International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 11 | Nov 2023 www.irjet.net p-ISSN: 2395-0072

Design and Development of a Secure Cloud-Based Medical Data Management System

Yaroslav Kliuchka[1], Oleksander Shmatko[2]

[1]Postgraduate student, Department of Software Engineering and Management Information Technologies, National Technical University „Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2]PhD, Associate Professor, Department of Software Engineering and Management Information Technologies, National Technical University „Kharkiv Polytechnic Institute", Kharkiv, Ukraine

---

Abstract - *This paper presents a unique architectural framework for a secure medical data storage management system that is based on the tangle technology. The utilisation of electronic health information exchange enables healthcare practitioners and patients to securely access and electronically communicate essential medical information with other healthcare providers. However, the current health systems designed for the sharing of medical data encounter several challenges, notably security concerns, confidentiality issues, and the fragmentation of medical data. Data information systems in the medical field are often separated due to the utilisation of distinct systems by individual medical institutions, laboratories, and doctors. The timely availability of medical information remains a challenge for patients since they currently lack access to these systems. The transmission of medical information among physicians is facilitated either by conventional mail or by patients personally carrying their own medical records upon admittance to a healthcare facility. Within the healthcare sector, the absence of a unified system that facilitates enduring access for both medical practitioners and patients to comprehensive records pertaining to a patient's medical history and recommended therapeutic interventions is evident. This study examines the eHealth system, which is a digital platform for managing health-related information and services. In this particular system, the entirety of medical data is maintained within a single component, which subsequently grants physicians utilising information systems the ability to access this data. Nevertheless, it is important to acknowledge the limits of this system. These drawbacks include the presence of a single point of failure, the absence of unified medical information systems, and the continued lack of patient access to their own medical data. Hence, a potential resolution to these challenges is the establishment of directed acyclic graph (DAG)-based systems for facilitating the exchange of medical information. The Directed Acyclic Graph (DAG) facilitates the secure and reliable transmission of data while ensuring its integrity. The medical records of the patient will be saved in a decentralised ledger rather than being hosted on the server of the medical facility. In order to ensure the integrity and accessibility of patient data, it is imperative that no unauthorised individuals possess the ability to modify or restrict a patient's access to their own data. The utilisation of directed acyclic graphs (DAGs) is examined in the context of transmitting medical patient data to healthcare professionals. The procedure of generating and transmitting medical data to a Directed Acyclic Graph (DAG) is elucidated through a concrete illustration. The present study focuses on the utilisation of directed acyclic graphs (DAGs) within an electronic healthcare system for the purpose of healthcare data exchange. Specifically, the study examines the exchange of medical patient data using information and web technologies.*

Key Words: IOTA Tangle, electronic healthcare system, medical patient data, blockchain technology

1. INTRODUCTION

The health industry is now experiencing a significant transformation with the integration of technology into many processes. The integration of information and communication technology is important for the effective implementation of contemporary medicine. Technology has the potential to facilitate the transformation of health systems that are now unsustainable into sustainable ones. Additionally, it may promote equitable relationships between medical professionals and patients while offering cost-effective, efficient, and improved methods for combating illnesses [1]. The emergence of e-health may be attributed to the demand for enhanced documentation and increased quality in healthcare, together with the necessity to effectively monitor patients' health states and the medical operations they undertake. Healthcare practitioners often maintain physical copies of patient records. The emergence of electronic tracking systems can be attributed to the increasing expenses of healthcare and advancements in technology. The emergence of telemedicine, a novel approach in the field of medicine, has been facilitated by advancements in technology. Telemedicine involves the utilisation of telecommunications technologies to provide medical treatment remotely [2]. The utilisation of technology has facilitated the accessibility of diverse resources for both patients and healthcare professionals, hence enhancing the efficiency and cost-effectiveness of healthcare delivery. Electronic healthcare gives patients the chance to be involved in their own care, which helps them learn more about their illness and how different treatments work. Individuals are inclined to adhere to treatment regimens

prescribed by medical professionals when they have access to the findings of research studies pertaining to a certain treatment modality. This enables them to acquire knowledge about the advantages of prescribed medications, exercises, and other interventions designed to enhance their well-being. This enables patients to have a comprehensive understanding of the specific actions undertaken by their healthcare provider in order to assist them [3]. The healthcare sector has seen significant transformations throughout the past five years. This may be mostly attributed to the advancements in technology and the widespread use of many creative digital solutions on a daily basis. Numerous technological advancements have been developed with the primary objective of addressing the myriad challenges encountered in the field of medicine on a global scale. The following technologies have been identified as the leading advancements in the field of medicine in 2021: artificial intelligence and the Internet of Medical Things. These technologies have brought about significant changes and improvements in the medical sector [4].

