How to Control User Private Data Access in Mixed Reality Platforms using Blockchain?

Somnath Mazumdar[a], Abid Hussain[a,b], Raghava Rao Mukkamala[a,b]
[a]Department of Digitalization, Copenhagen Business School, Denmark
[b]Kristiania University College, Norway
{sma, ah, rrm}.digi@cbs.dk

Abstract

Mixed reality (MR) has recently emerged as a popular technology enabling people to interact with virtual and physical worlds. MR involves a combination of complex and advanced technologies, including hardware and software, where users' private data are collected, stored, and processed. Keeping user data secure and private while letting users control their data is not popular among current MR platform owners or third parties. This research proposes a generic blockchain-based MR framework to protect users' private data and alert them about their data access. Blockchain is a data protection layer on MR platforms and relies on fog to support latency-sensitive MR applications. This article presents a framework with core components, followed by a case study elaborating on accessing medical records to present its usefulness. We also present the results of network performance tests, design considerations, and existing technical challenges.

Keywords: Blockchain, Cloud, Data, Fog, Health, Privacy, Mixed Reality.

1. Introduction

Mixed reality (MR) is an advanced form of augmented reality and virtual reality Milgram and Kishino (1994). MR platform combines advanced image processing methods, machine learning (ML), and human-computer interaction technology to develop a three-dimensional (3D) virtual environment. MR-based solutions help humans understand complex processes (such as medical and complicated product manufacturing) and analyze and solve them more accurately.

Problem Context: The Internet of Things (IoT) sensors incorporated in the MR platforms collect vast amounts of heterogeneous data (such as biometric and physiological), combining human interaction with the physical and digital worlds Bailenson (2018). For example, MR platforms can collect sensitive eye tracking David-John et al. (2023) and heart rate data from a user Dick (2021)[1], which can be used for personalized recommendations or to persuade a user to buy a product or service Bailenson (2018)[2]. In general, there is privacy[3] concerns related to immersive virtual world-focused platforms such as MR David-John et al. (2023) and Guzman et al. (2021). However, no existing data management framework improves data confidentiality, user anonymity, and content awareness on MR platforms.

Research Context: Complex privacy-preserving rules (such as the General Data Protection Regulation (GDPR) in Europe) can complicate data sharing, such as medical data sharing Bradford et al. (2020). Therefore, we need a robust, flexible, and privacy-focused framework that can protect user data privacy and compliance on MR platforms. Such a framework can inform the user about their data access patterns and securely delegate access control that can improve mutual trust and cooperation between users and MR platforms Warin and Reinhardt (2022). It has already been observed that blockchain can improve the security of medical records and images by maintaining the transaction log for future processes. In general, it enhances the trust and transparency of medical data access Hossein et al. (2021), Shi et al. (2020), Xia et al. (2017), and Xu et al. (2019). In this research, we explore the research question: *How can blockchain help to protect MR users's private data and provide transparent access control over it?*

Proposed Framework: To answer the research question, our proposed framework aims to improve data protection through blockchain and let users know how their data is accessed. Our framework focuses on three aspects, input data, access, and output protection, out of five listed by Guzman et al. (2019). To ensure that only legitimate third parties can access private user data, we

[1]Oculus Privacy Policy. https://www.oculus.com/legal/privacy-policy/

[2]Even without informing the user.

[3]We define *privacy* as free from intrusion and having the ability to control one's data, while *security* refers to data protection against unauthorised access to user data. In some cases, privacy and security may overlap.

URI: https://hdl.handle.net/10125/106835
978-0-9981331-7-1

have selected open-source Hyperledger Fabric (HLF) as our blockchain platform Androulaki et al. (2018). It supports secure and confidential communication within the network. Here, the blockchain will not hold any user's primary data but only the metadata, such as hash pointers, so that the blockchain is GDPR-compliant regarding user data. The selection of the HLF platform is based on three reasons: *i)* our prior experience working on various blockchain platforms, *ii)* HLF has a higher implementation success rate in many applications than the leading public blockchain such as Ethereum Vadgama and Tasca (2021), and *iii)* it also has lower code-related vulnerabilities compared to Ethereum Chen et al. (2020).

We consider cloud storage as primary data storage (called off-chain storage) and fog computing for fast processing and delegating latency-sensitive MR applications. The platform uses a holographic (MR glass) device, Microsoft HoloLens 2. Domain experts (e.g., physicians) who use MR applications for medical purposes must always place data access requests with their relevant credentials. Metadata about such data access requests will always persist on the blockchain. After delegating the data, the framework will alert users about who accessed their personal data. In addition, other data protection rules and compliance frameworks can be encoded in smart contracts, which are types of application logic contracts. The contributions of this research work are as follows:

- A blockchain-based generic data protection framework for the MR platform has been proposed. We provide a detailed description of the architecture and core components.
- The applicability of the proposed architecture has been validated with a medical use case.
- Finally, we outline the design and technical challenges related to implementation.

2. Background

We first describe the MR platform, then blockchain, and finally, a basic cloud/fog computing introduction.

