due to machine learning and artificial intelligence. Originally created to give machines their own version of thought, the metaverse is the simulated environment of reality or augmented reality and its development has grown to include facial recognition, natural language processing, 3D object scanning, blockchain, and digital twinning. This technology has improved greatly as a result of machine learning, which is the teaching and training of a computer to autonomously complete tasks and perform various functions. This innovation has provided researchers and engineers the ability to significantly expand upon the capabilities of new and existing technologies using adaptable methods for usage within the metaverse. With advancements in Internet of Things and Cloud platforms, the metaverse does not seem far fetched, however, with unexplored areas brings unexplored threats and challenges in these spaces. It comes with many unknown factors for industry giants such as the healthcare industry. The issues and challenges brought by a simulated, interoperable virtual environment that is suppose to remotely view pertinent, sensitive information can bring vulnerabilities due to the shared platform experience. In addition, outside factors such as body sensor networks and smart devices can bring a plethora of risks to the healthcare system. Identifying the possible risks and vulnerabilities can bring potential hardening measures for an increase of trustworthiness and utilization.

The rest of the paper is organized as follow: Section II provides an overview of a medical domain metaverse along with a definition of the metaverse and its technologies. Section III displays an brief overview of DeepFake and its current utilization in healthcare. Section IV reviews the potential threats and challenges that are faced in a medical domain metaverse. Section V displays the research challenges and our perspective. Section IV provides some closing remarks.

In this survey article, we will discuss the following:

- Provide reason the industry is interest in using the metaverse for healthcare purposes.
- Discuss the different application of the Metaverse in Healthcare: Augmented Reality and Virtual Reality.
- Explore the threats and challenges of the Metaverse in Healthcare.
- Present the use of Deepfakes within the healthcare field.

II. Overview of Medical Domain Metaverse

This sections provides an overview on the technologies that are currently of interest for the adaption of a medical domain metaverse. Their medical practices and patient experience must transcend beyond the simple tele-medicine approach. By looking into advance computational technologies, the patient experience and treatment process in a digital environment can have some resemblance of a real healthcare environment. A medical domain metaverse can provide a variety of services within the healthcare industry such as behavioral health, patient education, pain management, disease awareness, real time E-surgery learning, and medical consultation [1]. Some services are too complex to be adapted by the metaverse such as surgical procedures and palpable examinations which require a professional to touch or percuss certain parts in order to effectively diagnose. Nonetheless, the available technology can greatly enhance compatible medical services within the metaverse. We discuss the use of these technologies and their characteristics.

A. The Metaverse

The metaverse is a term coined from a definition of both digital information (meta-data) and universe platform. Its intent is to bring the real world into simulated virtual environment with endless opportunities. According to [2], it is a computer generated world that has a consistent value and implication but also has an independent eco-system with links to the physical world. Many industries are investing on digital spaces in order to conduct their business as usual from the virtual world. However, the metaverse is a loose term. It encompasses anything and everything that simulated real environments. In [2] [3], the metaverse integrates particular technologies that focus on digital twinning such as virtual reality and augmented reality. The applicability of the metaverse can extended to any industry such as business, marketing, entertainment, and healthcare.

B. Augmented Reality in Healthcare

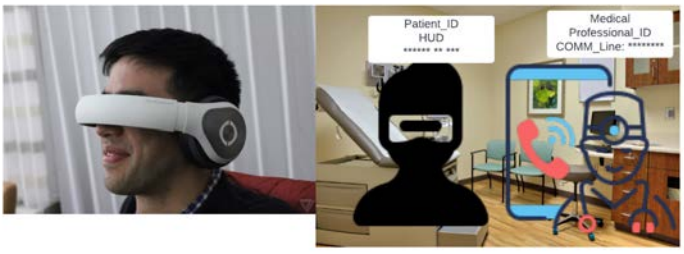

Fig. 1. Patient virtual reality display in a healthcare environment.

