BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

On Monetizing Personal Wearable Devices Data: A Blockchain-based Marketplace for Data Crowdsourcing and Federated Machine Learning in Healthcare

Mohamed Emish[1*] Hari Kishore Chaparala[1] Zeyad Kelani[1,2] Sean D. Young[1,3]

1. Department of Informatics, University of California, Irvine, 92697, United States of America
2. Department of Political Science, Faculty of Economics and Political Science Cairo University, Egypt
3. Department of Emergency Medicine, University of California, Irvine, 92697, United States of America

ARTICLE INFO

Article history
Received: 14 December 2022
Revised: 6 January 2023
Accepted: 9 January2023
Published Online: 2 February 2023

Keywords:
Wearable devices
Data integrity
Data validation
Federated learning
Blockchain
Trusted execution environment
Health informatics
Healthcare data collection
Data monetization

ABSTRACT

Machine learning advancements in healthcare have made data collected through smartphones and wearable devices a vital source of public health and medical insights. While wearable device data help to monitor, detect, and predict diseases and health conditions, some data owners hesitate to share such sensitive data with companies or researchers due to privacy concerns. Moreover, wearable devices have been recently available as commercial products; thus large, diverse, and representative datasets are not available to most researchers. In this article, the authors propose an open marketplace where wearable device users securely monetize their wearable device records by sharing data with consumers (e.g., researchers) to make wearable device data more available to healthcare researchers. To secure the data transactions in a privacy-preserving manner, the authors use a decentralized approach using Blockchain and Non-Fungible Tokens (NFTs). To ensure data originality and integrity with secure validation, the marketplace uses Trusted Execution Environments (TEE) in wearable devices to verify the correctness of health data. The marketplace also allows researchers to train models using Federated Learning with a TEE-backed secure aggregation of data users may not be willing to share. To ensure user participation, we model incentive mechanisms for the Federated Learning-based and anonymized data-sharing approaches using NFTs. The authors also propose using payment channels and batching to reduce smart contact gas fees and optimize user profits. If widely adopted, it's believed that TEE and Blockchain-based incentives will promote the ethical use of machine learning with validated wearable device data in healthcare and improve user participation due to incentives.

*Corresponding Author:
Mohamed Emish,
Department of Informatics, University of California, Irvine, 92697, United States of America;
Email: memish@uci.edu

DOI: https://doi.org/10.30564/aia.v4i2.5316

1. Introduction

Big data analytics and the Medical Internet of Things (MIoT) are becoming integral to a proactive healthcare system [1]. One source of this information is wearable devices such as smartwatches that constantly track participants' vital signs. The wearable devices market is expected to soar around threefold (115.8 billion US dollars to 380 billion US dollars) between 2021 and 2028 [2]. However, users of wearable devices have privacy concerns regarding sharing data about vital signs and their location [3]. We have identified three reasons data owners are hesitant to share their wearable devices' data. First, some data owners fear being watched by "digital big brother" and the potential threat to their data privacy rights [4]. Some data owners also have major concerns about confidentiality. They desire control over what the data can be used to infer about them, especially when combined with data from other platforms [5]. Moreover, the value of data in the information economy has made it a target of attacks, leading to data breaches and personal data theft outside of trusted organizations [6]. Second, even when data owners share their data, some data consumers don't know if they can trust it, as it may be malicious. For example, automated bots can generate low-quality sets by creating fake records that simulate real user behavior [7]. Third, many data owners may feel they are not fairly compensated for their data. In contrast, data brokers accumulate large amounts of data and use it to create products for surveillance and marketing [8]. In addition to privacy, creating machine learning models that work effectively for individuals from different backgrounds is inhibited by the inaccessibility of inclusive datasets to researchers [9].

Previous studies have explored use cases for machine learning models and wearable device data. They have shown significant promise for such an approach in detecting health conditions. For example, accelerometer sensor data from smartwatches were used to detect sleep apnea and sleep classification, respectively [10,11]. Another study used biosensor data in armbands to monitor skin temperature, respiratory rate, blood pressure, pulse rate, and blood oxygen saturation. It used this data to create an early detection model for COVID-19 [12]. Wearable device data from wristbands were also used to continuously monitor the physiological parameters of patients in urgent care and train machine learning models that detect clinical deterioration [13]. Other studies have collected data from emerging wearable devices such as headbands [14] or Respiratory Belts (RB) [15] to detect seizures [16-18], monitor emotions [19,20] and track rehabilitation tasks [21-23], as well as detecting and monitoring heart diseases (arrhythmia [24-26], hypertension [27], and strokes [28,29]).