2.1. MR Platform

MR applications are now becoming mainstream, thanks to advanced high-performance mobile networks enabling high-end Internet bandwidth. Such advances help to delegate compute-intensive tasks (such as image processing) to fog for better performance Costa et al. (2022). MR software stack consists of 3D model generation tools, gesture recognition tools, and spatial mapping tools, where hardware components allow users to access and feel the virtual world. Inside an MR platform, spatial mapping in real-time and interaction between real and virtual objects with synchronized communication occur to improve user experiences in application-specific contexts (such as medical applications). For example, physicians can use the MR platform to convert standard 2D imaging models to 3D holographic models for better visualization. This information can be used to analyze patients' problems (i.e., wounds, fractures) from different perspectives and to understand them better.

Figure 1 describes an MR platform and can be divided into *host* and *MR* units. The host unit (left side of Figure 1) is a computing device (or a handheld device) that has enough computing, memory, and network capacity to run MR applications. Current MR services are mainly web services that offer faster deployment and a scalable execution environment. The input data are stored in the cloud, a scalable and economical storage option. For instance, compute-intensive image processing tasks can be executed in fog while primary data is streamed from the cloud. The host may be connected to an internal accelerator or coprocessor based on hardware implementation to speed up the execution. Complex ML models have already been used successfully for image classification in MR Matrone et al. (2020).

The right side of Figure 1 shows a standard block diagram of an MR holographic glass device. The host connects to an MR unit divided into hardware and sensor modules. The displayed MR hardware unit supports vision, gesture, and acoustic supports. Such devices collect data while the MR application is in use and send the data back to the host unit, which processes and stores (or transfers) data based on computational capacity. MR unit consists of various sensors (such as IoT, special sensors, headsets, displays, advanced haptics, and smart glasses) to measure the physical activity of devices or humans. Existing display devices can be grouped into head-mounted, handheld, projection, and popular monitor-level displays. However, it is not trivial to combine display and gesture-tracking devices.

2.2. Blockchain

The blockchain is a data structure to implement distributed ledger technology (DLT) Androulaki et al. (2018). Each transaction is stored inside a block on a blockchain. As shown in Figure 2, different types of data structures exist, such as linear (blockchain), nonlinear, and directed acyclic graphs, and all inherit the primary features of DLT. However, they differ in the structure of blocks and transactions. The blockchain platform can be divided into four components, i.e., resources, data management, consensus, and network type.

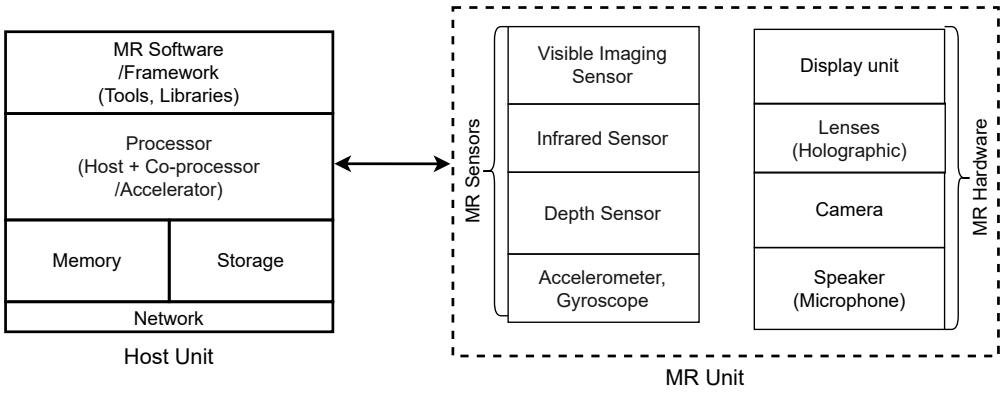

Figure 1. A representation of MR platform with hardware and software components.

