American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
http://asrjetsjournal.org/

How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery

Kiran Sharma Panchangam Nivarthi*

31108 Algonquin Trail, Chisago City, MN, 55013, USA
Email: Kiransnandu@gmail.com

Abstract

Privacy Enhancing Technologies (PETs) are playing a crucial role in maturing digital healthcare delivery for mainstream adaption from both a social and regulatory perspective. Different PETs are improving different aspects of digital healthcare delivery, and we have chosen seven of them to observe in the context of their influence on digital healthcare and their use cases. Homomorphic encryption can provide data security when healthcare data is being collected from individuals via IoT or IoMT devices. It's also a key facilitator for large-scale healthcare data pooling from multiple sources for analytics without compromising privacy. Secure Multi-Party Computation (SMPC) facilitates safe data transfer between patients and healthcare professionals, and other relevant entities. Generative Adversarial Networks (GANs) can be used to generate larger data sets from smaller training data sets directly obtained from the patients, to train AI and ML algorithms. Differential Privacy (DP) focuses on combining multiple data sets for collective or individual processing without compromising privacy. However, its addition of noise to obscure data has some technical limitations. Zero-Knowledge Proof (ZKP) can facilitate safe verifications/validation protocols to establish connections between healthcare devices without straining their hardware capacities. Federated learning leans quite heavily towards training AI/ML algorithms on multiple data sets without margining or compromising the privacy of the constituents of any dataset. Obfuscation can be used in different stages of healthcare delivery to obscure healthcare data.

Keywords: Privacy enhancing technology; Digital Healthcare.

1. Introduction

The rapid and radical evolution of digital healthcare is facilitated by technologies like the cloud, AR/VR, digital twins, 3-D printing, etc. However, there are security and compliance concerns associated with data sharing between patient and physician/healthcare facility or data shared between facility to facility [1] for comprehensive digital healthcare delivery and research purposes. These concerns impede the advent of digital healthcare delivery. Privacy Enhancing Technologies (PETs) are positively transforming digital healthcare delivery by enhancing data security.

---

* Corresponding author.

Different PETs are contributing differently to the transformation of digital healthcare delivery, and for this paper, we are looking into the impact of seven PETs. Homomorphic encryption is a privacy-enhancing technology that allows data processing and operation in encrypted form. As healthcare becomes more reliant on cloud computing, confidentiality concerns are rising. Patient data can be routed through multiple third-party entities for analysis, and if each entity has to decrypt the data to process it, it creates multiple privacy weak points. By allowing data to be processed in its encrypted form, Homomorphic Encryption, especially Fully Homomorphic Encryption, has the potential to facilitate digital healthcare [2]. It can also be used to keep personal healthcare information secure on a blockchain-based platform for patients that use the keyword search to look for their records, making them more susceptible to breaches/cyberattacks [3].

Secure Multi-Party Computation (SMPC) is a cryptography technique that allows multiple parties to work on a data set/computation without revealing the data to the other parties. One of the most significant transformative contributions of this privacy-enhancing technology to digital healthcare, in particular, and healthcare in general, is that it allows multiple healthcare facilities/departments to pool their patient data without compromising patient confidentiality [4]. The collective data pool can make it significantly easier to track patterns across large population samples (city, country, etc.). It's also used to share patients' Electronic Health Records (HER) with multiple entities without breaking confidentiality, assuming a pre-approval from the patients when they are incapacitated to give consent to sharing data [5].

Generative Adversarial Networks (GANs) train two separate neural nets by forcing them to compete. A common application of this PET is to generate data from a primary data set that is statistically similar to the original data set without any of the details of the original data set. GANs can be used to generate synthetic Electronic Health Records (EHRs) from original patient records (including imaging data/scans) that can be used for training Artificial Intelligence Systems without compromising data confidentiality [6].