Augmented reality can be described in [4] as having systems that augment the senses and perception of the real world environment in a real time manner. This sub-field has been use to enhance the environment with graphical user interface interaction methods in order to bring effective practices by the respective industry. According to [5] [6], augmented reality has been applied in across multiple industries such as specialized medicine, environmental sciences, chemistry, geology, and so much more. Its ability to adapt and provide virtual replication (a.k.a Digital twinning) in real environments has been desired in healthcare industry a patient and medical professional utilization tool. However, this technology is for enhancement of current physical objects and individuals. In the healthcare field, the use of body sensor networks to enhance current smart devices and treatment process in a remote environment.

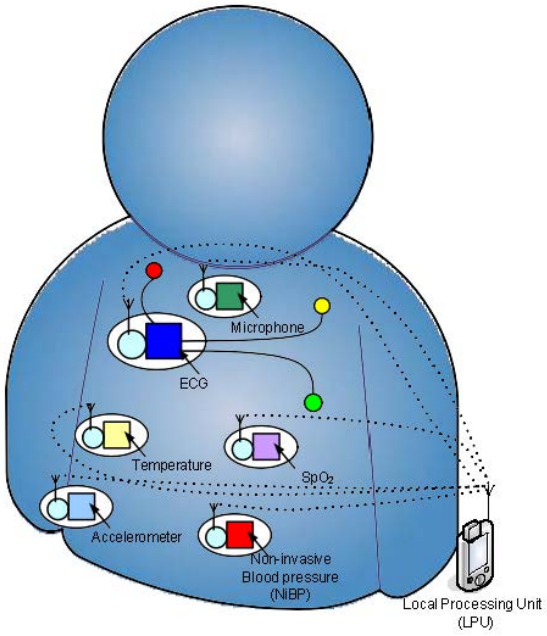

Fig. 2. Body Sensor Network Design [7]

1) Body sensor network in augmented healthcare: Body sensor network (BSN) or sometimes referred as wireless sensor network are embedded systems that is able to remotely monitor and compute real time physiological data [8]. In Fig. 2, we can see that small embedded systems such as a wireless body area network is gathering information for multiple aspects. These body sensor networks come in a variety of use case device such as hearing implants, cardiopulmonary implants, musculoskeletal sensors, and electrocardiogram sensors [9] [10]. Wireless body area networks are gaining much interest in the healthcare field due to its unique attribute of remote surveillance and swift detection. The possibilities of these embedded systems can be surmounted to a plethora of applicability within the healthcare industry. The most applicable health information technological field would be augmented reality. Due to the nature of wireless body area network having the attributes of gathering real time physiological data, an augmented setting such as a surgery room can provide much use. The need of display monitors would be replaced with augmented surgical visors with health user display. With the capabilities of Internet of Things within embedded medical

systems, data residing in multiple smart devices can be collected and displayed for immediate use [11].

C. Virtual Reality in Healthcare

In [12], it defines virtual reality in healthcare as an enriched, interactive, engaging virtual environment that is able to transcend the individual to different environment. The adoption of virtual reality in healthcare depends on the advancement of augmented reality for enhancement capabilities. In Fig. 3, it displays the patient experience in a virtual setting using body area networks for augmented physiological display for medical professional in order to provide effective treatment process. The body area network are acquiring real time health data in order to be brought to the virtual environment and shared with the medical professional as a health user display (HUD).

1) Digital Twinning: Digital twinning is the set of virtual information that is constructed from the original physical object or process [13]. In both virtual and augmented reality, the need for proper digital twinning techniques are drastic in order to have a fully simulated environment. For example, the ability to digitally twin oneself in order to provide a visual representation on current conditions as a patient. This benefits greatly as having an accurate model for review by a medical professional that increase diagnostic accuracy.

