Article

A Lightweight Authentication Framework for Privacy-Preserving Virtual Health Services

Qian Qu, Ronghua Xu, Han Sun, Yu Chen*

Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA; qqu2@binghamton.edu (Q.Q.); rxu22@binghamton.edu (R.X.); hsun28@binghamton.edu (H.S.)

* Corresponding author: ychen@binghamton.edu

Abstract: Seniors safety is a compelling need, which necessitates 24/7 real-time monitoring and timely dangerous action recognition. Being able to mirror characteristics of physical objects (PO) to corresponding logical objects (LO) and seamlessly monitor their footprints thus detect anomaly parameters, Digital Twins (DT) has been considered a practical way to provide virtual health services for seniors safety. Meanwhile, widely adopted Internet of Medical Things (IoMT) consisting of wearable sensors and non-contact optical cameras for self and remote health data monitoring also raises concerns on information security and privacy violation. Therefore, security of POs, LOs and reliable data sharing among healthcare professionals are challenging as constructing trust and privacy-preserving virtual health services. Thanks to characteristics of decentralization, traceability and unalterability, Blockchain is promising to enhance security and privacy properties in many areas like data analysis, finance and healthcare. This paper envisions a lightweight authentication framework (LAF) to enable secure and privacy-preserving virtual healthcare services. Leveraging Non-Fungible Token (NFT) technology to tokenize LOs and data streams on blockchain, anyone can certify the authenticity of a digital LO along with its synchronized data between PO without relying on a third-party agency. In addition, the NFT-based tokenization not only allows owners fully control their IoMT devices and data, but it also enables verifiable ownership and traceable transferability during data sharing process. Moreover, NFT only contains references to encrypted raw data that are saved on off-chain storage like local files or distributed databases, such a hybrid storage strategy ensures privacy-preservation for sensitive information. A proof-of-concept prototype is implemented and tests are conducted on a case study of seniors safety. The experimental evaluation shows the feasibility and effectiveness of the proposed LAF solution.

Keywords: Digital Twin; Internet-of-Medical-Things (IoMT); Security; Privacy; Blockchain; Non-fungible Token (NFT); Virtual Healthcare Services; Access Control; Data Sharing

1. Introduction

Thanks to technical advancements in Artificial Intelligence (AI) combined with Internet-of-Things (IoT) and Big Data, the rise in smart cities has contributed to the practical improvements on human life in various fields, such as industrial automation, transportation, agriculture and even the healthcare sector. As personal health monitoring IoT devices in the form of mobile applications or build-in sensors, Internet-of-Medical-Things (IoMT) can actively capture user's vital health parameters in terms of electrocardiogram (ECG), BP, heart rate, and the sugar level. The real-time monitoring data is anonymously transferred to the cloud server of a healthcare system, then intelligent healthcare services uses collected data and historical data to diagnose symptom of any illness and notify the appropriate healthcare professionals. By increasing the accuracy of collected health data and facilitating the health workflows based on convenient medical records sharing capabilities, IoMT-based intelligent context-awareness healthcare systems increase effective health support and reduce the mortality rate [1].

With the unprecedented increasing of population aging and more elders living alone, seniors safety is a compelling need in healthcare systems, which necessitates 24/7 real-time monitoring and timely dangerous action recognition. Nowadays, IoMT devices like wearable sensors and optical cameras are widely used for remote safety monitoring and action recognition in personal healthcare services [2]. Utilizing digitized information, such as real-time IoMT data and electronic medical records (EMR), continuously monitoring and simulation play very important roles in seniors safety, especially for abnormal behaviors recognition, unusual activity predication and medical resource allocation. As an emerging concept of the interconnects between physical and virtual entities, Digital Twin (DT) virtually represents both the structural elements and dynamics of any physical entity (e.g., a patent) throughout its lifetime [3]. Therefore, integrating DT with IoMT and data-driven methods (e.g., machine learning) is promising to provide efficient and accurate personalized healthcare services for seniors safety. DT-based healthcare systems [1,3,4] not only allow for continuous monitoring, fast diagnosing and accurate predicting aspects of the health of individuals, it also reduces uncertainty related to effectiveness and progression of medical treatments by healthcare professionals.

Conventional cloud-assisted DT healthcare (DTH) systems aims to enable an intelligent and comprehensive health ecosystem through interaction and convergence between medical physical and virtual spaces. However, it is also incurs more concerns on performance, security and privacy as constructing trust and scalable virtual health services. From architecture level, existing DTH solutions rely on a centralized infrastructure which is prone to single point of failures (SPF). The entire system may be paralyzed if malfunctions of centralized server or successful distributed denial-of-service (DDoS) attacks happen. Other than that, a large number of IoMT devices connected to the centralized server under distributed network environments may lead to performance bottleneck (PBN). As a result, higher latency for end-to-end communications can reduce Quality-of-Service (QoS). In addition, logic objects (LO) in virtual spaces demands continuous aggregation of sensitive data coming from IoMT devices to mirror corresponding characteristics of physical objects (PO). The identity authentication of PO & LO and integrity of synchronized data are significant to ensure accurate healthcare services. Moreover, storing data in centralized servers can support analytic tasks and information sharing among healthcare professionals. As patients have limited control over how their devices and information can be properly accessed and used, it's difficulty to prevent against security and privacy breaches such that health data are misused to reveal sensitive information.

Thanks to attractive features such as decentralization, immutability, transparency and availability, Blockchain has demonstrated great potentials to revolutionize centralized DTH systems. All participants in Blockchain cooperatively execute a cryptographic consensus protocol vie a Peer-to-Peer (P2P) networking infrastructure to maintain a transparent, immutable, and auditable public distributed ledger. As no single entity can control a blockchain, such a decentralized manner can enhance fault tolerance, remove SPF, improve system availability and mitigate PBN as integrating with DTH systems containing distributed IoMT devices and users. Through bringing programmability into the blockchain, Smart contract (SC) can support a variety of customized business logic rather than classic P2P cryptocurrency payments, like Bitcoin [5]. As coded specifications of SCs deployed on the blockchain, non-fungible token (NFT) technology can tokenize the digital representation of an asset such that anyone can easily proof existence, ownership and full-history tradability of a digital asset [6]. Thus, Blockchain and NFT are promising to enable verifiable and traceable and privacy-preserving virtual health services in DTH systems.