Differential privacy is the process of introducing a calculated amount of noise in any database so that it's enough to diffuse/obscure identifiable information without compromising the patterns/insights the data can be used to generate. It can be used to create collective data pools of patient Electronic Health Records (EHRs), including medical images, to train Artificial Intelligence and Machine Learning models for better diagnostics without compromising data confidentiality. It can be used in conjunction with other technologies like blockchain [7] and Federated Learning.

A Zero-Knowledge Proof (ZKP)allows one entity to prove to another entity that a statement is true without actually sharing the statement or any other information to back up this claim. This facilitates permissions and authorizations without actual information changing hands and has multiple uses in digital healthcare delivery. A ZKP can offer relevant entities (like insurance companies) access to patients' Electronic Healthcare Records (EHR) when they are stored in a blockchain with other data security features in place [8].

Federated Learning allows multiple devices/entities to train a single machine learning system or learn from an algorithm that's trained using data from all the devices without the exchange of data between individual entities or between an entity and a central system. This will allow healthcare facilities to keep data like patient

Electronic Healthcare Records confidential while still training useful models like AI-based tumor detection through federated learning.

Obfuscation is a set of PETs used to encrypt/obscure data to ensure that only relevant entities (with the requisite keys/permissions) can decrypt data. In healthcare, it can be used to safely encrypt Wireless Body Area Network (WBAN) data [9] and to protect the JPEG compression processors in medical imaging instruments from potential threats [10].

The purpose of this research is to determine how various PETs are transforming Digital Healthcare Delivery and if the impact is substantial in some areas and mild/absent in others. We will determine that by looking at established applications for individual PETs and overlapping them with the key pain points and goals of digital healthcare delivery.

2. The Impact Of Individual PETs On Transforming Digital Healthcare Delivery

Each Privacy-Enhancing Technology (PETs) has its own overlap with the digital healthcare industry. Some PETs facilitate better healthcare delivery through innovations in research, while others offer more security to healthcare data in transit. Understanding the overlap of each PET with digital healthcare is critical to making smart decisions regarding technological adaptions and defining new protocols.

2.1 Homomorphic Encryption

There are two types of Homomorphic Encryptions:

Partially homomorphic encryption (PHE) allows you to perform one mathematical function – addition or multiplication (for the purpose of encryption) infinite times on the text/data that needs to be encrypted. A variation is "Somewhat homomorphic encryption," which limits you to a function *and* a finite number of times it can be performed. An example of partially homomorphic encryption is the most commonly used RSA cryptosystem.

Fully homomorphic encryption (FHE) facilitates multiple mathematical functions (both addition and multiplication), resulting in more complex encryptions that are extensively being used in cloud computing. The most significant benefit it offers is the possibility of working on encrypted data without decrypting it first [11].

Homomorphic encryption, especially FHE, is contributing to better healthcare delivery in multiple ways. This includes:

- Data compliance has become a major concern for most regulatory bodies as healthcare becomes more digitized. Healthcare is also one of the most heavily cyber-attacked industries, making security and data compliance even more profoundly important, especially when it comes to migrating and processing healthcare data on the cloud and using cloud-based applications [12]. This is a hindrance in digital healthcare delivery, which FHE can help overcome by offering “Encryption as a service.” [13]

- FHE can be a key facilitator of the upcoming Internet of Medical Things or IoMT, a variation of IoT which specifies the widespread interconnectivity of healthcare devices and patients [14]. Specific FHE areas can be applied to include cloud-based health monitoring [15] and wearable devices (connected to a network) [16].
- The most significant contribution of FHE to transforming digital healthcare delivery, however, will be in the realm of data analytics [17] and federated learning [18]. Cloud is the ideal way for healthcare facilities, research organizations, individual researchers, and all other entities working on healthcare research to pool their data for a massive data repository that can be used to train AI and ML models. Applications of this phenomenon can already be seen in the healthcare industry, with AI systems examining chest X-rays on par and, in some cases, better than their human counterparts. These models can become even more productive and accurate if they have more data to train on. But healthcare data sharing is a compliance nightmare, limiting these collaborations and interactions that may push digital healthcare delivery years ahead of its time. Here, techniques and technologies like FHE can provide a valid solution.

