Review Article

BIOMEDICAL
Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2024.54.008608

Health-IT Reference Architecture – The Internet of Medical Things Architecture for Healthcare Use Cases

Venkatesh Upadrista*

Venkatesh Upadrista, Department of Computing, Glasgow Caledonian University, Scotland

***Corresponding author:** Venkatesh Upadrista, Department of Computing, Glasgow Caledonian University, Glasgow G4 0BA, Scotland

ARTICLE INFO

Received: January 14, 2024

Published: February 01, 2024

Citation: Venkatesh Upadrista. Health-IT Reference Architecture – The Internet of Medical Things Architecture for Healthcare Use Cases. Biomed J Sci & Tech Res 54(5)-2024. BJSTR. MS.ID.008608.

ABSTRACT

This paper explores the Health-IT Reference Architecture which offers comprehensive framework with interconnected components that facilitates the implementation of IoMT solutions for diverse healthcare use cases. Notably, it ensures scalability and robust security through blockchain integration, aligning with global data privacy and security standards. The success of this reference architecture is exemplified in critical scenarios such as preventive care for life-threatening diseases, including cancers, dementia, and advanced lung, heart, kidney, and liver diseases. The Royal Brompton and Harefield hospitals in London have effectively deployed this Health-IT Reference Architecture, leading to the early detection of cancers in 70% of patients at Stage 1, a significant advancement in healthcare outcomes. Additionally, the paper discusses the challenges faced by enterprises in IoMT implementation and provides insights into overcoming these challenges using the Health-IT Reference Architecture. It explores principles guiding the selection of health devices, Smart IoMT Gateways, and IoMT Cloud Platforms tailored to specific use cases, thus enabling effective mitigation of challenges. In collaboration with Cambridge University in the United Kingdom, this paper presents a cutting-edge IoMT architecture for healthcare systems, showcasing the potential of technology in revolutionizing healthcare delivery and patient outcomes.

Keywords: Internet of Medical Things; Reference Architecture; Healthcare; Blockchain; Machine Learning; Internet of Medical Things

Abbreviations: IDC: International Data Corporation; CAGR: Compound Annual Growth Rate; IioMT: Industrial Internet of Medical Things; AI: Artificial Intelligence; DLT: Distributed Ledger Technology

Introduction

The rapid expansion of health-related devices connected to the Internet, collectively referred to as the Internet of Medical Things, is on a trajectory of significant growth. According to projections by the International Data Corporation (IDC), it is estimated that by 2025, approximately 41.6 billion connected IoMT health devices will be responsible for the generation of 79.4 zettabytes of data [1]. This substantial increase in connected devices is associated with a compound annual growth rate (CAGR) of 28.7% in data creation from the year 2018 to 2025. As it evolves, the IoMT ecosystem is becoming an increasingly crucial medium for the exchange of information among devices, individuals, and processes. This emphasizes the role of data as a central element for value creation across various sectors. As the market matures, IoMT is progressively forming the infrastructure that facilitates information exchange involving ‘things’, people, and processes. Here, data stands out as the common thread, being captured, processed, and utilized across both near and distant network edges to generate value for industries, governmental bodies, and individual lives. Given the range of technologies that underpin IoMT, a one-size-fits-all architecture is unfeasible. For example, the application of IoMT in manufacturing, often termed as Industrial Internet of Medical Things (IIoMT), is markedly different from its use in the healthcare sector. IoMT encompasses a broad spectrum of both internet-enabled and non-internet-enabled health devices and computing systems.

Therefore, the architecture of IoMT needs to be flexible, incorporating open protocols to cater to a variety of network applications and use cases. The necessity for middleware is pronounced, as it is essential for ensuring scalability, security, and semantic represen-

DOI: 10.26717/BJSTR.2024.54.008608

tation, thereby facilitating the integration of diverse health devices. In light of these considerations, this paper introduces the Health-IT Reference Architecture. This architecture is an abstract framework that consists of interconnected components, designed to function as a domain-specific ontology. It empowers enterprises in the effective implementation of IoMT solutions. Due to its abstract nature, the reference architecture is versatile, capable of accommodating a range of IoMT architectures that are based on standardized components. This model not only streamlines the integration of varying IoMT systems but also aligns with the evolving needs of the healthcare industry and other sectors leveraging IoMT technology.