In recent years, there has been a growing interest within the healthcare sector regarding distributed ledger technology, specifically in relation to blockchain technology. Blockchain is an illustrative instance of a decentralised ledger system. One of the primary benefits of blockchain technology is its ability to facilitate the safe exchange of patient data among various medical organizations. Nevertheless, in recent years, the blockchain has emerged as a technology with inherent limitations. The developers opted to construct alternative networks due to the presence of systemic inefficiencies and challenges associated with scalability. These newly designed networks deviate from utilising the blockchain data structure entirely. An instance of a cryptocurrency that uses Directed Acyclic Graph (DAG) technology in lieu of a traditional blockchain is IOTA. When comparing DAG with blockchain, it is seen that DAG exhibits more flexibility and scalability. Over time, the directed acyclic graph (DAG) demonstrates enhanced speed and increased computational capabilities. Conversely, blockchain technology experiences a decrease in speed and productivity. Furthermore, the Directed Acyclic Graph (DAG) technology has the advantage of being cost-effective since it eliminates the need for nodes to incur substantial costs for transaction verification. Within the context of blockchain technology, it has been observed that the transaction cost is too high, hence impeding the efficient confirmation of transactions. Additionally, there appears to be a deficiency in the established protocols or mechanisms to facilitate the confirmation process. Consequently, in order to mitigate the occurrence of confirmation delays, nodes are required to pay substantial transaction fees [5]. Hence, it is vital to examine the utilisation of Directed Acyclic Graphs (DAG) in the healthcare sector in order to ensure the secure flow of data.

2. LITERATURE REVIEW

The fragmentation of medical data has been identified as a significant factor that has a detrimental impact on the quality of medical services and patient outcomes. Healthcare professionals have challenges accessing current, comprehensive, and timely patient medical information. Patients have the ability to seek medical care from several healthcare facilities, resulting in the creation of individual medical records at each institution. The lack of comprehensive aggregation of a patient's medical data may result in several adverse outcomes, such as misdiagnosis, redundant documentation, and inappropriate medicine selection. The utilisation of Tangle technology is suggested in the study [6] as a means to defragment medical data, hence enhancing communication between patients and healthcare professionals. The utilisation of this technology is expected to enhance the calibre of medical services and optimise patient outcomes.

A significant number of doctors and institutions are transitioning from traditional paper-based medical records to electronic health records (EHRs). If this system was put into place, it would be easy to get medical records no matter where you are or how much time you have. This would improve the quality of healthcare services and make medical staff more productive. Medical records are considered to be highly confidential and private personal data that necessitates regular sharing with various entities, such as healthcare providers, insurance companies, pharmacies, researchers, and other relevant parties. Typically, personal information is kept across many storage systems. Nevertheless, there exists a subset of patients who lack confidence in the security measures used inside the systems responsible for storing their personal data. Consequently, the healthcare industry is actively seeking efficient measures to safeguard the confidentiality and integrity of patients' data. Contemporary blockchain-based technologies are poised to address the issue of safeguarding the privacy of medical data. The study conducted by the authors [7] presents a proposed solution that utilises blockchain technology to facilitate the secure and efficient exchange of medical data among healthcare providers. This proposed solution aims to guarantee the preservation, security, and availability of medical data. The authors describe a solution in [8] that utilises blockchain technology for the purpose of facilitating the sharing of medical records. The sharing of data occurs in a direct manner between medical organizations. The level of transparency has been enhanced due to the system's capability of enabling nodes to see and monitor transactions. The system offers functionalities for the administration of data, ensuring security measures, and facilitating interoperability.

Blockchain technology is an esteemed and substantial technological innovation with considerable implications for the healthcare sector. The blockchain platform BlocHIE,

which facilitates the sharing of medical information, is introduced in reference [9]. This research looks at two different types of medical data: electronic medical records and personal medical data. It also looks at the different requirements needed to store and share these types of data. According to the study conducted, the platform utilises a combination of two loosely coupled blockchains. Specifically, the EMR-Chain is employed for the management of electronic health records, while the PHD-Chain is utilised for the handling of personal health data. In the aforementioned study [10], the authors introduce the Healthchain system, which utilises blockchain technology as a means of securely storing medical data. The present system employs two distinct blockchains, namely Userchain and Docchain, in order to ensure the integrity and immutability of patient data and physicians' diagnoses, thereby preventing any potential deletion or falsification. The utilisation of this technology in the healthcare sector has been substantiated by safety studies and empirical findings. The authors of [11] propose a system that utilises blockchain technology to effectively manage and securely store electronic medical records. This study further elucidates the Medicalchain platform, which facilitates the simple and safe storage of patient medical data through the utilisation of blockchain technology. Medicalchain is a platform that enables individuals to authorise healthcare practitioners to access their personal medical information. Medical practitioners have the ability to incorporate textual annotations, visual representations, and laboratory findings into the patient's records, which are documented as individual transactions.