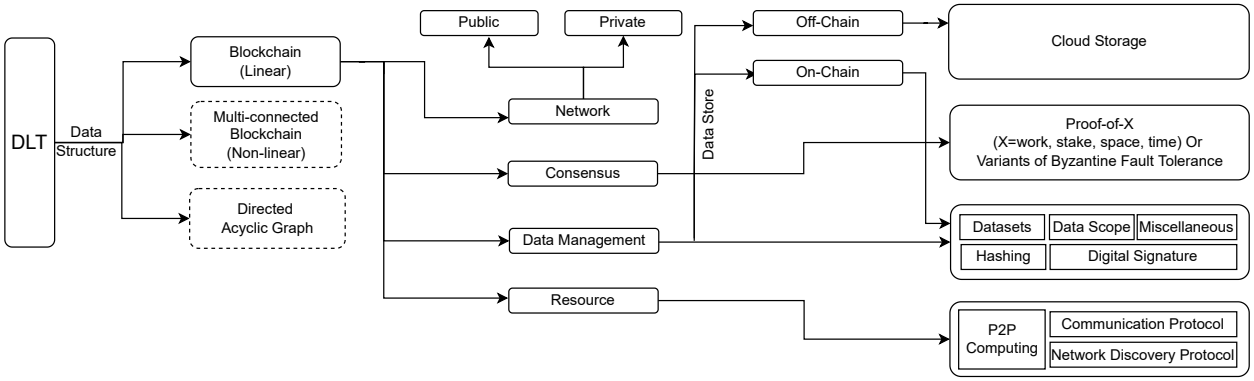

Figure 2. A representation of a blockchain platform with basic components

The peer-to-peer (P2P) computing platform presents the resource part of a blockchain network. Data can be stored inside or outside the blockchain (on/off-chain storage). To handle the blockchain scaling problem, it is a good approach to store primary data in the cloud or in external storage with suitable hash pointers on blockchain to ensure immutability while metadata (including the hashing of input data) on blockchain Faber et al. (2019). This approach helps to scale the network and improves data protection. One out of several consensus algorithms can be used in blockchain platforms based on the requirements. Based on the platform, the applied data protection mechanisms, such as the hashing algorithm and the digital signature, can differ. The blockchain network can be of public or private (also known as permissioned) type. In a permissioned network, the administrator delegates access to the network after thorough user verification. The current framework implementation is based on HLF, which is a permissioned blockchain network. HLF uses the SHA-256 hashing algorithm and the elliptic curve digital signature algorithm as the digital signature. HLF applies a traditional crash fault tolerance consensus mechanism. Specifically, it uses a variant of the Raft consensus algorithm.

2.3. Cloud/Fog Computing

Cloud has become the de facto model for processing enormous amounts of data because it offers low-cost, on-demand computing resources and efficient data storage solutions. However, it is not ideal for latency-sensitive applications. Recently, cloud infrastructure has started to extend from large data centres to smaller distributed computing infrastructures that span multiple locations, known as fog Costa et al. (2022). It acts as an intermediary layer between end users and the cloud so that end users can offload their applications to nearby fog units for better application performance Murshed et al. (2021). Some commercial solutions offer cloud-specific data transfer and storage services, but there needs to be a well-accepted data management security model for user data. For instance, during the implementation of object detection and spatial location mapping applications from images, it has been seen that the cloud services, including the storage facility, should be from the same manufacturing company of holographic devices. It becomes more

challenging when huge amounts of data are distributed across multiple locations. Furthermore, for a better MR platform, cloud/fog-based data management with security is very much required.

3. Related Work

Existing work on the security and privacy properties of MR applications focused primarily on authorization, confidentiality, and undetectability Guzman et al. (2019). Organizations such as the World Economic Forum also focused on MR governance and aimed to develop a secure and interoperable MR platform. Yang et al. (2019) opined that combining blockchain and edge computing makes it possible to create a system that offers secure access and control of the network, storage, and computation. Another work, Shi et al. (2020), surveyed blockchain-based healthcare data management systems to improve data privacy and security.

MR focused works. David-John et al. (2023) examined user biometric identification to detect user privacy threats based on user eye movement on MR devices. Along similar lines, Guzman et al. (2021) show that attackers can infer spaces with high accuracy for HoloLens spatial data and also investigate the spatial characteristics that affect the leakage of spatial privacy. Maharjan et al. (2021) aims to improve image security and reduce the processing time for encryption and decryption in an MR-based surgical telepresence training application. Ryskeldiev et al. (2018) proposes a blockchain-based multiple MR space distribution model for remote collaboration, where spaces are represented as blocks. Furthermore, Vilk et al. (2015) proposes a web application based on the principle of least privileges to render web content while addressing privacy challenges.

Blockchain focused privacy works. Liang et al. (2022) proposes a user data privacy protection method that stores original encrypted data with a Paillier homomorphic encryption mechanism. Hossein et al. (2021) proposes a blockchain architecture to allow privacy-sensitive healthcare data owners to define their data access policies. Research work by Xu et al. (2019) proposes another blockchain-based healthcare system to preserve health data privacy and separate transactions through fine-grained access control. Xia et al. (2017) proposes a blockchain-based medical data sharing model among big data custodians in a trustless environment. The proposed system aims to offer data provenance, auditing, and control.

Compared to the research above, our study primarily focused on using blockchain as a data protection layer on MR platforms (for privacy) and relies on fog to support latency-sensitive MR applications (for better quality of experience).

4. Framework Architecture

As shown in Figure 3, our proposed framework can be broadly divided into *i)* data generation, *ii)* data storage, *iii)* data processing, and *iv)* data delegation stages. Suppose a patient performs a Magnetic Resonance Imaging (MRI) test in a hospital. This activity leads to data generation, and MRI raw data (in Digital Imaging and Communications in Medicine (DICOM) format, refer to Figure 5 (left side)) can be stored in the cloud by calling the relevant APIs. After the primary data are held in the cloud storage, the hash value of the metadata (including the content of the file and other relevant information) is generated by the hashing function (refer to Figure 6 (right side)).

Such metadata represents transactions, and multiple such transactions are bundled up in a data block of a blockchain. In some cases, MR platforms can also generate data (while in use), mainly called MR operations. These operational MR data can be stored in the cloud, and a hash pointer to operational MR data can be stored in the blockchain. The blockchain uses an append-only ledger, meaning MR platform-generated data will be added as a new transaction. Such data may benefit physicians for a faster decision-making in the later stages. Blockchain can protect user data because it is computationally infeasible to compute the correct input data from a given hash digest. The framework also includes fog computing to improve latency, which improves the overall application response rate. The required data can be moved back and forth to fog from the cloud, supported by an extensive network bandwidth.