The Health-IT Reference Architecture

To embark on an IoMT journey, enterprises must meticulously select health devices, networks, and IoMT platforms. Early attention to security allows proactive design, ensuring resilience against potential threats. Figure 1 illustrates the Health-IT Reference Architecture, delineated into three horizontal services namely Health devices, Full Stack IoMT Platform and IoMT Smart Gateways. Device Management and Artificial Intelligence (AI) are two specific services that are either part of Smart IoMT gateway or Full Stack IoMT Platform. The choice of where these services should reside is dependent on the IoMT use cases and is therefore considered as a vertical within the reference architecture. Security is applied across all horizontal services using blockchain, underscoring its pivotal role for the overall reference architecture. The Health-IT Reference Architecture is composed of several critical layers, each playing a distinct role in the functionality of the system. The initial layer is the device layer, consisting of physical objects located within hospital settings. These devices form the foundational elements of the IoMT environment. Following this is the Smart IoMT Gateway, a crucial component responsible for gathering data from various health devices and transmitting it to the broader system. In many instances, the Smart IoMT Gateway also undertakes preliminary data processing, which includes analytics.

Additionally, the Smart IoMT Gateway often handles Device Management. This entails processes such as provisioning, authentication, configuration, maintenance, monitoring, and diagnosing of health devices within the IoMT framework. While some enterprises opt to manage their devices at the Smart IoMT Gateway level, others prefer to conduct these operations at the Full Stack IoMT Platform level. The Full Stack IoMT Platform functions akin to an enterprise's nervous system, where IoMT data relayed from health devices via the Smart IoMT Gateway is amalgamated with other non-IoMT data. This integration facilitates the derivation of valuable insights through analytics systems or applications. Another pivotal function within a Health-IT Reference Architecture is Artificial Intelligence (AI). AI enables the creation of intelligent machines that can mimic smart behavior and assist in decision-making processes with minimal human intervention. The application of AI models varies among enterprises; some implement them at the IoMT Smart Gateway level, others at the Full Stack IoMT Platform level, and a few at both levels. The choice of implementation depends on the specific IoMT use cases that enterprises aim to execute.

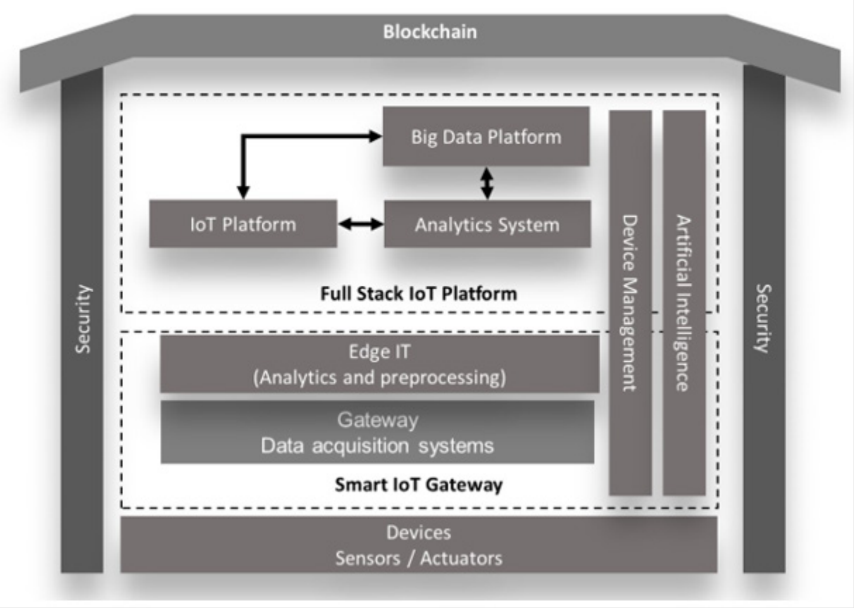

Figure 1: Health-IT Reference Architecture.

Security is a paramount, albeit implicit, requirement of the Health-IT Reference Architecture. It is essential for enterprises to ensure that the tools and platforms selected as part of their Health-IT Reference Architecture are thoroughly vetted for security. This encompasses all layers, from the health devices and Smart IoMT gateways to the Full Stack IoMT Platform. A pivotal element powering the Health-IT Reference Architecture is Blockchain technology. Although Blockchain in the context of IoMT is still evolving, it is crucial for enterprises to consider this function while designing their IoMT architecture. Looking forward, Blockchain is anticipated to become a fundamental component for enterprises aiming to succeed with IoMT. he subsequent chapters of this paper will delve into detailed discussions of each of these functions. A brief overview of these topics is provided below, setting the stage for a comprehensive exploration of the Health-IT Reference Architecture.