The absence of dependable and fortified systems for the storage and transmission of medical data is a significant challenge within the healthcare industry. Given the paramount significance placed on the confidentiality and security of medical data, Consequently, an increasing number of healthcare systems are being created that utilise blockchain technology for the purpose of organising and preserving data. In addition to the utilisation of blockchain technology, novel forms of distributed registries have emerged as viable alternatives for application within the healthcare sector. One example of such a type is the directed acyclic graph. Prior to delving into the use of directed acyclic graphs (DAGs) in the healthcare domain, it is imperative to have a comprehensive understanding of DAGs and the advantages they offer.

3. PURPOSE AND OBJECTIVES OF THE STUDY

The main goal of this study is to look into how Directed Acyclic Graph (DAG) technology is used in the healthcare industry, focusing on how it helps with safe data sharing. In order to accomplish this objective, the following objectives are addressed: elucidate the fundamental nature and mechanisms of Directed Acyclic Graph (DAG); examine the overarching framework for transmitting medical data inside the electronic healthcare system known as eHealth; and ascertain the suitability of employing DAG within the healthcare industry to facilitate the secure exchange of data.

4. PROPOSED MODEL

The essence and mechanisms of a directed acyclic graph (DAG) pertain to a type of directed graph that lacks any directed cycles. However, it is possible for there to exist many "parallel" pathways that originate from a single node and terminate at the end node by distinct routes. From a visual perspective, a graph may be defined as a collection of vertices that are interconnected by edges. The term "directed" refers to the characteristic of each edge in a graph having a certain direction, indicating that the movement between vertices occurs exclusively in a predetermined direction. The term "acyclic" refers to the absence of a closed path, commonly known as a "cycle," inside the graph. It is associated with the development of IOTA, a cryptocurrency specifically built for the Internet of Things (IoT). Unlike conventional blockchains, IOTA employs a Directed Acyclic Graph (DAG), known as Tangle, as its underlying technology. The IOTA Tangle is a novel form of distributed ledger technology. One of the primary benefits of Tangle is its feeless transaction mechanism. The elimination of transaction costs presents an additional significant aspect of Tangle, namely the facilitation of microtransactions. The structure of records and the level of synchronicity are distinguishing factors between Tangle and blockchain [5]. Within the context of blockchain technology, it is essential to note that blocks are meticulously documented in a rigidly sequential manner, according to a rigorous chronological sequence. Consequently, the generation of block N+1 will be postponed until block N is filled and verified. This method does not support concurrent block creation, leading to a notable decrease in transaction verification speed. In the Tangle protocol, the absence of blocks is a notable characteristic. Instead, each newly generated transaction establishes a reference to the preceding two transactions. In the Tangle system, transactions are promptly verified by the network's nodes without being queued. Whenever a novel transaction is included in the Tangle, it proceeds to choose the two preceding transactions for validation, introducing two more edges to the graph (as seen in Figure 1).