We propose a decentralized, fully automated marketplace to capture these insights by securely sharing data from wearable devices between data owners and consumers. Our marketplace uses several advances in cryptography techniques and Federated Machine Learning (ML) to respond to the challenges of using wearable devices and ML in Healthcare. First, we propose Trusted Execution Environments (TEE) to verify data records' validity and ensure that they are not stolen or produced by bots. The marketplace then offers a platform for data owners to list their wearable device records as NonFungible Tokens (NFTs). Federated learning will train local models without copying or moving the data owners' sensitive data records from their devices. Alternatively, data owners can choose to sell their wearable device records to data consumers by transferring ownership of NFTs. Data owners will be rewarded for selling data or contributing to training ML models requested by the data consumers. We also use security measures to blacklist malicious data owners or consumers who try to break the system's rules. Our novel design for a fair and secure marketplace would collect genuine data that can be used for the accurate detection and prevention of diseases and reward users willing to share data with the broader research community. The design decisions of this marketplace aim to support the trustless trading of clean data with strong integrity checks, thwart malicious data owners and consumers, and an incentive mechanism for promoting fair user participation. While several existing studies and models [30-33], most focus on the privacy-preserving nature of trading sensitive data. They don't guarantee strong data validations and mechanisms to prevent malicious data sellers. On the other hand, our approach provides a privacy-preserving platform for trading data with strong integrity checks.

The main contributions of this paper are:

- Rewarding wearable device data sharing using NFTs in a scalable and cost-effective manner.
- Verifying the integrity of data records using TEE to thwart malicious data sellers.
- Applying a pay-per-usage model based on federated learning and secure aggregation using TEE.

2. Literature Review

2.1 Existing Marketplaces

Alan et al. [30] proposed a marketplace where the users define data-sharing policies translated into smart contracts. In their model, the wearable device users generate

the data stored in Data Custodian or wearable device manufacturer's cloud storage. The users also set policies on how their data can be accessed in Blockchain. A data broker entity matches users and data consumers based on their preferences. Once a match is made, based on a set of policies, a smart contract for trading the data is created and the data transaction takes place. The authors point out that since data come from the device manufacturer's cloud storage, data integrity is preserved. However, it's not shown exactly how the device manufacturer preserves the data integrity. Moreover, it requires data consumers to trust the device manufacturer. In contrast, our model uses TEEs in user devices that generate attested data from attested wearable device software. In addition, we also prevent data duplication attacks using sequence numbers. Also, there are several centralized and trusted components in their proposed architecture, like Data Anonymizer and Data Custodian's cloud, which can be compromised by a malicious entity, thus creating data privacy and integrity concerns. Our model addresses privacy concerns using federated learning with a TEE-backed secure aggregation and NFT transactions. In addition, the data anonymizer resides within secure enclaves that ensure a consistent data format.

Sterling [31] is another privacy-preserving data marketplace. It uses a TEE to perform secure machine learning using the policies set in the data provider and consumer smart contract. The authors suggest using machine learning model parameters to check whether the data are fake. But a malicious user can always generate duplicate data or corrupt the model in several steps, ensuring that at each step of the training, the model parameters don't deviate enough creating a red flag. Also, there are no mechanisms proposed to blacklist a malicious data provider. Our model uses the TEE identity to blacklist users. Using a TEE identity-based blacklisting, users can't arbitrarily create fake identities, and purchasing a new wearable device to bypass a blacklist will most likely cause negative incentives.

Gonzalo et al. [32] performed a systematic literature review on IoT data markets' privacy-enhancing technologies. Some surveyed papers employed Truth Discovery and reputation-based systems for data integrity checks. However, these approaches are not practical for wearable device data, where we treat every user as an anonymous entity. Most of the studies [32] were more inclined to preserve data generators' privacy rather than ensure data integrity. On the other hand, our model is privacy-preserving and ensures strong data integrity.

Primal [33] is a cloud-based privacy-preserving marketplace. It is not decentralized, and if the cloud is compromised, consumer and producer data are at risk. Primal's proposed data validation protocol requires the consumers to estimate the data quality based on the trained machine learning model. Our model does not require any effort from the consumer's end, as the TEE attests to the data.

One study proposed a design for a decentralized data marketplace on the Blockchain that uses arbitration to settle disputes between data owners and data consumers [34]. In the authors' design, untrustworthy data buyers or sellers are detected using an arbitrators alliance that both parties in the transaction nominate. The arbitrator's decision will be executed using secure smart contracts; however, this design still requires the intervention of external actors, which can take time and might not lead to accurate resolutions. Zhang et al. [35] proposed a data marketplace with a network storage service verification mechanism. But it lacks the performance needed for scalability. Makhdoom et al. [36] designed a framework for rewarding data sharing from IoT devices in smart cities based on smart contracts and digital tokens (PrivyCoin). While data security and rewards are available for data owners, creating a customized coin to distribute rewards requires a large blockchain infrastructure. This can be avoided by using all-propose tokens widely traded between cryptocurrency owners, such as Ethereum, Solana, and Binance. Li et al. [37] proposed a rewarding system for sharing IoT data based on Monero Technology to ensure anonymous data exchange and multi-sharing. All these models lack strong data validation techniques, which are especially important for healthcare data as a minor trained machine learning model corruption might cause serious consequences.