Health Devices (The Sensors and Actuators)

The foundational layer of every Internet of Medical Things system is the connected health devices or objects, which are pivotal in providing data, the core element of IoMT. Health devices employ sensors to capture physical parameters either externally or within the device itself. An IoMT device typically comprises hardware and software, including an operating system, computational capabilities, storage, and connectivity. The primary distinction between a conventional computer and an IoMT device lies in their inputs and outputs; health devices are characterized by sensors and actuators. Sensors, either integrated within the health devices or as standalone entities, are responsible for measuring and collecting telemetry data. For instance, a thermometer's role is to measure parameters such as human body temperature. Notably, not all IoMT health devices possess output capabilities. Those with outputs can execute actions in response to specific events, like alerting a physician when a patient's blood pressure exceeds a critical threshold. Actuators, in synergy with sensors, convert the data from health devices into physical actions. Consider a smart health system equipped with essential sensors; based on the sensor inputs, the system real-time analyzes and instructs the actuators to activate specific oxygen pumps for heart disease patients, maintaining operation until the sensors indicate the completion of the required duration.

Continuous connectivity is crucial for health devices to transmit and receive data and execute instructions effectively. In the contemporary connected health device landscape, inter-device communication is essential for gathering, sharing information, and collaborating in real-time, thereby enhancing the overall value of the IoMT deployment. However, achieving this interconnectedness is challenging, especially in environments with legacy health devices that are resource-constrained and battery-operated. These devices often struggle with limitations in computing power, energy, and bandwidth. Additionally, the diverse communication protocols (languages) used by different devices add complexity to direct inter-device communication. This is where Smart IoMT Gateways become crucial, offering a solution for both modern and legacy devices to communicate securely and optimally with other healthcare devices.

Smart IOMT Gateways

Smart IoMT gateways play a pivotal role in the IoMT architecture, primarily performing three critical functions as illustrated in Figure 2.

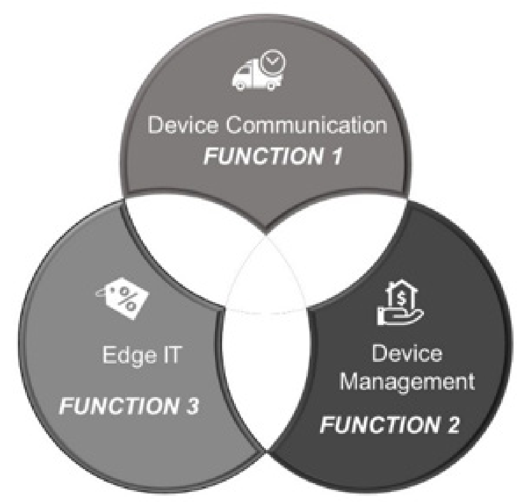

Figure 2: Functions of Smart IoMT gateway.

Device Communication (Data Acquisition and Communication): Acting as a data acquisition layer, they enable health devices to communicate and share data with each other and with the rest of the systems in an IoMT architecture. This function is fundamental to ensure seamless interaction and data exchange between diverse health devices, irrespective of their individual communication protocols.

Device Management: The management of IoMT health devices is another essential function. Some enterprises choose to delegate this task to the Smart IoMT gateways, while others opt for a Full Stack IoMT Platform approach. This decision typically depends on the specific use cases the enterprise aims to implement.

Data Preprocessing and Analytics (Edge IT): Edge Computing is a distributed computing paradigm that brings together computation and data storage closer to the location where it is needed, to improve response times and save bandwidth interval [2-5]. Edge computing is transforming the way data is being handled, processed, and delivered from millions of health devices around the world. The explosive growth of internet-connected health devices – the IoMT – along with new applications that require real-time computing power, continues to drive edge-computing systems [6].

Often referred to as Edge IT or Analytics at the Edge, this involves the preprocessing of data received from IoMT health devices. It's important to note that not all IoMT Gateways are equipped for this; standard IoMT Gateways primarily facilitate device communication, while Smart IoMT Gateways go a step further by processing and analyzing data at the gateway level. This approach brings computation and data storage closer to the health devices, enhancing response times and conserving network bandwidth [7]. Gartner defines edge computing as "a part of a distributed computing topology in which information processing is located close to the edge, where things and people produce or consume that information" [8]. The necessity for Smart IoMT gateways is determined by the specific needs of the enterprise and the IoMT use cases they are pursuing. Not all IoMT architectures require Smart IoMT gateways; hence, a judicious selection based on enterprise requirements is crucial.