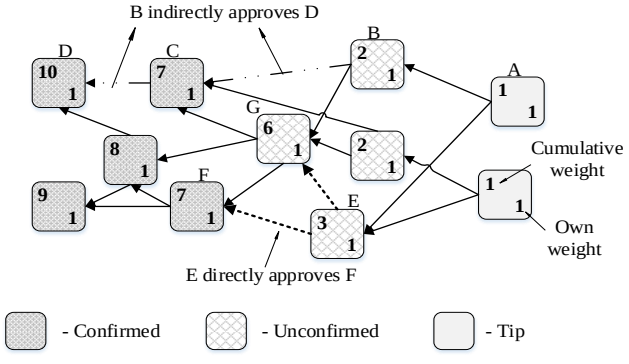

Figure -1: Directed Acyclic Graph

Figure 1 presents a directed acyclic graph illustrating the relationships between transactions. It is observed that transaction E directly approves transactions F and G, whereas transaction A indirectly approves transactions C, D, G, F, and others. The core concept behind Tangle is that the successful execution of a transaction necessitates the active participation of users in the approval process of subsequent transactions. Hence, the individuals who engage in the transaction contribute to the security of the network by validating and confirming the cumulative weight of previous transactions. Specifically, the transaction participants directly approve certain transactions, while others remain unconfirmed. Additionally, the participants indirectly approve transactions through a network of connections. The aforementioned process ensures the integrity and reliability of the network. To successfully execute a transaction within the network, a node undertakes a series of actions. Firstly, the node employs an algorithm to select two transactions for approval. Subsequently, the node verifies that these two transactions are devoid of conflicts and do not endorse conflicting transactions, as the tangle may contain such conflicting transactions. Lastly, for the new transaction to be deemed valid, the node must resolve a cryptographic problem akin to those encountered in the Bitcoin system [12]. It is of significance to acknowledge that the IOTA network operates in an asynchronous manner. According to reference [12], it is not necessary for nodes to have visibility of an identical set of transactions. Nevertheless, it is imperative that all nodes reach a consensus on a single ledger state, hence determining the eligibility of transactions to be included in the ledger. In contrast to a blockchain, wherein the determination of which transaction should be retained is made by the miners.

In order to achieve agreement in Tangle, two approaches are employed: the Coordinator, which follows a centralised approach, and the Markov chain Monte Carlo (MCMC) tip selection algorithm, which adopts a distributed and probabilistic approach. The Coordinator is a distinct node managed by the IOTA Foundation, responsible for facilitating zero-cost transactions. The Markov Chain Monte Carlo (MCMC) procedure is a probabilistic consensus methodology that is anticipated to supplant the Coordinator in due course. The approach employs stochastic processes known as random walkers, which traverse the graph by moving towards leaf nodes at a specified depth [13]. The concept of cumulative weight is introduced in Tangle (Figure 1) to signify the significance of a particular transaction. The weight assigned to a transaction is directly proportionate to the level of computational effort required for validating that transaction. In the present iteration of IOTA, the weight is represented as 3^n, where n is a natural number. The concept of aggregate weight is established by considering the inherent weight of a transaction along with the cumulative weight of the transactions that directly or indirectly endorse it [12]. The aggregate weight of the ancestors in the tangle is increased by the weight of each new transaction that is added. The resolution of conflicting transactions can be achieved by the execution of the Markov Chain Monte Carlo (MCMC) algorithm iteratively, enabling the determination of the transaction that holds a higher probability of being authorised [13]. Consider a scenario in which the Tangle, a distributed ledger technology, consists of two transactions, Tx1 and Tx2, that are in dispute with each other. A transaction possessing a substantial cumulative weight holds greater significance compared to a transaction characterised by a smaller weight. If transaction Tx1 possesses a higher cumulative weight in comparison to transaction Tx2, it will be granted approval, and transaction Tx2, which is equipped with Tx2, will be discontinued. Branches with a substantial cumulative weight exhibit a higher priority and are expected to experience continuous growth over an extended period. While other branches will be eliminated.

The Tangle employs the Winternitz one-time signature scheme (W-OTS) for the purpose of signing transactions, as it offers resistance against potential assaults facilitated by quantum computers. The W-OTS system is a digital signature scheme that exhibits resistance to quanto attacks and employs key and signature sizes that are quite modest. Given that this particular cryptographic strategy is designed as a one-time signature scheme, its primary use lies in the ability to generate a signature for a singular message. In accordance with cryptographic protocols, it is imperative that the private key be utilised just once for the purpose of signing a single message. The security of the system is compromised when a private key is employed to sign several messages. Furthermore, the MAM (Masked Authenticated Messaging) protocol [5] ensures the provision of safe and encrypted data transmission across nodes. Masked Authenticated Messaging (MAM) is a data transfer protocol situated at layer 2, which facilitates the safe transmission of encrypted data streams over the IOTA distributed ledger [14].

The eHealth system is a telecommunication and information system utilised in the field of healthcare. This system facilitates the automation of medical service record keeping and the administration of medical information through the creation, uploading, publishing, and exchange of electronic information, data, and documents. The system comprises a central database (CDB) and electronic health information systems that provide the automated interchange of information, data, and documents via an application programming interface (API) [15]. The architecture of the system is depicted in Figure 2.