2.2 Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) is an old cryptography concept/approach to data protection that has experienced a revival with the advent of blockchain and the cloud. When properly implemented, SMPC allows a group of individuals/entities to compute/run calculations on a collective data set without revealing which portion of the data set is theirs. This has promising implications for the healthcare sector at large and digital healthcare delivery in particular. The Healthcare industry, like all others, must resolve the conflict between digital security concerns and the need to contribute to and take advantage of business intelligence available through collaboration. This is one of the avenues where SMPC can aid the healthcare industry. Another of the most promising applications of SMPC is the development of mobile applications and web applications that allow patients to share their data with third parties for processing/assessment without risking their privacy. It can be integrated with typical databases and novel ones, including blockchain-based databases [19].

Data communication and safety/security of medical data in transit is becoming another complex facet of digital healthcare delivery. In addition, to live sessions between healthcare professionals and patients, which may rely on other cryptography and cybersecurity protocols and technologies for protection, there is also the matter of medical data, which has to be circulated to multiple entities. The problem will only grow with IoT advents and integration, and other encryption solutions may prove too expensive to be feasible for all healthcare establishments, departments, and patients. SMPC-based solutions can be more affordable, though they have severe scale limitations [20].

2.3 Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) are a Machine Learning (ML) model for training two neural nets. It requires an adversarial setting where the two neural nets compete against each other, where one's loss is another's gain. The two neural nets are the Generator and Discriminator. The generator is tasked with generating data similar to test data and are rewarded for its originality, i.e., disassociation from the original data set while mimicking the same characteristic – akin to forging an art piece or currency. The Discriminator is rewarded

when it can identify the generative data as fake [21].

A GAN's ability to generate data that are indistinguishable from real without carrying over the identification features or traceability to real data makes it incredibly useful for healthcare. Some of the possible applications in the digital healthcare delivery being explored include:

- Enlarging retinal image datasets for the training of AI and ML algorithms for medical image analysis. With the right input methodology, GANs offer superior-quality images/data sets from comparable methods [22].
- Using GAN for Skin Lesion Synthesis [23]. It can be used to generate samples of realistic skin lesion images that can be used against skin cancer.
- A variation of GAN can be used for Medical Image Segmentation of MRI and CT images [24].

All three of these are the facets of digital healthcare, which are improved and sustained by collective datasets and pooled resources. The AI and ML algorithms trained by the data sets generated by GAN can be used in multiple areas of digital healthcare delivery, including pre-screening of patients' reports, AI-assisted diagnosis, and self-care routines. An individual may leave skin lesions unattended for days, even weeks, but if a simple mobile app (using an AI/ML model trained by GAN-generated data) is available that offers 60% to 70% accuracy in determining whether a particular skin lesion can lead to cancer, early identification rates might soar.

2.4 Differential Privacy (DP)

Differential privacy is a PET designed to use large data sets without compromising the privacy of the individuals constituting the data sets (or contributing to a collective pool of data). This is done by adding random noise to the data, obscuring it in a way that can't be used to identify or trace an individual. This doesn't make the data useless because the law of large numbers allows for random noises to be canceled out, revealing a statistical average that might not be too different from a hypothetical dataset of accurate information. More sophisticated DP approaches might be present. In DP for healthcare data, different methods of adding noise are available that may impact the quality of the resultant data based on how large the sample is [25]. From a digital healthcare delivery perspective, this may be used to anonymize healthcare records from sources that generate small sample sizes, like healthcare centers in rural areas or data sets pertaining to rare diseases, while preserving the accuracy with the right noise-adding mechanism. However, a sophisticated attack that generates a systemic set of queries may still have a high probability of isolating information regarding an individual (or a few individuals) even if the noise is added. This can be countered using an adaptive Differential Privacy Algorithm [26]. Different DP techniques and algorithms offer different levels of accuracy in the resulting data (without private information) that can be computed and worked on, especially in sensitive data sets like identifying patterns in breast cancer patients [27]. The more fine-tuned the DP techniques are, the better it is for digital healthcare delivery, as many of its core advantages rely upon the accurate processing of collective data pools/data sets for research.

