Ref. Ares (2023)4658183 - 15/07/2023

rEaLIzing healthcare 4.0 eXploIting the 6G netwoRk evolution

Marie Skłodowska-Curie Actions (MSCA) & Support to Experts

Doctoral Networks

HORIZON-MSCA-2022-DN-01

101120135 – ELIXIRION

WP3 – AI-driven E2E Healthcare service provisioning over 6G

D3.1: Use cases and SoA review on E2E network management towards Healthcare 4.0

Contractual Date of Delivery:	M12
Actual Date of Delivery:	22/11/2024
Responsible Beneficiary:	LIU
Responsible Person:	Nikolaos Pappas
Contact email:	Nikolaos.pappas@liu.se
Contributing Beneficiaries:	LIU, ORAN, FOG, SUIT
Security:	Public
Nature:	R
Version:	V4.0

PROPRIETARY RIGHTS STATEMENT

Document Information	
Version Date:	22/11/2024
Total Number of Pages:	45

List of Authors	
Organization	**Authors**
LIU	Erfan Delfani and Nikolaos Pappas
SUIT	Konstantinos Filopoulos, and Dimitris Panopoulos
FOG	Panagiota Xepapadakou, and Dionysis Xenakis
ORAN	Lechoslaw Tomaszewski

Document History			
Revision	**Date**	**Modification**	**Contact Person**
0.1	20/10/2024	ToC created	Nikolaos Pappas
0.2	1/11/2024	First round of contributions	Nikolaos Pappas, Erfan Delfani, Dimitris Panopoulos, Konstantinos Filopoulos, Dionysis Xenakis, Panagiota Xepapadakou
0.3	8/11/2024	Second round of contributions	Nikolaos Pappas, Erfan Delfani, Dimitris Panopoulos, Konstantinos Filopoulos, Dionysis Xenakis, Panagiota Xepapadakou
0.4	22/11/2024	Final review by the Coordinator's team	Amalia Miliou, Agapi Mesodiakaki

Table of Contents

Lists of Figures

Lists of Tables

Executive Summary

The effective management of network resources is essential for achieving secure, robust, energy-efficient, and cost-effective performance in end-to-end (E2E) healthcare services. This management includes the efficient generation, communication, processing, and utilization of data for decision-making and action within the Internet of Medical Things (IoMT) network. This report provides a state-of-the-art (SoA) review of key enablers supported by 6G technologies that can contribute to enhancing E2E healthcare services. These enablers include four research challenges: i) AI-enabled E2E slicing and zero-touch orchestration, ii) Blockchain-backed incentive engineering mechanisms, iii) Semantics-aware network management, and iv) Big data analytics leveraging explainable AI. Specifically, the review examines both the related works that have been accomplished and the work that remains undone with respect to these enablers. This includes an exploration of how:

- AI-enabled E2E slicing and zero-touch orchestration can contribute to cost and energy efficiency in network operations,
- Blockchain technology enhances healthcare systems by ensuring data security, privacy, interoperability, and integrity, while also improving supply chain management, clinical trials, and electronic health record management,
- Semantics-aware communication proposes information-handling schemes to optimize the generation, transmission, and utilization of the right amount of data at the right time, with the goal of minimizing uninformative data in relation to the system's goals,
- Explainable AI (XAI) contributes to healthcare systems by enhancing transparency, trust, and accountability in AI decision-making, ensuring ethical standards, promoting informed decisions, and balancing model effectiveness with data privacy concerns.

This deliverable introduces relevant concepts and technological frameworks, emphasizing the importance of incorporating and developing methodological tools to address existing gaps essential for achieving secure, energy-efficient, and cost-effective healthcare services, as these enablers are currently underutilized in healthcare systems and IoMT networks.

ABBREVIATIONS

ACK	Acknowledgement
AoI	Age Of Information
AoII	Age of Incorrect Information
API	Application Programming Interface
CMDP	Constrained Markov Decision Process
CSI	Channel State Information
DRL	Deep Reinforcement Learning
DRO	Distributionally Robust Optimization
EH	Energy Harvesting
IDE	Integrated Development Environment
IoMT	Internet of Medical Things
IoT	Internet of Things
LP	Linear Programming
M2M	Machine to Machine
MDP	Markov Decision Process
ML	Machine Learning
NACK	Negative Acknowledgment, Not Acknowledged
OSI	Open Systems Interconnection
POMDP	Partially Observable Markov Decision Process
PT	Prospect Theory
QAoI	Query Age of Information
QoS	Quality of Service
RF	Radio Frequency
RL	Reinforcement Learning
RVI	Relative Value Iteration
Rx	Receiver
SHS	Stochastic Hybris Systems

Tx	Transmitter
UI	User Interface
VAoI	Version Age of Information

2. Introduction

The Internet of Medical Things (IoMT) connects medical devices, sensors, and systems to collect and share real-time health data, enabling continuous patient monitoring, remote care, and personalized treatment. The vast amount of data generated by IoMT devices necessitates a self-sustaining healthcare ecosystem that incorporates reliable AI, efficient data analytics and information handling schemes, secure distributed systems, and processing capabilities to ensure low latency in time-critical healthcare applications. These components are essential for improving healthcare services, enhancing energy efficiency, and increasing cost-effectiveness. Specifically, in end-to-end (E2E) services within IoMT networks, it is essential to address the challenges related to autonomous resource allocation across network segments, ensuring data security, privacy, and integrity, reducing uninformative and stale data, and enhancing transparency, trust, and accountability in decision-making. Despite the advances anticipated by current 5G networks, the following limitations continue to hinder the radical transformation of healthcare:

- **E2E Network Management & Automation:** Although 5G enables the creation of a dedicated pool of resources, i.e., a slice, for different verticals, autonomous rearrangement of heterogeneous resources (communication, computing, and storage) among different slices is still required. The need for autonomous resource allocation through a zero-touch E2E orchestrator is further substantiated by the various Key Performance Indicators (KPIs) in Healthcare 4.0 (H4.0), such as energy efficiency. Another recently emerged metric for efficient network management is the Age of Information (AoI), which reflects the prioritization of data based on its timeliness, reducing the amount of stale information. These novel approaches have either not been adopted in 5G (AoI) or their full-scale realization is compromised by the limited uptake of AI in 5G.

- **AI Explainability:** The massive amount of generated health data can be transformed into useful information and insights for improving healthcare delivery. However, the lack of interpretability of AI-based decisions can significantly compromise trust in healthcare. This calls for novel eXplainable AI (XAI) models that enable people to understand the algorithm's logic and how specific inputs affect the results, leading to trustworthy performance, e.g., through data corrections to avoid bias in training or identifying entry points for adversarial attacks.

- **Security and Data Transparency:** In H4.0, the involved stakeholders need to securely share sensitive information, e.g., Electronic Health/Medical Records (EHRs/EMRs). Existing distributed ledger solutions for secure data management are only limited to a few applications on private networks. AI approaches could be also used to effectively detect security breaches of EHRs/EMRs by analyzing a massive number of events. In parallel, in systems where intensive cryptographical computation may be prohibitive, e.g., in low-complexity IoMT devices, physical layer security solutions could be used leveraging physical channels properties. However, the limited uptake of these methods in 5G prevents them from reaching their full potential.

In ELIXIRION's WP3, we aim to address the limitations of these E2E healthcare services by i) AI-enabled E2E slicing and zero-touch orchestration, ii) blockchain-backed incentive engineering mechanisms, iii) semantics-aware network management, and iv) big data analytics leveraging XAI. Deliverable D3.1 is the first deliverable of WP3, in which we conduct a state-of-the-art (SoA) review of these challenges. The remainder of this report is organized as follows:

- In Chapter 2, a review of SoA regarding AI-enabled E2E slicing and zero-touch orchestration is presented. E2E slicing and zero-touch orchestration can contribute to cost and energy efficiency in network operations.

- In Chapter 3, a review of SoA on blockchain is provided. Blockchain technology enhances healthcare systems by ensuring data security, privacy, interoperability, and integrity, while also improving supply chain management, clinical trials, and electronic health record management.

- In Chapter 4, the SoA review of semantics-aware network management is presented. Semantics-aware communication proposes information-handling schemes to optimize the generation, transmission, and utilization of the appropriate amount of data at the right time, with the goal of minimizing uninformative data in relation to the system's objectives.

- Chapter 5 provides a review of the SoA regarding big data analytics leveraging XAI. XAI contributes to healthcare systems by enhancing transparency, trust, and accountability in AI decision-making, ensuring adherence to ethical standards, promoting informed decisions, and balancing model effectiveness with concerns over data privacy.

3. AI-enabled E2E slicing and zero-touch orchestration

This chapter will be filled when the DC from ORAN will join the project. Until then the deliverable will be uploaded in a draft version.

4. State of the Art: Blockchain in Healthcare

4.1. Introduction to Blockchain technology

Blockchain has been an emerging technology the last few years in many research fields. It is a decentralized distributed ledger system that keeps record of cryptographically secured transactions into blocks. The participating users form a network of nodes that maintain the blockchain without needing a central authority to control them. This eliminates the risk of single points of failure. The core component of the blockchain is the consensus protocol used to ensuring that all participating nodes agree on a common transaction history that is serialized and crystallized due time into consecutive blocks. [1], [2]. This mechanism eliminates the cases of fraudulent transactions. Some of the most common consensus protocols are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), Proof of Space and Time (PoST), Proof of Burn (PoB), Proof of History (PoH), Federated Byzantine Agreement (FBA), Federated Byzantine Agreement (FBA). Blockchain technology ensures that each transaction added to the chain is immutable, meaning that it cannot be altered or deleted during the whole lifetime of the chain. Moreover, every transaction is transparent to all participating users, making it trustworthy. Blockchain technology ensures the security and integrity of the data using cryptography. Each block in the chain contains a cryptographic hash of the previous block. All users contribute to the blockchain with at least one unique public address, but when using several addresses a high degree of anonymity can be ensured. Recent blockchain platforms use Smart Contracts (SC), which are self-executing scripts that reside on the blockchain and enable general-purpose computations to occur on chain. Every SC possesses a unique address and transactions containing data can be sent to that address to trigger the execution of the SC code.

In Healthcare, blockchain technology can be used in various cases. Some of them are **storing patients' records**, providing security of the data stored and privacy from unauthorized access, **interoperability of data sharing** between different healthcare entities, **management of the supply chain** from production to distribution, which can reduce counterfeiting of medicines and **clinical trials and research**, which can be easily deducted with anonymity, accuracy and trust. The two research areas most commonly found in literature combining blockchain technology and Healthcare, where for the management of the Healthcare Supply Chain and the Electronic Healthcare Record (EHR) keeping.

4.2. Blockchain for enhancing the Healthcare Supply Chain

In this section, we present works in literature that enhance the healthcare supply chain by using the blockchain technology. The main disadvantage that the traditional healthcare supply chains face is the complexity of their structure and the centralized management that is difficult to be used by multiple organizations. This leads to inaccurate information and lack of transparency and as a consequence to counterfeit medicine.

In work [3], the authors propose an Ethereum blockchain-based system for drug traceability in the healthcare supply chain and present algorithms of the principles used. The major problems of tracking the healthcare products that this paper is presenting are complexity of tracking supplies, inaccurate information, lack of transparency, centralized tracking systems and counterfeit products. The blockchain technology is proposed as a solution, as it uses cryptography to validate transactions, records are publicly available to any node of the distributed ledger network, and it is very difficult for someone to counterfeit the record already in the chain. The related works section of this paper is split into two subsections, regarding whether they use blockchain technology or not for the drug traceability. The solutions that don't use blockchains are referred to as traditional solutions and most of them use a centralized database that is vulnerable to be tampered, where others that use different databases in the attempt of decentralization, have the countermeasure of interoperability. The blockchain-based solutions are also analyzed as SotA. Then, the proposed architecture for drug traceability system was presented, as shown in Figure 1. An API is also proposed to be used to let devices access the on-chain resources and smart contracts. In more detail, the proposed system model consists of a) **Stakeholders,** such as regulatory agencies, manufacturers, distributors, pharmacies and patients. These entities participate in the smart contract and have specific roles and functions each one. They also have access to the on-chain and off-chain data. b) **Decentralized Storage System** is an off-chain data storage that keeps all the transaction data. These uploaded files are cryptographed in unique hashes and then the different hashes of all files are stored on the blockchain. c) **Ethereum Smart Contract** is used for the deployment of the supply chain, tracking the transaction history and defining the functions and roles of each stakeholder. d) **On-chain resources** are used to store the logs and events that are created by the smart contract, as well as the Ethereum addresses of the different participants.