2.2 Detecting Malicious Actors

Some applications of integrating federated learning with Blockchain have been proposed in industry and academia. A privacy-preserving blockchain-based federated learning study [38] shows how home appliance manufacturers can gather information from users to improve smart home systems. In the author's model, first, the users train a publicly available model on the Blockchain, then the Blockchain acts as the aggregator of models from different users. Blockchain prevented prevent malicious manufacturers or users. In the second stage, the smart contract performed a crowdsourcing task that aggregated and computed the average model. Incentives were also awarded to the miner in the crowdsourcing task. The authors also used a Differential Privacy Preserving algorithm for data privacy. However, manufacturers are not considered malicious to corrupt the model as they are the model owners. Another study used homomorphic encryption to encode the gradients of ML models to preserve user privacy and

prevent possible inference attacks [39] but this may not be feasible for types of machine learning models.

3. System Design

3.1 Architecture Overview

This section introduces our proposed system design for the wearable devices data marketplace. Our marketplace has two groups of stakeholders: Data consumers and data owners. Data consumers employ a crowdsourcing model based on federated learning, with the initial models running on user devices. Data owners list their data as a Non-Fungible Token (NFT) in health data marketplaces. We utilize TEE to ensure data integrity, addressing threats from malicious users (data owners) and malicious data consumers trying to compromise data privacy. Our model consists of a wearable device with TEE, a user-owned mobile device for performing federated model training, a secure aggregator using TEE for preserving user privacy, a smart contract hosting a federated learning model, and an ERC-721-based [40] NFT contract that verifies the final model output and NFT data. ERC-721 tokens are used to incentivize users in the federated learning-based and NFT-based data-selling approaches.

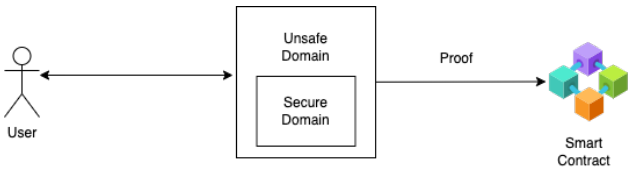

Figure 1. Health data attestation.

3.2 Verification of Data Records

Malicious data owners could try to fake the data or copy existing data to resell in our health data marketplace. Moreover, a group of malicious users could collaboratively try to corrupt the machine learning models using invalid data. Using hashing algorithms to ensure data integrity is insufficient because a malicious user can modify data to generate a unique record. For this reason, we propose using TEE in wearable devices. The TEE can attest that a valid workflow genuinely generates the data. In the case of a wearable device, data records represent a physical activity or other monitored vital signs. Within a TEE, the code and data loaded are immune from modification and eavesdropping, thus ensuring data privacy and integrity. TEE has dedicated, private regions of memory called "enclaves." The isolated memory runs a private Operating System (OS). ARM TrustZone [41], Intel Software Guard Extensions [42], and AMD Platform Security Processor [43] are popular examples of private OS's that run in enclaves. In our design, we use an ARM Cortex-M23 series processor [44] using TrustZone-M, which has been widely used in IoT devices [45] and is currently listed as a small and energy-efficient processor suitable for wearable devices. Data owners' activities are processed within the TEE, and the data are attested using the TEE's private key $\rho = SIG(data, pk_{tee})$ where SIG is the signing function and ρ is the attestation. The private key pk_{tee} associated with the TEE is unique and only known within the TEE. A public key pub_{tee} can be used to verify the attestation. For a user to list the health data, a hash h is generated on the data record using a one-way hashing algorithm $H(data)$. The user can optionally save the data in an InterPlanetary File System (IPFS) like Pinata [46]. To mint an NFT corresponding to a health record, the smart contract uses pub_{tee} to verify a health record hash. To prevent duplication and reselling of the same health records, every record is associated with a stepwise increasing sequence number, verified at smart contract. Figure 1 shows the overview of health data attestation using a smart contract and a TEE.

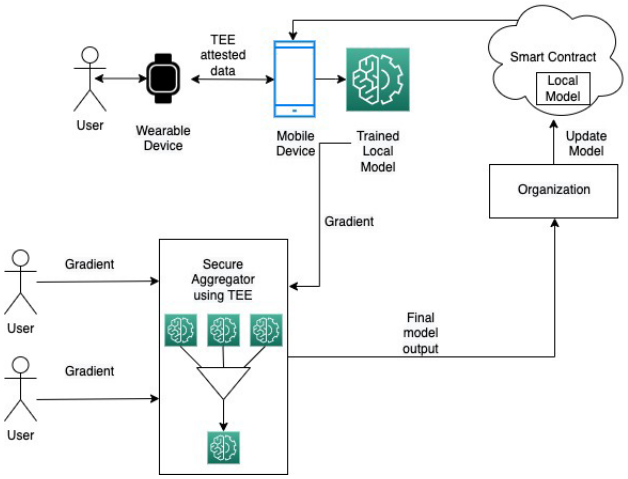

Figure 2. Federated Learning with users.

