Complex & Intelligent Systems
https://doi.org/10.1007/s40747-021-00610-8

ORIGINAL ARTICLE

PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle

Sidrah Abdullah[1] · Junaid Arshad[2] · Muhammad Mubashir Khan[1] · Mamoun Alazab[3] · Khaled Salah[4]

Received: 9 June 2021 / Accepted: 26 November 2021

Abstract

Healthcare has evolved significantly in recent years primarily due to the advancements in and increasing adoption of technology in healthcare processes such as data collection, storage, diagnostics, and treatment. The emergence of the industrial internet of things (IIoT) has further evolved e-Health by facilitating the development of connected healthcare systems which can significantly improve data connectivity, visibility, and interoperability leading to improved quality of service delivered to patients. However, such technological advancements come with their perils—there are growing concerns with regards to the security and privacy of healthcare data especially when collected, shared, and processed using cutting-edge connected sensor devices affecting the adoption of next-generation e-healthcare systems. In particular, during the front-end and back-end data transfer in health information exchange (HIE) there exist a security risk in term of confidentiality, integrity, authentication and access control of the data due to the limited capabilities of IoT devices involved. In this paper, we investigate the use of distributed ledger technologies (DLT) to address such security concerns for emerging healthcare systems. In particular, we use masked authenticated messaging (MAM) over the *Tangle* to achieve secure data sharing within a healthcare system and provide a proof-of-concept of applying the proposed approach for securing healthcare data in a connected IIoT environment. Further, we have performed the evaluation and analysis of data communication against the metrics of encryption and efficiency in transaction time.

Keywords Digital healthcare · Distributed ledger technologies · Industrial internet of things · IOTA · Tangle · Masked authenticated messaging

Introduction

Healthcare has evolved significantly in recent years primarily due to the advancements in and increasing adoption of technology in healthcare processes such as data collection, storage, diagnostics, and treatment. Computing infrastructure is omnipresent within healthcare facilities. More recently, the industrial internet of things (IIoT) has emerged as a disruptive computing paradigm with applications across various domains such as smart cities [1–3], manufacturing [4,5], and healthcare [6,7]. In particular, the emergence of IIoT has further evolved e-Health by facilitating the development of connected healthcare systems which can significantly improve data connectivity, visibility, and interoperability leading to improved quality of service delivered to patients. Consequently, sharing of healthcare data, in the life of patients and users, has become ubiquitous [8,9] transforming healthcare from digital to intelligent [10]. E-health is the term often used exchangeably with telemedicine and

✉ Muhammad Mubashir Khan
mmkhan@cloud.neduet.edu.pk

Sidrah Abdullah
hafizasidrah@cloud.neduet.edu.pk

Junaid Arshad
Junaid.Arshad@bcu.ac.uk

Mamoun Alazab
alazab.m@ieee.org

Khaled Salah
khaled.salah@ku.ac.ae

[1] Department of Computer Science and IT, NED University of Engineering and Technology, Karachi, Pakistan

[2] School of Computing and Digital Technology, Birmingham City University, Birmingham, UK

[3] College of Engineering, IT and Environment at Charles Darwin University, Darwin, NT, Australia

[4] Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, UAE

Published online: 21 January 2022

telehealth. The term "telemedicine" mostly refers to clinical services from a distance, while the term "telehealth" covers a wide scope of health administration and health education. Both "e-Health" and "telehealth" can be considered as an evolutionary term for "telemedicine" [11].

However, such technological advancements come with their own perils—there are growing concerns with regards to security and privacy of healthcare data especially when collected, shared, and processed using cutting-edge connected sensor devices affecting the adoption of next generation e-healthcare systems. For instance, the use of wearable and embedded devices to aid diagnostic and treatment procedures is increasingly common [12,13] leading to concerns about privacy and security of patient data.

Although use of IoT to enhance diagnostic and treatment procedures has remarkably improved the quality of healthcare service; however, these data are also an attractive target for cyber attacks [14]. Generally, the data sent by IoT devices do not follow any end-to-end encryption and decryption scheme. Furthermore, as patient data are shared across different tiers of the healthcare system, achieving security and privacy of such data is a challenge [12,13]. Any disruption in transfer, update or sharing of data can lead to exposition of vulnerable patient data [15,16].

Also, healthcare sector is more prone to cyber security breaches as health data is considered more lucrative than credit cards on the illegal market [14,17]. Furthermore, regulations such as General Data Protection Regulation (GDPR) [18] has made regulations to protect individual's data, which makes data sharing onerous. In this research, GDPR is considered as it is one of the most recent, generic, and comprehensive frameworks that has been established to date. Additionally, it covers broader domains regarding user privacy and access to data. GDPR is mentioned here as an example. In comparison, other policies such as HIPAA, PCI DSS, SOX, and CCPA are domain-specific.