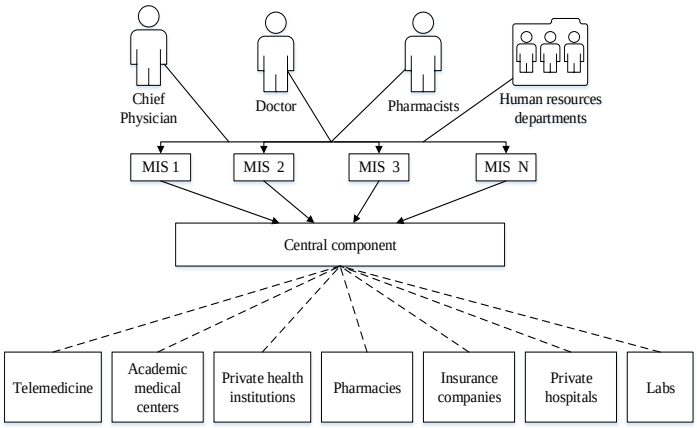

Figure -2: System architecture

The system architecture depicted in Figure 2 encompasses various entities within the healthcare sector, including human resources departments, pharmacists, doctors, chief physicians, and central components such as Management Information Systems (MIS) 1, MIS 2, MIS 3, and MIS N. Additionally, academic medical centres, telemedicine services, private health institutions, pharmacies, insurance companies, and private hospitals are integrated into this architecture. The electronic health care system consists of two main components. In this system, users engage with a medical information system (MIS) to communicate with a central database (CDB). The eHealth system has many components, including a central component (CC) that ensures the reliable availability of information and is responsible for the storage and processing of data. Additionally, electronic medical information systems are integrated into the eHealth system, enabling the automation of tasks inside medical institutions (CDB) [16]. Figure 3 illustrates the comprehensive framework for the migration of medical records to the eHealth system.

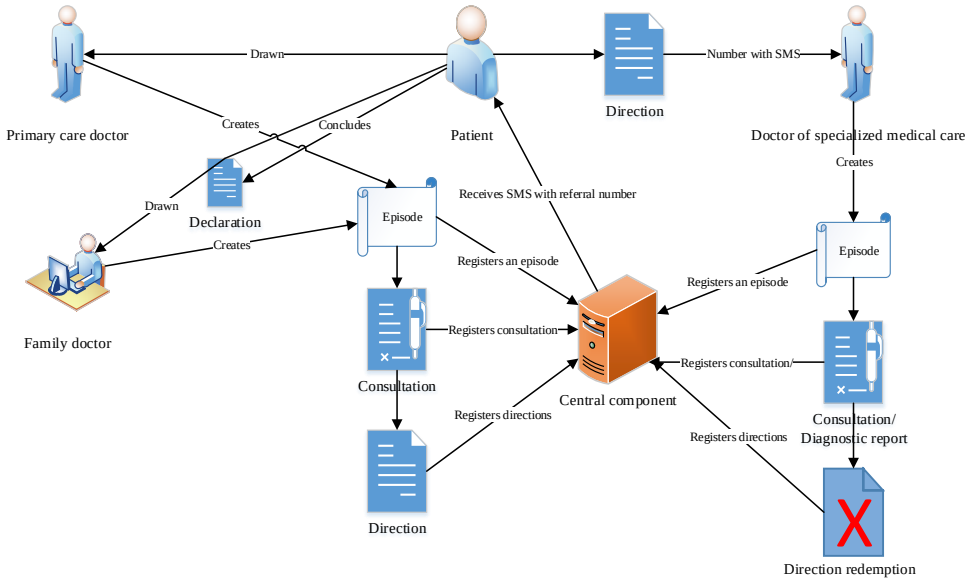

Figure -3: Transfer of medical records to the eHealth system

In Figure 3, the process of transferring medical records to the eHealth system is depicted. The patient is sent to either the admissions department of primary medical assistance or their designated family doctor, where the necessary documentation is submitted. The physician initiates an encounter in which the patient seeks medical attention. An episode refers to the whole engagement between a patient and a medical practitioner, encompassing the initial treatment and subsequent encounters, all centred around addressing a specific health issue or sickness. The physician records the generated episode in the patient's medical chart. Subsequently, the physician initiates a consultation and proceeds to record all pertinent information. The process of consultation registration with the CC was initiated. If a patient requires a referral for hospitalisation or diagnostic procedures from another medical professional, the primary care physician (referred to as "P") initiates the process. The patient's family doctor is responsible for documenting the patient's medical history and creating a declaration episode. This episode serves as a central component in the referral process. The primary care physician then consults with the specialised medical care doctor, who creates a consultation or diagnostic, generates a referral, and proceeds to formally record and submit this reference to the Central Committee. Subsequently, the patient is sent a Short Message Service (SMS) containing the referral number. Upon obtaining the computerised reference number, the patient is eligible to request specialised medical care. The patient is sent to either