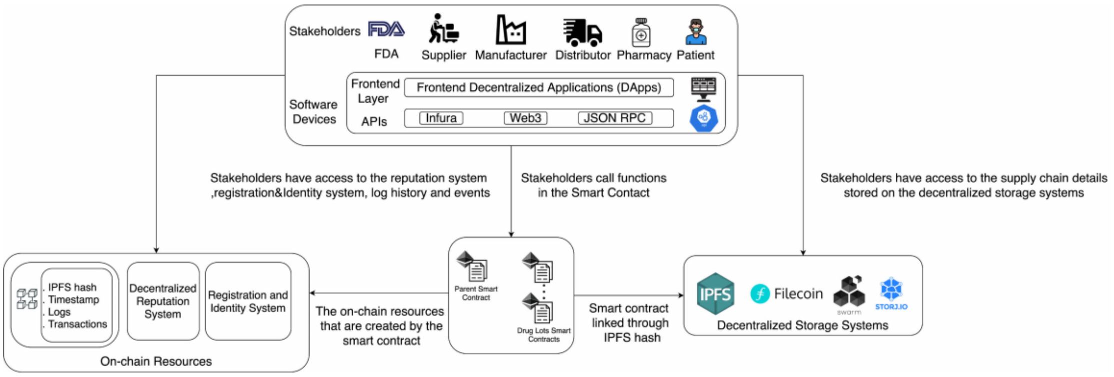


Figure 1 A high-level architecture for the proposed blockchain-based system for pharmaceutical supply chain. [3]

Afterwards, the proposed system is compared with other existing solutions in literature that don't use blockchain and with others that are blockchain-based. The full implementation of the proposed system is also presented, with respective examples and algorithms used. Finally, the discussion and evaluation section present:

a) a cost analysis of the Ethereum blockchain is presented
b) a security analysis for the blockchain-based healthcare supply chain
c) a smart contract security analysis and
d) Blockchain limitations

Work [4] provides a systematic literature review (SLR) on research that uses blockchain technology in Healthcare Supply Chains. The authors found applications of blockchain technology in healthcare in the sectors of medical insurance, remote patient monitoring, medication supply chain management, electronic health records (EHRs), etc. The benefits of using blockchain in healthcare were also presented. Then the authors continue with the review of 124 research articles, which are recent, mainly around 2021-2022 and the majority is from IEEE Access journal, which has a great impact on the research community. The articles are thoroughly analyzed based on their content under different scopes. First, these articles were divided into 5 clusters. Cluster 1 deals with Healthcare supply chain issues and how they can be solved, as well as, with parameter's influence on performance, technology adaptation and digitization of the healthcare supply chains. Cluster 2 consists of articles that show the evolution and progress of blockchain technology, the integration of blockchain with other technologies such as machine learning, IoT, Cloud of Things and Artificial Intelligence. Cluster 3 reviews articles that refer to healthcare challenges and their current status, implementation issues of blockchain technology in healthcare and emerging areas. Cluster 4 overviews applications of blockchain technology in the healthcare sector, some of them are blockchain-based applications on healthcare data and electronic medical record, blood, vaccine, and drug supply chain, waste management systems. Cluster 5 focuses on blockchain technology's potential, and its integration with supply chains, analysis of factors for adoption of blockchain technology in supply chains and blockchain's relevance for sustainable supply chain management. After this categorization in the aforementioned clusters, the authors distinguished the articles based on the methodology they use and concluded that the majority of the articles (70 articles) do a literature review of blockchain in health supply chain, 16 articles use Technology Model, 13 studies have Multiple-criteria decision-making (MCDM) techniques, 12 are empirical works, 3 articles follow hybrid approaches, 2 articles use mathematical modeling and 1 is a case study. The outcomes are shown in Figure 2.

S. No.	Methodology	Method	No. of Articles
1	Case Study		1
2	Literature Review	Review	24
		SLR	35
		Conceptual Framework	4
		Discussions	7
		Bibliometric analysis	3
3	MCDM		13
4	Empirical study	Statistical	11
		Survey, Focus Groups	1
5	Mathematical based		2
6	Hybrid		3
7	Technology Model	Proposal	13
		Implementation	3

Figure 2 Article categorization based on the methodology used [4]

Another work regarding the medical supply chain is [5]. The authors mention the problem of counterfeit medicines which mainly occurs because of the structure of today's supply chain. Data transparency and decentralization of supply chain are the gaps that the authors are trying to cover in order to have open access to medicine information during its lifecycle that cannot be altered by anyone. Blockchain technology can be used to cover this gap, as some of its main characteristics are decentralization, immutability and security. The authors propose each medicine to have a unique ID from the manufacturer and every transaction made with this specific medicine will be recorded to the blockchain until it reaches the final patient. The entities participating in the blockchain may be manufactures, distributors, sellers and regulators. The consensus mechanism that the authors propose is based on the practical Byzantine fault tolerance (PBFT) algorithm with the enhancement of scorekeeping between the nodes, so the highly ranking will participate in the consensus process. Afterwords, the proposed algorithms were presented, as well as a testing scenario where they were applied to verify the traceability of a medicine. Finally, a security analysis was performed assuming a mathematical model of attacking the blockchain and a performance analysis was presented comparing the proposed consensus mechanism with the baseline PBFT.

4.3. Blockchain for Electronic Healthcare Record (EHR) keeping

In this section, works in literature that use blockchain technology for enhancing the Electronic Healthcare Records (EHR) are presented. In traditional systems, different healthcare entities (i.e hospitals) keep local records for their patients. So, the full healthcare record of a particular patient is difficult to be obtained, sharing such records may fail due to interoperability issues between different providers and the centralized control of the data makes them vulnerable to single point of failure. Blockchain technology can be used for solving all these issues.

Article [6] is about securing and sharing of the EHRs, which is stored in a cloud database, utilizing the smart contracts for giving access and the blockchain to keep track of the hashes of the encrypted data stored in the cloud. The authors refer to related works that use blockchain for access control and blockchain for EHRs. The main disadvantage of blockchain technology that they state is that if it is used as storage for big data, it suffers from increased latency of accessing the data and making requests and responses. Their proposed system architecture is shown in Figure 3. To avoid latency and overhead in the blockchain the EHRs are stored in the cloud server, while only their hashes are stored in the blockchain. There are two main functionalities described for the proposed architecture, which are the access control of the EHR data, and the secure EHR upload and retrieval.

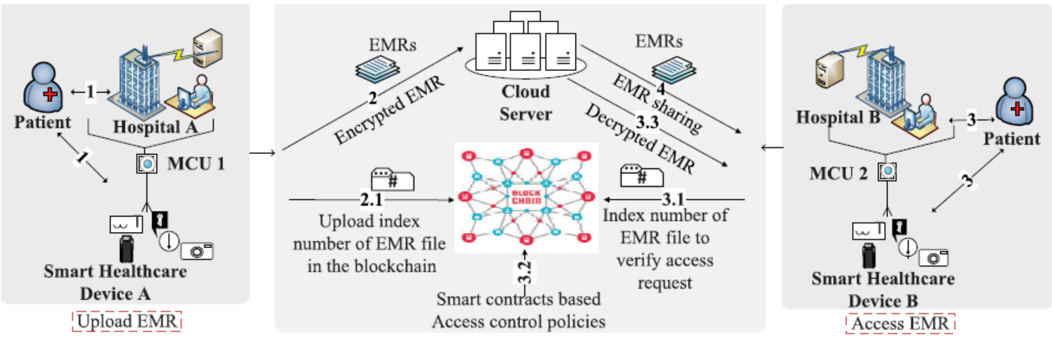


Figure 3 Proposed architecture: Access model for IoT-enabled smart healthcare devices. [6]

Data owners give access control rights to anyone that wants to access their data, through smart contract based access control policies. These smart contracts are validation contract (VC), Get Access contract (GAC), grant contract (GC), and revoke contract (RC). VC is responsible for validating and verifying that each participant is registered and has a unique address in the blockchain. GAC checks the agreement policies between an EHR requester and the EHR owner to decide whether to grant access or not to the data requested. GC grands access permissions to the EHR request for a limited time. RC is responsible for revoking access in any suspicious action. The use and the connection between the aforementioned smart contracts are depicted in Figure 4.

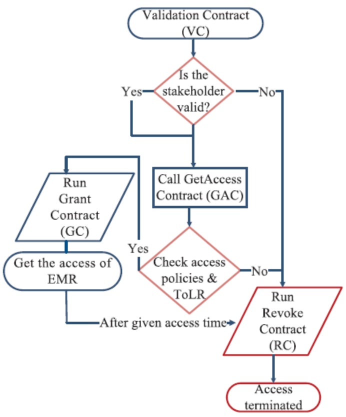


Figure 4 Access control flowchart [6]

For EHR sharing between a requester and the owner, the authors use Elliptic Curve Cryptography (ECC)-based encryption and decryption using Elliptic Curve Diffie-Hellman (ECDH). The two parties share their ephemeral keys, and they calculate the ephemeral shared secret key, that is going to be used only for that session. Each hospital is using Edwards-curve digital signature algorithm (EdDSA) to sign new EHRs that are going to be stored in the cloud for authenticity reasons. All keys expire after a specific time, so the patient's EHR is protected and a new request should be made to regain access, which the patient need to approve from the beginning. The proposed scheme for uploading a new record and retrieving it, is summarized in Figure 5.

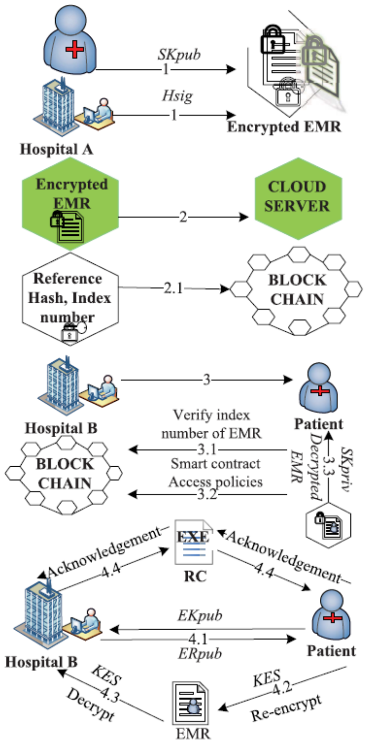


Figure 5 Illustration of upload and retrieval of EHR in the proposed scheme [6]

For the simulation/implementation one laptop and one desktop computer were used to run multiple virtual Ethereum nodes. The performance analysis was made based on the following parameters:

- Latency for Smart Contracts Deployment and Execution
- Computational Latency Analysis
- Latency of Access-request Response
- Security Against Various Attacks

Also, the proposed system was compared to six related works in literature, concluding that the proposed scheme outperforms the others.

A Systematic Literature Review (SLR) over Electronic Health Records (EHR) that use Blockchain technology is presented in [7]. 46 research articles, focusing on interoperability and security, privacy and security tools in healthcare, open issues of the use of blockchain in EHR, ways to store EHRs, big data handling in blockchain systems and Federated Learning for privacy of EHRs, were selected. The triggering problem to make a review in Blockchain-based EHRs studies was that each healthcare entity keeps their records locally for each patient, without knowing the full history of the patient and this centralized data may be vulnerable to attacks. So, the main objective is to have interoperability among different systems, while maintaining privacy and security of the data collected. The main technologies/ techniques that are considered in this work were Blockchain, Deep Learning, Machine Learning and Federated Learning. First, the authors make a report of works in healthcare combining these fields separately, i.e. BC in Healthcare, DL in healthcare, ML in healthcare and FL in healthcare. DL, ML, FL mostly apply to decision-making process and analysis of the dataset, while DL is used for storing and handling the EHRs. Then, they form some research questions, and they provide answers based on the literature studies. Finally, the authors propose a Blockchain and cloud-based framework for EHRs ensuring security and interoperability.