3.3 Federated Learning

Federated learning [38,47,48] is used to train an ML model in a distributed manner while data stays on-premises—in our case, on the data owners' devices. After locally training models on multiple devices, they are gathered and aggregated by the data consumer. In our design, as shown in Figure 2, the user data from wearable devices are collated into a mobile device that pulls a local model for federated learning from the blockchain. As the model is present on the blockchain, it reduces the chances of the model being malicious. Once the local model is trained, it is sent to a secure aggregator based on a trusted execution environ-

ment. We use Intel SGX OS to handle secure enclaves on the external aggregation server. The aggregation server enclaves collect and aggregate the ML model's gradients from all users. The final model output is signed by the TEE and sent to the data consumer. We are not sending individual gradients to the organization but rather the aggregated model. This ensures that user information cannot be inferred from the gradients. The gradient transfer is encrypted to prevent the eavesdropping of gradients by the system encompassing the TEE, and the security keys can be transmitted using the RSA algorithm [49].

The gradients generated by the users have signed $SIG(gradient,pk_{user})$ using user private keys, and the final gradient is also signed by the TEE $SIG(final\ \_output,pk_{tee})$. This protects organizations from model corruption.

3.4 User Incentives from Federated Learning

Data owners can earn incentives from locally training ML models and publishing the gradients to data consumers. The secure aggregator collects the TEE-signed gradients from users, which determines the number of ERC-20 tokens to be sent to the data owner as an incentive. A signed message $SIG(gradient,pk_{tee\ user},wallet\ id,data\ size,hash)$ is sent to the secure aggregator from all users. $pk_{tee\ user}$ is the private TEE key used in the user's wearable device to sign the message. *Data size* is the size of the new data used to train the federated learning model. Data owners will be rewarded with Ethereum tokens based on the number of new data records they contribute to the local ML model. Then, we acquire a unique hash for $H(data)$, on the data records used for training. The secure aggregator uses the hash to tackle replay attacks in which the user can try to send the same training output again to get incentives. The secure aggregator maintains a hash table of records and prevents data owners from using the same data more than once. As we are using a TEE for storing these hashes, any downtime in the enclave could lead to the loss of the hash table. The hash data can be periodically synced with external encrypted storage (or an IPFS) that the TEE can only modify to prevent this loss. Once the signed local model outputs reach the secure aggregator, it can verify the signatures signed by $pk_{tee\ user}$ and the *hash* information. The appropriate award to the data owner is then calculated based on the amount of data they contributed. A signed message from the secure aggregator $SIG([[u_1,p_1],[u_2,p_2],...],hash,pk_{sg})$ is sent to the smart contract for the award payment. The smart contract verifies the signature and the hash. A hash table is also maintained in the smart contract to prevent replay attacks. A daily quota on the transfer is set on the data consumers' wallets for safety. Incentives are transferred from the data consumers' wallets to the data owners' wallets while the quota lasts. Algorithm 1 shows the smart contract logic to send incentives to data owners. As the payments are usually small, a low-gas fee network like Polygon [50] or Payment Channels [51] will reduce the fees required to complete the transactions between the two parties (data owner and data consumer). Algorithm 1 shows how the payments flow in the smart contract, and Figure 3 details the overview of user incentives with federated learning.

Algorithm 1 User payments in Smart Contact

fn pay users($\rho = SIG([[u_1,p_1],[u_1,p_1],...],hash,pk_{sg})$)
VERIFY(ρ,pub_{sg}) if hash not in Hash Table then
payments ← $[[u_1,p_1],[u_1,p_1],...]$ balance ← Remaining Organization daily quota for all p_i,u_i in payments do
if p_i − balance ≥ 0 then transfer(p_i, u_i)
balance ← p_i − balance
Update remaining quota end if
end for end if

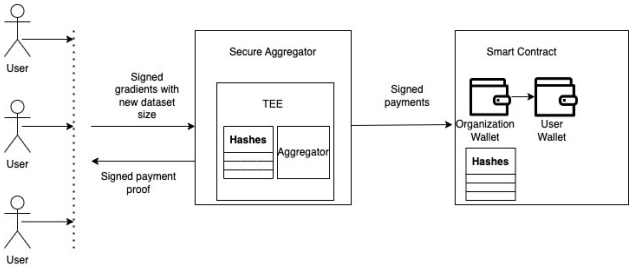

Figure 3. User Incentives.