In This paper, we propose a lightweight authentication framework (LAF), which leverages NFT enabled tokenization on the blockchain to guarantee security and privacy-preserving properties of virtual healthcare services for senior safety. A digital entity in healthcare systems (eg,. LO and health data) can be tokenized as a NFT, which contains the owner, the quantity information and functions of authorizing access rights and transferring ownership. The uniqueness of a NFT recorded on the blockchain ensures there is only a single canonical tokenization of a digital entity even if the digital representation of itself may be duplicated. Given reference to a NFT, anyone can certify the authenticity of a LO along with its synchronized data between PO without relying on a third-party agency. Thus, the provenance and legitimacy of digital entities are guaranteed to support verifiable and accountable virtual healthcare services. In addition, the ownership of LOs & POs and the permissions to use health data can be individually owned and transferable. The owners (e.g,. patients) can fully control their assets like IoMT devices and health data, while all participants can also trust a transparent data sharing process with the help of verifiable ownership and traceable transferability within healthcare systems. Moreover, a NFT only contains references recording the location of its associated digital entity, while raw data and sensitive information are encrypted and saved on off-chain storage, such as local files or distributed databases. Such a hybrid on-chain & off-chain strategy not only improve availability and efficiency by decoupling data records from transactions in the blockchain, it also ensures privacy-preserving for sensitive health data.

In brief, the key contributions of this paper are highlighted as follows:

(1) A comprehensive LAF architecture is demonstrated along with details of key components and workflows in DTH-based senior safety.
(2) The core design of NFTs used in LAF is explained in detail, which consists of NFT-CapAC, NFT-DataAC and NFT-DataTracker.
(3) A proof-of-concept prototype is implemented and tested under a physical network that simulate the case of seniors safety. The experimental results show that LAF only incurs about 5 sec end-to-end latency of updating NFTs in twin data recording cycle demanding 30 sec and less than 200 ms to query status of NFTs in verification process. Moreover, accessing data on DDS only incurred less than 30 ms and data encryption brings extra 32% and 53% processing time on desktop and Raspberry Pi separately.

The remainder of the paper is organized as follows: Section 2 provides background knowledge of DT and NFT technologies and reviews existing solutions to blockchain based healthcare systems. Section 3 introduces rationale and system architecture of LAF. Details of NFT implementation and workflows are explained in Section 4. Section 5 presents prototype implementation, experimental setup, and performance evaluation. Finally, Section 6 summarizes this paper with a brief discussion on current limitations and future directions.

2. Background and Related Work

This section describes the DT concepts underlying the healthcare systems and explains blockchain and NFT technology used to tokenize digital assets. Then we introduce the state-of-the-art decentralized solutions to secure healthcare fields.

2.1. Digital Twins and Healthcare Systems

The concept of DT was proposed in 2002 by Grieves for the formation of a Product Lifecycle Management (PLM) [7]. Essentially, a DT is a digital representation of components or dynamics in a physical system [8]. A typical DT system consists of physical objects (PO), logical objects (LO) and the data connecting them. In general, the DT systems can be roughly categorized into: monitoring DTs, simulational DTs, and operational DTs [9] according to their functionalities. The monitoring twins enables system operators to learn the status of a physical system, while simulation twins are used to predict the future status of the physical system with help of different simulation tools and Machine Learning (ML) algorithms. Similar to human-machine teaming [10], the operational twins aim to construct a *complex sensing and control system* which allows human operators to interact with cyber-physical systems and performs different actions in addition to monitoring, analysis and prediction [11].

Earlier studies of DT mainly focused on the area of industrial process which cover different key factors to achieve intelligent manufacturing and control systems. Recently, redefined DT is adopted by healthcare scenarios that contain living objects [12] and physical medical devices to enable reliable and smart healthcare systems. The DT technique could create a digital representation of the patients and contribute to establish and update medical records reporting historical and current statement of about them. With the development of wearable devices and sensor technology, researchers and industry have shown more interest in DTH systems [4]. Continuous and effective monitoring of symptoms and treatments has great impact on DTH system. To provide continuous monitoring of patients and achieve prediction and decision-making when applying medical treatments, a self-adaptive and autonomic computing DT reference model is designed for engineering smart and flexible healthcare systems [3]. The real-time sensing and data acquisition of health-related measurements from wearable devices feed a reference model to represent a human digital twin. However, the proposed work is not fully supported by experimental implementations, and security and privacy issues in DTH systems are not considered.

To support personal health management throughout the entire lifetime of elderly health, a cloud-based DTH framework (CouldDTH) [4] is proposed to enable real-time monitoring, accurately diagnosing and intelligent predicting for personal healthcare services. With the help of DTs deployed on a cloud server, CouldDTH ensures interaction and convergence between medical physical and virtual spaces. A case study demonstrates the feasibility of applying CouldDTH to practical health scenarios, like real-time supervision service and crisis warning for the elderly in terms of hospital bed capacity. However, prototype implementation and experimental results are not provided to evaluate performance, security and privacy preservation as operating CouldDTH.

To enhance patient's healthcare and improve healthcare operations, an intelligent context-aware healthcare system using DT, IoMT, and machine learning technologies is proposed [1]. In processing and prediction phase, smart IoMT devices capture real-time data of patients' body metrics and transfer them to a could server for raw-data storage. Then, monitoring and correction phase leverages trained classifiers and detective models to identify anomalous behaviors and events. By using uses patients' DT, comparison phase not only improves accuracy of prediction but also allows healthcare professionals to make more advanced and accurate decisions. The experimental results based on a case study of electrocardiogram shows that neural-network-based algorithms have better performance than traditional ML algorithms for heart disease detection. However, security and privacy issues are not evaluated.

2.2. Blockchain and NFT

As a public distributed ledger technology underlying prevalent digital crypto-currencies, like Bitcoin [5] and Ethereum [13], blockchain has emerged as a critical facilitator for the advancement of decentralized security infrastructures [14,15]. By using a peer-to-peer (P2P) network architecture for message propagation and data transmission, all miners cooperatively execute a cryptographic consensus protocol (e.g,. Proof-of-Work (PoW)) to store blocks on a totally-ordered distributed ledger. Blockchain provides a decentralized and trust platform such that all participants maintain a transparent, immutable, and auditable distributed ledger, as opposed to establishing trust through a centralized third-party authority. A smart contract (SC) combines protocols with user interfaces to formalize and secure the relationships over computer networks [16]. Though encapsulating pre-define rules into self-executing chain code deployed on the blockchain, SC introduces programmability into a blockchain. Thanks to secure execution of predefined operational logic, unique address and public exposed ABIs, SC can support a variety of customized business logic to support decentralized app (DApp) rather than simple P2P payments.