4.4. Blockchain for IoT-based Healthcare

As a different section, work [8] is presented, because it combines applications of both Healthcare Supply Chain management and EHR keeping. The main reason for separating this section is because of the characteristics of the IoT devices and the limitations that they face towards a classic blockchain approach that needs high computational operations. So, [8] focuses on leveraging blockchain technology while using IoT devices on healthcare applications. First, the authors make a short literature review on existing papers that combine Blockchain, IoT and Healthcare and summarize the research gaps. Then, the need to have decentralized communication of the IoT devices together with reliability and security of the data is presented and the authors conclude that Blockchain technology is the best solution to this point. More specifically, a shift from the traditional server-client mode, where all devices and connections are controlled centrally and the cost may be increased in large networks, to a peer-to-peer network, as Blockchain is, where all the functions (computational, storage, etc) are shared between the nodes, the single point of failure is eliminated and privacy, reliability and security are ensured using cryptography. Then, twelve Blockchain consensus algorithms are compared based on the following characteristics to show the compatibility of each one in the context of IoT devices in healthcare:

- IoT compliant
- Constrained
- Basic Concept
- Adaptability
- Energy
- Popularity
- Accessibility
- Example
- E-Health support

A most remarkable part of the paper is the review of some use cases where blockchain technology can be exploited in healthcare systems that use IoT devices. The first use case is about Medical Record Access, where a patient can be served by different health organizations which keep his Electronic Health Record (EHR). The IoT devices can be sensors, wearables, actuators which measure the health of the patient. Smart contracts are responsible for giving access upon patient's request to any of these health organizations and the blockchain keeps track of all the authorizations, EHR data and EHR accesses. Another case that the blockchain technology can be used in healthcare is for clinical research, where the patients' data used for trials should be disconnected from the personal information in order to make them deidentified. The patients should share and trust their data for clinical analysis and research, which can be made easier, more secure and more transparent with the use of a blockchain application. Furthermore, with an IoT interface patients can modify as they wish the access to their EHR data to each involving party, which may be full access to the personal doctor but limited or no access to the research staff. Authors also mention that in many cases the billing or the claims of the provided health services may be incorrect, and intermediates may benefit of this lack of proper communication. With the development of an IoT-based blockchain e-healthcare system, the process of billing, payment and claim adjustments between the parties should be automated and fraudulent free. One more use case is about the Managements of the drug supply chain. Records of all the intermediate stages from manufacturing to final patient should be kept in a blockchain, so human mistakes or frauds are eliminated.

Finally, the authors propose their own system, IoBHealth, that merges all these technologies and consists of IoT-based e-health provider node, IoT-blockchain platform and IoT-based e-healthcare patient node, as shown in Figure 6.

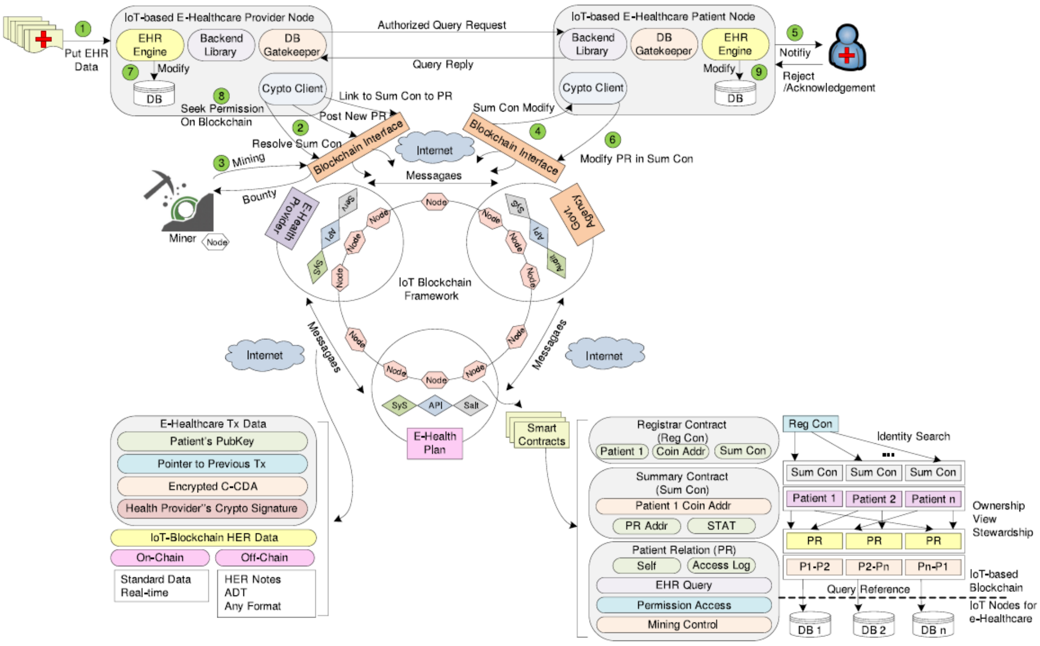


Figure 6 IoBHealth: IoT-based blockchain data-flow architecture for accessing and managing e-healthcare EHR data [8]

5. Semantics-Aware Network Management (LIU)

5.1. Introduction and Motivation

The development of communication networks for various Internet of Things (IoT) and Internet of Medical Things (IoMT) applications is being extensively studied, and new solutions are being offered. These networks serve as powerful tools for exchanging information between different devices, where low-latency connectivity plays a critical role. The *status update systems* represent the primary information-handling setup in IoT/IoMT networks, where update packets from an information source are generated and transmitted through a communication network to a destination node for subsequent processing and utilization [9]. This process fulfills application-driven goals, including remote healthcare, monitoring environmental status, and telemedicine. Communicating timely and informative data is crucial for status update systems within real-time IoT/IoMT networks. However, there are limitations in these networks, as IoT/IoMT devices are highly energy-limited, and the network resources are restricted in terms of bandwidth, channel reliability or availability, and other factors. These limitations necessitate more effective, cost- and energy-efficient approaches for status updating, particularly when communication from a low-energy device to a destination network is involved.

The semantics-aware communication paradigm introduces novel approaches that address the transmission and utilization of the right amount of data at the right time to achieve the designated goals within status update systems [10], [11]. This is accomplished by employing semantics-aware performance metrics and managing the information chain from generation to transmission and utilization within a communication network. Recent studies have demonstrated substantial benefits of this paradigm in status update systems. At the core of semantics-aware communication are semantic metrics that capture the freshness, relevance, or value of information [11]. The freshness of information relates to the staleness of information packets in the network from their generation until their utilization. Higher freshness corresponds to lower staleness of the data packets. The relevance of information relates to sampling the appropriate piece of information from the source. In contrast, the value of information involves providing the destination node with the right piece of information regarding the benefits of having it compared to the cost of its transmission. We can refer to the relevance and value of information as the significance of information. In IoT/IoMT networks, utilizing the freshness and significance of information enables a large number of devices to coexist without the need for additional network resources. By leveraging semantics-aware information handling approaches, a reduction in data management and signaling, and consequently in energy and cost, is expected, without compromising the integrity of the conveyed information within the network. This is particularly important, especially in IoMT networks, where the semantics of information remain underutilized. As a result, key characteristics of the traffic and device properties are often ignored, leading to suboptimal performance in proposed schemes.

In the following sections, we review the background and related works concerning semantics-aware network management approaches. We first present the architecture of the IoT and IoMT networks, followed by a typical system setup for status updates, while introducing the key concepts of this system model. Next, we introduce the semantics-aware performance metrics. Finally, we explore the information-handling approaches proposed for optimizing these semantic metrics.

5.2. Background

5.2.1. The architecture of IoT networks

The Internet of Things (IoT) refers to physical devices that communicate with each other over the internet, enabling automatic information transfer without human intervention. IoT connects various entities like devices, people, animals, processes, and plants. It plays a key role in enabling emerging smart technologies across various sectors, including smart homes, e-health, smart grids, manufacturing, and smart cities, and is expected to drive significant future growth [12].

Various technologies are integrated into IoT systems, including sensor and actuator devices, signal and data processing, user interface (UI) and machine learning (ML), artificial intelligence, machine-to-machine (M2M) communication, internet technology, and embedded systems. Additionally, integrated development environments (IDEs) are used for system software development. The complexity of an IoT system varies depending on its specific application.

These technologies are systematically integrated and understood within an interconnection architecture, typically based on a layered model. A conventional architecture commonly used in communication systems is the OSI layer model, as illustrated in Figure 7. In an IoT architecture, some layers may be merged or modified. Various IoT architectures have been introduced, including three-layer, five-layer, cloud-based, fog-based, edge-based, mist-based, big data, and QoS-based architectures. While most applications align with the first three architecture types, certain IoT applications are better suited for edge-based architecture. Here, we present the three-layer architecture as a foundational model, serving as a good basis for developing the subsequent sections on status update systems and semantics-aware approaches [12].

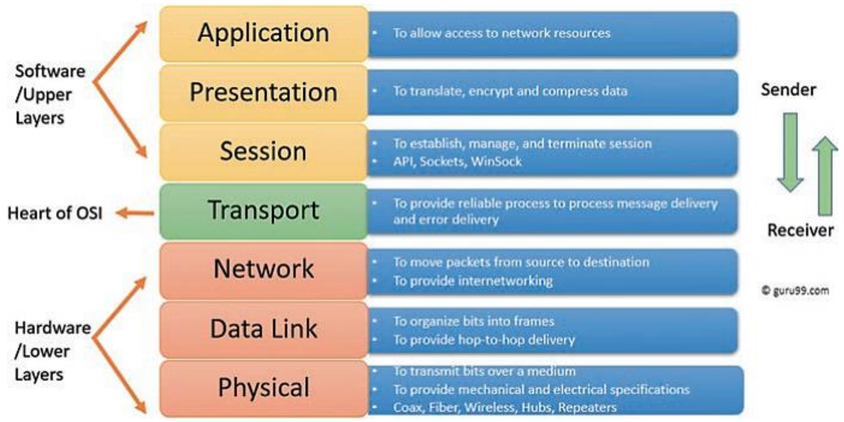


Figure 7 OSI layer architecture of communication [12]

5.2.1.1. Three-layer IoT architecture

An IoT system can be described using a three-layer architecture, which consists of the layers as depicted in Figure 8 [12]:

1. Thing or device layer
2. Network layer
3. Application layer

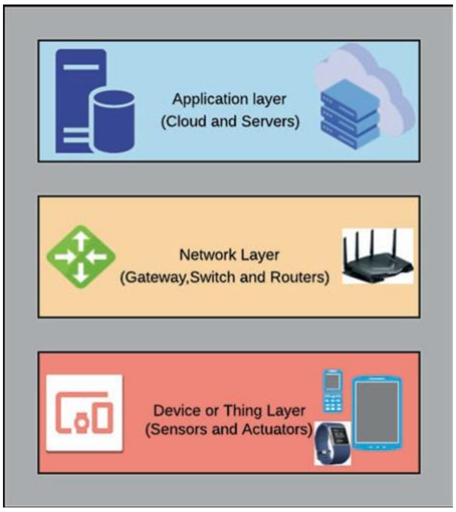


Figure 8 Three-layer IoT architecture [12]

Thing or device layer: The thing or device layer consists of physical devices like sensors and actuators that interact with the environment by sensing, capturing, and controlling parameters. These edge devices connect to the Internet via wired or wireless links, such as Bluetooth, Wi-Fi, or Ethernet, supporting machine-to-machine (M2M) communication. Their functionality can range from sensing only to both sensing and connecting to the Internet. Device features, including sensors and actuators, must be tailored to the specific application, making sensor/actuator type a key differentiator among devices. Understanding these requirements is crucial when designing IoT systems [12].

Network Layer: In the IoT architecture, devices access the Internet through gateways, switches, or routers, forming a network layer optimized for data collection and distribution. This layer acts as a messenger between devices and the cloud, where applications reside. Large IoT systems may utilize multiple gateways to handle high volumes of edge nodes, normalizing, connecting, and transferring data between the physical device layer and the cloud server. Data transfer occurs via gateways, often referred to as "intelligent gateways" or "control tiers," which can support computing functions such as telemetry, protocol translation, artificial intelligence, data pre-processing, and device management. Security measures, including data encryption and monitoring, are increasingly implemented on these gateways to guard against "man-in-the-middle" attacks. Some gateways provide real-time operating systems tailored for embedded and IoT systems, along with low-level support for various hardware interfaces and functional libraries that facilitate network layer functionality based on standard IoT development protocols [12].

Application Layer: The cloud or data server, as the application layer, communicates with the gateway via wired or cellular Ethernet. It consists of powerful server systems with databases that support robust IoT applications and integrate services such as data storage, big data processing, filtering, analytics, third-party APIs, business logic, alerts, monitoring, and user interfaces. Within a three-layer IoT architecture, the cloud also manages and configures events at the gateway and edge devices [12].

5.2.2. Status update systems

A basic status update system model has been depicted in Figure 9. In this system, update packets or samples originating from an information source are generated and transmitted from a source node (Tx, typically an IoT/IoMT device) to a destination node (Rx) within a network according to an update policy [9], [13]. This policy dictates when the update packets are generated/transmitted to the destination node. In a more complex setup, there may be additional nodes for relaying or receiving the updates. In this system model, the update packets are forwarded through a channel or network, which may be either reliable (error-free) or unreliable (error-prone). A backward channel from the receiver to the transmitter is also considered, serving to send ACK/NACK feedback in the system. The ultimate objective is to determine the optimal policy that maximizes performance by optimizing semantic metrics within the system while adhering to system constraints.