Challenges with IoMT Smart Gateways: While IoMT Smart Gateways equipped with edge computing offer data storage and computational power, they face limitations in terms of the data volume and computational capacity at the gateway level [9]. Enterprises with millions of connected health devices necessitating extensive compute capabilities must strategize on data processing allocation between the Smart IoMT gateway and the Full Stable IoMT Platform, typically situated in the cloud. To address the constraints of data storage and computation at the IoMT Edge Gateway level, some enterprises are exploring specialized models to provide near-limitless compute capabilities [10] adjacent to the Smart IoMT gateways or health devices. These initiatives involve maintaining and managing servers regionally to minimize the need for transferring workloads over the Internet, thus reducing latency. Additionally, these efforts extend to facilitating connections across multiple cloud providers and between private and public clouds. This approach is particularly vital for larger enterprises who opt for a hybrid cloud environment, balancing mission-critical or sensitive applications and data between private and public clouds. An exemplary implementation of this concept is the Cloud Interconnect Fabric by Equinix. Siemens' introduction of the Industrial Edge concept [11] exemplifies this trend. This solution allows enterprises to analyze data at the machine level and preprocess it swiftly, with optimized data then transferred to the cloud for more extensive computing and storage. This innovation reflects the ongoing evolution and growing importance of edge computing in the IoMT landscape.

Full Stack IOMT Platform

The Full Stack IoMT platform is engineered to store, process, and analyze substantial volumes of health data, providing deeper insights through sophisticated data analytics engines and machine learning mechanisms. This platform is instrumental in creating and managing applications, executing analytics, and ensuring the security and storage of enterprise IoMT data. The decision to undertake device management at the IoMT Platform level is contingent upon the specific use case. Therefore, the selection of the appropriate IoMT Platform, one that can facilitate this feature, is crucial.

The market today offers a variety of IoMT platforms, with many supporting device management. These platforms cater to specific industries, such as commercial real estate or family health, and some focus on particular types of devices, like augmented-reality headsets, or specific functions relevant to sectors like manufacturing and healthcare. It's important to recognize that no singular Full Stack IoMT platform is universally applicable across all industries or capable of addressing every business challenge. Selecting the right IoMT platform requires a thorough understanding of the enterprise's IoMT strategy, the types of problems and opportunities they aim to address through IoMT, and the primary industry focus, be it manufacturing, retail, or healthcare. An ideal IoMT platform should effectively manage data from its collection at health devices (via IoMT Smart Gateways) through to the generation of insights. This involves processing highly specific data derived from industrial protocols or healthcare devices, which is then normalized and standardized for optimal use by the analytics platform.

Role of AI in IoMT Platforms and Gateways: Artificial Intelligence (AI) is a critical component in the Health-IT Reference Architecture. AI is defined as the simulation of human intelligence in machines programmed to think, act, and learn like humans, exhibiting traits such as problem-solving and adaptive learning. Machine learning, a subset of AI, leverages data and statistical methods to improve performance on tasks over time, without being explicitly programmed for those tasks. In the context of IoMT, AI's significance is magnified due to its integration with big data, enabling the architecture to harness immense computational power.

In the IoMT ecosystem, health devices generate substantial amounts of data. This data, stored in extensive data lakes, forms the backbone of AI applications in healthcare. AI's role extends to various functions like anomaly detection and root cause analysis, crucial for healthcare automation and predictive modeling. For example, AI can predict critical health events such as heart attacks or cancers. Traditional IoMT systems relied on rule-based engines for repetitive tasks, like triggering an alert when a patient's temperature exceeds a certain threshold. However, with AI integration, these static rules are replaced by dynamic, learning models, allowing for more nuanced and responsive healthcare interventions. The introduction of AI in IoMT has revolutionized healthcare delivery. For instance, at Royal Brompton and Harefield hospitals in London, an IoMT-based solution incorporating AI successfully predicts cancers based on patient history and real-time health data. This system has notably increased early cancer detection rates to 70% at Stage 1, significantly impacting patient outcomes and healthcare efficiency. However, AI in IoMT is not without challenges. The need to transfer large volumes of data to the cloud for processing can introduce delays and raise concerns about data privacy and security in regulated healthcare environments [12-14].

To mitigate these issues, AI algorithms are increasingly being executed closer to the source of data generation – at the Smart IoMT gateways, a concept known as AI at the edge. This approach, however, depends on the computational capabilities of these gateways. AI at the edge means that such tasks needs to be performed by the Smart IoMT gateways which is also called AI at the edge. But not all smart gateways will have such compute power to run AI algorithms on the edge. There are several enterprises that have come up with Smart IoMT gateways which is capable to running AI algorithms near to the health devices. Enterprises adopt various models to implement AI in IoMT architectures. In some cases, AI processing is conducted directly at Smart IoMT gateways using health device data. In scenarios involving vast data volumes, AI tasks are split between the Smart IoMT gateway and the Full Stack IoMT Platform. For example, a healthcare company utilized Amazon AWS Snowball Edge for intensive compute operations near IoMT health devices. This approach involves training the AI model in the cloud and deploying it to the IoMT Gateway for local processing. The model returns to the cloud for retraining when accuracy drops, illustrating a continuous improvement cycle.