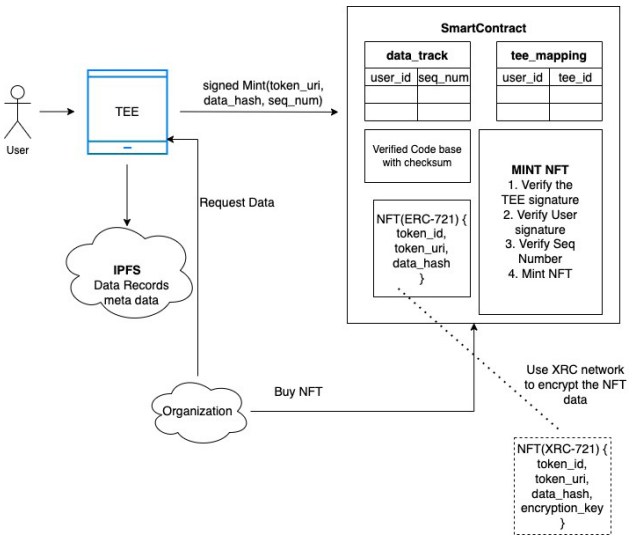

Figure 4. Minting health data as NFT.

3.5 Minting Wearable Device Data as NFTs

In some cases, federated learning might not work accurately for all health data-related machine learning applications. Also, data owners may be comfortable with sharing health data from wearable devices. To surmount these bar-

riers, we propose extending our framework to allow data owners to mint health records from wearable devices as NFTs. As a result, data consumers can directly train their ML models on the data. We use the same TEE architecture to attest the data records, and each record is associated with a sequence number as described in subsection III-B. While listing the NFT, the data owners' personal and sensitive information is removed from the records. For this purpose, the TEE in the data owners' devices only uses the publicly visible, verified codebase on the blockchain. This codebase is responsible for encapsulating the data from the wearable device without any sensitive information. The codebase will also generate metadata helpful for data consumers filtering the data. Before minting the data records as NFTs, they are made visible to the data owners for review. When a data owner decides to list their health record, they can create an IPFS record with the metadata. Since minting NFT requires gas fees, wearable device data will be minted in batches large enough for the data owner to receive incentives. A call is then made to the smart contract signed by the TEE with *token url*, *data hash* for integrity verification, and *seq num* to prevent reselling the data. The minting process is shown in Figure 4. In the smart contract, we keep track of *the user id* and *tee _id* mapping and the *seq _num* associated with the user. During the minting process, we verify the TEE attestation, user signature, and whether *seq num* ≥ last sequence number from the user is present in the mapping. Upon passing all checks, we mint the NFT. It is possible to perform lazy minting [52] to delay the payment of the gas fee until the NFT is sold. Data consumers can now buy the listed NFTs on the marketplace.

Currently, the original data only resides with the user. Unlike artwork NFTs, if the wearable device data is public, organizations could access the records without purchasing NFT; thus, users will not be rewarded. If a user denies sending the data to a data consumer, they can be blacklisted by the consumer using the tee_{id}. Creating new user profiles cannot escape from the blacklist, as the tee_{id} is embedded with the device. Given that a wearable device with TEE support is likely more valued than the user data, a malicious user has no incentive to reject data share requests by the organization. Once the data is shared with the data consumer, its integrity can be verified using the checksum in the smart contract's NFT data. To list and purchase NFT and perform atomic transactions with ERC-20 tokens and NFT tokens, we recommend using the Wyvern protocol [51], as popular marketplaces like OpenSea currently use it [53]. If data owners lack storage for all their listed data records, they can use the XRC-721 standard offered by XDC-Network and store the encrypted NFT information in IPFS. Using this standard, it is possible to encrypt NFT data so that only the NFT owner can access the encryption key to decrypt the NFT data. But this requires switching to a different blockchain.

4. Discussion

ML and wearable device data records have great potential to improve well-being and advance scientific healthcare research. Clean and trusted data can create accurate ML models and reach this potential. Our novel wearable device data marketplace design utilizes Federated Learning, TEE, and blockchain to provide a privacy-preserving way for the owners to share health data and guarantee strong data validations. Our marketplace allows users to participate in the data-sharing workflow using Federated learning or NFT-based data record sales. Our data marketplace stores the metadata of records, making data that belong to populations of interest findable by scientists and data consumers. The marketplace is open to all data owners and consumers with the appropriate wearable device with TEE support. Our design consists of secure and fair incentive mechanisms for the users selling the data records as NFTs or participating in crowdsourced federated learning. Our security model tackles malicious sellers, data consumers, and external third parties. This makes our marketplace a Findable, Accessible, Interoperable, and Reusable (FAIR) data source [55]. Our approach is also practical if major wearable device manufacturers start supporting TEE-based data attestation. Also, since federated learning is distributed and the initial models run on user devices, it may help small organizations save infrastructure costs associated with model training and data storage.

The main limitations of our approach are, unlike software patches for any discovered vulnerabilities, any wearable device vulnerabilities in the TEE might require device replacement or withdrawal from marketplace participation. It may not be possible to onboard existing wearable devices onto our marketplace. Also, federated learning might only be best suited for training some types of models.