the reception section of the institution or directly to the doctor (specialist). It is the patient's responsibility to provide the electronic referral number, enabling the doctor to identify and access the referral accordingly. Subsequently, the physician generates an episode and proceeds to record it within the C system. Once a consultation or diagnostic report has been recorded in the central component, the physician proceeds to cancel the reference and documents the cancellation of the referral in the same central component. One significant drawback of this method is the existence of a solitary point of failure. In the event that the CC emerges from a state of inertia, it will result in the system's overall collapse. The functionality of the entire system is contingent upon the central component (CC). Another drawback is the absence of a cohesive medical information system. Medical institutions have the option to select a Management Information System (MIS) from a pool of systems that have successfully undergone verification and are integrated with the central component (CC) of the eHealth system. Furthermore, it is worth noting that patients continue to have challenges accessing their medical data, therefore impeding their ability to obtain crucial information in a timely manner. Figure 4 illustrates the process of transmitting patient medical data to a physician through the utilisation of Tangle.

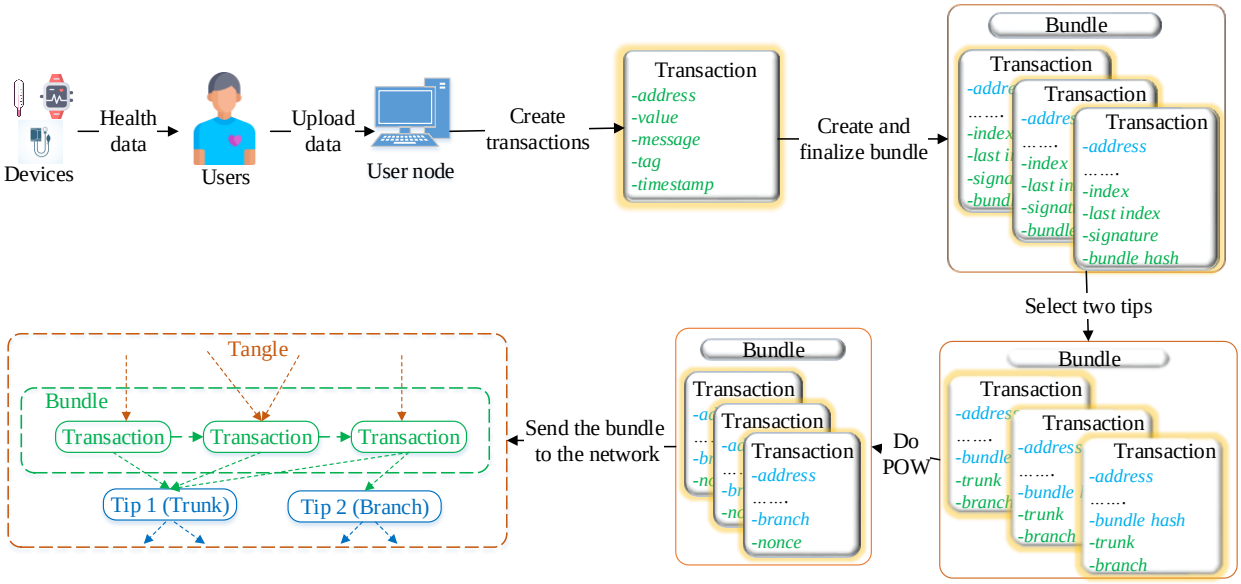

Figure -4: Transferring patient medical data to a doctor using Tangle

In Figure 4, the process of transferring patient medical data to a doctor is depicted using the Tangle User Node Transaction. This transaction involves multiple steps, including the creation of transaction bundles and the utilisation of tips (trunk and branch) within the Tangle. Each transaction within the bundle contains relevant information such as the address, value, message, tag, and timestamp. Additionally, users can upload their health data through various devices, which then generate the necessary transactions for data transfer. The elements in question are an index, a last index, a signature, a bundle hash, a bundle transaction, and an address. The elements mentioned are an index, a final index, a signature, a bundle hash, a transaction, and an address. The process involves the creation and finalisation of a bundle transaction, which includes the generation of an index, last index, signature, and bundle hash. Additionally, an address is associated with the transaction. The concepts being referred to are the bundle hash, trunk, branch, transaction, and address. The concepts being discussed are bundle hash, trunk, branch, transaction, and address. In the context of distributed ledger technology, two fundamental concepts are the bundle hash and the transaction address. The bundle hash refers to a cryptographic hash value that is generated by combining many transactions together. This hash value serves as a unique identifier for the bundle of transactions. On the other hand, the transaction address represents a specific location inside the distributed ledger where a transaction is stored. It is important to note that in this context, the terms "trunk" and "branch" are also relevant. These terms refer to the two branches of a directed acyclic graph structure that is used to organise and validate transactions within it. The concept of a "branch" in the context of a nonce transaction is associated with a specific location. The concept of a "branch" in the context of a nonce transaction address is being discussed. The branch and nonce are utilised in the Proof of Work (PoW) process to validate and append the bundle to the network. The user proceeds to input their medical data, including body temperature, heart rate, symptoms, and laboratory reports, among other relevant information. In order to transmit data to the physician, the patient generates transactions. A transaction refers to the most basic unit of data that may be disseminated across a network. The act of transmitting transactions is executed through the utilisation of a container known as a bundle. Once all the individual transactions have been generated, it is now necessary to proceed with the