The integration of AI and machine learning in IoMT has led to a shift from reactive to predictive maintenance, significantly enhancing healthcare delivery and patient monitoring. This convergence is opening new avenues in IoMT, evident in applications like connected cars, which exemplify edge computing on wheels, processing data in real-time. Similar advancements are seen in other sectors like aviation, where aircraft employ edge computing for enhanced operational efficiency. In addressing the complexities of IoMT, understanding the distinct roles of Smart IoMT gateways and Full Stack IoMT Platforms is crucial. While both serve overlapping functions, their specific responsibilities can vary. Smart IoMT gateways are typically responsible for basic data visualization, short-term data analytics, data caching, buffering, streaming, pre-processing, and Edge AI. On the other hand, Full Stack IoMT Platforms handle more complex analytics, big data mining, long-term data storage, and advanced machine learning algorithms. This distinction is vital for enterprises to effectively allocate tasks and leverage the full potential of IoMT systems. Below is a typical guidance that splits the responsibilities between Smart IoMT gateways and Full Stack IoMT Platform (Table 1).

Table 1.

Smart IoMT gateway	Full Stack IoMT Platform
Basic data visualization	Complex analytics
Basic data analytics and short-term data historian features	Big Data mining
Data caching, buffering and streaming	Sources of business logic
Data pre-processing, cleansing, filtering and optimization	Machine learning rules
Some data aggregation	Advanced visualizations
Device to Device communications/ M2M	Long term data storage/warehousing
Artificial Intelligence (Edge AI)	Artificial Intelligence

Security

Security in an IoMT environment must be comprehensively addressed across all three layers within the Health-IT Reference Architecture. These layers include: first, device-level security; second, security at the Smart Gateway Level; and third, security at the IoMT Platform level. Beyond the hardware and software security within these layers, network-level security is paramount and must be foolproof, as communications across these layers in an IoMT model occur over the internet. IoMT security has garnered significant attention following several high-profile incidents where common IoMT devices were exploited to infiltrate and compromise larger networks. The implementation of robust security measures is crucial to safeguard the networks and the connected IoMT health devices.

Device Security: In the IoMT ecosystem, device security is paramount. Enterprises must prioritize deploying health devices with inherent security features, accompanied by mechanisms for timely software updates or upgrades to address emerging security concerns. Traditional IoMT health devices, often constrained in computational resources, lack advanced security capabilities. For instance, typical sensors for humidity or temperature monitoring cannot support advanced encryption. Many such devices, designed for prolonged field deployment, rarely receive security updates, posing a significant risk. While integrating security from inception may seem costly and time-consuming, it is essential for healthcare enterprises embracing IoMT for long-term use. However, the required security level varies based on the device's use case. For example, the risk of a hacker targeting a thermometer is lower compared to the risks associated with a hospital's edge or cloud servers, which contain sensitive patient data. Access control to health devices and the encryption of data, both stored and transmitted, are critical. Enterprises must ensure that only authorized users or systems can access these devices and the data they produce.

Smart IoMT Gateway Security: IoMT Gateways, crucial in the IoMT infrastructure, present significant vulnerability as single points of potential exploitation. Their higher processing power, which supports more intensive applications, also introduces more software vulnerabilities. Positioned as edge devices between the internet and the intranet, gateways are often targeted by hackers due to their critical role in network security.

When selecting IoMT Gateways, several factors must be considered:

- Message Security: Strong end-to-end encryption is essential. Messages should be encrypted in a manner that allows only the intended recipient to decrypt them.
- Device Onboarding Security: The process of adding new devices to the IoMT ecosystem presents vulnerabilities. Key management and the security of key exchanges during device onboarding are critical areas.
- Integration Security: Secure data movement between health devices, gateways, and back-end databases is crucial. Continuous scanning and testing are necessary to maintain data integrity.
- Over-the-Air Security Updates: Understanding the process of firmware updates and how they are securely managed within the IoMT ecosystem is essential.

IoMT Platform Security: IoMT platforms, serving as data hubs and device management centers, require robust security measures. Fortunately, major platform vendors like Amazon, Microsoft, and Google provide comprehensive security solutions, including encryption and access control, along with continuous monitoring and auditing capabilities.