This framework also relies on the containerization of the MR application. Each container will process the data of one user for better privacy. For better security within the blockchain, HLF offers *channels*, which are private communication tunnels. The user and the registered hospital 'X' can only be channel members. The physicians will not be on the same channel. Physicians must generate a data access request using relevant credentials to the blockchain whenever required. After successful validation, data are sent to the physician, and an alert is sent to the patient. Using such a framework, users can see how their information is accessed in real time. From the deployment point of view, a health network (blockchain) can be created per region, including all regional hospitals and health centres. A national-level blockchain network can also contain multiple regional networks. A large cloud service provider should build a dedicated national health cloud/fog platform to store and process these data.

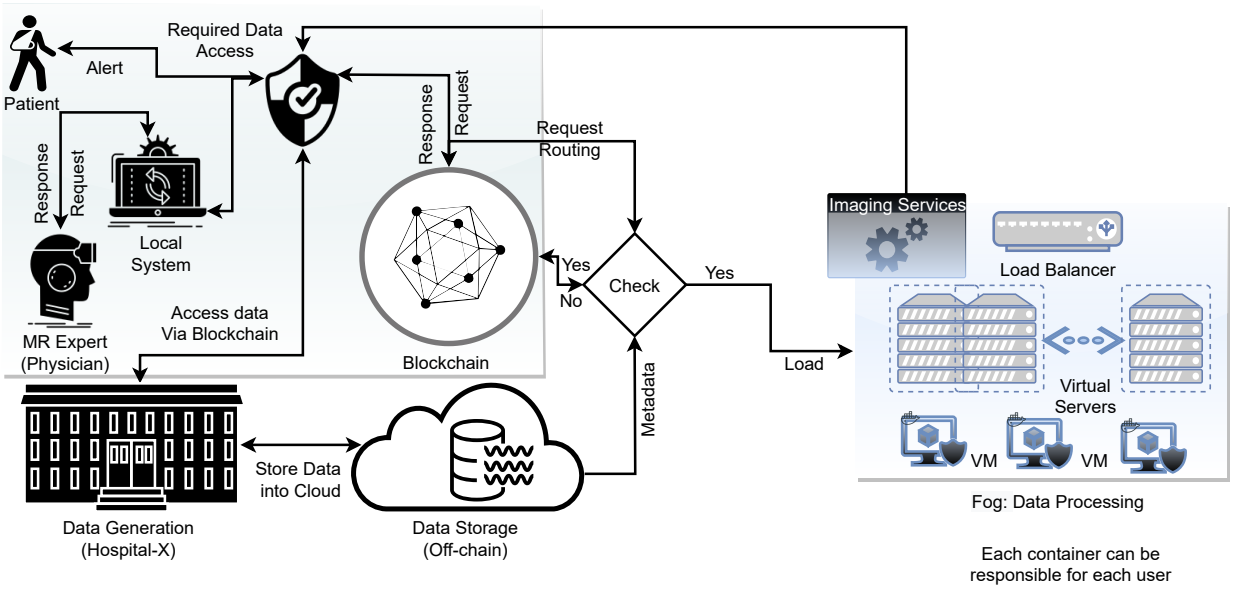

Figure 3. Representation of proposed framework.

4.1. Use Case: Medical Data Access

The holographic display can present the human parts (under observations) in 3D models. Such a 3D visualization offers better visual guidance to develop a better treatment plan. Figure 4 presented a workflow using an MR glass to view 3D holographic images of MRI data from a patient. The primary objective of this use case is to employ an MR platform to improve the quality and precision of health treatment. Patient

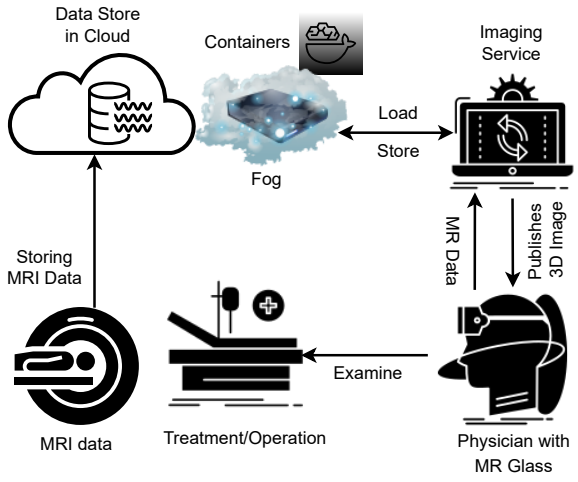

Figure 4. User medical data flow in an MR ecosystem.