2.5 Zero-Knowledge Proof (ZKP)

Data compliance is one of the primary concerns when it comes to digital healthcare delivery. Digital information

like healthcare records, especially when kept in the cloud, may have multiple vulnerabilities if several entities have access to it. Here, a PET like Zero-Knowledge Proof (ZKP) which allows two entities to establish trust *before* any identifiable information is transferred/transmitted, can add a much-needed layer of data security. An example of such an application would be the compliant connectivity of mobile units in a Vehicular ad hoc network (VANET) that is used for patient monitoring [28] with cloud-based healthcare networks while the patient is en route [29].

ZKP-based solutions like Authenticated Key Agreement (AKA) can facilitate a safe and compliant merger of IoT and Healthcare, referred to as the Internet of Healthcare Applications (IoHA) as well as the Internet of Medical Things (IoMT). This includes bypassing an inherent limitation of IoT (limited memory on connected devices), which renders more sophisticated compliance protocols and security measures obsolete [30]. Another variation of the same application is using ZKP for wearable biosensors, allowing them to connect safely with a healthcare application instead of using vulnerable connections like Bluetooth. This can also work for an application where patient data is stored on a Blockchain [31].

The applications of ZKP as a PET in transforming digital healthcare delivery lean quite heavily towards facilitating lightweight yet compliant and secure connections through which healthcare data can be transmitted between devices and cloud-based healthcare applications. This makes it a less resource-consuming alternative to more sophisticated peers.

2.6 Federated Learning

Federated learning is also described as decentralized machine learning that facilitates data privacy, a trait that makes it ideal for training on healthcare data for which privacy is of paramount importance. Prototypes of this PET for digital healthcare delivery are already being tested. One example is the detection of early signs of Dementia by analyzing audio recorded by various IoT devices in a smart home [32]. A Dementia diagnosis in the early stages can lead to significant social and financial repercussions, including job loss, and patient confidentiality is crucial. A federated learning-based scheme, augmented by another PET (Differential Privacy), can become a powerful digital healthcare tool that can lead to early diagnosis and better treatment.

One test case for digital healthcare delivery facilitated by federated learning involved edge computing for COVID diagnosis. The models were trained on datasets, including X-rays and ultrasound, and promising results were achieved [33].

In addition to training datasets already available with healthcare institutions and facilities, Federated Learning can facilitate the training of ML algorithms using data collected directly from patients using medical IoT (and regular IoT devices) while adhering to the most stringent data privacy practices. However, from data collection to its anonymization and processing, multiple PETs may have to be employed in the process.

2.7 Obfuscation

Data obfuscation is a set of techniques and individual PETs used to obscure data in a way that it’s difficult to

reverse engineer to its original form. Encryption, tokenization, and data masking are three common types of data obfuscation. Obfuscation techniques are already widely used to enhance data privacy and have both mature and potential uses in the digital healthcare delivery arena.

Ontology-Based obfuscation can be used for healthcare data anonymization so that it can be safely shared with relevant entities for research without significantly reducing the accuracy of the data [34]. Obfuscation can also be used alongside GAN for remote healthcare monitoring while preserving data privacy, i.e., audio data collected on patients from sensors in IoT devices is obfuscated to protect the privacy of the individuals, and GAN generates the data to train the remote monitoring models [35]. Another proposed solution that merges digital healthcare delivery and obfuscation as the PET is using indistinguishability obfuscation in the RFID authentication system. Indistinguishability obfuscation is the cryptography technique that can obscure a computer code/program to make it completely unintelligible yet just as functional as the original code/program. Its proposed use for RFID authentication aims to capitalize on the mainstream use of RFID technology in the IoT [36]. With the right approach, Obfuscation-based models/tools can offer better data privacy while retaining a higher degree of predictive utility (for training ML models) than comparable PETs like differential privacy [37].