Conflict of Interest

There is no conflict of interest.

References

[1] Dimitrov, D.V., 2016. Medical internet of things and big data in healthcare. Healthcare Informatics Research. 22(3), 156.
DOI: https://doi.org/10.4258/hir.2016.22.3.156

[2] Elshafeey, A., Mhaimeed, O., Al Ani, J., et al., 2021. Wearable devices and machine learning algorithms for cardiovascular health assessment. Machine Learning in Cardiovascular Medicine. 10(1), 353-370.
DOI: https://doi.org/10.1016/b978-0-12-820273-9.00015-4

[3] Cilliers, L., 2019. Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal. 49(2-3), 150-156.
DOI: https://doi.org/10.1177/1833358319851684

[4] Raposo, V.L., 2021. Big brother knows that you are infected: Wearable devices to track potential COVID-19 infections. Law, Innovation and Technology. 13(2), 422-438.
DOI: https://doi.org/10.1080/17579961.2021.1977214

[5] Kostkova, P., Brewer, H., de Lusignan, S., et al., 2016. Who owns the data? Open data for healthcare. Frontiers in Public Health. 17(4), 7. Available from: https://pubmed.ncbi.nlm.nih.gov/26925395/.

[6] Seh, A.H., Zarour, M., Alenezi, M., et al., 2020. Healthcare data breaches: Insights and implications. Healthcare. 8(2), 133.
DOI: https://doi.org/10.3390/healthcare8020133

[7] Pozzar, R., Hammer, M.J., Underhill-Blazey, M., et al., 2020. Threats of bots and other bad actors to data quality following research participant recruitment through social media: Cross-sectional questionnaire. Journal of Medical Internet Research. 22(10).
DOI: https://doi.org/10.2196/23021

[8] Sadowski, J., 2019. When data is capital: Datafication, accumulation, and extraction. Big Data & Society. 6(1), 205395171882054.
DOI: https://doi.org/10.1177/2053951718820549

[9] Huhn, S., Matzke, I., Koch, M., et al., 2022. Using wearable devices to generate real-world, individual-level data in rural, low-resource contexts in Burkina Faso, Africa: A case study. Frontiers in Public Health. 10, 972177.
DOI: https://doi.org/10.3389/fpubh.2022.972177

[10] Hayano, J., Yamamoto, H., Nonaka, I., et al., 2020. Quantitative detection of sleep apnea with wearable watch device. Plos One. 15(11), e0237279.
DOI: https://doi.org/10.1101/2020.07.24.219261

[11] Sundararajan, K., Georgievska, S., te Lindert, B.H., et al., 2021. Sleep classification from wrist-worn accelerometer data using random forests. Scientific Reports. 11(1).
DOI: https://doi.org/10.1038/s41598-020-79217-x

[12] Wong, C.K., Ho, D.T., Tam, A.R., et al., 2020. Artificial intelligence mobile health platform for early detection of COVID-19 in quarantine subjects using a wearable biosensor: Protocol for a randomised controlled trial. BMJ Open. 10(7).
DOI: https://doi.org/10.1136/bmjopen-2020-038555

[13] Un, K.C., Wong, C.K., Lau, Y.M., et al., 2021. Observational study on wearable biosensors and machine learning-based remote monitoring of COVID-19 patients. Scientific Reports. 11(1).
DOI: https://doi.org/10.1038/s41598-021-82771-7

[14] Laureanti, R., Bilucaglia, M., Zito, M., et al. (editors), 2020. Emotion assessment using machine learning and low-cost wearable devices. 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC); 2020 Jul 20-24; Montreal, QC, Canada. USA:IEEE. p. 576-579.
DOI: https://doi.org/10.1109/embc44109.2020.9175221

[15] Ayata, D., Yaslan, Y., Kamasak, M.E., 2020. Emotion recognition from multimodal physiological signals for emotion aware healthcare systems. Journal of Medical and Biological Engineering. 40(2), 149-157.
DOI: https://doi.org/10.1007/s40846-019-00505-7

[16] Regalia, G., Onorati, F., Lai, M., et al., 2019. Multimodal wrist-worn devices for seizure detection and advancing research: Focus on the empatica wristbands. Epilepsy Research. 153, 79-82.
DOI: https://doi.org/10.1016/j.eplepsyres.2019.02.007

[17] Onorati, F., Regalia, G., Caborni, C., et al., 2021. Prospective study of a multimodal convulsive seizure detection wearable system on pediatric and adult patients in the epilepsy monitoring unit. Frontiers in Neurology. 12, 724904.
DOI: https://doi.org/10.3389/fneur.2021.724904

[18] Onorati, F., Regalia, G., Caborni, C., et al., 2017. Multicenter clinical assessment of improved wearable multimodal convulsive seizure detectors. Epilepsia. 58(11), 1870-1879.
DOI: https://doi.org/10.1111/epi.13899