MRI data is generated during medical activity, and the resulting data can be stored on dedicated cloud services that support medical data format. MR devices such as HoloLens 2 require high-quality image data to render high-resolution 3D images (Figure 5, right side). To achieve this, large data streams must be sent to MR devices from cloud storage. The data can then be fetched from the cloud and processed in fog due to low latency. MR applications or services can be hosted in fog. Streaming data from the cloud to the fog is seamless, as the cloud backs up the fog resourcefully. Based on such an implementation, the cloud/fog platform can offer a computational service based on the national health data privacy preservation rule. The terminal located in the hospital can work as a slave unit to receive the processed 3D images from fog, and the required data format can be sent to the MR glass unit, where relevant 3D holographic displays would be projected. Using an MR glass (such as HoloLens 2), the 3D holographic model is projected precisely to the required place. If the navigation functionality for enhanced guidance is implemented accurately, the physician can expect accurate and flexible MR guidance during treatment (including operation). A physician can operate relying on virtual 3D models. The MR expert (physician) can move, rotate, and scale the 3D holographic image by gesture or voice control. Such an application of MR not only makes the treatment/operation processes more accurate but also faster and cost-effective. During treatment, some new data from the MR device can also be stored for future use, and these 3D models can be securely shared with other hospitals or physicians. Only the physicians of the hospitals listed on the HLF channels can access user health records. This feature

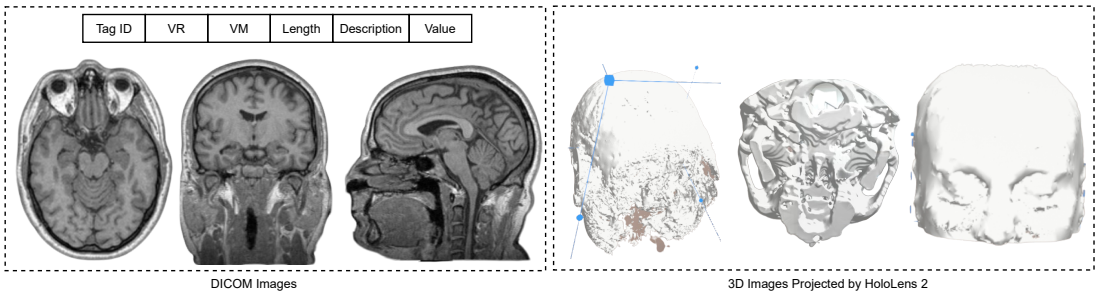

Figure 5. A representation of DICOM images (left side) and 3D transformation by HoloLens 2 (right side).

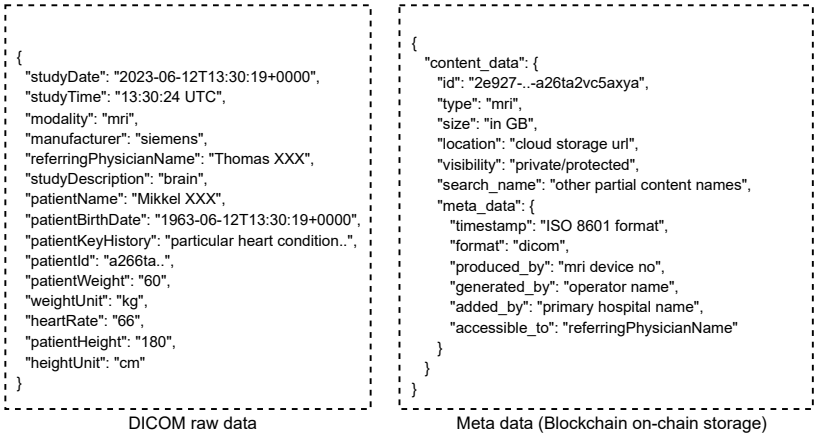

Figure 6. Selected DICOM tags showing patient's critical data (left side) and representation of blockchain-based metadata structure (right side).

is unique to the framework and minimizes the risk of sharing undocumented health records. In these cases, the added hospitals and associated physicians can access data in a time-bound manner as specified in smart contracts.

Medical Imaging. Figure 5 (left side) shows what DICOM images look like. It can also be seen that each DICOM image also has six primary features. They are *i)* Tag ID which identifies the attribute, *ii)* Value Representation (VR) that describes the type and format of the attribute value, *iii)* Value Multiplicity (VM) that specifies the number of values that can be encoded in the Value field, *iv)* Length supports a 16/32-bit unsigned integer based on VR, *v)* Description field describes attributes, and *vi)* Value field contains the values of the Data element. Figure 5 (right side) shows how our HoloLens 2 device projects DICOM images.

DICOM Data. Figure 6 (left side) presents a high-level structure of the DICOM file format. It is a file format that is a de facto standard for the storage and sharing of critical medical data of the patient along with the image data (generated typically by advanced medical machines such as MRI and computed tomography scans) DICOM (2006). At the highest level, the DICOM format comprises three elements: *i)* metadata, which contains personal critical information about the patient, *ii)* hierarchical information about the image series included in the file, and *iii)* the data of the image(s) itself. Figure 6 illustrates a selected tag list containing private patient information. Efforts have been made to emphasize the importance of protecting images embedded within DICOM and its associated metadata Kobayashi et al. (2009).