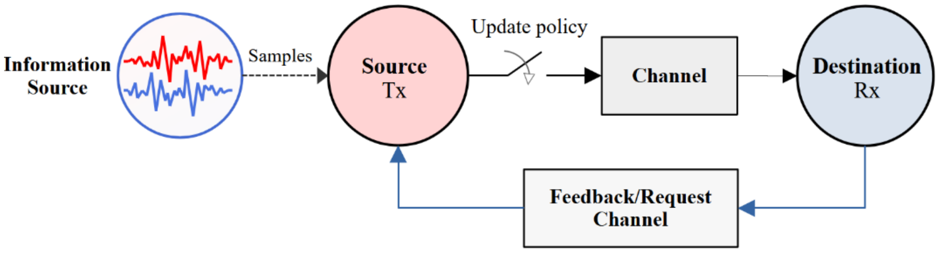


Figure 9 A status update system

5.2.3. Some concepts regarding the status update systems

5.2.3.1. *Push-based and Pull-based Scenarios*

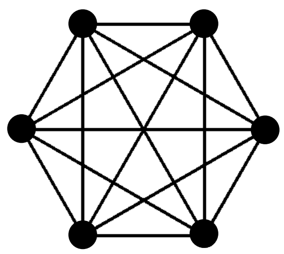
The status updates can be either pushed towards the receiver according to the transmitter's decision in a push-based scenario or requested and controlled by the receiver in a pull-based scenario. In the latter case, the device determines the actions upon the receiver's request; otherwise, it remains idle.

5.2.3.2. *Cache-enabled networks*

Caching is another important aspect of practical IoT/IoMT networks for managing resources and enhancing network performance. Caching involves storing and delivering frequently accessed information or content at the edge of the network, closer to sensors or devices. Effectively, it can reduce the need to retrieve data from the source, which can be energy-consuming and less efficient.

5.2.3.3. *Gossiping networks*

Gossiping offers efficiency in resource-constrained networks where centralized information handling is inadequate. In gossiping networks, the update packets are randomly forwarded among the network nodes [14]. Several gossiping topologies exist, including Ring and Fully Connected ones.



Fully connected

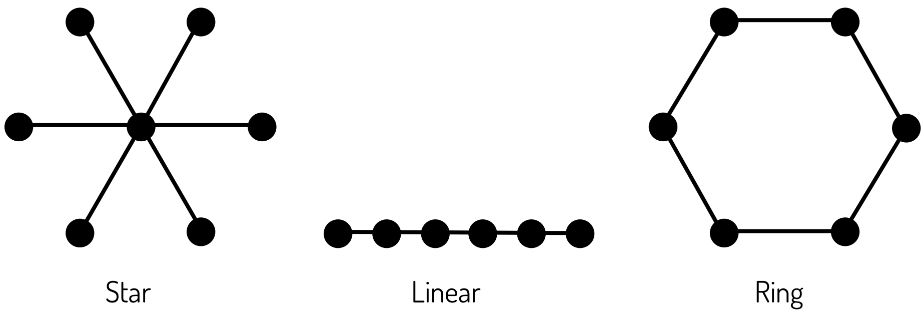


Figure 10 Gossiping topologies

5.2.3.4. Energy harvesting devices

In practical IoT/IoMT applications with battery-powered sensors, there is a severe limitation against frequent updates because each update consumes energy, and the batteries have a finite capacity. In the current systems, a class of Energy Harvesting (EH) sensors with rechargeable batteries are being deployed and promise cost-efficient and self-sustainable IoT networks [15]. In this case, the intermittent nature of harvested energy requires more intelligent energy budget management while ensuring timely updates.

5.2.4. Semantic metrics

Various semantic metrics have been introduced in the literature, including Age of Information (AoI) [16], non-linear AoI [17], Age of Incorrect Information (AoII) [18], Query Age of Information (QAoI) [19], Version Age of Information (VAoI) [20], and State-Aware AoI [21]. Among these, AoI is a freshness metric that quantifies the time elapsed since the generation time of the last successfully received packet at the destination node. Version AoI (VAoI) is a semantic metric that quantifies jointly the freshness and relevance of information, measuring the number of versions by which the receiver lags behind the source. Query AoI (QAoI) is another performance metric that represents the freshness and value of information. QAoI considers the AoI only when there is a request from the destination node, i.e., only in query instances when the information is assumed to be useful to the receiver.

5.2.4.1. AoI and its variations

AoI is defined as the time elapsed since the generation time of the last received update, i.e.,

$$\Delta^{AoI}(\mathrm{t}) = \mathrm{t} - \mathrm{u}(\mathrm{t}),$$

where $\mathrm{u}(\mathrm{t})$ is the timestamp of the current update at the receiver. The AoI is the most widely used metric in the literature, and its optimization yields the freshest updates in status update systems across various configurations, including energy harvesting setups.

5.2.4.2. AoII

Unlike AoI, which fails to capture the content of information, AoII takes the content of information into account. AoII measures the elapsed time between the present time (t) and the most recent time when source collects a sample that contains the same content as the sample stored at the receiver ($V(t)$),

$$\Delta^{AoII} = (t - V(t)) \times \mathbf{1}\{\hat{X}(t) \neq X(t)\},$$

where $X(t)$ represents the content or state of the source, and $\hat{X}(t)$ represents the content or state of the receiver. $\mathbf{1}\{\cdot\}$ is the indicator function.

The following example illustrates the difference between the AoI and AoII metrics in a remote reconstruction application involving a two-state Markovian source. In this example, four time intervals are considered. During the first time interval ($0 \leq t < t_1$), the source and the receiver are in the same state (0), so the error indicator function, $\mathbf{1}\{\hat{X}(t) \neq X(t)\}$, is zero. In this interval, no updates occur, and the AoI increases linearly. In the second time interval ($t_1 \leq t < \tau_1$), at time t_1, the state of the source changes from 0 to 1, but no updates are transmitted to the receiver. As a result, there is a discrepancy between the source and the receiver during this interval, and the error indicator function becomes one, while the AoI continues to increase. At time τ_1, a transmission occurs, and the receiver's state is updated to 1. This update resets the AoI to zero, followed by a linear increase, and also resets the error indicator function to zero. Finally, in the fourth time interval, the state of the source changes back to 0 without any updates, causing the AoI to increase linearly and the error indicator function to change.

- First time interval: $0 \leq t < t_1$

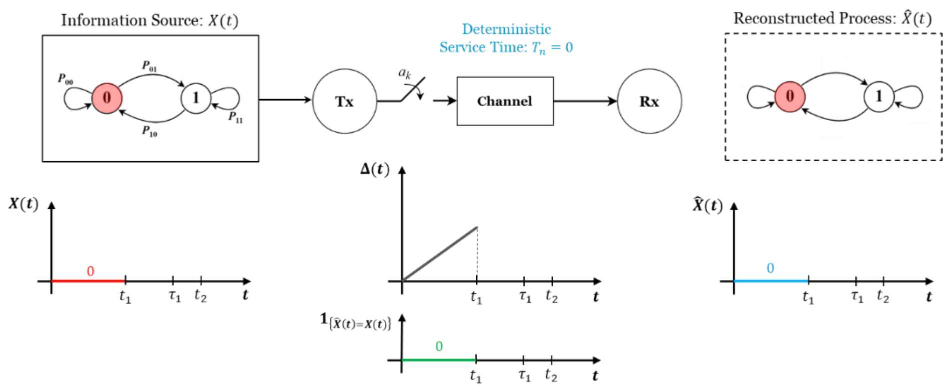


Figure 11 AoI and error as a function of time ($0 \leq t < t_1$)

- Second time interval: $t_1 \leq t < \tau_1$

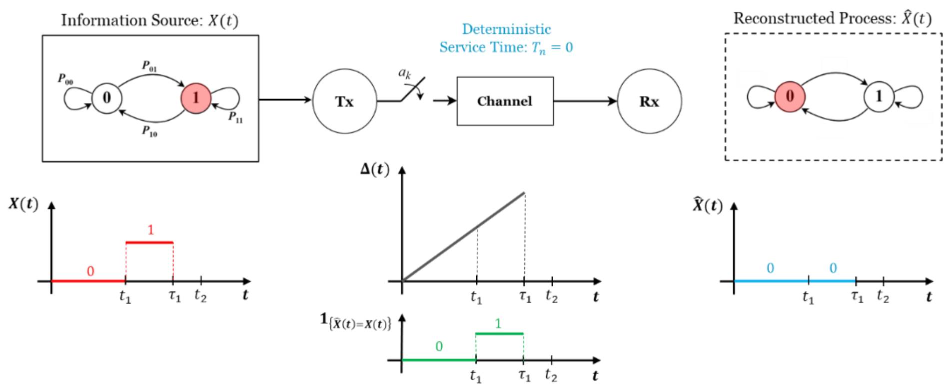


Figure 12 AoI and error as a function of time ($t_1 \leq t < \tau_1$)

- Third time interval: $\tau_1 \leq t < t_2$

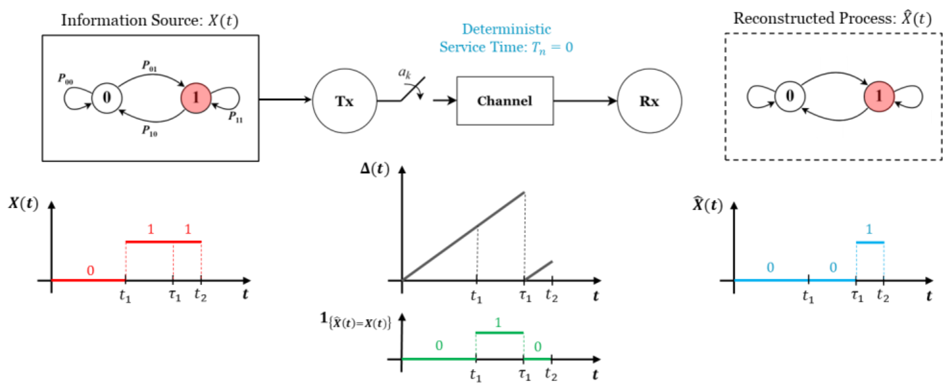


Figure 13 AoI and error as a function of time ($\tau_1 \leq t < t_2$)

- Fourth time interval: $t \geq t_2$

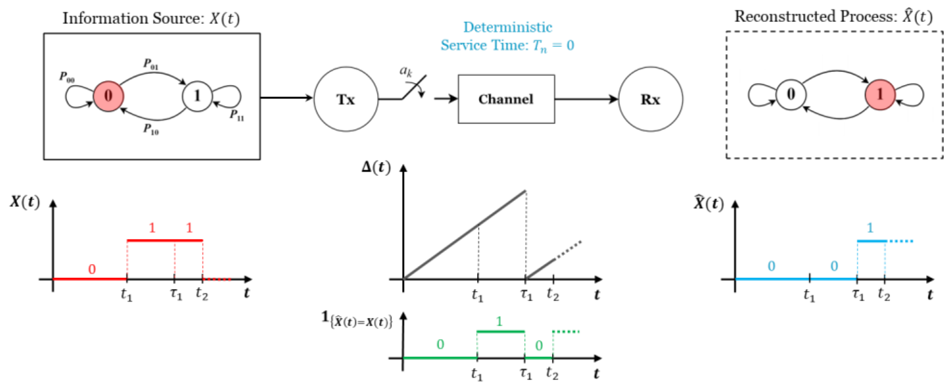


Figure 14 AoI and error as a function of time ($t \geq t_2$)

The AoI metric does not account for the content of the information; it only considers the timestamp of the most recent update in the system. In contrast, the AoII incorporates the content of the information and increases only when there is an error or discrepancy between the source and the receiver. It can be observed in Figure 15.

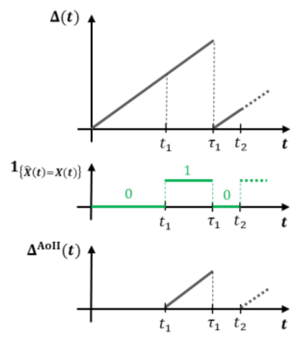


Figure 15 AoI vs. AoII

5.2.4.3. VAoI

VAoI quantifies the number of versions by which the receiver lags behind the source, i.e.,

$$\Delta^{VAoI} = N_S(t) - N_R(t),$$

where $N_S(t)$ and $N_R(t)$ represent the version numbers of the current updates at the source and receiver, respectively. By version, we refer to any significant change in the content or new generation of information at the source.

Figure 16 illustrates the time evolution of both VAoI and AoI as functions of time. In this example, a status update occurs at $t = 4$, after which the AoI begins to increase linearly. It can be observed that the AoI reaches 14 by time slot 19, while the VAoI increases to 7. This is because there are only 7 version changes at the source.