Smart contracts can tokenize digital information or assets in the form of cryptographic tokens saved on the blockchain to facilitate transactions [6]. According to fungiblity that defines if digital assets are identical and interchangeable during a transacting process, tokens are roughly categorized into fungible tokens (FT) or non-fungible tokens (NFT) [17]. FT are interchangeable and identical in all respects and they are divisible, such as crypto-currencies and stakes. While NFT cannot be substituted for other tokens of the same kind and they are indivisible [17]. By using NFTs on the blockchain, a creator can easily proof the existing and ownership of digital assets in the form of images, videos and games [18]. Recently, NFTs are widely used for protecting digital assets, like patents and intellectual property [19], Event ticketing applications [20] and scarcity of arts [21]. Thanks to key characteristics in terms of verifiable originality (authenticity), auditable ownership and traceable transferability, NFT and blockchain are promising to tokenize digital objects in virtual healthcare systems and enhance security and privacy features.

2.3. Related Work

In the past decade, the blockchain technology including NFT has been widely adopted in data sharing of medical information. MedRec [22], a blockchain-enabled EMR authentication and management framework, was proposed to provide the patients a user-friendly access to their own information. This prototype ensures the sharing process of the EMR is maintained in a decentralized form and the raw data is stored outside the blockchain. Off-chain storage brings great convenience and the participating entities involved helps to avoid single point of failures. As EMR are locally stored in separate provider or patient databases, blackout or other system failure on the database would disable the access to the raw medical data which might bring issues in case of emergencies.

On the other hand, MeDShare [23], a blockchain based system is designed for medical data sharing in trust-less virtual environment. All transition or sharing behaviors of data is tracked by the access control mechanism thus reduce the risk in data security and privacy. One possible problem is when the number of users increases inside the cloud environment, it might be difficult for real-time operation as the latency would be large.

Some researches mainly focused on blockchain based medical information management leveraging the benefits of off-chain data storage. BlocHIE [24], combined on-chain and off-chain storage techniques to secure privacy and authentication of medical data sharing and storing. Similarly, another work [25] introduced Inter Planetary File System (IPFS) to store sensitive data of the patients.

As mentioned, NFT technology possesses the properties of being unique, immutable, transferable, verifiable and traceable. Researchers explored these properties and designed a reference architecture using NFT to represent and transfer the consent of patients regarding the use of their medical data [26]. Although the proposed architecture list some components and process of the whole system, no detailed case study or experimental analysis is given in this work.

A health record marketplace based on the NFT technique was considered [27], which claimed that the designed system can provide dual ownership along with finer access control and efficiency in data sharing. InterPlanetary File System (IPFS) is adopted to store the data in an off-chain manner for security and efficiency. However, the system design in this paper mainly focused on game theory enabled pricing strategies and some popularity evaluation. The presented experimental study did not include any evaluation such as efficiency of data sharing or traceability of transferred ownership.

Similar to the previous study, a user friendly mobile application was created to store patients health records in a single platform [28]. The corresponding patient would be able to track the usage of their personal medical information with the help of NFT. However, this paper did not demonstrate how NFT works as the key technique component for data tracking and the experimental results are preliminary and unconvincing to prove efficiency or security of the proposed system.

3. LAF: Design Rationale and System Architecture

Medical issues brought by the aging society have become one of the major aspects in IoMT. Figure 1 presents the statistics from U.S. Census Bureau by 2020. The number of seniors aging 65 and older in the U.S. has reached 54 millions by 2019 and would approximately reach 80 millions by 2040. Owing to factors like geographical location or low visiting rate to medical institutions, there are increasing risks for seniors who live alone and

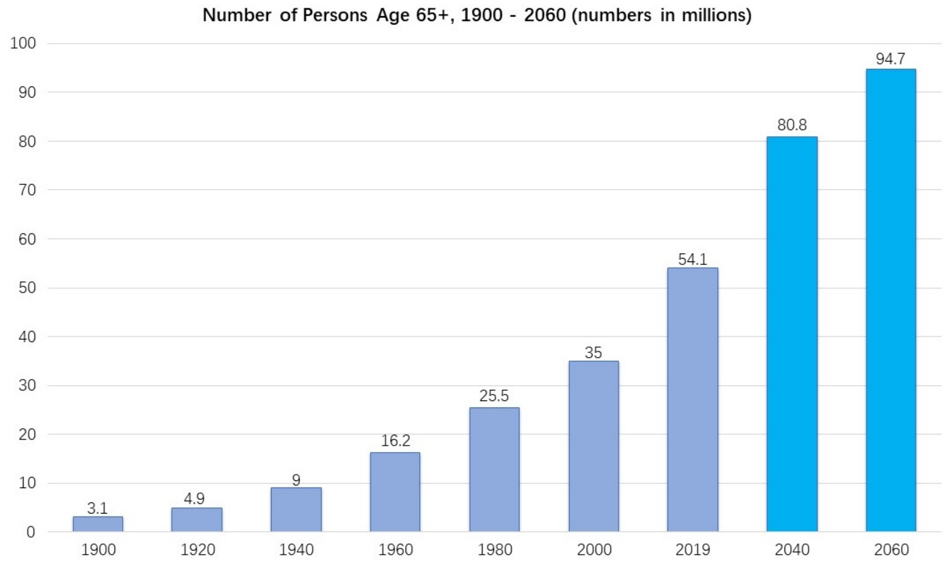

Figure 1. Number of Persons Age 65 and older in the U.S.

need medical supports. The elderly persons require not only regular medical consultation but also timely emergency assistant. To satisfy aforementioned demands on QoS, security and privacy preservation for senior patients healthcare scenarios, we propose a secure-by-design LAF, which leverages IoMT, DT and NFT technologies to provide reliable and trustful medical monitoring and healthcare consulting services. Figure 2 demonstrates an overview of LAF system architecture that consists of: i) a DT-based virtual healthcare application for senior patients; ii) a NFT enabled security fabric that provides decentralized and lightweight authentication for upper-level healthcare services. The rationale behind the system design is described as follows.

3.1. DT-based Virtual Healthcare Application

We assume a smart home environment based on a permissioned network, and it contains a trust support unit that is deployed on a personal computer (PC) or an edge server and other registered IoMT devices within the network. The support unit works as a gateway that aggregates data steams from IoMT devices, and it also plays the role of processing data, maintaining the virtual space of senior patients and performing intelligent decision-making operations, like ML-based abnormal event detection and on-site emergency alarms. The physical object essentially consists of the senior who lives in the house, smart camera providing continuous monitoring and wearable devices carrying various body sensors. Since the collected data from POs may be transmitted in various communication protocols, we need to uniform them before using DT technology to create corresponding LOs in the virtual space. DT allows to link physical object in a smart home and logical objects of virtual space, and DTH models for senior patients can be constructed by the support unit.