Blockchain: Trust is a fundamental component in human interactions, crucial for individual relationships, business operations, and the foundation of civilizations. Traditionally, centralized institutions have managed the aspect of trust in transactions. For instance, in financial exchanges, banks serve as trusted intermediaries, facilitating transactions between parties who may not directly trust each other. This model has been instrumental in enabling transactions, yet intermediaries introduce friction, increased costs, and various transactional challenges. Blockchain technology proposes a more secure and cost-effective solution to this trust issue, eliminating the need for intermediaries. This application extends beyond financial institutions to sectors like healthcare and pharmaceuticals, where secure data exchange is vital.

Blockchain is a decentralized, distributed digital ledger, comprising records called blocks [15-18]. It is designed to record transactions across multiple computers, ensuring that any involved block cannot be altered retroactively without changing all subsequent blocks [19]. This distributed ledger technology (DLT) allows data storage on a global network of servers, providing real-time visibility of entries to all network participants, thereby preventing single-user control or unauthorized network alterations. Blockchain is a system of recording information in a way that makes it difficult or impossible to change or hack the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain [20-24]. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every (participant's) ledger.

However, blockchain is not a solution for all marketplace issues. It is specifically tailored to address certain problems, particularly in reducing transaction costs and increasing security. For example, in a typical online transaction, several verifications are required — from participant identities to transaction amounts. Currently, this verification process involves multiple intermediaries, leading to significant resource and monetary expenditure. Blockchain significantly reduces the cost of verifying transactional attributes, ensuring authenticity and integrity. There is a lot of debate around blockchain trying to solve every marketplace problem, but blockchain is a technology that is tailored to address few problems only. One of its primary applications is in reducing transaction costs. For instance, when an individual engages in an online transaction, this process involves multiple verification steps, such as confirming the identities of those involved and the amounts exchanged. Currently, this verification is resource-intensive, often requiring several intermediaries, which adds complexity and expense to the transaction. Blockchain technology has the potential to significantly reduce these costs by streamlining the verification process and ensuring the authenticity of each transaction attribute. In essence, blockchain provides a novel approach to managing information. It facilitates exchanges between parties who may not inherently trust each other but have a mutual interest in a particular outcome. An example of this is the pharmaceutical supply chain, from the production of medicine to its sale by pharmacists and eventual consumption by patients.

This process involves various stakeholders, including pharmaceutical companies, transportation services, pharmacies, and consumers. Blockchain, in conjunction with the Internet of Medical Things, can manage information across this spectrum transparently and securely, thereby ensuring the integrity of the medicine and building trust among consumers. Blockchain has significantly augmented the value of IoMT in numerous instances. A notable example is in areas where counterfeit medications pose a public health risk. With blockchain and IoMT, the entire chain of custody for a medication—from production to sale—can be transparently tracked, reducing the dependency on intermediaries. This transparency is crucial for ensuring that the information fed into the blockchain is accurate and trustworthy. For instance, IoMT devices can periodically send tamper-proof data, like storage temperatures, to the blockchain, enhancing the reliability of the traceability solutions offered by blockchain.

And in terms of costs, the fundamental thing which blockchain will address is reducing cost of transaction. As an example, Person A wakes up and authenticate himself, buys something online and engages in some sort of digital transaction. Every such transaction needs to be verified such as who is involved, the amounts exchanged and so on and society spends a lot of resources and money to making sure that those attributes (transactions and actors) are correct and that transactions are executed without problems. Currently there are several intermediaries as part of each such transactions. Blockchain is a technology that drastically reduces the cost to verify that a specific attribute is true and genuine. In simple terms blockchain is a new decentralized distributed way of managing information across parties who do not necessarily trust each other but have an interest in a common outcome.

As an example, a common outcome of a "medicine from lab to shelf" process in a drug development, starts from medicine production to selling the medicine by pharmacist to consumption by a consumer. In such a set-up there are different actors involved such as pharmaceutical companies who produce drugs, freight management companies who transport these drugs from pharmaceutical companies to Pharmacy using right temperature-controlled fridges, pharmacies who sell these drugs and patients who buy and consume these drugs. Managing information across all these actors in a transparent and tamper proof way is the most important element in this use case based. The common outcome of this use case is that the patients can trust quality of the drugs and consume them safely without any doubts that drugs has been tampered and this can be enabled with IoMT and blockchain technology. This is the main reason why Blockchain has become an integral part of the Health-IT Reference Architecture.

On one side there are several examples where IoMT has created tremendous value from blockchain and there are opposite examples where blockchain has added a lot of value to IoMT. In pharmaceutical industry, the issue of counterfeit drugs, a problem estimated to be worth $200 billion [25], can be effectively tackled using blockchain and IoMT. By recording each step in the drug supply chain on a blockchain, from the procurement of raw materials to the final delivery to consumers, and tagging these steps with tamper-proof tags, the authenticity of drugs can be assured. Blockchain not only enables traceability but also builds additional trust by ensuring that the recorded transactions cannot be altered. Another area where blockchain contributes significantly is in the realm of connected cars. There have been instances where third-party hackers have exploited software upgrade processes to gain unauthorized access to car systems. Blockchain can mediate these software updates, ensuring that only authenticated actors with the correct permissions can initiate transactions within the car's systems, enhancing the overall security of the process. However, the implementation of blockchain in enterprise environments is not without its challenges.