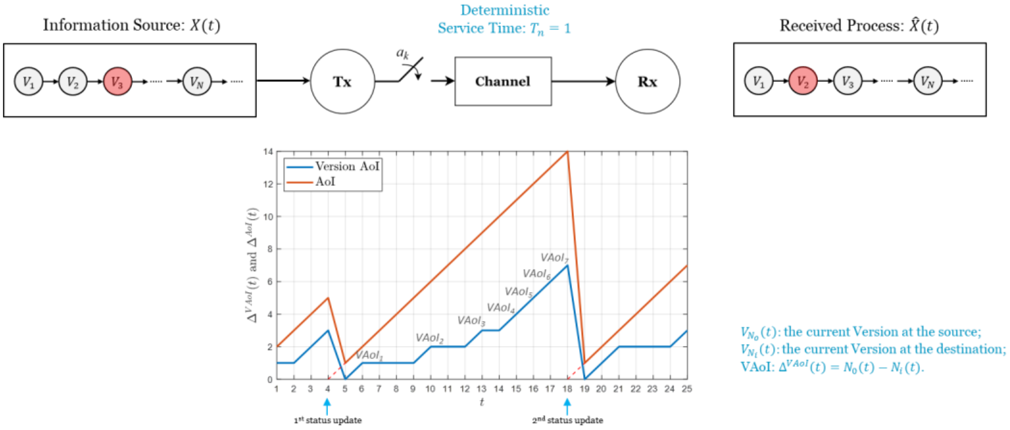


Figure 16 AoI and VAoI as a function of time

5.2.4.4. QAoI

QAoI is an extension of AoI and considers the age at instances when there is a request from the destination node. This metric is suitable for pull-based status update systems, wherein the destination node requests and controls the generation or transmission of updates as needed and when they are valuable for utilization. If we presume a binary request arrival process $r(t)$, where $r(t)$ equals 1 when there is a request from the receiver and 0 otherwise, then QAoI is defined as $\Delta^{QAoI}(t) = r(t) \times \Delta^{AoI}(t)$. This metric penalizes system staleness only when requests are demanded. In a practical scenario where there is a lag (τ) between the request time and when the system controls are applied, the definition can be corrected to $\Delta^{QAoI}(t) = r(t - \tau) \times \Delta^{AoI}(t)$.

5.2.4.5. State-Aware AoI

In some status update system, the information source has two operational/contextual states, or macro-states, within which underlying events, or micro-states, evolve. These micro-states represent the raw evolution of the information source. The contextual macro-states, *normal* and *alarm*, primarily determine the level of demand for timeliness, with a higher freshness required in the alarm state. The State-Aware AoI addresses the timeliness of the source's micro-evolution under the contextual macro-states, i.e., the AoI during the different macro-states. Specifically, two distinct AoI variables are employed, each corresponding to a different state of the stochastic process. The AoI for the z-th state of the stochastic process at time k is defined as $\Delta_k^z, z \in \{0,1\}$, where $z = 0$ indicates a normal operational state. In contrast, $z = 1$ signifies an alarm operational state. The proposed metric (or cost function) at time k is defined as,

$$\Delta_{\mathrm{k}}^{\text{State-Aware}} = (1 - Z_k)\Delta_k^0 + Z_k\left(\Delta_k^1\right)^2.$$

We observe that when the source is in the normal state $(Z_k = 0)$, the cost increases linearly with Δ_k^0, while when the stochastic process is in the alarm state $(Z_k = 1)$ the cost increases with the square of Δ_k^1.

5.3. Literature Review

5.3.1. Optimizing semantic metrics in energy constrained systems

Several works have investigated the optimization of information freshness in energy-constrained IoT networks [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42]. A few recent studies have also incorporated AoI as a freshness metric within healthcare systems, including channel allocation for users in IoMT networks [43], power allocation in cellular-based IoMT systems with imperfect channel state information (CSI) [44], and privacy preservation in healthcare metaverse systems [45].

5.3.2. Optimizing information freshness in energy harvesting systems with MDP

In this section, we primarily focus on discrete-time systems that adopt the Markov Decision Process (MDP) framework to optimize information freshness in energy harvesting networks. These works can be classified into two groups: push-based (or permanent query) systems and pull-based (or request-based) systems.

In the first group, the system's action does not depend on external requests or queries from the server or destination nodes, making them permanent query systems. One such work is presented in [22], where the authors investigate a system employing an energy harvesting sensor to monitor a two-state stochastic process and transmit status updates to a destination node. The cost function of the MDP problem incorporates two AoI variables with different exponents, considering higher demand in the alarm state. The optimal status updating policy is determined using the Value Iteration algorithm.

In [35], the authors consider an IoT-enabled monitoring system in which an RF energy harvesting device samples and sends update packets to a destination node. They formulate an MDP problem to find the optimal online status updating policy that minimizes the long-term average AoI. The optimal policy accounts for battery dynamics, AoI, and channel state information, determining the allocation of each time slot for energy harvesting or status updating. The study also presents analytical results on the value function and optimal policy structure and compares age-optimal and throughput-optimal policies. Building upon the previous work, [36] extends the system to multiple source nodes. The optimal policy aims to minimize the long-term average weighted sum of AoI values associated with different physical processes monitored by the source nodes. Additionally, the authors propose a computationally efficient Deep Reinforcement Learning (DRL) algorithm to learn the age-optimal policy.

In [37], the focus shifts to a cognitive radio system where the secondary user is an energy harvesting sensor. The sensor decides between spectrum sensing and status updating operations at each time slot. The sequential decision-making problem is modeled as a Partially Observable Markov Decision Process (POMDP) and solved using dynamic programming. The study also explores the structural properties of the optimal policy.

Considering a status update system over an error-prone channel, [38] investigates an energy harvesting transmitter (Tx) that can sample and transmit a new update, remain idle, or retransmit the last update to a receiver (Rx). An average-cost MDP problem is formulated, accounting for the energy consumption during sampling and transmission, as well as the limited battery capacity of the TX. The age-optimal scheduling policy is determined using the proposed Relative Value Iteration (RVI) and Reinforcement Learning (RL) algorithms for known and unknown channel and energy harvesting statistics, respectively.

In [39], the authors consider an energy harvesting monitoring node with a finite battery capacity. The node receives status updates from multiple heterogeneous information sources, each measuring an underlying process. These sources exhibit varying energy consumption and AoI values. The monitoring node aims to minimize the average AoI by selecting an optimal action at each time slot, including requesting an update from a source or remaining idle. The problem is formulated as an MDP, and the optimal solution structure is analyzed. The Value Iteration algorithm is employed for finding the optimal policy.

The paper [46] delves into time-averaged AoI minimization in an EH remote sensing system. An EH source samples processes opportunistically and transmits updates to a sink node over a time-varying wireless link, where a trade-off exists between information freshness and energy availability. Using MDP theory, the paper formulates the problem and derives optimal sampling policies for scenarios with single or multiple processes and channel state information at the transmitter. Optimal policies are threshold-based, considering process age, energy availability, and channel quality.

The study [47] presents an MDP model for an automatic repeat request transmission system powered by energy harvesting. This study explores transmission policies to minimize the AoI for correctly delivered packets, examining the trade-off between retransmitting unsuccessfully transmitted packets and sending new ones, considering varying energy costs for each action.

The work [48] addresses timely information updating in an EH IoT system for monitoring a physical process, optimizing ON-OFF scheduling to minimize AoI. Through MDP, optimal policies for single-unit and infinite battery cases are derived. A state-adapted waiting before turning on policy is proposed, with comparable performance to the optimal one. The scenarios without a battery, along with a policy that waits for state transitions, are also considered, highlighting the importance of batteries and optimal waiting times.

Regarding the pull-based approach, [40] focuses on minimizing the on-demand Age of Information subject to energy causality and transmission constraints in a multi-user and multi-sensor IoT energy harvesting sensing network. The problem is formulated as an MDP, and an iterative algorithm is proposed to obtain the optimal status updating policy at the cache-enabled edge node. Additionally, a sub-optimal low-complexity algorithm is developed to handle scenarios with a large number of sensors.

In [41], the authors address the problem without transmission constraints using an MDP framework. A model-free Q-learning method is proposed to search for an optimal policy in cases where transition probabilities are unknown.

Lastly, in [42], a pull-based communication model is introduced, which assesses the freshness of status updates only when queries are made. The Age of Information at Query (QAoI) metric is employed as the cost function of an MDP problem. The optimal status updating policy is determined for a monitoring scenario where an edge node receives periodic queries from a server regarding the information of an energy harvesting sensor (with known periodicity).

5.3.3. Optimizing semantic metrics using CMDP

The optimization of information freshness under constraints has been examined in many studies. Among these, [49] minimizes average AoI by scheduling updates over an error-prone channel with transmission constraints, studying optimal policies under various feedback mechanisms. [50] addresses minimizing average AoI under transmission power constraints, transforming the CMDP problem into an unconstrained MDP through Lagrangian relaxation. In [51], the AoI in a status update system is minimized under an average energy cost constraint for both sampling and transmission. The stochastic problem is formulated as a CMDP and is transformed into an MDP using the Lagrangian method. [18] introduces AoII metric and solves the CMDP problem with a Lagrangian approach. [52] focuses on fresh data collection from power-constrained sensors in industrial IoT networks, optimizing average AoI with scheduling algorithms and Linear Programming (LP)-based optimization. The work [53] investigates the minimization of age in a two-hop relay system, subject to a constraint on the average number of forwarding actions at the relay, where the Lagrangian method transforms the CMDP into an MDP. [54] minimizes AoI in wireless networks with peak power-constrained base stations, using CMDP with strict and relaxed power constraints and proposing a truncated multi-user scheduling policy. [40] minimizes average AoI in resource-constrained IoT networks using a CMDP model and Lagrangian multipliers, offering an asymptotically optimal, low-complexity algorithm. [55] employs a similar Lagrangian approach to optimize the freshness and usefulness of information in a pull-based setup.

The works mentioned above primarily rely on formulating the constrained optimization problem using the CMDP framework and subsequently proceed to solve it through a Lagrangian approach, which is the most common method for obtaining the exact solution, in contrast to other approximate or learning-based approaches ([56], [57], [58], [59]).

5.3.4. Analysis of semantic metrics using Markov chains

The freshness of information has been modeled and analyzed using Markov chains in various studies related to queuing [60], [61] and real-time reconstruction [62] setups. Markov chain analysis can facilitate obtaining closed-form equations for stationary scheduling policies.

5.3.5. Analysis of semantic metrics in gossiping networks using SHS

By utilizing SHS analysis, several works [20], [63], [64], [65], [66], [67], [68] have focused on examining the growth or scaling of average Version AoI within push-based gossiping networks of varying sizes, topologies, and with different adversarial factors such as timestomping and jamming.

5.3.6. Summary of the SoA

In Table 1, a summary of the State of the Art is presented. As observed, the majority of previous works consider AoI as the performance metric in a push-based status update setup, though these setups remain largely unused in IoMT scenarios. In semantics-aware network management for IoMT networks, our aim is to propose appropriate semantic metrics and incorporate goal-oriented, semantics-aware information handling approaches that are well-suited to IoMT scenarios, with a focus on energy and cost efficiency in such networks.

Table 1 Summary of the SoA

Ref.	Formulation and Optimization Methodology	Utilized semantic metrics	IoMT scenario	System setup
[22]	MDP	State-Aware AoI	×	EH device monitoring a Markovian source / Push-based
[38]	MDP	AoI	×	EH device monitoring a source / Push-based
[39]	MDP + DRL	Weighted sum of AoI	×	EH device monitoring multiple sources / Push-based
[40]	POMDP	AoI	×	Cognitive radio system with EH secondary user / Push-based
[41]	MDP + RL	AoI	×	EH device monitoring a source over an error-prone channel / Push-based
[42]	MDP	AoI	×	EH device monitoring multiple heterogenous sources / Push-based
[43]	MDP + CMDP	On-demand AoI	×	A multi-user and multi-sensor IoT EH sensing network / Pull-based
[44]	MDP + Q-learning	AoI	×	A multi-user and multi-sensor IoT EH sensing network / Pull-based
[45]	MDP	QAoI	×	EH device monitoring a source with periodic queries from the receiver / Pull-based

[18]	CMDP	AoII	×	A status update system with transmission cost / Push-based
[49]	CMDP	AoI	×	A status update system with various feedback mechanisms / Push-based
[50]	CMDP	AoI	×	A status update system with transmission cost / Push-based
[51]	CMDP	AoI	×	A status update system under an average energy cost constraint for both sampling and transmission / Push-based
[52]	CMDP + LP	AoI	×	Power-constrained sensors in industrial IoT networks / Push-based
[53]	CMDP	AoI	×	A two-hop relay system under a constraint on the average number of forwarding actions at the relay / Push-based
[54]	CMDP	AoI	×	Wireless networks with peak power-constrained base stations / Push-based
[55]	CMDP	AoI combined with usefulness of data	×	A status update system with transmission cost / Pull-based
[60], [61]	Markov chains	AoI + PAoI	×	Status update queuing from multiple IoT devices to a single monitor / Push-based
[62]	Markov chains	AoI + Reconstruction Error	×	A status update system from a device to a remote actuator for reconstruction / Push-based
[20], [63], [64], [65], [66], [67], [68]	SHS	VAoI	×	Status updating in gossiping networks with various configurations / Push-based
[43]	MDP + Deep Q-learning	AoI	✓	A multi-user and multi-sensor IoMT network / Push-based
[44]	DRO	AoI	✓	An EH healthcare IoT device updates a base station / Push-based
[45]	PT-based Optimization	AoI	✓	Time-sensitive learning tasks in healthcare metaverses involving FL training.