The DTH model of a senior patient contains different information including personal body status, environment data, and location coordinates. With the help of the model, the MSPs like doctors can perform regular medical check or consultation. In addition, the DTH model can set certain privacy policies for emergencies according to the demands and situation of the seniors. For instance, the smart camera could generate the body skeleton image of the physical person to protect users' privacy and a smart watch can be used to test the heart rate. Furthermore, all collected personal data by support units and history EMR managed by medical service providers can be shared with different professionals for further diagnosis and governmental intuitions for medical resource allocations.

doi:10.20944/preprints202209.0009.v1

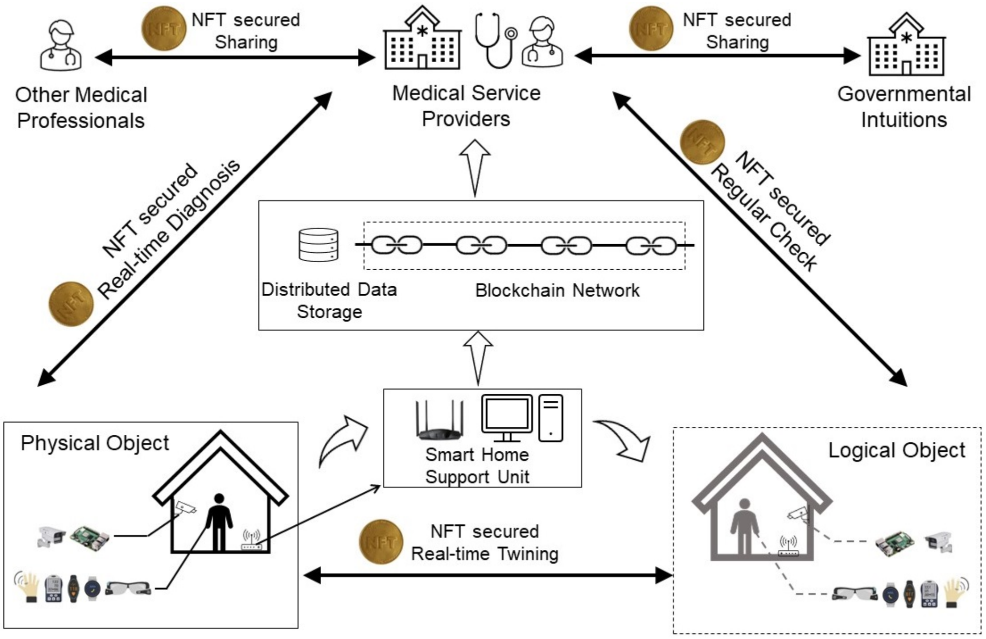

Figure 2. Illustration of LAF system architecture consisting of DT-based virtual healthcare applications and NFT enabled security fabric.

3.2. NFT enabled Security Fabric

Thanks to a decentralized fundamental networking infrastructure based on blockchain and DDS, NFT services including different types of NFTs aim to enable lightweight authentication for upper-level DT-based virtual healthcare application, as Figure 2 shows. With help of the NFT-enabled access control (AC) mechanism, owners (patients) have the fully control over their resources, such as IoMT devices and data oriented logical objects in virtual space. Thus, only medical service providers that have ownership of AC NFT with granted access rights are allowed to access resources. In real-time twinning process, encrypted data streams from POs to LOs can be saved to DDS and then tokenized as unique NFTs that contains references to raw data on DDS along with authenticators. As all data have been encrypted before recording on DDS, it is promising to ensure patients' privacy without directly exposing sensitive information, it is also improve data availability compared with centralized database. In addition, each data streams is uniquely addressed and tamper-proofing verified by using its data NFT. Regarding medical data sharing operations, data owners can use NFTs to control data sharing process. Therefore, all participants can track ownership transfers. The owner can update data access policies given status of data usages and even stop sharing data if any violations are detected.

4. NFT-based Lightweight Authentication Framework

This section presents details about design and implementation of security NFTs which enable lightweight NFT-based authentication framework for DTH systems. Regarding security functionalities demanded by then system, NFT tokens the LAF are classified into three types: *NFT-CapAC*, *NFT-DataAC* and *NFT-DataTracker*.

4.1. NFT-CapAC: NFT-based Capability Access Control

To achieve both regular medical check and emergency situation solution, we designed a novel NFT, which adopts a decentralized capability access control protocol [29] to ensure that only authorized entities are allowed to get data streams of POs and LOs according to assigned access rights. Figure 3 illustrates the lifecycle of a NFT_CapAC token and workflows are explained as follows.

doi:10.20944/preprints202209.0009.v1

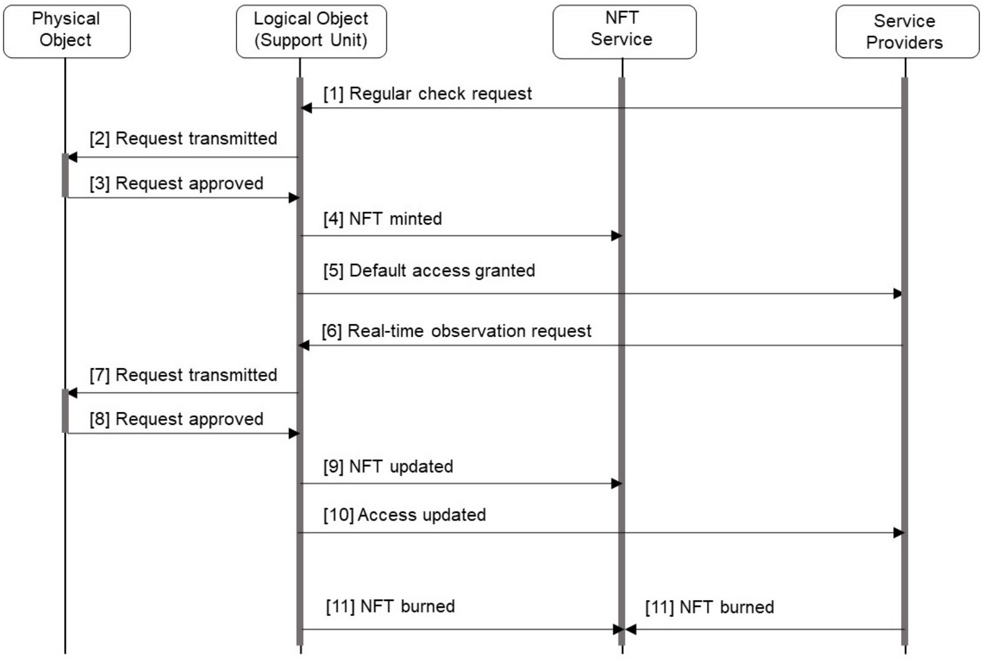

Figure 3. Lifecycle of NFT-based Capability Access Control.