3. Results

Two out of five of the most common challenges identified for digital healthcare delivery [38] are directly connected with data privacy, and two (AI and Genomics) are partially connected to it. This indicates that data privacy is one of the core challenges to mainstream digital healthcare delivery and may even be impacting the widespread rollout.

Privacy Enhancing Technologies (PETs) provide some answers to privacy concerns, and since these concerns are diverse and varied, so are the solutions. The most common application we found for most PETs was to train Artificial Intelligence (AI) and Machine Learning (ML) algorithms for better diagnosis, early diagnosis, identifying patterns in demographics, etc. This indicates that PETs facilitate a specific aspect of digital healthcare delivery more than all others. However, many of the advancements in PETs for healthcare focused on the safe transmission of data between healthcare institutions and healthcare and other entities can also apply to the first phase of the data transfer, i.e., from patients to the healthcare facility. Most PETs aim to adhere to data compliance laws pertaining to healthcare records within specific jurisdictions (Europe, the US, etc.) in particular use-case scenarios.

Many PETs are oriented toward medical IoT, which focuses on safe, privacy-oriented healthcare data collection and storage (on the cloud). These are also connected to edge-computing practices in digital healthcare delivery. However, these might be farther into the future than the mainstream adoption of digital healthcare in our societies, like AI/ML-based pre-assessments from available patient data, symptoms, family history, etc.

4. Discussion

Many PETs are aiming to solve the data privacy concerns of tomorrow, resulting from the merger of healthcare

and more accessible digital healthcare, but we are not yet seeing a specific PET (or a group of PETs) enabling digital healthcare platforms that may evolve to the same scale as prominent social media platforms. But it's a distinct possibility that we may see a standardization of the use of certain PETs in certain digital healthcare delivery use cases and once the chain is complete, starting with data collection from patients and ending at unobstructed data sharing between healthcare researchers – and every step adhering to all healthcare compliance regulations. Significant research and trend monitoring is needed to identify how far the existing PETs are from offering optimal, feasible, and compliant data privacy solutions for comprehensive digital healthcare platforms. The closer we get, the more consolidation and the movement of "big money" from both tech and healthcare giants we may observe in this arena.

The technical limitations of PETs need to be addressed as well. Some PETs are better suited for edge computing, and their adoption in digital healthcare may be expedited as we move closer to Web 3.0 and decentralized networks. They will leverage the computing power available at or near the nodes. Other PETs still rely upon the massive computing power that cloud-based platforms may be able to offer. The hardware, time, tech, maintenance, and risk cost associated with each PET might result in a hierarchy for each use case, and a healthy combination of PETs at different layers of digital healthcare delivery may be an optimal solution. This aspect needs extensive research and a standardized measurement approach to compare the efficiency of different PETs in different scenarios for different sample sizes and data accuracy levels (for research data).

5. Conclusion

The evolution and standardization of PETs are crucial for the positive transformation of digital healthcare delivery. Until the most optimal PETs, which also adhere to the compliance requirements, are not powering comprehensive and end-to-end digital healthcare delivery solutions, we may see societal and legal opposition to mainstream digital healthcare adoption. PETs can neutralize many of the concerns regulatory bodies and patients might have regarding the safety of healthcare data and are, therefore, crucial in transforming digital healthcare delivery from a novel practice to a part of everyday life alongside IoT.

References

[1] J. Scheibner , J. L. Raisaro , J. R. Troncoso-Pastoriza , . M. Ienca, J. Fellay, E. Vayena and J. Hubaux, "Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis," *JMIR Publications*, 2021.