[19] Laureanti, R., Bilucaglia, M., Zito, M., et al. (editors), 2020. Emotion assessment using machine learning and low-cost wearable devices. 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC); 2020 Jul 20-24; Montreal, QC, Canada. USA:IEEE. p. 576-579
DOI: https://doi.org/10.1109/embc44109.2020.9175221

[20] Al Zoubi, O., Awad, M., Kasabov, N.K., 2018. Anytime multipurpose emotion recognition from EEG data using a liquid state machine based framework. Artificial Intelligence in Medicine. 86, 1-8.
DOI: https://doi.org/10.1016/j.artmed.2018.01.001

[21] Potluri, S., Chandran, A.B., Diedrich, C. (editors), et al., 2019. Machine learning based human gait segmentation with wearable sensor platform. 2019 41st

Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC); 2019 Jul 23-27; Berlin, Germany. USA:IEEE. p. 588-594.
DOI: https://doi.org/10.1109/embc.2019.8857509

[22] Zhang, H., Guo, Y., Zanotto, D., 2020. Accurate ambulatory gait analysis in walking and running using machine learning models. IEEE Transactions on Neural Systems and Rehabilitation Engineering. 28(1), 191-202.
DOI: https://doi.org/10.1109/tnsre.2019.2958679

[23] Moore, S.R., Kranzinger, C., Fritz, J., et al., 2020. Foot strike angle prediction and pattern classification using LOADSOLTM wearable sensors: A comparison of machine learning techniques. Sensors. 20(23), 6737.
DOI: https://doi.org/10.3390/s20236737

[24] Hannun, A.Y., Rajpurkar, P., Haghpanahi, M., et al., 2019. Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. Nature Medicine. 25(1), 65-69.
DOI: https://doi.org/10.1038/s41591-018-0268-3

[25] Kwon, S., Hong, J., Choi, E.K., et al., 2020. Detection of atrial fibrillation using a ring-type wearable device (CardioTracker) and deep learning analysis of photoplethysmography signals: Prospective observational proof-of-concept study. Journal of Medical Internet Research. 22(5).
DOI: https://doi.org/10.2196/16443

[26] Mei, Z., Gu, X., Chen, H., et al., 2018. Automatic atrial fibrillation detection based on heart rate variability and spectral features. IEEE Access. 6, 53566-53575.
DOI: https://doi.org/10.1109/access.2018.2871220

[27] Miao, F., Wen, B., Hu, Z., et al., 2020. Continuous blood pressure measurement from one-channel electrocardiogram signal using deep learning techniques. Artificial Intelligence in Medicine. 108, 101919.
DOI: https://doi.org/10.1016/j.artmed.2020.101919

[28] Lown, M., Brown, M., Brown, C., et al., 2020. Machine learning detection of atrial fibrillation using wearable technology. Plos One. 15(1).
DOI: https://doi.org/10.1371/journal.pone.0227401

[29] Liu, Y., Fang, B., Zhao, Y., et al. (editors), 2021. Ensemble learning for atrial fibrillation screening from a single lead ECG wave of wearable devices. 2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC); 2021 Nov12-14; Greenville, SC, USA. USA: IEEE. p. 590-594.
DOI: https://doi.org/10.1109/icftic54370.2021.9647218

[30] Colman, A., Chowdhury, M.J., Baruwal, C.M. (editors), 2019. Towards a trusted marketplace for wearable data. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC); 2019 Dec 12-14; Los Angeles, CA, USA. USA: IEEE. p. 314-321.
DOI: https://doi.org/10.1109/cic48465.2019.00044

[31] Hynes, N., Dao, D., Yan, D., et al., 2018. A demonstration of sterling. Proceedings of the VLDB Endowment. 11(12), 2086-2089.
DOI: https://doi.org/10.14778/3229863.3236266

[32] Garrido, G.M., Sedlmeir, J., Uludağ, Ö., et al., 2022. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IOT: A systematic literature review. Journal of Network and Computer Applications. 207, 103465.
DOI: https://doi.org/10.1016/j.jnca.2022.103465

[33] Song, Q., Cao, G., Sun, K., et al. (editors), 2021. Try before you buy: Privacy-preserving data evaluation on cloud-based machine learning data marketplace. ACSAC'21: Annual Computer Security Applications Conference; 2021 Dec 6-10; New York: Virtual Event, USA. ACM. p. 13.
DOI: https://dl.acm.org/doi/10.1145/3485832.3485921

[34] Tang, H., Qiao, Y., Yang, F., et al., 2022. DMOBAs: A data marketplace on blockchain with arbitration using side-contracts mechanism. Computer Communications. 193, 10-22.
DOI: https://doi.org/10.1016/j.comcom.2022.06.029

[35] Zhang, C., Xu, Y., Hu, Y., et al., 2022. A blockchain-based multi-cloud storage data auditing scheme to locate faults. IEEE Transactions on Cloud Computing. 10(4), 2252-2263.
DOI: https://doi.org/10.1109/tcc.2021.3057771