5.4. Mathematical Tools: Optimization of Semantic Metrics and Information Handling Schemes

There are several approaches to the analytical modeling and optimization of semantic metrics in various status update setups [13], [69]. These approaches can lead to the development of information-handling policies aimed at enhancing energy and cost efficiency, either by minimizing the number of updates or by optimizing semantic objectives through a holistic, goal-oriented strategy that encompasses information generation, transmission, and utilization in the system.

5.4.1. Markov chains

Many status update systems, in which a sequence of events occurs stochastically, exhibit the Markov property. According to Markov property, the probability of the system's next state is determined solely by its current state. The scheduling of update transmissions in queuing scenarios serves as a relevant example of this approach, where a Markov chain can be employed to regulate packet storage or transmission within the queue.

For a given information handling policy, the steady-state probabilities in a Markov chain are determined by solving a system of linear equations derived from the transition matrix. These equations express the condition that, in the long run, the probability of being in any particular state remains constant, also known as the stationary distribution. The steady-state probabilities represent the long-term behavior of the system, and they are obtained by solving the balance equations, along with the normalization condition that the sum of all probabilities must equal one. Given the steady-state probabilities of the semantic metrics in the system, the performance of the information handling policy can be analyzed.

5.4.2. Markov Decision Process (MDP) and its variations

By incorporating the Markov property and integrating cost or reward functions into a status update system characterized by stochastic behavior, the Markov Decision Process (MDP) framework can be employed to determine the optimal sequence of actions (the optimal policy) aimed at minimizing costs or maximizing rewards within the system. This framework can be employed to schedule the generation/transmission of information updates.

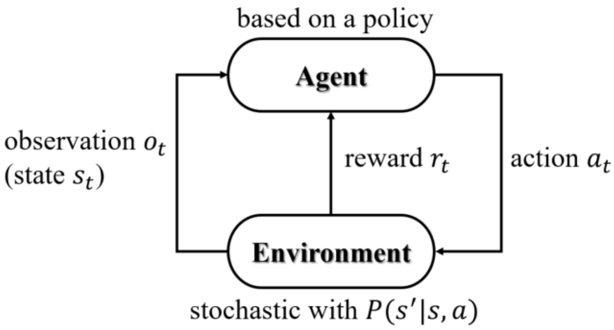


Figure 17 The Components of a Markov Decision Process [70]

An MDP comprises of a tuple $< S, P, A, C >$, where S is the state space, A is the set of actions, P is the state transition probability function, and C is the cost function of MDP. The cost function can be optimized over a finite or infinite horizon by taking optimal actions as the system evolves through states according to the state transition probabilities. This optimization can be conducted under system constraints, such as energy limitations, which leads to the Constrained Markov Decision Process (CMDP) problem. In other cases where the states of the system are not fully observable, a different framework known as the Partially Observable Markov Decision Process (POMDP) can be employed.

5.4.2.1. Reinforcement Learning

Several works have recently applied reinforcement learning-based algorithms to characterize semantics-aware approaches. Reinforcement Learning (RL) is a subfield of machine learning focused on how agents can take actions in an environment to maximize cumulative rewards (or minimize costs). RL is a framework used to address problems that can be modeled as incompletely known MDPs. Unlike supervised learning, where models learn from labeled data, reinforcement learning involves learning through interactions with the environment [70].

5.4.3. Stochastic Hybrid System (SHS)

Stochastic hybrid system provides a powerful framework for analyzing and designing complex systems that exhibit both continuous and discrete behaviors under uncertainty. By capturing the interplay between deterministic and stochastic elements, these models facilitate the development of robust and adaptive solutions in various status update systems [20], [71].

6. Big Data Analytics Leveraging XAI Models Towards Healthcare 4.0

6.1. Introduction

Artificial Intelligence (AI) has revolutionized industries by facilitating, in depth data analysis and streamlining decision making procedures. The fields of finance and transportation as well as healthcare have seen notable progress thanks to AIs ability to handle vast amounts of data and uncover valuable information. However following advancements in learning techniques AI models have evolved into "black boxes" masking their internal decision making mechanisms [72]. The lack of transparency in this situation is worrying and particularly critical in fields like healthcare where decisions carry weight. It's crucial to comprehend the reasoning, behind decisions made by AI to establish trust and ensure ethical standards are met.

Explainable AI (also known as XAI) has become a focus of research, with the goal of clarifying AI models by revealing their decision making processes in a way that's understandable to humans [73]. By shedding light on how AI models reach conclusions XAI builds trust and simplifies the incorporation of AI systems, into decision making processes. This section delves into the realm of XAI by examining its concepts significance and approaches utilized. A detailed overview is offered on the existing intelligence (XAI) solutions, in the healthcare sector which covers models utilized and their applications along with the frameworks that support them. The discussion also delves into privacy protection methods for handling medical information by tackling the challenges involved and suggesting areas for future research.

6.2. Explainable AI

6.2.1. What is XAI

Explainable AI (XAI) refers to a set of methods and techniques designed to make the decision-making processes of AI models transparent and understandable to humans [74]. Traditional AI models, particularly complex ones like deep neural networks, can provide accurate predictions but often lack interpretability, making it difficult for users to comprehend how these models arrive at specific outcomes.

XAIs core purpose is to close the distance by unveiling the mechanics of AI systems in a way that resonates with humans and fosters trust and utilization of AI technologies, among stakeholders. In a diagnosis context, as an example an AI system might forecast the likelihood of a disease where XAI would clarify this forecast by pointing out the particular symptoms test results or imaging characteristics that influenced the prediction.

6.2.2. Importance of Explainability

The importance of explainability in AI systems is multifaceted:

- **Trust and Adoption**: Users are more likely to trust and adopt AI systems when they can understand the reasoning behind decisions. This is particularly critical in high-stakes domains where decisions have significant consequences [75].

- **Accountability and Compliance**: Regulatory frameworks, such as the General Data Protection Regulation (GDPR), require organizations to provide explanations for automated decisions that significantly affect individuals [76]. XAI helps organizations meet these legal obligations.

- **Ethical Considerations**: Explainability ensures that AI systems operate fairly and do not perpetuate biases or discrimination. It allows for the detection and mitigation of unintended biases in AI models [77].

- **Improved Decision-Making**: By understanding the factors influencing AI decisions, stakeholders can make better-informed decisions, combining human expertise with machine insights [78].

- **Debugging and Model Improvement**: Explanations can help developers identify errors or weaknesses in AI models, leading to enhancements in performance and robustness [79].

In essence, explainability is a cornerstone for the responsible and effective deployment of AI technologies across various sectors.

6.2.3. Evaluating Explainability

Evaluating the effectiveness of XAI methods is crucial to ensure that explanations are meaningful and serve their intended purpose. Several criteria have been proposed [80], [79], [81]:

- **Interpretability**: Refers to how easily a human can understand the explanation provided by the AI model. An interpretable explanation should be clear, concise, and free of unnecessary complexity.

- **Fidelity**: Measures how accurately the explanation reflects the AI model's internal decision-making process. High-fidelity explanations ensure that the representation is truthful to the model's operations.

- **Consistency**: Assesses whether similar inputs lead to similar explanations. Consistent explanations enhance trust, as users can anticipate how the model will behave.

- **Comprehensiveness**: An explanation should cover all relevant factors influencing the decision, providing a holistic understanding.

- **Computational Efficiency**: Considers the resources required to generate explanations. Efficient methods are essential for real-time applications where delays are unacceptable.

- **User Satisfaction**: The usefulness of an explanation is ultimately determined by the end-user. User satisfaction measures how well the explanation meets the user's needs and expectations.

By employing these evaluation metrics, developers and researchers can assess the quality of XAI methods and select the most appropriate techniques for their specific applications.

6.2.4. Models and Methods in XAI

The most known methods applied after model training in order to explain complex models are presented next. Each method offers unique advantages, and the choice depends on factors such as the complexity of the model, the type of data, and the needs of the users.

- **LIME (Local Interpretable Model-Agnostic Explanations)**: LIME explains individual predictions by approximating the model locally with a simpler, interpretable model. It perturbs input data to see how changes affect the output. *Example*: Explaining why a text classification model labeled an email as spam by highlighting significant words.

- **SHAP (SHapley Additive exPlanations)**: SHAP assigns each feature an importance value for a particular prediction based on cooperative game theory [82]. It provides consistent and locally accurate explanations. *Example*: Determining how various financial indicators contribute to a stock price prediction.

- **Grad-CAM (Gradient-weighted Class Activation Mapping)**: Grad-CAM generates visual explanations for convolutional neural networks by highlighting important regions in input images [83]. *Example*: In medical imaging, highlighting areas in an MRI scan that influenced a tumor detection.

- **Counterfactual Explanations**: These explanations describe how minimal changes to the input can alter the prediction, offering actionable insights [84]. *Example*: Indicating how a patient might reduce their risk of diabetes by adjusting certain lifestyle factors.

- **Feature Attribution Methods**: Techniques like Integrated Gradients and DeepLIFT attribute the prediction to input features, helping understand feature importance [85], [86]. *Example*: Identifying which genes are most influential in predicting a genetic disorder.

6.2.5. Legal and Ethical Considerations

Legal Considerations

Regulations such as the General Data Protection Regulation (GDPR) have significant implications for AI applications:

- **Right to Explanation**: While the GDPR does not explicitly grant a "right to explanation," it requires that organizations provide meaningful information about the logic involved in automated decisions [76].

- **Data Protection**: The GDPR mandates strict data protection measures, including data minimization, purpose limitation, and security requirements.

- **Accountability**: Organizations must demonstrate compliance with GDPR principles, necessitating transparency in AI systems.

Ethical Considerations

Ethical AI involves principles ensuring that AI systems are developed and used responsibly [87]:

- **Fairness**: AI models should not exhibit bias or discrimination. Explainability helps identify and correct biases.

- **Transparency**: Users should understand when and how AI is being used and have access to explanations of decisions.

- **Accountability**: There should be mechanisms to hold AI systems and their creators accountable for their actions.

- **Beneficence**: AI should contribute positively to society, enhancing well-being.

- **Privacy**: Personal data must be protected, respecting individuals' rights.

In healthcare, these considerations are paramount due to the potential impact on patient care and outcomes. XAI supports ethical practices by providing transparency and facilitating informed consent.

6.3. XAI in Healthcare

6.3.1. Importance of XAI in Healthcare

The decisions regarding healthcare can have impacts, on ones life and well being; therefore trust and openness are elements in this field. Bringing AI technology into the healthcare sector brings about the potential for advancements in accuracy and personalized medical care well as predictive data analysis [88]. Nevertheless the intricate nature of AI models may pose challenges to their acceptance, among both healthcare providers and patients.

Key Reasons for XAI in Healthcare:

- **Clinical Trust**: Clinicians need to understand AI recommendations to trust and effectively use them [89]. Explainable models enable clinicians to verify AI outputs against their expertise.

- **Patient Safety**: Transparent AI systems help identify errors or unintended behaviors, enhancing patient safety [78].

- **Regulatory Compliance**: Healthcare is subject to stringent regulations that require accountability and transparency in decision-making processes [90].

- **Ethical Practice**: Explainable AI supports ethical obligations to provide clear information to patients, aiding in informed consent and shared decision-making [91].

- **Education and Training**: XAI can serve as a tool for educating clinicians about complex patterns and relationships in medical data.

6.3.2. Models Used in Healthcare

Interpretable Models

- **Decision Trees and Random Forests**: Used for their simplicity and ability to handle complex datasets. Random forests, while more complex, can provide feature importance measures [92].

- **Generalized Additive Models (GAMs)**: Offer flexibility in modeling non-linear relationships while remaining interpretable [93].

Deep Learning Models with Explainability Techniques

Convolutional Neural Networks (CNNs): Essential in analyzing medical images. Techniques like Grad-CAM make CNNs more interpretable by highlighting relevant image regions [94].

Attention Mechanisms: Used in models processing sequential data, such as patient records, to focus on critical information [95].

Autoencoders and Variational Autoencoders: Used for anomaly detection in medical data, with latent spaces that can sometimes be interpreted [96].

6.3.3. Applications and Solutions

Diagnostic Support

- **Medical Imaging Analysis**: AI models assist in diagnosing diseases from imaging data. Explainable models help clinicians understand AI findings [88].