In this scenario, the MSP, i.e. a doctor, first performs a regular check which requires the prior approval from the senior users. After the approval of the patient, the NFT is minted and default access is granted to the doctor. In this case, the doctor would get access to the LO in virtual space, in another word, the timely updated data of the patient. If any anomaly is detected after the diagnosis, as shown in step (6), the doctor can request higher access to get real-time data such as the live stream of the camera for further diagnosis. At the end of the lifecycle like in step (11), both the support unit and the MSP could burn the NFT. On the other hand, if an emergency alarm is triggered by the preset algorithms installed in the support unit, the corresponding default access can include the real-time data from the PO. The algorithms are customized based on personal situation of the users under the guidance of their medical service providers.

4.2. NFT-DataAC: NFT-based Data Access among DTs

The data exchange between POs and LOs is important to maintain DTH models demanding high QoS and reliability. To guarantee the integrity and authenticity of data streams in real-time twining process, we designed a NFT based data access protocol to ensure tamper-proofing data synchronization between POs and LOs. Figure 4 shows the lifecycle of a NFT-DataAC token used in continuous synchronization.

After the NFT is firstly minted before the real-time twining starts, the support unit collects the data from different sensors during a certain time interval. Since the sensors may have various communication protocols, the support unit need to uniforms the data and then sends them to update the LO in virtual space. Meanwhile, the support unit encrypts the data and uploads them to the DDS which would return the hash value as the reference. At the end of this round of synchronization, the NFT will be updated with the hash value as an new reference together with the new authenticator.

4.3. NFT-DataTracker: NFT-based Data Sharing between Medical Professionals

The sensitive data stored in the EMR is often the target of malicious third parties, such as unauthorized insurance company, hackers who sell personal information and even scammers. To guarantee the integrity, traceability and impenetrability of data sharing, we designed an NFT based EMR sharing protocol with the help of DDS. Figure 5 presents

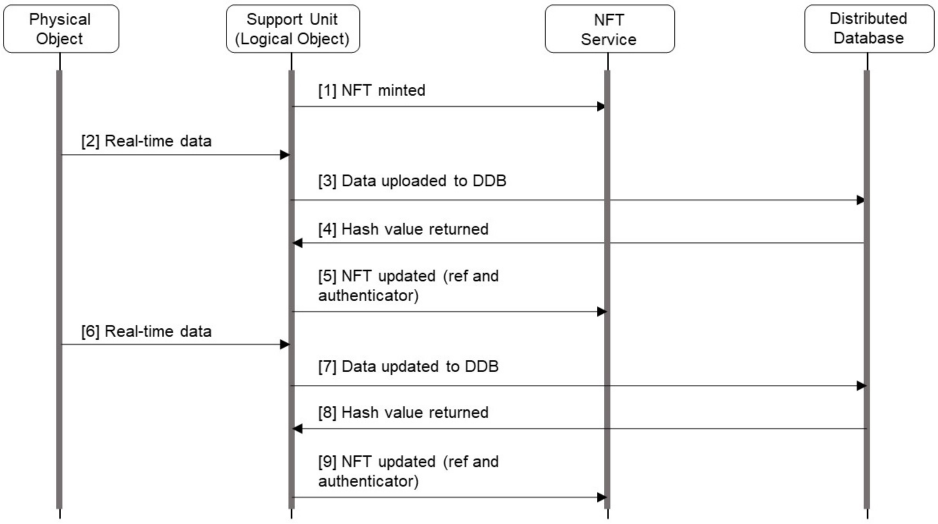

Figure 4. Lifecycle of NFT-based data access in Digital Twin.

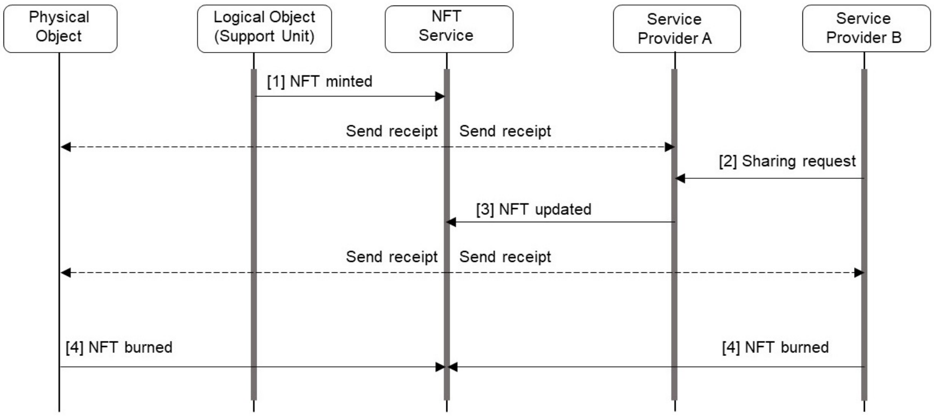

Figure 5. Lifecycle of NFT-based EMR sharing.

how NFT-DataTracke can be used to track data sharing operations, and workflows can be illustrated as follows.

We define a service provider A here as the default agent who is authorized by the senior patient (PO) when the NFT is minted. Whenever NFT is created or updated, the patient (PO) and the new owner can get a receipt notifying the change of access control status. If any third party, defined as service provider B here, ask for sharing of the EMR from A, the NFT will be updated. Afterwards, B can get the EMR from the DDS as NFT defines B as the new owner of the data. PO and the last owner can burn the NFT while PO always have the history of all transactions.

A patient's medical record may contain the personal information, diagnostic report, prescription history and regular health parameters, etc. Considering these large volumes of sensitive data, it is necessary to store them in a distributed off-chain way. The above NFT based data sharing algorithm not only ensures the sufficiency and privacy of EMR usage but also make every transaction traceable to owners (patients).

5. Experimental Results and Evaluation

In this section, experimental configuration based on a proof-of-concept prototype implementation is described. Following that, we evaluate performance based on numerical results, such as cost (e.g., network latency and gas consumption) required by key NFT operations, processing time of accessing data on distributed data storage (DDS), and computation overhead incurred by data encryption.

doi:10.20944/preprints202209.0009.v1

Table 1. Configuration of Experimental Nodes.