Blockchain-based Metadata. Figure 6 (right side) represents the current block structure implemented on the HLF platform to handle MRI data. It can be seen that the structure presented in Figure 6 (right side) is generic and can support various types of medical imaging techniques. The `id` is the hashed value of the patient, while the `location` field represents the actual data storage (cloud storage) link. Next, `visibility` can be set to *protected* if the data needs to be shared between other hospitals. It can be seen that under `meta_data`, multiple fields exist which are very particular to the imaging process. Finally, `accessible_to` field is related to the designated physician responsible for the patient. As previously mentioned, even the responsible physician cannot access the data without alerting the

Table 1. Public cloud performance while accessing the compute and storage services

Region	Compute Throughput (Uplink) Mbits/s			Compute Throughput (Downlink) Mbits/s			Storage Throughput (Downlink) Mbits/s			Avg. Latency (ms)	
	Mean	SD	90th Percentile	Mean	SD	90th Percentile	Mean	SD	90th Percentile	Compute	Storage
Microsoft Azure (France)	40.98	12.13	54.97	27.28	13.7	43.36	15.31	9	23.97	42	20
Microsoft Azure (Norway)	47	7.58	57.22	35.64	10.4	48.9	34.67	15.24	50.13	24	36
Amazon Cloud (Stockholm)	39.82	10.97	49.61	33.56	19.78	60.99	26.21	13.44	41.91	36	39
Amazon Cloud (Frankfurt)	30.39	6.57	35.41	27.52	12.95	44.23	16.51	4.51	21.25	25	25
Google Cloud (Frankfurt)	38.22	9.28	48.04	24.93	8.08	32.22	14.04	6.92	21.54	26	11
Google Cloud (Finland)	43.23	8.85	51.36	26.11	8.88	37.54	8.57	4.97	14.62	47	11

patient.

5. Network Test Result

3D image rendering, object recognition, and hand-tracking applications are the core of an MR application. Multiple technical factors severely impact the experience of MR applications. Streaming 3D holographic models requires significantly higher bandwidth than existing networks. Higher requirements on existing network infrastructure increase network congestion, and network delays also hamper the quality of services. MR applications can require a minimum of 60 hertz, and the maximum delay between the process and the rendered frame should be limited to 16.6 ms ITU (2022).

Table 1 shows the throughput and latency for the compute units (virtual machine) and cloud storage. The latency uses the ping, mainly ICMP `ECHO_RESPONSE`, to test the target endpoint. The throughput results are divided into mean, standard deviation (SD), and 90^{th} percentile. SD is used to show the variation in performance, and the 90^{th} percentile is used for performance testing. For the throughput calculation, a file size of 128 kilobytes is used. EU nations are selected during the tests because the MR platform will not store data outside the European Union following the GDPR regulation. It can be seen that changing public cloud service providers, including location, also change the average compute and storage latency. In general, Google Cloud offers the best storage latency. Microsoft Azure cloud service provides the best throughput for computing and storage services, while the average latency is not good during the experiment.

The ITU recommends latency and throughput for MR applications based on mathematical analysis. It focuses on full- and partial-offloading MR application scenarios. It considers image processing for full offloading and recommends a latency between two and three milliseconds (ms) while uploading at a speed of 180 Mbit/s and downloading at a speed of 1000 Mbit/s. For partial offloading or full offloading of the image processing algorithm, the required latency ranges from 3.5 to 6 ms, while upload and download speeds should be 180 Mbit/s and 18 Mbit/s, respectively ITU (2022). Although we now have good enough hardware to build the MR platform, we do not have the necessary network support for good quality of experience, making *a strong case for having a fog unit backed by the cloud to improve latency*.

6. Design Challenges

MR applications have already influenced the medical, industrial, and educational domains. Combining the MR platform and blockchain while meeting multiple design choices is not trivial, mainly when multiple heterogeneous devices and software stacks communicate asynchronously. Each of these devices and components will have its own performance, authentication, security, and integration requirements. For the framework's design, two design features, *performance* and *security*, are primarily selected.

Performance:

- *Throughput* is an important factor, and the framework should have a throughput on par with existing MR applications.
- *Overheads* related blockchain should be minimal, and due to non-standardization, managing blockchain platforms is not easy.
- *Energy efficiency* is often difficult for a blockchain network. It depends on the consensus algorithm used and the size of the data blocks. We selected HLF with a simple and energy-efficient consensus algorithm.
- *Interoperability* between heterogeneous devices/platforms must be supported by standard protocols/interfaces for seamless data exchange.
- *Compatibility.* MR devices and other hardware components must comply with standard data communication protocols for data transfers with the blockchain.
- *Scalability* helps to extend the blockchain network by adding nodes.

Security

- *Authentication* controls unwanted access to user data, so a permissioned blockchain is selected.

- *Confidentiality and privacy* ensure that user data is handled, managed, and exposed according to predetermined rules such as GDPR.
- *Data integrity* preserves the accuracy and consistency of user data throughout the data life cycle.

Blockchain can improve the security and transparency of user medical data by providing traceability. Writing data exchanges into a persistent storage system is required to achieve robust traceability.