creation of the bundle. A packet refers to a collection of transactions that, upon transmission to the network, undergoes processing as a fundamental unit. The transactions inside a bundle are individually indexed (as index and final index) and include information on the remaining number of transactions within the bundle. Subsequently, it will be necessary to authenticate ownership by affixing a signature to transactions using a private key. Subsequently, the generation of the bundle hash is required. The package hash serves as a distinct and exclusive identification for the package. The subsequent procedure involves identifying the two tips inside the tangle that will be subjected to validation, specifically the trunk and branch tips. The next step involves the computation of the proof of work (PoW) for every transaction inside the given batch. The computation of the Proof of Work (PoW) needs to be performed for each transaction in a discrete manner, resulting in an increase in processing time as the number of transactions in a batch grows. The outcome of the Proof of Work (PoW) algorithm yields a nonce value, which is then appended to the transaction. The final stage involves transmitting the packet to the network. In the network, a node will disseminate transactions to its adjacent nodes, which in turn will propagate these transactions to their respective adjacent nodes. Consequently, the dissemination process ensures that transactions efficiently propagate throughout the majority of nodes in a timely manner. As a result of this, transactions will be directed to the node belonging to the doctor. According to the cited sources [17–18], there is a positive correlation between the size of the Tangle network and the speed of communication among nodes, as well as the speed at which transactions are verified. In order to transmit a diagnosis and provide medical guidance, the physician must adhere to the same procedures as the patient. The initial step involves the creation of transactions and subsequent bundling. Please choose two recommendations from the Tangle framework and do a calculation of the proof of work (PoW). Subsequently, disseminate transactions to the network in order to obtain verification.

5. RESEARCH FINDINGS AND DISCUSSION

The healthcare sector has encountered notable obstacles, encompassing issues related to interoperability, accessibility, security, and the immutability of medical data. The utilisation of blockchain technology has been employed as a means to address these aforementioned issues. The utilisation of blockchain technology enables the safe, transparent, and decentralised storage of medical data. There are projects focused on various areas [19]. These areas include the supervision of supply chains and the combat against counterfeit products, such as the MediLedger Project, Ambrosus, and Blockpharma. Additionally, there are projects related to telemedicine, such as PointNurse, Docademic, MDsquare, TrustedHealth, and MyClinic. Furthermore, there are projects in the field of diagnostics, such as Skychain, DeepRadiology, and eHealth First. Lastly, the utilisation of blockchain technology enables medical organisations to efficiently exchange medical data while also safeguarding data confidentiality and integrity. The utilisation of blockchain technology enables the comprehensive tracing of pharmaceutical items, including their whole supply chain journey, commencing with the maker and concluding with the ultimate recipient. Blockchain technology enhances telemedicine services by providing safe, trustworthy, decentralised, and trusted remote medical assistance. The emergence of Tangle has prompted companies to embark on the development of medical systems utilising this technology, yielding preliminary findings. The SmartOptz initiative facilitates patient engagement in monitoring their personal medical data and enables the sharing of vital signs with healthcare practitioners via Tangle. The Pact project facilitates the safe and reliable sharing of medical data between healthcare organisations and individuals by utilising an application programming interface (API) that interacts with Tangle. This article provides an overview of the current eHealth system in Ukraine, known as eHealth, and suggests a contemporary method utilising Tangle as a potential replacement. The approach being discussed facilitates safe, transparent, and decentralised communication of medical data between healthcare professionals and patients. The use of decentralisation and the absence of a single point of failure in Tangle can effectively guarantee continuous data availability. The primary element of the eHealth system is a centralised database that aggregates data into a single repository. The failure of the primary component will result in the complete incapacitation of the entire system. The utilisation of blockchain technology has demonstrated its efficacy in healthcare systems. In contrast, Tangle, another distributed ledger technology, possesses significant potential to establish its value within the healthcare business.