- **Pathology**: AI aids in detecting cancerous cells in histopathology slides. Explainable models enhance pathologists' confidence in AI assistance [97].

Treatment Recommendations

- **Personalized Medicine**: AI models suggest treatments tailored to individual patients. Explainability ensures clinicians understand the rationale behind recommendations [98].

- **Drug Interaction Warnings**: AI predicts potential adverse interactions. Explainable systems help healthcare providers make informed decisions [99].

Risk Prediction

- **Predictive Analytics**: AI models estimate the risk of future health events. Explanations help clinicians and patients understand risk factors [100].

- **Early Warning Systems**: AI monitors patient data to predict adverse events. Explainable models allow for timely interventions [101].

6.3.4. Tools Supporting XAI in Healthcare

The following tools facilitate the development and deployment of explainable AI solutions in healthcare, supporting developers in creating models that meet the needs of clinicians and patients.

- **IBM AI Explainability 360**: Provides a suite of algorithms to enhance the interpretability of AI models [102].

- **Microsoft InterpretML**: Offers tools for creating interpretable models and explaining black-box systems [103].

- **Captum**: An open-source library for model interpretability in PyTorch, supporting a variety of methods [104].

- **SHAP Library**: Implements SHAP values for a range of models, aiding in feature attribution explanations [82].

6.4. Privacy-Preserving XAI for Healthcare

6.4.1. Importance of Privacy in Healthcare AI

Health data is extremely delicate. Holds personal and medical details that need to be safeguarded to uphold patient confidence and adhere to legal rules [105]. In healthcare AI applications privacy worries revolve around data protection measures well as meeting the requirements of laws like GDPR regulations, for Health Insurance Portability and Accountability Act compliance is crucial when incorporating explainable AI (XAI) to avoid unintentionally disclosing sensitive data.

6.4.2. Privacy-Preserving Techniques

Federated Learning

Federated learning allows multiple institutions to collaboratively train a shared model without exchanging raw data [106]. Each institution trains the model locally and shares only model updates, preserving data privacy. This approach enhances privacy, leverages diverse datasets, and promotes collaboration among institutions. However, challenges include managing communication overhead and ensuring model convergence across heterogeneous data sources.

Differential Privacy

Differential privacy introduces statistical noise to data or outputs to prevent the identification of individuals [107]. By providing mathematical guarantees of privacy, it aids compliance with regulations. The main challenge lies in balancing the trade-off between privacy and model utility, as excessive noise can degrade performance.

Secure Multi-Party Computation (SMPC)

SMPC enables computation on encrypted data from multiple parties without revealing the data to each other [108]. This technique allows collaborative computation without compromising data privacy. The challenges associated with SMPC include high computational cost and complexity, which can hinder scalability in practical applications.

6.4.3. Challenges and Future Directions

Incorporating privacy protection, in the field of healthcare XAI comes with hurdles that must be overcome to unlock its capabilities. One key obstacle lies in finding the balance between privacy and clarity. Privacy safeguards could restrict the depth and value of explanations, making them less enlightening for professionals. Additionally, the computational burden is another issue to consider as privacy preservation methods may demand resources impacting the scalability and effectiveness of AI systems.

Collaborative methods such as federated learning face challenges due to the diversity of data among organizations and institutions. Differences in data formats, quality standards and collection processes may affect how models perform and converge. Moreover, dealing with the web of demands in different areas contributes to the complexity of implementation.

In the future researchers are looking into creating techniques that protect privacy while still ensuring transparency and effectiveness are not greatly affected. This entails coming up with methods that also deliver results. Setting up guidelines and procedures for maintaining privacy in healthcare using Explainable Artificial Intelligence (XAI), could make it easier for systems to work together seamlessly.

Effective collaboration across disciplines is essential in tackling these issues by uniting experts in technology alongside healthcare professionals and policymakers to work together cohesively. Educational initiatives and training courses play a role in providing stakeholders with insights into privacy protection methods and their consequences to encourage informed choices. Introducing automated tools for compliance can further support the adherence of AI systems to applicable laws and regulations while lessening the challenges for organizations in navigating frameworks.

Understanding AI is crucial for the efficient use of AI in healthcare settings. Its transparency and comprehensible decision-making help build trust and accountability while ensuring compliance with ethical standards. XAI enables healthcare providers to make informed decisions that promote safety and uphold ethical standards in caring for patients.

Nevertheless challenges continue to arise when trying to strike a balance, between the effectiveness of models and the ability to explain them while also safeguard data privacy.

Progress in this area will help make AI widely used in healthcare settings and enhance results and medical understanding while maintaining ethical standards and responsibility at the highest level.

7. Conclusions

In this deliverable, the main enablers of the AI-driven E2E Healthcare service were introduced, highlighting the key concepts, literature review, and methodological tools that can be used to enhance healthcare services. We provided an overview of the challenges: i) AI-enabled E2E slicing and zero-touch orchestration, ii) blockchain-backed incentive engineering mechanisms, iii) semantics-aware network management, and iv) big data analytics leveraging XAI. We presented relevant concepts and technological frameworks, emphasizing the importance of incorporating and developing methodological tools to address existing gaps that are essential for achieving secure, energy-efficient, and cost-effective healthcare services. These enablers are currently underutilized in healthcare systems and IoMT networks, where we aim to incorporate them in ELIXIRION's WP3.

8. REFERENCES

[1] D. Xenakis, A. Tsiota, C.-T. Koulis, C. Xenakis, and N. Passas, “Contract-Less Mobile Data Access Beyond 5G: Fully-Decentralized, High-Throughput and Anonymous Asset Trading Over the Blockchain,” *IEEE Access*, vol. 9, pp. 73963–74016, 2021, doi: 10.1109/ACCESS.2021.3079625.
[2] D. Xenakis, I. Zarifis, P. Petrogiannakis, A. Tsiota, and N. Passas, “Blockchain-driven mobile data access towards fully decentralized mobile video trading in 5G networks,” in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–7. doi: 10.1109/ICC40277.2020.9149263.
[3] A. Musamih *et al.*, “A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain,” *IEEE Access*, vol. 9, pp. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.
[4] S. Dhingra, R. Raut, K. Naik, and K. Muduli, “Blockchain Technology Applications in Healthcare Supply Chains—A Review,” *IEEE Access*, vol. 12, pp. 11230–11257, 2024, doi: 10.1109/ACCESS.2023.3348813.
[5] P. Zhu, J. Hu, Y. Zhang, and X. Li, “A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability,” *IEEE Access*, vol. 8, pp. 184256–184272, 2020, doi: 10.1109/ACCESS.2020.3029196.
[6] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, “A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System,” *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021, doi: 10.1109/JIOT.2020.3032997.
[7] U. Zukaib, X. Cui, M. Hassan, S. Harris, H. J. Hadi, and C. Zheng, “Blockchain and Machine Learning in EHR Security: A Systematic Review,” *IEEE Access*, vol. 11, pp. 130230–130256, 2023, doi: 10.1109/ACCESS.2023.3333229.
[8] P. P. Ray, D. Dash, K. Salah, and N. Kumar, “Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases,” *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.
[9] M. A. Abd-Elmagid, N. Pappas, and H. S. Dhillon, “On the role of age of information in the Internet of Things,” *IEEE Commun. Mag.*, vol. 57, no. 12, pp. 72–77, 2019.
[10] M. Kountouris and N. Pappas, “Semantics-empowered communication for networked intelligent systems,” *IEEE Commun Mag.*, vol. 59, no. 6, 2021.
[11] E. Uysal and others, “Semantic communications in networked systems: A data significance perspective,” *IEEE Netw.*, vol. 36, no. 4, 2022.
[12] V. S. Chakravarthi, *Internet of Things and M2M communication technologies*. Springer, 2021.
[13] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, “Age of information: An introduction and survey,” *IEEE J. Sel. Areas Commun*, vol. 39, no. 5, 2021.
[14] E. Modiano, D. Shah, and G. Zussman, “Maximizing throughput in wireless networks via gossiping,” *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 34, no. 1, pp. 27–38, 2006.
[15] D. Gunduz, K. Stamatiou, N. Michelusi, and M. Zorzi, “Designing intelligent energy harvesting communication systems,” *IEEE Commun. Mag.*, vol. 52, no. 1, pp. 210–216, 2014.
[16] S. Kaul, R. Yates, and M. Gruteser, “Real-time status: How often should one update?,” in *IEEE INFOCOM*, 2012, pp. 2731–2735.
[17] X. Zheng, S. Zhou, Z. Jiang, and Z. Niu, “Closed-form analysis of non-linear age of information in status updates with an energy harvesting transmitter,” *IEEE Trans Wirel. Commun*, vol. 18, no. 8, 2019.
[18] A. Maatouk, S. Kriouile, M. Assaad, and A. Ephremides, “The age of incorrect information: A new performance metric for status updates,” *IEEEACM Trans. Netw.*, vol. 28, no. 5, pp. 2215–2228, 2020.
[19] F. Chiariotti *et al.*, “Query age of information: Freshness in pull-based communication,” *IEEE Trans Commun*, vol. 70, no. 3, 2022.

[20] R. D. Yates, "The age of gossip in networks," in *IEEE International Symposium on Information Theory (ISIT)*, 2021.
[21] E. Delfani, G. J. Stamatakis, and N. Pappas, "State-Aware Timeliness in Energy Harvesting IoT Systems Monitoring a Markovian Source," *ArXiv Prepr. ArXiv240503628*, 2024.
[22] G. Stamatakis, N. Pappas, and A. Traganitis, "Control of status updates for energy harvesting devices that monitor processes with alarms," in *IEEE Globecom Workshops*, 2019.
[23] B. T. Bacinoglu, E. T. Ceran, and E. Uysal-Biyikoglu, "Age of information under energy replenishment constraints," in *Information Theory and Applications Workshop (ITA)*, 2015.
[24] R. D. Yates, "Lazy is timely: Status updates by an energy harvesting source," in *IEEE International Symposium on Information Theory (ISIT)*, 2015.
[25] B. T. Bacinoglu and E. Uysal-Biyikoglu, "Scheduling status updates to minimize age of information with an energy harvesting sensor," in *IEEE international symposium on information theory (ISIT)*, 2017.
[26] Y. Sun, E. Uysal-Biyikoglu, R. D. Yates, C. E. Koksal, and N. B. Shroff, "Update or wait: How to keep your data fresh," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7492–7508, 2017.
[27] B. T. Bacinoglu, Y. Sun, E. Uysal–Bivikoglu, and V. Mutlu, "Achieving the age-energy tradeoff with a finite-battery energy harvesting source," in *IEEE International Symposium on Information Theory (ISIT)*, 2018.
[28] A. Arafa, J. Yang, and S. Ulukus, "Age-minimal online policies for energy harvesting sensors with random battery recharges," in *IEEE international conference on communications (ICC)*, 2018.
[29] S. Farazi, A. G. Klein, and D. R. Brown, "Average age of information for status update systems with an energy harvesting server," in *IEEE INFOCOM Workshops*, 2018.
[30] S. Feng and J. Yang, "Minimizing age of information for an energy harvesting source with updating failures," in *IEEE International Symposium on Information Theory (ISIT)*, 2018.
[31] Z. Chen, N. Pappas, E. Björnson, and E. G. Larsson, "Age of information in a multiple access channel with heterogeneous traffic and an energy harvesting node," in *IEEE INFOCOM Workshops*, 2019.
[32] S. Feng and J. Yang, "Age of information minimization for an energy harvesting source with updating erasures: Without and with feedback," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5091–5105, 2021.
[33] A. Arafa, J. Yang, S. Ulukus, and H. V. Poor, "Age-minimal transmission for energy harvesting sensors with finite batteries: Online policies," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 534–556, 2019.
[34] B. T. Bacinoglu, Y. Sun, E. Uysal, and V. Mutlu, "Optimal status updating with a finite-battery energy harvesting source," *J. Commun. Netw.*, vol. 21, no. 3, pp. 280–294, 2019.
[35] M. A. Abd-Elmagid, H. S. Dhillon, and N. Pappas, "Online age-minimal sampling policy for RF-powered IoT networks," in *IEEE Global Communications Conference (GLOBECOM)*, 2019.
[36] M. A. Abd-Elmagid, H. S. Dhillon, and N. Pappas, "A reinforcement learning framework for optimizing age of information in RF-powered communication systems," *IEEE Trans. Commun.*, vol. 68, no. 8, 2020.
[37] S. Leng and A. Yener, "Minimizing age of information for an energy harvesting cognitive radio," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019.
[38] E. T. Ceran, D. Gündüz, and A. György, "Reinforcement learning to minimize age of information with an energy harvesting sensor with HARQ and sensing cost," in *IEEE INFOCOM Workshops*, 2019, pp. 656–661.
[39] E. Gindullina, L. Badia, and D. Gündüz, "Age-of-information with information source diversity in an energy harvesting system," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1529–1540, 2021.
[40] M. Hatami, M. Leinonen, Z. Chen, N. Pappas, and M. Codreanu, "On-demand AoI minimization in resource-constrained cache-enabled IoT networks with energy harvesting sensors," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7446–7463, 2022.