7. Technical Challenges

MR platforms require huge computational power for large-scale conversion of 2D data to 3D holographic images, including object detection and spatial location mapping. There are a few commercial MR platforms that are very custom, leading to vendor lock-in issues. Thus, interfacing two diverse MR platforms today is very complicated due to different hardware-software co-design approaches and proprietary communication protocols. Such a gap opens the possibility of data leakage and an outside attack. Issues related to blockchain interfacing occur primarily at the software level. In addition to that, MR platforms also suffer from image freezing and non-synchronized model-related issues.

7.1. Blockchain Related Challenges

Data Block Size. The standard data block size of the blockchain is 'small', and the size lies in the range of kilobytes. Individual nodes' data storage capacity reduces fast because all block changes must be written into the blockchain, and all nodes must have a synchronized local copy of the ledger. Generally, throughput is based on transaction validations, while block size also influences the node's average network capacity Bonneau et al. (2015). Large blockchain networks increase power consumption, and inefficient network management can reduce network throughput. Thus, the performance of blockchain is significant for latency-sensitive MR applications. To counter such issues, *sharding* can also be used where only a few latest versions of ledger states are kept for future reorganization. The existing shard-based blockchain offers $O(n)$ as communication complexity and $O(\frac{b}{logn})$ as storage complexity for a single transaction Zamani et al. (2018).

Scalability. The permissioned blockchain (such as HLF) can employ a less energy-intensive consensus algorithm (such as round-robin and raft) than the public blockchain (such as proof-of-work). Data storage is one of the technical hurdles behind network scalability. Scalability prevents the blockchain from being used for latency-sensitive applications. Software-defined storage can improve the quality of service of off-chain storage solutions. The primary advantages of software-defined storage are hardware abstraction and more data storage control, extending the capabilities from virtualization to data storage types. It adds a software layer to hardware storage and user applications for more data storage control and retrieval capabilities.

DevOps Challenges. An attacker can exploit bugs in public blockchain data transfers. It has been seen that Solidity coded and EVM compiled smart contracts have some critical vulnerabilities, such as authentication and authorization failures. The solidly based Ethereum platform also suffers from too many external dependencies and unreliable programming Chen et al. (2020). Therefore, the framework prefers HLF over Ethereum. However, it is worth noting that HLF also suffers from bugs and unstable libraries.

7.2. Privacy and Stakeholders Types in MR

Each stakeholder must have the necessary access privileges to access the user data. Data privacy should be implemented according to privacy regulations (such as GDPR). Such practices can be implemented through smart contracts. To accommodate the GDPR's 'right to be forgotten' clause, blockchain combine on- and off-chain data storage mechanism. To exercise such a clause, the primary data stored in cloud storage can be deleted by the network administrator if necessary. In contrast, the metadata on the blockchain (e.g., hash pointer to data storage) will not contain any sensitive information. After primary data deletion, the hash pointer left on the blockchain becomes useless.

Additionally, users should control all features of an MR platform. For example, if the virtual and real world are not properly synchronized, the user must be able to return to the physical world easily. Such features should be adequately defined when delegating MR features to users' real and virtual worlds. We need to consider the requirements of all types of stakeholders (including different ages) when designing MR applications. There should be a discussion of who to control and how to control virtual and physical objects. It should be noted that blockchain can also improve the privacy preservation and auditability aspects of fog Yang et al. (2019).

7.3. Security Issues

MR data can be used to infer spaces and allow an attacker to recognize the space belonging to a specific user with fewer visual images Guzman et al.

(2021). There should be more data protection strategies in widely used MR platforms Guzman et al. (2019). MR platforms work with distributed computing systems like cloud/fog and IoT. Security vulnerabilities in one of these platforms can lead to possible MR platform security attacks. Latent security and privacy risks are associated with the functionality of MR platforms. MR glasses are a commercial product, and widely commercial IoT devices are also prone to frequent attacks Al-Garadi et al. (2020). Interestingly, ML models can secure IoT devices but with reduced performance. However, popular ML models (such as the Naive Bayes decision tree and the support vector machine) are vulnerable to security attacks due to poisoning attacks (malicious data in training data sets), leading to decreased model performance Mozaffari-Kermani et al. (2014).

7.4. Standardization

Standardization can increase interoperability between the blockchain and MR platforms. One of the primary issues of standardizing MR platforms is that we need to understand the benefits of applications. There needs to be a more credible effort to standardize MR platforms. The blockchain standardization process is far from complete König et al. (2020). Standardization not only improves the overall blockchain platforms but will also reduce the *vendor lock-in* and improve the interoperability between two popular heterogeneous blockchain platforms, such as HLF and Ethereum.

8. Conclusion and Future Research

MR platforms are making their way into our society. It is a complex ecosystem. In many cases, it handles a large amount of sensitive private data. This paper proposes a generic blockchain-based framework to protect and delegate user private (such as health) data. Here, first, the framework has been discussed together with the components. Later, it is applied to the use case of MRI data visualization in the medical domain. Next, several design and technical challenges are discussed. Our preliminary results also show that current large public cloud providers need to meet the requirements of running MR applications as per ITU recommendations. We realized a successful cloud/fog integration to reduce MR applications' latency, leading to better user acceptance. Future work should focus on developing models to decide which part of the MR application should be offloaded to fog and cloud. Currently, there are two popular cloud storage services: Azure blob storage and Amazon block storage. We are also interested in exploring *how these storage services can influence the performance of MR applications based on unstructured and semi-structured data.*

References

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (iot) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685.