D. Blockchain Technology for Health Record Management

The integration of blockchain has given a majority of industry giants a significant advantage to its computational, distributional, and immutable capability [3], [14]. A particular issue conflicting the health industry is its management of health records [15]. Medical data is vast and multiple entities are involved in the management of a singular patient's data. The authors in [15] proposed switching the current record management infrastructure from centralized to decentralized in order to promote accountability and accuracy of record management practices. By having patients more involved in the record management process, it allows for a sustainable verifiable process that ensures an increase in data exchange efficiency. The foundation of blockchain emphasizes unique serialization and identification of data that cannot be changed once verified. This allows for better traceability of any appended or redacted block of information. In a medical domain metaverse, this can be easily adapted in a permissioned based blockchain that is configured for closed networks and requires permission for access [16]. Nonetheless, blockchain technology can greatly enhance the capabilities for record management and other aspects within a medical domain metaverse.

E. Artificial Intelligence in Healthcare

The rise of artificial intelligence has opportunity and innovation within the industry. Artificial intelligence techniques have been used for specialized medical domains such as neurology, cardiology, nephrology, and much more. It has provided advanced algorithms that can analyze enormous data for specialty services. Artificial intelligence can generate large quantities of data and produce quality intelligence. Similar to how a medical provider reviews a patient's data to determine an accurate illness, it can be done with artificial intelligence. For a medical domain metaverse, it can create a more robust and efficient system for any speciality. In [17], Using the heart illness dataset, researchers investigated feature-based and example-based machine learning approaches. This experiment was to draw conclusions from the findings of various procedures and choose one technique over the other for a certain area of healthcare. Artificial Intelligence in healthcare is using two subsections for optimizing care: Supervised learning and unsupervised learning.

1) Supervised Learning: As a predictive model, supervised machine learning is used to categorize unknown data into predefined categories and anticipate trends and future change [18]. A supervised machine learning model will learn to recognize objects and the attributes that categorize them. Supervised machine learning methods are often used to train predictive models. Supervised machine learning models may predict outcomes from fresh and unknown data by learning patterns between input and output data. This might be in the form of anticipating changes in medication prescription values or behavioral tendencies. Classifying various file formats such as photographs, documents, or written words is a common application for supervised machine learning. Using learning patterns in training data to forecast future trends and results. The main classification techniques are Binary, multi-class, and multi-label.

2) Unsupervised Learning: The training of models using raw and unlabeled training data is known as unsupervised machine learning. It is often used to find patterns and trends in raw datasets, as well as to group comparable data into a specified number of groups [18]. It's also a common strategy employed early in the exploratory phase to better comprehend the datasets.

Unsupervised machine learning, as the name implies, is less hands-on than supervised machine learning. A person will select model hyper-parameters like the number of cluster points, but the model will analyze massive amounts of data efficiently and without human intervention. As a result, unsupervised machine learning is well suited to answering queries concerning previously undiscovered patterns and correlations within data. However, since there is less human monitoring, unsupervised machine learning should be given extra consideration for adapting explainable models.

III. Overview of Deepfakes

DeepFake is a term that refers to the technological innovation of artificial intelligence that trains models to manipulate pictures, videos, and audio to create a synthetic media output that appears realistic [19]. One of the first modern instances of its use can be traced to 1997, when researchers from the Interval Research Corporation published the Video Rewrite project, which was able to successfully map the audio from a separate source to an original video. This became the foundation for future works that manipulate media through the utilization