Device	HPC	Dell Optiplex 760	Raspberry Pi 4 Model B
CPU	Intel Core TM i5-3470 (4 cores), 3.2GHz	Intel Core TM E8400 (2 cores), 3GHz	Broadcom ARM Cortex A72 (ARMv8) , 1.5GHz
Memory	16GB DDR4	4GB DDR3	4GB SDRAM
Storage	500GB HHD	250GB HHD	64GB (microSD)
OS	Ubuntu 20.04	Ubuntu 16.04	Raspbian (Jessie)

5.1. Experimental Setup

A proof-of-concept prototype is implemented in Python language. We use a micro-framework called Flask [30] to develop RESTful web services. All security primitives like symmetric cryptography and hash functions are developed by using standard python library cryptography [31]. We use Solidity [32] and openzeppelin-contracts [33] to develop NFTs, that are deployed on a private Ethereum test network. The experimental infrastructure worked under a physical local area network (LAN) environment and included multiple desktops and IoT devices. Table 1 describes the devices used for the experimental setup. Dell Optiplex 760 (desktop) simulates edge servers that run local support units, while Raspberry Pi 4 (RPi) simulates IoT gateways that collect data from IoMTs. The HPC works as a cloud server that support data sharing among healthcare professionals. A private Ethereum network consists of 6 miners that are deployed on the HPC as 6 containers separately, and each containerized miner is assigned one cpu core. While RPis only work in a light-node mode without mining blocks. All participants use Go-Ethereum [34] as client applications to interact with Ethereum network. To simulate a DDS, we built a private Swarm network [35] consisting of 5 desktops as service sites.

5.2. Performance Evaluation

This section discusses the performance of executing operations regarding different NFT types at the edge network. In general, transaction operations like mint (creation), burn (destruction) and update are processed as writes to the state of NFTs, and they are greatly influenced by block conformation time of the blockchain network. Thus, we evaluate end-to-end latency of a successful transaction operation, which sends a transaction (write) and waits until its receipt has been received. In addition, query operations like getCapAC and getDataAC are processed as reads from the state of NFTs, and scaling up read requests have impacts on performance of query operations. Therefore, we evaluate processing time per query operation given different transaction (read) send rate Th_S as transaction per second (TPS). Data Encryption is not performed in NFT transactions. Finally, we analyze computation overheads incurred by accessing data of DDB and performing symmetric encryption on data. We conducted 50 Monte Carlo test runs for each test scenarios and used the averages to measure results.

5.2.1. End-to-End Latency by Transaction Operations

Given Th_S=1 tps for each transaction operation, figure 6 presents the network latency of committing transactions on the blockchain to change the state of NFTs. Each green bar indicates standard deviation with a mean represented by red dot. The gray line shows whole data range and black star is median. Here we observe that all mint, update and burn operations by NFTs demonstrate almost the similar delays as the blockchain confirmation time in our private Ethereum network (about 4 sec). However, gas used in transactions may vary regarding different computation complexity and processed data

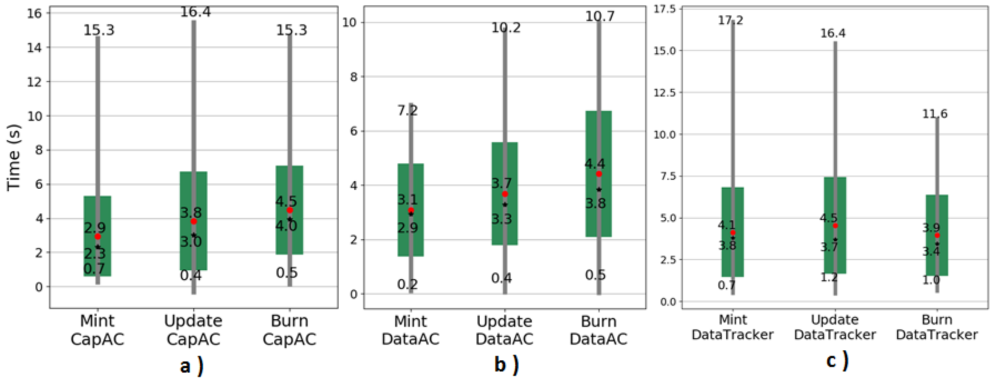

Figure 6. Comparison of latency by NFT operations of an entire lifecycle: a) NFT_CapAC; b) NFT_DataAC; c) NFT_DataTracker.

Table 2. Gas used in NFT operations.

	Mint CapAC	**Update CapAC**	**Burn CapAC**
Gas	189556	195540	66442
	Mint DataAC	**Update DataAC**	**Burn DataAC**
Gas	227056	391111	92495
	Mint DataTracker	**Update DataTracker**	**Burn DataTracker**
Gas	190670	46739	56975

required by NFT operations. Table 2 shows gas fees used in transaction operations of NFTs. Compared to NFT-CapAC that only manages access rights, NFT-DataAC needs to maintain data references (swarm hash) along with their access rights. As a result, all mint, update and burn operations of NFT-DataAC consume more gas than NFT-CapAC. The NFT-DataTracker only maintains data sharing participants' addresses (from and to) when ownership transfer happens, therefore, it requires less gas than other two NFTs.

5.2.2. Network Latency and Throughput by Query Operations

Figure 7 shows average delays that evaluate how long a read CapAC token request can be successfully handled by host machine as increasing Th_S from 2 tps to 100 tps. Regarding the fixed bandwidth of test network, the capacity of host machines that provide NFT token services dominates performance of query transactions. Because desktop is powerful than RPi device, the delays of reading token data and then returning to requester are higher than desktop regarding the same Th_S. Likely, we found that the incremental rate of processing time per transaction on RPi is much greater than desktop does when $Th_S \geq 20$ tps. Thus, the higher Th_S also means the longer latency to handle a query token transaction given multiple service requests.

To evaluate the end-to-end network delay and transaction throughput of query token operations, we let a client send multiple query requests to a NFT token service node and waits until that all responses are received. Regarding NFT service node on RPi, the network latency is scale to Th_S, and it varies from 0.22 sec at 2 tps to 11 sec at 100 tps. Similar test cases performed by desktop produce lower network latency than those done by RPi devices, which varies from 0.12 sec at 2 tps to 6 sec at 100 tps. Figure 8 presents the transaction throughput of querying CapAC token data when Th_S changes from 2 tps to 100 tps. Compared to powerful platform provided by desktop, service node on RPi device demonstrates lower transaction throughput than those on desktop even if Th_S is the same. Moreover, as transaction throughput is subject to system capacity. Therefore, it is almost saturate under scenarios that $Th_S \geq 20$.