The success of a blockchain-based system depends on the participation of all relevant actors in a given transaction. If not all parties involved in the transaction subscribe to the blockchain model, the full benefits of the technology may not be realized. This necessitates the importance of subscription by all stakeholders, including manufacturers, transportation companies, retailers, and delivery services. In any blockchain system, governance is a critical factor. Questions such as who owns the data, who controls the business logic running on the blockchain, who can introduce new services, and who decides the criteria for joining or leaving the network are essential considerations. These governance issues need to be addressed for the effective implementation of a blockchain solution in an IoMT framework. Furthermore, there are two primary types of blockchains: public and private. A public blockchain is permissionless, allowing anyone to join and participate in the network. It is decentralized, with no single entity controlling the network. Once data have been validated on a public blockchain, it is secure and cannot be altered [26,27].

On the other hand, a private blockchain is permissioned and operates based on access controls that limit network participation. It is typically managed by one or more entities, leading to a dependency on third parties for transactions. In a private blockchain, only the entities involved in a transaction have access to the relevant information. In the context of IoMT, a private blockchain is often more appropriate. This is because IoMT is inherently industry and enterprise-centric, with limited relevance for the general public. A combination of IoMT and blockchain is one of the most secure methods for enabling comprehensive business insights. However, it is crucial to choose the appropriate type of blockchain to align with the specific requirements and constraints of the IoMT landscape.

Conclusion

In this paper, I explore the Health-IT Reference Architecture as applied in healthcare. The Health-IT Reference Architecture is delineated into three distinct layers. The initial layer, known as the device layer, consists of physical objects situated within hospital environments. These devices are integral to the collection of medical data. The second layer is the Smart IoMT Gateway. This layer plays a pivotal role in gathering data from the aforementioned devices and transmitting it to other systems. Additionally, the Smart IoMT Gateway often engages in preliminary data processing, which includes analytics. Another critical function of this layer is Device Management, which varies in implementation; some enterprises opt to manage devices at the Smart IoMT Gateway level, while others prefer management at the Full Stack IoMT Platform level. The third and final layer is the Full Stack IoMT Platform. Here, IoMT data, routed through the Smart IoMT Gateway, is integrated with other non-IoMT data. This integration facilitates the derivation of valuable insights through the use of analytics systems or applications [28,29].

Artificial Intelligence (AI) also plays a significant role in the Health-IT Reference Architecture. The deployment of AI models varies among enterprises: some apply AI at the Smart IoMT Gateway level, others at the Full Stack IoMT Platform level, and a few opt for AI implementation at both levels. A fundamental, implicit requirement of the Health-IT Reference Architecture is the security of devices, Smart IoMT gateways, and the Full Stack IoMT Platform. To address this necessity, blockchain technology is proposed as an integral component of the reference architecture. The practical application of this reference architecture is evident in several critical healthcare scenarios, such as preventive care for life-threatening diseases, including various cancers, dementia (Alzheimer's disease), and advanced pulmonary, cardiac, renal, and hepatic conditions. A notable implementation example is the deployment of the Health-IT Reference Architecture at the Royal Brompton and Harefield hospitals in London. This implementation has enabled the prediction and early detection of cancer in approximately 70% of patients at Stage 1, as opposed to Stage 3, significantly contributing to life-saving interventions across the United Kingdom.

Declarations

Authors' Contributions

The corresponding author contributed to the study conception and design. Material preparation, data collection and analysis was performed by Venkatesh Upadrista.

Acknowledgements

I would like to thank Cambridge University for providing all the required support to complete this paper.

Ethical Approval

This work does not involve the use of human and/ or animal subjects.

Funding

No funding was received for conducting this study.

Conflict of Interests

The authors have no relevant financial or non-financial interests to disclose.

Availability of Data and Materials

The data generated during and/or analyzed during the current study can be made available from the corresponding author on reasonable request.