Distributed ledger technologies (DLT) exemplified by Bitcoin have evolved as a major technological advancement of recent times facilitating decentralized data collection and processing in a tamper-proof manner [19–21]. In this paper, we investigate the use of DLT to address security concerns for emerging healthcare systems. In particular, we use masked authenticated messaging (MAM) over the *Tangle* to achieve secure data sharing within a healthcare system and provide a proof-of-concept of applying the proposed approach for securing healthcare data in a connected IIoT environment. We present the design and development of a proof-of-concept for a smart healthcare system to enhance the trustworthiness of the system by facilitating secure data sharing across them.

In the previous studies such as [22–24], similar healthcare models on distributed ledger technology have been proposed. However, this paper emphasizes secure sharing of health data in the digital healthcare system [14,19,25,26] by exploring the potential of a DLT, IOTA Tangle [27], and its ability to cope with the limitations of blockchain technology. The objective of the research is to provide a decentralized framework that enables sharing and transport of health data in a secure and private environment by integrating the *Tangle* [28] which could support secure, fee-less, highly-scalable and granular medical data exchange. It primarily focuses on the transport of medical data to the *Tangle*. Masked authenticated messaging (MAM) is also employed to broadcast data to the *Tangle*.

Thus, there is a need for such a digital healthcare system that can meet the above-mentioned challenges and provides an immutable, secure, fee-less, highly scalable, and verifiable system that could gain the trust of medical entities. By implementing the healthcare system with distributed ledger technologies, the gap between healthcare systems and their challenges might be bridged. To address this, the designed framework offers a fee-less, and scalable system for the healthcare industry. It also deals with the security concerns such as confidentiality, accessibility and accuracy. The proposed framework keeps the data confidential by providing an extra encryption layer using MAM. It also enables the healthcare user to have access control over their data and share the data on their own accord. The data on IOTA Tangle is tamper-proof which maintains the credibility of the data.

This study brings contributions to the field of medical and healthcare industry. The demand for secure, private, and reliable digital healthcare has been around for a long time. Thus, by implementing this framework, the healthcare industry will be able to have a secure and scalable architecture for the communication of health data. Not only the users will have access control over the data, but the provided data will also be kept confidential. For medical professionals, this study will help them uncover patient's diagnostics with the help of shared medical history.

Contributions

The main contributions of the paper include:

(1) Discussion and demonstration on how the *Tangle* Version 1 (before Coordicide) provides improved security and privacy to the data sent by IoT devices.
(2) Design of a scheme for secure transmission of medical or health data based transferred through IoT sensors to the *Tangle* using masked authenticated messaging (MAM) communication protocol.
(3) Working "Proof-of-Concept" for transport of health data to a distributed ledger using masked authenticated messaging (MAM). MAM provides extra layer of security with its cryptographic functionality, thereby maintaining the integrity, authenticity, and confidentiality of the data.

(4) Evaluation of the current performance of *the Tangle* with and without masked authenticated messaging (MAM).

Paper organization

The rest of the paper is organized as follows. Section "Design goals" summarizes the use of technology within healthcare and outlines security requirements and design goals for an e-health system. Section "Related work" provides insights into the historical background and research in the area of blockchain for the IoT-based healthcare systems. The next section, Section "Background", of the research presents necessary background information and theoretical concepts related to distributed ledger technologies with an emphasis on *Tangle* and masked authenticated messaging (MAM). Section "Implementation" provides the information regarding the setup to collect performance data about the *Tangle*, its evaluation, and results. Sections "Methods" and "Evaluation" explains the implementation fragment and also discusses how the results are achieved. The last section concludes the paper. It also sets directions for future research work and recommends how this framework can be extended.

Design goals

The use of e-terminology began in the 1990s with the advancement in Information and Communication Technology (ICT) [29]. The term e-Health was coined in the year 2000, but since then it has been used widely [30]. The World Health Organization (WHO) [31] has described e-Health as "the use of ICT for health" [32]. E-Health is defined as an amalgamation of information and communication of that information in terms of sharing and storage of healthcare data. The distribution of electronic health records (EHRs) is an important application of healthcare information technology (HIT) [33].

The idea of EHRs has been around for more than a decade [34]. Recent technological advancements have also revolutionized and reshaped the storage, processing, and access control of the health data [33]. With the shift in status quo, digital health information is prone to misinterpreted health information and unreliable data that could put a patient's life to risk [35]. Furthermore, unauthorized third-party access to health data generated from smart devices and wearable devices might put sensitive information at risk [36]. In addition to that, quality medical devices, smartphones, and sensors [37] are required to provide accurate health data and the validation of these devices is also necessary [38].