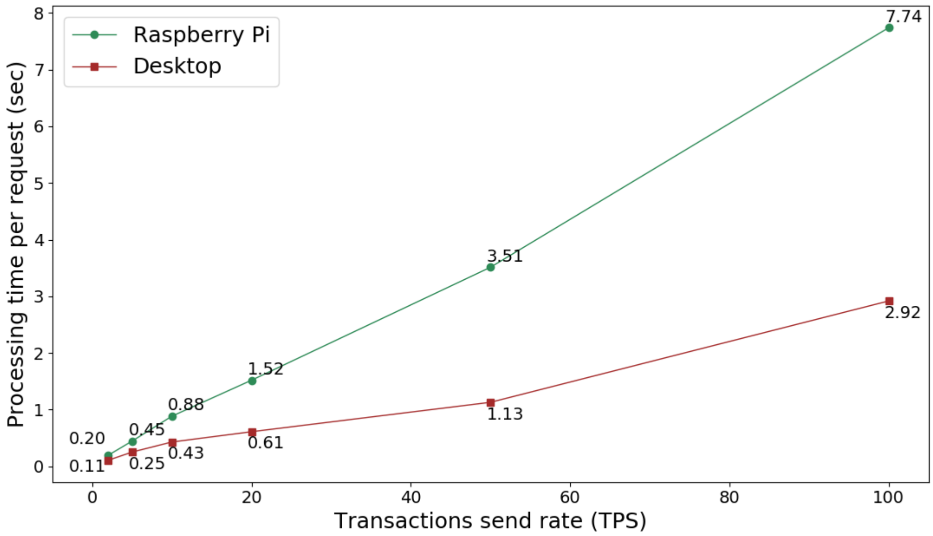

Figure 7. Comparison of processing time by query transactions on different host platform.

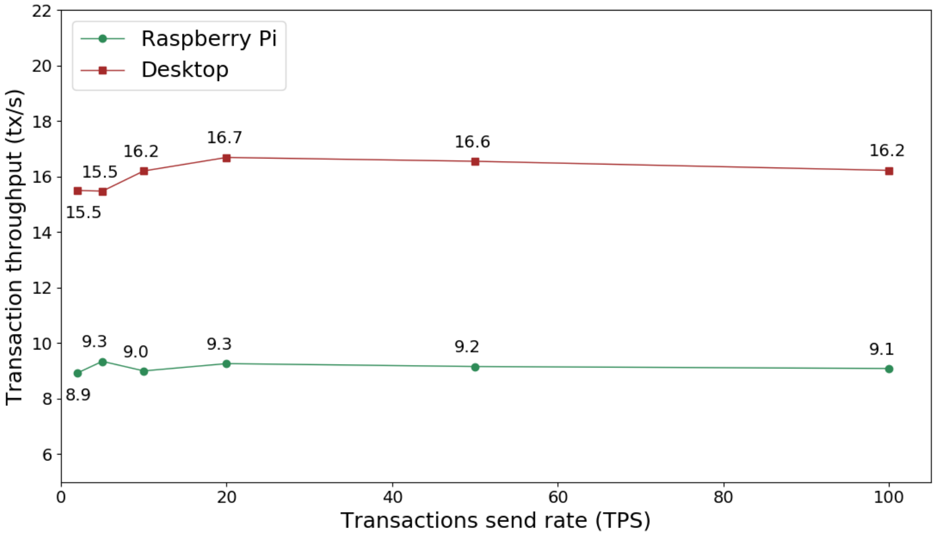

Figure 8. Transaction throughput on different host platform as scaling up transaction send rate.

5.2.3. Processing Time of Accessing DDB and Data Encryption

We assume that data streams of twinning a pair of PO and LO are encrypted and then recorded into DDB for each 30 sec duration by a support unit. As a result, each data file is about 128 KB, and we use these sample data to evaluate computation overheads incurred by DDB and encryption. Figure 9 show processing time of accessing data on swarm and data encryption given different host platform. Rewarding swarm operations, delays by uploading data to swarm network and downloading from a service site are almost same on both platform. Owing to different computation resource, RPi takes longer process time to encrypt and decrypt data then desktop does. Compared with a 30 sec cycle of twin data recording, encrypt data and upload data only marginal delays (0.2 sec on desktop and 1 sec on RPi). Unlike swarm operations, data encryption brings extra overheads in query transactions on both platforms. Given $Th_S = 20$ tps, data encryption incurs 32% processing time on desktop and 53% processing time on RPi. It is a trade-off that uses encrypted data to ensure privacy preservation.

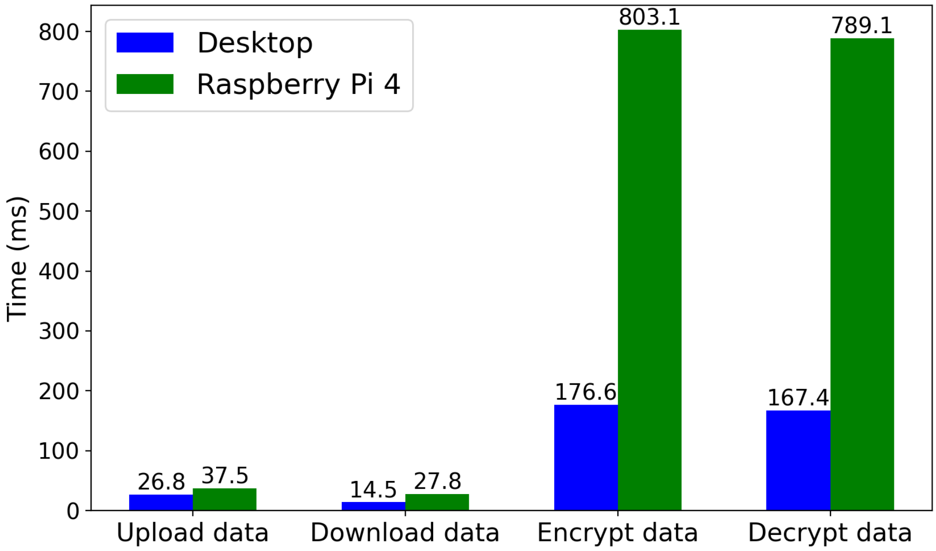

Figure 9. Processing time of data operations: accessing Swarm and symmetric encryption.

6. Conclusions and Future Work

Growing need of virtual health services for senior citizens has brought great challenges in terms of performance, security and privacy. By leveraging Blockchain, NFT and DT technology, we design a lightweight authentication framework to ensure ownership of sensitive medical data as well as verifiable ownership and traceable transferability during data sharing process. The combination of hybrid on-chain & off-chain data storage strategy and data encryption not only guarantees privacy-preservation of patients' data but also ensures data integrity and availability in digital twining and EMR sharing process. We implemented proof-of-concept prototype NFTs and performed the case study of DTH system for seniors safety. The experimental results are encouraging, and they demonstrate efficiency and effectiveness of the porpoised LAF.