References

1. (2020) D Technologies, Internet of Things and data placement.
2. R Fu, Z Xu, B Wong, H Qian, L Ju, et al. (2021) Switch State Identification in Distribution Network Based on Edge Computing, IEEE Sustainable Power and Energy Conference (iSPEC), pp. 2318-2323.
3. N Bassama, S A Hussain, A A Qaraghuli, J Khan, E P Sumesh, et al. (2021) IoT based wearable device to monitor the signs of quarantined remote patients of COVID-19. Informatics in Medicine Unlocked 24: 101618.
4. W Y Chen, M Yu, C Sun (2021) Architecture and Building the Medical Image Anonymization Service: Cloud, Big Data and Automation, International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), pp. 149-153.
5. G A R, Y P Singh, N S Narawade (2022) Design of Fog Based Remote Health Monitoring System, IEEE 7th International conference for Convergence in Technology (I2CT), p. 1-7.
6. A Jenifer, G Jeba, L Paulraj, N K K, R Amoli, et al. (2022) Edge-based Heart Disease Prediction Device using Internet of Things, International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1500-1504.
7. A Qureshi, W Dashti, A Jahangeer, A Zafar (2020) A. Security challenges over cloud environment from service provider prospective, loud Computing and Data Science, p. 12-20.
8. (2021) Gartner, Edge Computing, Gartner.
9. (2021) equinix, 5 Top Practices of Successful Edge Computing Implementers, equinix.
10. (2023) siemens, Optimize production processes with Industrial Edge, siemens.
11. T Hayajneh, B J Mohd, M Imran, G Almashaqbeh, A V, et al. (2016) Networks, Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor, Mobile Sensor Computing: Theory and Applications 16: 424.
12. P P Ray, D Dash, K Salah, N Kumar (2021) Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Systems Journal (Early Access) 15(1): 85-94.
13. N Garg, M Wazid, A K Das, D P Singh, J J P C Rodrigues, et al. (2020) BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access 8: 95956-95977.
14. M H Chinaei, H H Gharakheili, V Sivaraman (2021) Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract. IEEE Internet of Things Journal 8(12): 10117-10130.
15. A Jolfaei, S F Aghili, D Singelee (2021) A Survey on Blockchain-Based IoMT Systems: Towards Scalability. Institute of Electrical and Electronics Engineers (IEEE) 9: 148948-148975.
16. K N Griggs, O Ossipova, C P Kohlios, A N Baccarini, E A Howson, et al. (2018) Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of Medical Systems 42: 1-7.
17. G S Aujla, A Jindal (2021) A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. IEEE Journal on Selected Areas in Communications 39(2): 491-499.
18. K N Griggs, O Ossipova, C P Kohlios, A N Baccarini, E A Howson, et al. (2018) Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of Medical Systems 42(130).

19. X Chen, S Tian, K Nguyen, H Sekiya (2021) Decentralizing Private Blockchain-IoT Network with OLSR. Future Internet.

20. H F Atlam, M A Azad, A G Alzahrani, G Wills (2020) A Review of Blockchain in Internet of Things and AI, Big Data and Cognitive Computing 4: 28.

21. X Chen, S Tian, K Nguyen, H Sekiya (2021) Decentralizing Private Blockchain-IoMT Network with OLSR. Future Internet 13(7): 168.

22. H F Atlam, M A Azad, A G Alzahrani, G Wills (2020) A Review of Blockchain in Internet of Things and AI,, Big Data and Congnitive Computing 4(28).

23. K N Griggs, O Ossipova, C P Kohlios, A N Baccarini, E A Howson, et al. (2018) Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of Medical Systems volume 42(130).

24. B D Glass (2014) Counterfeit drugs and medical devices in developing countries, Res Rep Trop Med 5: 11-22.

25. Qinglin Yang, Yetong Zhao, Huawei Huang, Zehui Xiong, Jiawen Kang, et al. (2022) Fusing Blockchain and AI with Metaverse: A Survey 3: 122-136.

26. G K Behara, T Khandrika (2020) Blockchain as a Disruptive Technology: Architecture, Business Scenarios, and Future Trends. IGI Global, pp. 130-173.

27. M A H Wadud, T M A U H Bhuiyan, M A Uddin, M M Rahman (2020) A Patient Centric Agent Assisted Private Blockchain on Hyperledger Fabric for Managing Remote Patient Monitoring, International Conference on Electrical and Computer Engineering (ICECE), pp. 194-197.

28. T Ncube, N Dlodlo, A Terzoli (2020) Private Blockchain Networks: A Solution for Data Privacy, 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), p. 1-8.

29. F Buccafurri, G Lax, S Nicolazzo, A. Nocera (2017) Overcoming Limits of Blockchain for IoT Applications, Proceedings of the 12th International Conference on Availability, Reliability and Security 26: 1-6.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2024.54.008608

Venkatesh Upadrista. Biomed J Sci & Tech Res

Submission Link: https://biomedres.us/submit-manuscript.php