[41] M. Hatami, M. Leinonen, and M. Codreanu, "AoI minimization in status update control with energy harvesting sensors," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8335–8351, 2021.

[42] J. Holm *et al.*, "Freshness on demand: Optimizing age of information for the query process," in *IEEE International Conference on Communications*, 2021.

[43] K. Wei, L. Zhang, and S. Wang, "Intelligent channel allocation for age of information optimization in internet of medical things," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, p. 6645803, 2021.

[44] Z. Ling, F. Hu, H. Zhang, and Z. Han, "Age-of-information minimization in healthcare IoT using distributionally robust optimization," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16154–16167, 2022.

[45] J. Kang *et al.*, "Blockchain-empowered federated learning for healthcare metaverses: User-centric incentive mechanism with optimal data freshness," *IEEE Trans. Cogn. Commun. Netw.*, 2023.

[46] A. Jaiswal and A. Chattopadhyay, "Minimization of age-of-information in remote sensing with energy harvesting," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 3249–3254.

[47] L. Crosara and L. Badia, "A stochastic model for age-of-information efficiency in ARQ systems with energy harvesting," in *European Wireless 2021; 26th European Wireless Conference*, 2021, pp. 1–6.

[48] P. Rafiee, Z. Ju, and M. Doroslovački, "Adaptive on/off scheduling to minimize age of information in an energy harvesting receiver," *IEEE Sens. J.*, 2023.

[49] E. T. Ceran, D. Gündüz, and A. György, "Average age of information with hybrid ARQ under a resource constraint," *IEEE Trans Wirel. Commun.*, vol. 18, no. 3, 2019.

[50] Q. Wang, H. Chen, Y. Li, Z. Pang, and B. Vucetic, "Minimizing age of information for real-time monitoring in resource-constrained industrial IoT networks," in *IEEE 17th INDIN*, 2019.

[51] B. Zhou and W. Saad, "Joint status sampling and updating for minimizing age of information in the Internet of Things," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7468–7482, 2019.

[52] H. Tang, J. Wang, L. Song, and J. Song, "Minimizing age of information with power constraints: Multi-user opportunistic scheduling in multi-state time-varying channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, 2020.

[53] Y. Gu, Q. Wang, H. Chen, Y. Li, and B. Vucetic, "Optimizing information freshness in two-hop status update systems under a resource constraint," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1380–1392, 2021.

[54] G. Chen, Y. Chen, J. Wang, and J. Song, "Minimizing Age of Information in Downlink Wireless Networks With Time-Varying Channels and Peak Power Constraint," *IEEE Trans Veh. Technol.*, 2023.

[55] P. Agheli, N. Pappas, P. Popovski, and M. Kountouris, "Effective Communication: When to Pull Updates?," in *IEEE ICC*, 2024.

[56] C. Tessler, D. J. Mankowitz, and S. Mannor, "Reward Constrained Policy Optimization," in *International Conference on Learning Representations*, 2018.

[57] J. Achiam, D. Held, A. Tamar, and P. Abbeel, "Constrained policy optimization," in *International conference on machine learning*, 2017.

[58] G. Dalal, K. Dvijotham, M. Vecerik, T. Hester, C. Paduraru, and Y. Tassa, "Safe exploration in continuous action spaces," *ArXiv Prepr. ArXiv180108757*, 2018.

[59] S. Levine and V. Koltun, "Guided policy search," in *International conference on machine learning*, 2013.

[60] Q. Abbas, S. A. Hassan, H. Pervaiz, and Q. Ni, "A Markovian Model for the Analysis of Age of Information in IoT Networks," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 7, pp. 1596–1600, Jul. 2021, doi: 10.1109/LWC.2021.3075160.

[61] N. Akar and O. Dogan, "Discrete-Time Queueing Model of Age of Information With Multiple Information Sources," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14531–14542, Oct. 2021, doi: 10.1109/JIOT.2021.3053768.

[62] N. Pappas and M. Kountouris, "Goal-Oriented Communication For Real-Time Tracking In Autonomous Systems," in *2021 IEEE International Conference on Autonomous Systems (ICAS)*, Montreal, QC, Canada: IEEE, Aug. 2021, pp. 1–5. doi: 10.1109/ICAS49788.2021.9551200.
[63] B. Buyukates, M. Bastopcu, and S. Ulukus, "Version Age of Information in Clustered Gossip Networks," *IEEE J. Sel. Areas Inf. Theory*, vol. 3, no. 1, 2022.
[64] P. Kaswan and S. Ulukus, "Timely gossiping with file slicing and network coding," in *IEEE International Symposium on Information Theory (ISIT)*, 2022.
[65] P. Kaswan and S. Ulukus, "Susceptibility of Age of Gossip to Timestomping," in *IEEE Information Theory Workshop (ITW)*, 2022, pp. 398–403. doi: 10.1109/ITW54588.2022.9965757.
[66] P. Mitra and S. Ulukus, "ASUMAN: Age sense updating multiple access in networks," in *58th Annual Allerton Conference on Communication, Control, and Computing*, 2022.
[67] P. Kaswan and S. Ulukus, "Age of Gossip in Ring Networks in the Presence of Jamming Attacks," in *56th Asilomar Conference on Signals, Systems, and Computers*, 2022, pp. 1055–1059. doi: 10.1109/IEEECONF56349.2022.10051981.
[68] P. Mitra and S. Ulukus, "Age-Aware Gossiping in Network Topologies," *ArXiv Prepr. ArXiv230403249*, 2023.
[69] Q. Abbas, S. A. Hassan, H. K. Qureshi, K. Dev, and H. Jung, "A comprehensive survey on age of information in massive IoT networks," *Comput. Commun*, vol. 197, 2023.
[70] X. Xiang and S. Foo, "Recent advances in deep reinforcement learning applications for solving partially observable markov decision processes (pomdp) problems: Part 1—fundamentals and applications in games, robotics and natural language processing," *Mach. Learn. Knowl. Extr.*, vol. 3, no. 3, pp. 554–581, 2021.
[71] J. P. Hespanha, "Modelling and analysis of stochastic hybrid systems," *IEE Proc.-Control Theory Appl.*, vol. 153, no. 5, pp. 520–535, 2006.
[72] W. Samek, T. Wiegand, and K.-R. Müller, "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models," *ArXiv Prepr. ArXiv170808296*, 2017.
[73] A. Adadi and M. Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.
[74] D. Gunning and others, "XAI—Explainable artificial intelligence," *Sci. Robot.*, vol. 4, no. 37, p. eaay7120, 2019.
[75] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," *Nat. Mach. Intell.*, vol. 1, no. 5, pp. 206–215, 2019.
[76] B. Goodman and S. Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation,'" *AI Mag.*, vol. 38, no. 3, pp. 50–57, 2017.
[77] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nat. Mach. Intell.*, vol. 1, no. 9, pp. 389–399, 2019.
[78] A. Holzinger and others, "Towards multi-modal causability with Graph Neural Networks enabling information fusion for explainable AI," *Inf. Fusion*, vol. 79, pp. 259–278, 2022.
[79] P. Linardatos, V. Papastefanopoulos, and S. Kotsiantis, "Explainable AI: A review of machine learning interpretability methods," *Entropy*, vol. 23, no. 1, p. 18, 2021.
[80] C. Molnar, *Interpretable Machine Learning*, 2nd ed. 2022.
[81] U. Bhatt and others, "Explainable machine learning in deployment," in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, pp. 648–657.
[82] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Advances in Neural Information Processing Systems*, 2017, pp. 4765–4774.
[83] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-CAM: Visual explanations from deep networks via gradient-based localization," *Int. J. Comput. Vis.*, vol. 128, no. 2, pp. 336–359, 2019.

[84] S. Wachter, B. Mittelstadt, and C. Russell, "Counterfactual explanations without opening the black box: Automated decisions and the GDPR," *Harv. J. Law Technol.*, vol. 31, no. 2, pp. 841–887, 2017.
[85] M. Sundararajan, A. Taly, and Q. Yan, "Axiomatic attribution for deep networks," in *Proceedings of the 34th International Conference on Machine Learning*, 2017, pp. 3319–3328.
[86] A. Shrikumar, P. Greenside, and A. Kundaje, "Learning important features through propagating activation differences," in *Proceedings of the 34th International Conference on Machine Learning*, 2017, pp. 3145–3153.
[87] L. Floridi and others, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations," *Minds Mach.*, vol. 28, no. 4, pp. 689–707, 2018.
[88] E. J. Topol, "High-performance medicine: The convergence of human and artificial intelligence," *Nat. Med.*, vol. 25, no. 1, pp. 44–56, 2019.
[89] M. A. Ahmad, A. Teredesai, and C. Eckert, "Interpretable machine learning in healthcare," in *Proceedings of the 2018 ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*, 2018, pp. 559–560.
[90] M. D. McCradden, E. A. Stephenson, and J. A. Anderson, "Clinical research under COVID-19: The hidden costs of a global crisis," *Can. J. Anesth.*, vol. 67, no. 9, pp. 1355–1358, 2020.
[91] T. Panch, H. Mattie, and R. Atun, "Artificial intelligence and algorithmic bias: Implications for health systems," *J. Glob. Health*, vol. 9, no. 2, p. 010318, 2019.
[92] S. M. Lundberg and others, "From local explanations to global understanding with explainable AI for trees," *Nat. Mach. Intell.*, vol. 2, no. 1, pp. 56–67, 2020.
[93] T. Hastie and R. Tibshirani, "Generalized additive models," *Stat. Sci.*, vol. 1, no. 3, pp. 297–310, 2017.
[94] A. Esteva and others, "A guide to deep learning in healthcare," *Nat. Med.*, vol. 25, no. 1, pp. 24–29, 2019.
[95] Y. Xu *et al.*, "Leveraging auxiliary tasks with attention for medical code assignment," *J. Am. Med. Inform. Assoc.*, vol. 27, no. 8, pp. 1259–1266, 2020.
[96] T. Chen and others, "Unsupervised anomaly detection for x-ray images using deep learning," *IEEE Access*, vol. 9, pp. 119437–119448, 2021.
[97] G. Campanella and others, "Clinical-grade computational pathology using weakly supervised deep learning on whole slide images," *Nat. Med.*, vol. 25, no. 8, pp. 1301–1309, 2019.
[98] F. Xie, X. Ma, T. Sun, H. Zhou, J. You, and C. Zhang, "Deep learning in bioinformatics: Introduction, application, and perspective in the big data era," *Methods*, vol. 166, pp. 4–21, 2020.
[99] W. Zhang, W. Li, X. Li, Y. Liu, J. Jin, and L. Wang, "Explainable AI for pharmacovigilance: Unveiling adverse drug reactions through interpretable deep learning models," *J. Biomed. Inform.*, vol. 117, p. 103761, 2021.
[100] A. Rajkomar *et al.*, "Scalable and accurate deep learning with electronic health records," *NPJ Digit. Med.*, vol. 1, no. 1, p. 18, 2018.
[101] L. Wang, X. Hu, Y. Li, H. Wang, N. Zeng, and X. Liu, "Explainable AI in wearable devices for health monitoring: A survey," *IEEE Trans. Ind. Inform.*, vol. 18, no. 2, pp. 1350–1360, 2022.
[102] V. Arya and others, "AI explainability 360: Impact and design," *IBM J. Res. Dev.*, vol. 64, no. 1/2, p. 3:1-3:15, 2020.
[103] H. Nori, S. Jenkins, P. Koch, and R. Caruana, "InterpretML: A unified framework for machine learning interpretability," *ArXiv Prepr. ArXiv190909223*, 2019.
[104] N. Kokhlikyan and others, "Captum: A unified and generic model interpretability library for PyTorch," *ArXiv Prepr. ArXiv200907896*, 2020.
[105] B. K. Beaulieu-Jones and C. S. Greene, "Privacy-preserving data sharing for machine learning in decentralized clinical environments," *NPJ Digit. Med.*, vol. 2, no. 1, p. 62, 2019.
[106] N. Rieke *et al.*, "The future of digital health with federated learning," *NPJ Digit. Med.*, vol. 3, no. 1, p. 119, 2020.

[107] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends® Theor. Comput. Sci.*, vol. 9, no. 3–4, pp. 211–407, 2014.
[108] R. Agrawal and others, "Privacy-preserving data analysis," *Commun. ACM*, vol. 64, no. 3, pp. 86–96, 2021.