However, there are open questions which need to be addressed before applying the LAF to real-world DTH systems. We leave these limitations to our future works:

(1) The scale of the case study is rather small compared to the real-world size of a community that seniors lived in. To ensure the availability of NFT-based algorithm, we need further study in a large scale network.

(2) The emergency alarm highly relies on the emerging artificial intelligence technology including machine learning and information fusion. Apart from the skeleton recognition algorithm [2], we need to investigate more onsite diagnosis mechanisms and integrate them into our framework to improve accuracy of identifying emergent events for senior safety.

(3) The application of blockchain and NFT in health care should not violate local governmental policies. Further investigation and studies are required and certain standards need to be established.

Abbreviations

The following abbreviations are used in this manuscript:

AC	Access Control
AI	Artificial Intelligence
CapAC	Capability-based Access Control
DApp	Decentralized App
DDS	Distributed Data Storage
DDoS	Distributed Denial-of-Service
DT	Digital Twin
DTH	Digital Twin enabled Healthcare
ECG	Electrocardiogram
EMR	Electronic Medical Records
FT	Fungible Token
IoMT	Internet of Medical Things
IoT	Internet of Things
LAF	Lightweight Authentication Framework
LO	Logical Object
ML	Machine Learning
MSP	Medical Service Provider
NFT	Non-fungible Token
PBN	Performance Bottleneck
PO	Physical Object
PoW	Proof-of-Work
QoS	Quality-of-Service
SC	Smart Contract
SPF	Single Point of Failures

References

1. Elayan, H.; Aloqaily, M.; Guizani, M. Digital twin for intelligent context-aware IoT healthcare systems. *IEEE Internet of Things Journal* **2021**, *8*, 16749–16757.
2. Sun, H.; Chen, Y. Real-Time Elderly Monitoring for Senior Safety by Lightweight Human Action Recognition. In Proceedings of the 2022 IEEE 16th International Symposium on Medical Information and Communication Technology (ISMICT). IEEE, 2022, pp. 1–6.
3. Rivera, L.F.; Jiménez, M.; Angara, P.; Villegas, N.M.; Tamura, G.; Müller, H.A. Towards continuous monitoring in personalized healthcare through digital twins. In Proceedings of the Proceedings of the 29th annual international conference on computer science and software engineering, 2019, pp. 329–335.
4. Liu, Y.; Zhang, L.; Yang, Y.; Zhou, L.; Ren, L.; Wang, F.; Liu, R.; Pang, Z.; Deen, M.J. A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE access* **2019**, *7*, 49088–49101.
5. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.
6. Wang, G.; Nixon, M. SoK: tokenization on blockchain. In Proceedings of the Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion, 2021, pp. 1–9.
7. Grieves, M.W. Product lifecycle management: the new paradigm for enterprises. *International Journal of Product Development* **2005**, *2*, 71–84.
8. Erkoyuncu, J.A.; Butala, P.; Roy, R.; et al. Digital twins: Understanding the added value of integrated models for through-life engineering services. *Procedia Manufacturing* **2018**, *16*, 139–146.
9. Van Schalkwyk, P. The Ultimate Guide to Digital Twins. *https://xmpro.com/digital-twins-the-ultimate-guide//* **2019**.
10. Blasch, E.; Lambert, D.A. *High-level information fusion management and systems design*; Artech House, 2012.
11. Khan, L.U.; Saad, W.; Niyato, D.; Han, Z.; Hong, C.S. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *arXiv preprint arXiv:2102.12169* **2021**.
12. El Saddik, A. Digital twins: The convergence of multimedia technologies. *IEEE multimedia* **2018**, *25*, 87–92.
13. Welcome to Ethereum. https://ethereum.org/en/. accessed on August 2022.
14. Xu, R.; Chen, Y. μDFL: A Secure Microchained Decentralized Federated Learning Fabric atop IoT Networks. *IEEE Transactions on Network and Service Management* **2022**.
15. Qu, Q.; Xu, R.; Chen, Y.; Blasch, E.; Aved, A. Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT). *Future Internet* **2021**, *13*, 291.
16. Szabo, N. Formalizing and securing relationships on public networks. *First monday* **1997**.
17. Karandikar, N.; Chakravorty, A.; Rong, C. Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure. *Sensors* **2021**, *21*, 3822.
18. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447* **2021**.

19. Bamakan, S.M.H.; Nezhadsistani, N.; Bodaghi, O.; Qu, Q. Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports* **2022**, *12*, 1–13.
20. Regner, F.; Urbach, N.; Schweizer, A. NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application **2019**.
21. Kugler, L. Non-fungible tokens and the future of art. *Communications of the ACM* **2021**, *64*, 19–20.
22. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd international conference on open and big data (OBD). IEEE, 2016, pp. 25–30.
23. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access* **2017**, *5*, 14757–14767.
24. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: a blockchain-based platform for healthcare information exchange. In Proceedings of the 2018 ieee international conference on smart computing (smartcomp). IEEE, 2018, pp. 49–56.
25. Kumar, R.; Marchang, N.; Tripathi, R. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2020, pp. 1–5.
26. Cunningham, J.; Davies, N.; Devaney, S.; Holm, S.; Harding, M.; Neumann, V.; Ainsworth, J. Non-Fungible Tokens as a Mechanism for Representing Patient Consent. *Studies in Health Technology and Informatics* **2022**, *294*, 382–386.
27. Kumar, V.S.; Lee, J.J.; Hu, Q. Non-Fungible Token-Based Health Record Marketplace. *Available at SSRN 4130876*.
28. Vijayalakshmi, K.; Bushra, S.N.; Subramanian, N.; Ponnuramu, V. Blockchain based Medical Record Storage and Retrieval using NFT Tracking System. In Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2022, pp. 01–08.
29. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* **2018**, *7*, 39.
30. Flask: A Pyhon Microframework. [Online]. Available: https://flask.palletsprojects.com/. Accessed on August 2022.
31. pyca/cryptography documentation. [Online]. Available: https://cryptography.io/. Accessed on August 2022.
32. Solidity. https://docs.soliditylang.org/en/v0.8.13/. Accessed on August 2022.
33. openzeppelin-contracts. https://github.com/OpenZeppelin/openzeppelin-contracts. Accessed on August 2022.
34. Go-ethereum. https://ethereum.github.io/go-ethereum/. Accessed on August 2022.
35. Swarm. https://ethersphere.github.io/swarm-home/. Accessed on August 2022.