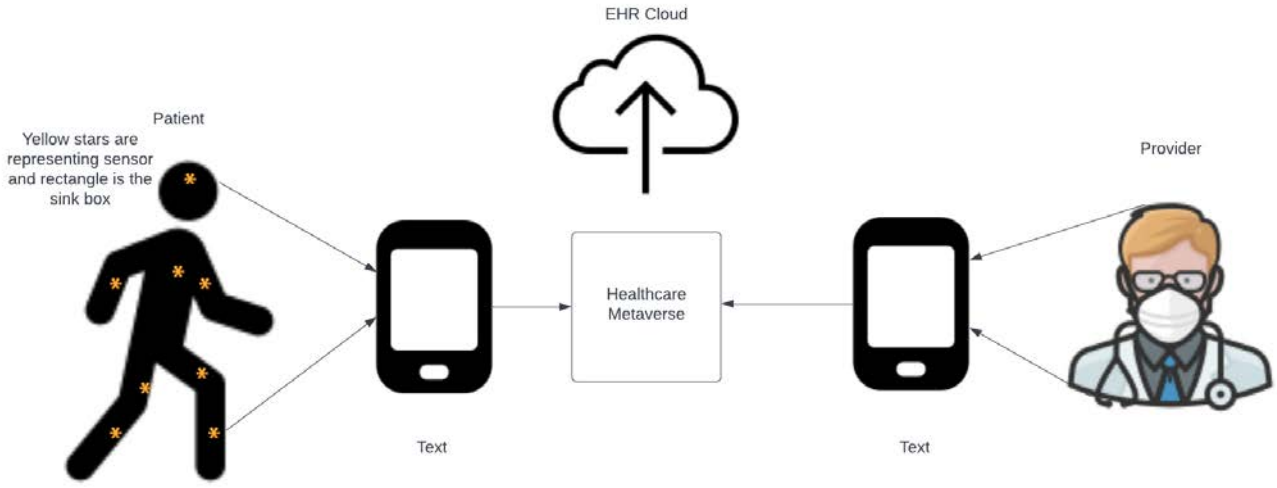

Fig. 3. Diagram of the patient and medical professional experience within the Healthcare Metaverse.

of machine learning algorithms. The name DeepFake gained notoriety in 2017 after a Reddit user by the same moniker uploaded shameful videos of celebrities and political figures in a sexually explicit manner. Since then, this technology has allowed individuals with a computer or phone to make a comedic, political, or even pornographic video of anyone saying whatever they desire, without the victim's consent [20]. A popular example of this occurred in 2017, when University of Washington researchers sampled audio footage of former President Obama to develop a photo-realistic video of him speaking with the pre-recorded audio [21]. The original video did not have to match exactly with the altered video, as the algorithms took into account the mouth shape, facial structure, and mannerisms. This research received positive recognition for mapping the mouth shape of a generated video to the voice in a given audio with incredible results. Since then, DeepFake technology has grown substantially, but a lot of its applications have proven dangerous to many.

1) Deepfakes in Healthcare: Through digital mapping or the generation of experimental data, DeepFake has the potential to significantly improve our current healthcare system. Alzheimer's patients can view younger versions of people they know by digitally reproducing their image and likeness [19]. This could assist with their memory recollection by reassuring them of their loved ones' presence. Another application of mapping in the medical profession is to provide surgeons and patients with a visual representation of what their procedure will look like. Transgender people, for example, would be able to view themselves as the gender with which they identify [19]. Hospitals can employ DeepFake technology to create simulated patient data that could be used for testing without the expense of using real patients [22]. They would ideally generate virtual patients using the data they already possess. This could help to improve data privacy and security among medical experts, as well as minimize bias in the sector. DeepFake's usage in healthcare may become more beneficial as the technology improves.

IV. Potential Threats and Challenges in Healthcare Metaverse

A. Deepfakes Spoofing Attacks

One of the most difficult aspects of DeepFakes is verifying the authenticity of the content being distributed. Authentication is more effective than detection since it assures the viewer that the media being presented is genuine and unmodified. This is especially important for identifying patients within the metaverse because it can compromised patient data integrity. In addition, impersonating not only the patient but the medical professional can be a possibility. Impersonation attacks can greatly affect the integrity of a healthcare based metaverse due to the nature of impersonating authorized individuals. The attacker would be able to acquire sensitive data unbeknownst to anyone [2]. Ideally, an autonomous system would be implemented that would initiate an authentication process to distinguish between fraudulent and genuine media [20]. Software that allows digital watermarking and block-chain provenance are an effective solution to this problem.