6. CONCLUSIONS

The examination of the mechanisms and characteristics of Tangle yields the deduction that this technology is most aptly employed for the storage and transmission of medical data. When considering the development of healthcare systems, it is crucial to give particular emphasis to three primary attributes of Tangle: its great scalability, absence of fees, and capacity to facilitate fast transactions. The incorporation of high scalability into your system will enable the efficient processing of a substantial and uninterrupted flow of medical data. The lack of transaction fees enables individuals to engage in microtransactions without the need to provide compensation to the miners. The lack of miners not only facilitates faster transaction processing but also reduces the equipment needed. The concept of eHealth was taken into consideration. The system is comprised of a core component and medical information systems in a structured manner. The central component is accountable for the centralised storage and processing of information, remaining imperceptible to end users such as patients and clinicians.

The Management Information System (MIS) is utilised for the purposes of patient registration, appointment scheduling, personal account maintenance, and reference issuance, among other functions. These systems facilitate collaboration between end users and the eHealth system. The applications of Tangle are examined using the illustration of transmitting a patient's medical data to a healthcare provider. The intricacies surrounding the creation and transmission of medical data to Tangle are thoroughly examined. The advantages of using Tangle are exemplified by a specific and tangible instance.

REFERENCES

[1] Ways Technology Is Changing Healthcare. The Medical Futurist. Available at: https://medicalfuturist.com/ten-ways-technology-changing-healthcare/ (accessed February 15, 2021).

[2] M. Glasser, K Peters, E-health. Available at: https://www.britannica.com/science/e-health (accessed February 21, 2021).

[3] What is eHealth?. Available at: https://www.usfhealthonline.com/resources/key-concepts/what-is-e-health/ (accessed February 24, 2021).

[4] R. Elezaj, How technology has changed the world of medicine. Available at: https://www.geospatialworld.net/blogs/how-technology-has-changed-the-world-of-medicine/ (accessed February 24, 2021).

[5] Y. Kliuchka, O. Shmatko, "Comparison of blockchain technology and directed acyclic graph during data storage and processing in a distributed registry", Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, (1) (3), pp. 106–116, 2020, DOI: 10.20998/2079-0023.2020.01.18

[6] E. Saweros, Y.-T. Song, "Connecting Personal Health Records Together with EHR Using Tangle". 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), DOI: 10.1109/SNPD.2019.8935646.

[7] A . Dubovitskaya, Z. Xu , S. Ryu, M. Schumacher, F. Wang, "Secure and trustable electronic medical records sharing using blockchain, AMIA annual symposium proceedings, pp. 650–659, 2017.

[8] J. Nuansanong, S. Kiattisin, "The electronic medical record exchange using a Blockchain technology", Songklanakarin Journal of Science and Technology. 43 (2), pp. 335-343, 2021.

[9] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, J. He, "Blochie: a blockchain-based platform for healthcare information exchange", 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 49-56, 2018, DOI: 10.1109/SMARTCOMP.2018.00073.

[10] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data", IEEE Internet of Things Journal, 6 (5), pp. 8770 – 8781, 2019, DOI: 10.1109/JIOT.2019.2923525.

[11] G. Capece, F. Lorenzi, "Blockchain and Healthcare: Opportunities and Prospects for the EHR", Sustainability, 12 (22), p. 9693, 2020, DOI: 10.3390/su12229693.

[12] S. Popov, The Tangle. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf (accessed February 24, 2021).

[13] I. Ullah, G. D. Roode, N. Meratnia, P. Havinga, "Threat Modeling—How to Visualize Attacks on IOTA?", Sensors, 21 (5), p. 1834, 2021, DOI: 10.3390/s21051834.

[14] IOTA Foundation, Introducing Masked Authenticated Messaging. Available at: https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/, (accessed March 6, 2021).

[15] Law of Ukraine "On state financial guarantees of medical service to the population, Available at: https://zakon.rada.gov.ua/laws/show/2168-19?lang=en#Text, (accessed March 10, 2021).

[16] eZdorovya, Electronic health care system in Ukraine, Available at: https://ehealth.gov.ua/, (accessed March 10, 2021).

[17] PyOTA. Creating transfers. Available at: https://pyota.readthedocs.io/en/latest/transfers.html, (accessed March 12, 2021).

[18] IOTA Developer Essentials. Available at: https://iota101.info/, (accessed March 12, 2021).

[19] Y. Kliuchka, O. Shmatko, S. Yevseiev, S. Milevskyi, "Peculiarities of blockchain technology introduction in the field of healthcare: current situation and prospects", Information processing systems, 1 (164), pp. 33-44, 2021, DOI: 10.30748/soi.2021.164.04.