[2] R. Bhatia and K. Munjal, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex & Intelligent Systems*, 2022.

[3] A. Ali, M. F. Pasha, J. Ali, O. H. Fang, M. Masud, A. D. Jurcut and M. A. Alzain, "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," *Sensors*, 2022.

[4] L. Vogelsang, M. Lehne, P. Schoppmann, P. Fabian , T. Sylvia , S. Björn and S. Josef , "A Secure Multi-Party Computation Protocol for Time-To-Event Analyses," in *Digital Personalized Health and Medicine*, 2020, pp. 8-12.

[5] K.-L. Tan, C.-H. Chi, and K.-Y. Lam, "Secure Multi-Party Delegated Authorisation For Access and Sharing of Electronic Health Records," arXiv:2203.12837, 2022.

[6] T. Amirsina and E. A. Fox, "CorGAN: Correlation-Capturing Convolutional Generative Adversarial Networks for Generating Synthetic Healthcare Records," in *The Thirty-Third International FLAIRS Conference*, Blacksburg, Virginia, 2020.

[7] A. W. Huang, A. Kandula and X. Wang, "A Differential-Privacy-Based Blockchain Architecture to Secure and Store Electronic Health Records," *ICBCT*, 2021.

[8] B. Sharma, R. Halder, and J. Singh, "Blockchain-based Interoperable Healthcare Using Zero-knowledge Proofs and Proxy Re-Encryption," in *2020 International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, India, 2020.

[9] Y. Zhang, D. He, Y. Li, M. Zhang, and K.-K. R. Choo, "Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks," *IEEE Systems Journal*, 2020.

[10] A. Sengupta and M. Rathor, "Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems," *IEEE Access*, 2020.

[11] M. A. Will and R. K. Ko, "Chapter 5 - A guide to homomorphic encryption," *The Cloud Security Ecosystem*, pp. 101-127, 2015.

[12] M. C. Compagnucci, J. Meszaros, T. Minssen, A. Arasilango, T. Ous, and M. Rajarajan, "Homomorphic Encryption: the 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?," *European Pharmaceutical Law Review*, pp. 144-155, 2019.

[13] A. E. Bouchti, S. Bahsani, and T. Nahhal, "Encryption as a service for data healthcare cloud security," in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, New Delhi, India, 2020.

[14] M. M. Salim, I. Kim, U. Doniyor, C. Lee and J. H. Park, "Homomorphic Encryption Based Privacy-Preservation for IoMT," *Applied Sciences (MDPI)*, 2021.

[15] O. Kocabas, T. Soyata, J.-P. Couderc, M. Aktas, J. Xia and M. Huang, "Assessment of cloud-based health monitoring using Homomorphic Encryption," in *IEEE*, Asheville, NC, 2013.

[16] A. Prasitsupparote, Y. Watanabe and J. Shikata, "Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices," in *ISDF*, Greece, 2018.

[17] Ö. Kocabaş and T. Soyata, "Medical Data Analytics in the Cloud Using Homomorphic Encryption," *E-Health and Telemedicine: Concepts, Methodologies, Tools, and Applications*, p. 18, 2016.

[18] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic Encryption-based Privacy-preserving Federated Learning in IoT-enabled Healthcare System," *IEEE Transactions on Network Science and Engineering*, pp. 1 - 17, 2022.

[19] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *Journal of Medical Systems*, 2016.

[20] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu and M. S. Hossain, "Privacy-Preserving Data Communication Through Secure Multi-Party Computation in Healthcare Sensor Cloud," *Journal of Signal Processing Systems volume*, pp. 51-59, 2017.

[21] B. Paria, A. Lahiri, and P. K. Biswas, "PolicyGAN: Training generative adversarial networks using policy gradient," in *IEEE*, Bangalore, India, 2017.

[22] Z. Yu, Q. Xiang, J. Meng, C. Kou, Q. Ren, and Y. Lu, "Retinal image synthesis from multiple-landmarks input with generative adversarial networks," *BioMedical Engineering OnLine*, 29.