B. Man-in-the-Middle Attacks

Privacy is the utmost practice within the healthcare field. Patient information must be kept within authorized users in order to protect the stakeholders. In a healthcare based metaverse, information can be viewed by an attacker due to it being a new concept. A Man-in-the-Middle attacker can spectate the exchange of information between the body sensor network and the metaverse. In [23], mentions that pervasive data collection can be acquired by the spectating of the user traversing through the metaverse. The nature of MIIM attacks is for espionage and have the ability to silently acquire the

knowledge, but in a user heavy environment like the metaverse it is difficult to identify if their is an attack present. Thus, prevention methods must be taken.

C. Data Injection Attacks

Data injection attacks can lead to deadly consequences in a healthcare based metaverse environment. For example, a patient using a body area network to detect physiological signs such a vitals and electrocardiogram. If a data injection attack occurred, it can manipulate the system to think the patient is either in a critical state or increase the sensitivity of the sensors. Data injection attacks can inject false data into the patient file such as incorrect vitals, location, and identity [24]. With false data and tampering, the trustworthiness of medical institutions would falter and lives would be complicated due to the corrupted data.

D. Establishing Trust Between Stakeholders

In Fig. 1, it displays a patient using a virtual reality device to enter a visual display of a healthcare environment. In this diagram, the patient is able to view the avatar of the provider along with an serialized indicator such as an identification number. This only solves a fraction of the problem with establishing trustworthiness in a medical metaverse. With new technology and lack of implementation, the stakeholders have skeptic views of a digital environment in which discussing sensitive information through a digital device without having the ability to verify authenticity. However, this is slowly becoming the norm since the majority of services and consultations have moved to a tele-medicine platform. Again, this solved only a fraction of a problem. The challenges of establishing trust between stakeholders come from the technology and data itself. Because medical data is abundant and distributed, the completeness of a patient record may hinder the ability of accurate diagnosis. The lack of medical data interoperability has caused an issue in the development of a medical domain metaverse because diagnostic models require accurate and traceable data. If pieces of data are missing, then misdiagnosis and incomplete datasets can cause a disruption in both services and trustworthiness.

V. Research Challenges and Perspective

The healthcare industry is a highly regulated system that serves to provide carefully crafted care to its constituents. A few challenges for adapting healthcare into the metaverse are maintaining a sense of privacy and trustworthiness, interoperability of cloud data information systems, and the lack of current technology being develop for a sustainable medical domain environment. However, the outlook for this field looks very promising. As previously mentioned, many companies are investing in the development of a metaverse platform in order to provide accountability and efficiency for their medical patients. The medical industry is already implementing cloud computing, Internet of Things, and tele-medicine into practice. The future perspective is to provide a shared environment for multiple health services with the assistance of virtual and augmented reality technology.

VI. Conclusion

The healthcare industry has brought many technological advances over the years. The interest to promote a safer, more secure environment for outpatient treatment is a reasonable investigation that should be considered in every healthcare organization. The usage of tele-medicine has superseded the expected amount due to the COVID-19 pandemic, thus finding methods to optimize that experience in a more virtual environment seems logical. However, the need to maintain privacy and security of health data in a shared, virtual platform also brings concerns on its implementation. In this paper, we briefly explained healthcare metaverse and its use case, we presented potential vulnerabilities on using deep fakes to override facial authentication, and we discussed the different methods of exploitable attacks that can occur within a healthcare based metaverse environment. We presented different state of the art artificial intelligence approaches within healthcare. Lastly, we briefly mentioned the ethical concerns of establishing trust in a medical domain metaverse.