[36] Makhdoom, I., Zhou, I., Abolhasan, M., et al., 2019. Privysharing: A blockchain-based Framework for Integrity and Privacy-preserving Data Sharing in Smart Cities. Computers & Security. 88, 101653.
DOI: https://doi.org/10.1016/j.cose.2019.101653

[37] Li, T., Wang, H., He, D., et al., 2022. Block Chain Based Privacy-preserving and Rewarding Private Data Sharing for IOT. IEEE Internet of Things Journal. 9(16), 15138-15149.
DOI: https://doi.org/10.1109/jiot.2022.3147925

[38] Zhao, Y., Zhao, J., Jiang, L., et al., 2021. Privacy-preserving Blockchain-based Federated Learning for IOT Devices [Internet] [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1906.10893.

[39] Facts & Factors, 2022. Insights on Global Wearable Technology Market Size & Share to Surpass

USD 380.5 Billion by 2028, Exhibit a Cagr of 18.5% Industry Analysis, Trends, Value, Growth, Opportunities, Segmentation, Outlook & Forecast Report by Facts & Factors [Internet]. GlobeNewswire News Room [Retrieved 2022 Dec 7]. Available from: https://www.globenewswire.com/news-release/2022/04/13/2421597/0/en/Insights-on-Global-WearableTechnology-Market-Size-Share-to-Surpass-USD-380-5-Billion-by-2028-Exhibit-a-CAGR-of-18-5-Industry-Analysis-Trends-ValueGrowth-Opportunities-Segmentatio.html.

[40] Entriken, W., Shirley, D., Evans, J., et al., 2018. EIP-721: Non-Fungible Token Standard. Ethereum Improvement Proposals [Internet] [Retrieved 2022 Dec 7]. Available from: https://eips.ethereum.org/EIPS/eip-721.

[41] LTE Cat-m a Cellular Standard for IOT—ARM Architecture Family [Internet] [Retrieved 2022 Dec 8]. Available from: https://community.arm.com/cfsfile/ key/telligent-evolution-components-attachments/01-2142-0000-00-00-68-74/LTE-Cat 2D00 M-2D00 -A-Cellular-Standard-forIoT.pdf.

[42] Intel Software Guard Extensions [Internet] [Retrieved 2022 Dec 7]. Available from: https://www.intel.com/content/www/us/en/developer/tools/softwareguard-extensions/overview.html.

[43] Microsoft Pluton Security Processor [Internet]. AMD Pro Security [Retrieved 2022 Dec 8]. Available from: https://www.amd.com/en/technologies/pro-security.

[44] System-Wide Security for IoT Devices [Internet]. Trustzone for Cortex-M-ARM® [Retrieved 2022 Dec 7]. Available from: https://www.arm.com/technologies/trustzonefor-cortex-m.

[45] Oliveira, D., Gomes, T., Pinto, S., 2012. UTANGO: An Open-source Tee for IOT Devices [Internet]. arXiv [Retrieved 2022 Dec 8]. Available from: https://arxiv.org/pdf/2102.03625.pdf.

[46] Your Home for NFT Media [Internet]. Pinata [Retrieved 2022 Dec 7]. Available from: https://www.pinata.cloud/.

[47] Konečný, J., McMahan, H.B., Yu, F.X., et al., 2017. Federated Learning: Strategies for Improving Communication Efficiency [Internet]. arXiv.org [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1610.05492.

[48] McMahan, H.B., Moore, E., Ramage, D., et al., 2017. Communication-efficient Learning of Deep Networks from Decentralized Data [Internet]. arXiv.org [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1602.05629.

[49] Fang, H., Qian, Q., 2021. Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning [Internet]. MDPI [Retrieved 2022 Dec 7]. Available from: https://www.mdpi.com/19995903/13/4/94.

[50] Polygon Wallet—Bring the World to Ethereum [Internet] [Retrieved 2022 Dec 7]. Available from: https://polygon.technology/.

[51] Lightning Network [Internet] [Retrieved 2022 Dec 7]. Available from: https://lightning.network/.

[52] Can I List an Item Without Paying to "Mint" It? [Internet] Opensea [Retrieved 2022 December 8] Available from: https://support.opensea.io/hc/en-us/articles/1500003076601-Can-I-list-an-item-without-paying-to-mint-it-.

[53] Powering Decentralized Crypto Commerce [Internet]. Wyvern Protocol [Retrieved 2022 Dec 7]. Available from: https://wyvernprotocol.com/.

[54] Explore, Collect, and Sell NFTs [Internet]. OpenSea, the Largest NFT Marketplace [Retrieved 2022 Dec 7]. Available from: https://opensea.io/.

[55] Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J.J., et al., 2016. The fair guiding principles for scientific data management and stewardship. Scientific Data. 3(1).
DOI: https://doi.org/10.1038/sdata.2016.18