[23] A. Bissoto, F. Perez, E. Valle, and S. Avila, "Skin Lesion Synthesis with Generative Adversarial Networks," Springer, 2018.

[24] V. Saaran, V. Kushwaha, S. Gupta and G. Agarwal, "A Literature Review on Generative Adversarial Networks with Its Applications in Healthcare," *Congress on Intelligent Systems*, vol. Volume 1, pp. 215-225, 2021.

[25] M. T. Zia, M. A. Khan, and H. El-Sayed, "Application of Differential Privacy Approach in Healthcare Data – A Case Study," in *14th International Conference on Innovations in Information Technology (IIT)*, Al Ain, United Arab Emirates, 2020.

[26] A. Alnemari, C. J. Romanowski and R. K. Raj, "An Adaptive Differential Privacy Algorithm for Range Queries over Healthcare Data," in *IEEE International Conference on Healthcare Informatics*, Rochester, NY, USA, 2017.

[27] A. Vadavalli and R. Subhashini, "An Improved Differential Privacy-Preserving Truth Discovery approach In Healthcare," in *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, Canada, 2019.

[28] S. Kalaiyarasi and A. J. S. Kumar, "Secured Healthcare and Patient Monitoring System using Vanet Based Wban," in *International Journal of Engineering Research & Technology (IJERT)*, Salem, India, 2015.

[29] J. A. Chaudhry, S. Member, K. Saleem, M. Alazab, H. M. A. Zeeshan, J. Al-Muhtadi and J. J. P. C. Rodrigues, "Data Security Through Zero-Knowledge Proof and Statistical Fingerprinting in Vehicle-to-Healthcare Everything (V2HX) Communications," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, vol. 22, no. 6, pp. 3869 - 3879, 2021.

[30] G. S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage and M. Alazab, "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," *Sustainable Cities and Society*, vol. 80, 2022.

[31] A. E. B. Tomaz, J. C. D. Nascimento, A. S. Hafid and J. N. D. Souza, "Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain," *IEEE Access*, vol. 8, pp. 204441-204458, 2020.

[32] J. Li, Y. Meng, L. Ma, S. Du, H. Zhu, and Q. Pei, "A Federated Learning Based Privacy-Preserving Smart Healthcare System," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2021-2031, March 2022.

[33] A. Qayyum, K. Ahmad, M. A. Ahsan, A. Al-Fuqaha and J. Qadir, "Collaborative Federated Learning for Healthcare: Multi-Modal COVID-19 Diagnosis at the Edge," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 172-184, 2022.

[34] L. H. Iwaya, F. Giunchiglia, L. A. Martucci, A. Hume, S. Fischer-Hübner and R. Chenu-Abente, "Ontology-Based Obfuscation and Anonymisation for Privacy," *IFIP Advances in Information and Communication Technology*, vol. 476, 2016.

[35] K. Vatanparvar, V. Nathan, E. Nemati, M. M. Rahman and J. Kuang, "A Generative Model for Speech

Segmentation and Obfuscation for Remote Health Monitoring," in *IEEE 16th International Conference on Wearable and Implantable Body Sensor Networks*, Mountain View, CA, USA, 2019.

[36] S. Xie, F. Zhang, and R. Cheng, "Security Enhanced RFID Authentication Protocols for Healthcare Environment," *Wireless Personal Communications*, vol. 117, p. 71–86, 2021.

[37] A. Yala, V. Quach, H. Esfahanizadeh, R. G. L. D'Oliveira, K. R. Duffy, M. Médard, T. S. Jaakkola and R. Barzilay, "Syfer: Neural Obfuscation for Private Data Release," arXIV, 2022.

[38] N. Cummins and B. W. Schuller, "Five Crucial Challenges in Digital Health," *Frontiers in Digital Health*, 2020.