Acknowledgemrnt

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) at Howard University under Contract W911NF-20-2-0277 with the U.S. Army Research Laboratory and in part by Meta (Facebook) research gift funds. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

References

[1] M. A. I. Mozumder, M. M. Sheeraz, A. Athar, S. Aich, and H.-C. Kim, "Overview: Technology roadmap of the future trend of metaverse based on iot, blockchain, ai technique, and medical domain metaverse activity," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, p. 256–261, Feb 2022.

[2] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *arXiv:2203.02662 [cs]*, Apr 2022. arXiv: 2203.02662.

[3] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," *arXiv:2203.09738 [cs]*, Mar 2022. arXiv: 2203.09738.

[4] J. Gerup, C. B. Soerensen, and P. Dieckmann, "Augmented reality and mixed reality for healthcare education beyond surgery: an integrative review," *International journal of medical education*, vol. 11, p. 1–18, Jan 2020.

[5] E. Zhu, A. Hadadgar, I. Masiello, and N. Zary, "Augmented reality in healthcare education: an integrative review," *PeerJ*, vol. 2, p. e469, Jul 2014.

[6] V. Ferrari, G. Klinker, and F. Cutolo, "Augmented reality in healthcare," *Journal of Healthcare Engineering*, vol. 2019, p. 9321535, Jul 2019.

[7] B. P. L. Lo, S. Thiemjarus, R. King, and G.-Z. Yang, "Body sensor network – a wireless sensor platform for pervasive healthcare monitoring," p. 4.

[8] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, p. 5561–5595, Jun 2011.

[9] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K. Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed, "Smart home-based iot for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *Journal of Medical Systems*, vol. 43, p. 42, Jan 2019.

[10] L. Quintero, P. Papapetrou, J. E. Muñoz, and U. Fors, "Implementation of mobile-based real-time heart rate variability detection for personalized healthcare," in *2019 International Conference on Data Mining Workshops (ICDMW)*, p. 838–846, Nov 2019.

[11] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, *IoT Sensing Capabilities: Sensor Deployment and Node Discovery, Wearable Sensors, Wireless Body Area Network (WBAN), Data Acquisition*, p. 127–151. Intelligent Systems Reference Library, Cham: Springer International Publishing, 2020.

[12] H. Aziz, "Virtual reality programs applications in healthcare," *Journal of Health & Medical Informatics*, vol. 9, p. 305, Mar 2018.

[13] M. M. Rathore, S. A. Shah, D. Shukla, E. Bentafat, and S. Bakiras, "The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities," *IEEE Access*, vol. 9, p. 32030–32052, 2021.

[14] T. Le Nguyen, "Blockchain in healthcare: A new technology benefit for both patients and doctors," in *2018 Portland International Conference on Management of Engineering and Technology (PICMET)*, p. 1–6, Aug 2018.

[15] V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, "Health record management through blockchain technology," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, p. 1411–1415, Apr 2019.

[16] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, p. 1–4, Nov 2017.

[17] D. Dave, H. Naik, S. Singhal, and P. Patel, "Explainable ai meets healthcare: A study on heart disease dataset," Nov 2020. arXiv:2011.03195 [cs].

[18] T. Huynh-The, Q.-V. Pham, X.-Q. Pham, T. T. Nguyen, Z. Han, and D.-S. Kim, "Artificial intelligence for the metaverse: A survey," *arXiv:2202.10336 [cs]*, Feb 2022. arXiv: 2202.10336.

[19] M. Somers, "Deepfakes, explained," Jul 2020.

[20] M. Westerlund, "The emergence of deepfake technology: A review," *Technology Innovation Management Review*, 2019.

[21] S. Suwajanakorn, S. M. Seitz, and I. Kemelmacher-Shlizerman, "Synthesizing obama: Learning lip sync from audio," *ACM Trans. Graph.*, vol. 36, jul 2017.

[22] S. Neethirajan, "Is seeing still believing? leveraging deepfake technology for livestock farming," *Frontiers in Veterinary Science*, vol. 8, p. 740253, Nov 2021.

[23] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52–61, 2018.

[24] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.