Androulaki, E., Barger, A., & et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the 13th EuroSys conference*, 1–15.

Bailenson, J. (2018). Protecting nonverbal data tracked in virtual reality. *JAMA pediatrics*, *172*(10), 905–906.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121.

Bradford, L., Aboy, M., & Liddell, K. (2020). International transfers of health data between the eu and usa: A sector-specific approach for the usa to ensure an 'adequate'level of protection. *Journal of Law and the Biosciences*, *7*(1).

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys*, *53*(3), 1–43.

Costa, B., Bachiega Jr, J., de Carvalho, L. R., & Araujo, A. P. (2022). Orchestration in fog computing: A comprehensive survey. *ACM Computing Surveys*, *55*(2), 1–34.

David-John, B., Butler, K., & Jain, E. (2023). Privacy-preserving datasets of eye-tracking samples with applications in xr. *IEEE Transactions on Visualization and Computer Graphics*, *29*(5), 2774–2784.

Dick, E. (2021). *Balancing user privacy and innovation in augmented and virtual reality* (tech. rep.). Information Technology and Innovation Foundation.

DICOM. (2006). Digital imaging and communications in medicine (dicom) standard, dicom.

Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). Bpdims: A blockchain-based personal data and identity management system. *Hawaii International Conference on System Sciences*.

Guzman, J. A. d., Seneviratne, A., & Thilakarathna, K. (2021). Unravelling spatial privacy risks of mobile mixed reality data. *Proceedings of the*

ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, *5*(1), 1–26.

Guzman, J. A. d., Thilakarathna, K., & Seneviratne, A. (2019). Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Survey*, *52*(6).

Hossein, K. M., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). Bchealth: A novel blockchain-based privacy-preserving architecture for iot healthcare applications. *Computer Communications*, *180*, 31–47.

ITU. (2022). *Quality of experience (qoe) requirements for real-time multimedia services over 5g networks* (tech. rep. GSTR-5GQoE). International Telecommunication Union.

Kobayashi, L. O. M., Furuie, S. S., & Barreto, P. S. L. M. (2009). Providing integrity and authenticity in dicom images: A novel approach. *IEEE Transactions on Information Technology in Biomedicine*, *13*(4), 582–589.

König, L., Korobeinikova, Y., Tjoa, S., & Kieseberg, P. (2020). Comparing blockchain standards and recommendations. *Future Internet*, *12*(12), 1–17.

Liang, W., Yang, Y., Yang, C., Hu, Y., Xie, S., Li, K.-C., & Cao, J. (2022). Pdpchain: A consortium blockchain-based privacy protection scheme for personal data. *IEEE Transactions on Reliability*.

Maharjan, R., Alsadoon, A., Prasad, P., Giweli, N., & Alsadoon, O. H. (2021). A novel secure solution of using mixed reality in data transmission for bowel and jaw surgical training: Markov property using sha 256. *Multimedia Tools and Applications*, *80*, 18917–18939.

Matrone, F., Grilli, E., Martini, M., Paolanti, M., Pierdicca, R., & Remondino, F. (2020). Comparing machine and deep learning methods for large 3d heritage semantic segmentation. *ISPRS International Journal of Geo-Information*, *9*(9), 1–22.

Milgram, P., & Kishino, F. (1994). A taxonomy of mixed reality visual displays. *IEICE Transactions on Information and Systems*, *77*(12), 1321–1329.

Mozaffari-Kermani, M., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2014). Systematic poisoning attacks on and defenses for machine learning in healthcare. *IEEE journal of biomedical and health informatics*, *19*(6), 1893–1905.

Murshed, M. S., Murphy, C., Hou, D., Khan, N., Ananthanarayanan, G., & Hussain, F. (2021). Machine learning at the network edge: A survey. *ACM Computing Surveys*, *54*(8), 1–37.

Ryskeldiev, B., Ochiai, Y., Cohen, M., & Herder, J. (2018). Distributed metaverse: Creating decentralized blockchain-based model for peer-to-peer sharing of virtual spaces for mixed reality applications. *Proc. of the 9th augmented human int'l conference*, 1–3.

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, *97*, 101966.

Vadgama, N., & Tasca, P. (2021). An analysis of blockchain adoption in supply chains between 2010 and 2020. *Frontiers in Blockchain*, *4*, 610476.

Vilk, J., Molnar, D., Livshits, B., Ofek, E., Rossbach, C., Moshchuk, A., Wang, H. J., & Gal, R. (2015). Surroundweb: Mitigating privacy concerns in a 3d web browser. *2015 IEEE Symposium on Security and Privacy*, 431–446.

Warin, C., & Reinhardt, D. (2022). Vision: Usable privacy for xr in the era of the metaverse. *Proceedings of the 2022 European Symposium on Usable Security*, 111–116.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, *5*, 14757–14767.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal*, *6*(5), 8770–8781.

Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1508–1532.

Zamani, M., Movahedi, M., & Raykova, M. (2018). Rapidchain: Scaling blockchain via full sharding. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 931–948.