EHR has numerous benefits, but there are several challenges associated with the establishment of such a system [33]. The possible challenges that are faced in the development of e-Health are security and privacy [39] which have hampered the deployment of existing e-health systems [40]. The reason is that these systems collect sensitive information that may influence a patient's life and social status [41]. Furthermore, with the advancement in e-Health solutions, more focus has been positioned on accomplishing the security and privacy of the health data as digitizing them will lead to an array of attacks such as denial of service, insider attacks, and information leak [42]. Thus, several organizations have set up guidelines for the administration of healthcare information for achieving the desired level of security and privacy [40]. The first act that was put forward by the US Congress in 1996 as federal law was Health Insurance Portability and Accountability Act (HIPAA) [43]. Another such act is the General Data Protection Regulation act which was put forward by EU law in 2018 [18].

There are several requirements of the e-health system. In this section, security and privacy requirements are discussed for a healthcare system, which includes authorization, accuracy, confidentiality, integrity, and availability of data.

Security

Security can be described as an extent to which shared personal information is authorized [39]. It deals with the protection of data in terms of authorized access to the health information [44]. The security of data emphasizes confidentiality, integrity, and availability of medical data which is managed by e-health system [45]. Confidentiality of data is also a prime factor in e-health. Medical data contains much sensitive information like medical history, behavior problems, and various issues that should be kept confidential. Illegal access to such data can be dangerous for the mental and physical health of a patient [39]. Accuracy in e-health deals with the exactness and correctness of data and confirms that the data is free from faults [44]. For a secure healthcare network, this paper focuses on confidentiality and authorization of medical data.

Confidentiality Confidentiality means that the data is kept hidden. Since health-related data contains sensitive information of a patient, such as the history of illness, general information, diagnostic information, treatment information, etc, hence, it should remain confidential.

Authorization Another critical factor in a e-health system is the authorization of the data. The patient has the access to their health data and they have complete authority over it. This authority also includes the right to share their data, and the right to revoke the access that is granted previously.

Privacy

Privacy can be described as a right of a person to communicate their data [39]. With the rise of cyber-fraud in the

digital era, the health data of the user is at risk. The privacy guidelines are formulated with the idea of defining the related factors: patients' privacy limits and rights. Moreover, it defines the importance of the protection of any part of the data that exposes the identification of a person not bounded to name, address, contact number, etc. because that health data are directly related to the patient's privacy. Whereas, liberty is given to any data that is unable to be linked to a person and no limits have been placed upon the disclosure of such information. There is also a factor of consent exception that enables the service provider to use the medical data of a certain person during a health crisis such as when a patient is in a coma or any other life-threatening scenarios [43].

Cloud computing notably contributes to the success of e-health as it can provide a framework to overcome the problems regarding the management of health data taking into account that the cloud infrastructures maintained by third parties may have some curious users that might be interested in the data is being stored. Hence, the issues regarding confidentiality, integrity, and privacy concerns have been heightened on the stored data [46,47]. Furthermore, the flexibility of e-Health schema orbits is around the capability of efficient and selective sharing of medical data amongst related entities.

In the framework of e-health, blockchain appears to be a secure and decentralized platform. Blockchain has changed the trend of storing and sharing health data. It controls the security and accuracy of the data whilst reducing maintenance cost [48]. The primary advantage of blockchain in healthcare organizations is the administration of (electronic medical records) EMRs. The patient medical data are stored in a distributed manner, without full access to that medical data [49]. These factors make the blockchain a platform that reduces cost and increases security [50]. However, there are certain limitations to blockchain technology as well, as discussed in Section "Limitations" which makes the *Tangle* a better choice for IoT-based e-health solutions.

There is a requirement for a framework that can deal with existing security and privacy challenges, growth in the number of users as well as reduced cost to administer processing needs and control capabilities.

Related work

Blockchain has been able to address prime concerns of privacy and security in digital health care systems. Private information in healthcare is highly sensitive, but it needs to be shared among required personnel as well. Blockchain technology provides fast, secure, accountable and transparent ledger for secure and trustable electronic medical records (EMR) systems. In this paper, the authors, in collaboration with Stony Brook University Hospital, have proposed a framework on management of EMR of cancer patients. They have used the permissioned blockchain to manage the health data. Since it is strenuous for patients to provide continuous treatment data, a model was designed to provide consent management system that could ensure availability of data to concerned entities. This permissioned model with verification also ensures that only concerned entities enter the system while providing scalability and integrity of the data [51].

With the shift in technology, the focus is shifting from electronic medical records (EMRs) to sharing of health data real-time generated from different sensors. In this type of scenario, privacy and confidentiality are of paramount importance. However, scalability and interoperability of data can not be compromised either. To handle this dilemma, the authors in this research have taken a dynamic outlook on EMRs and EHRs. They have proposed a system which not only highlights a secure solution, but also guarantees scalability. They have implemented the Ethereum client on blockchain technology [52].

Similar blockchain architecture for storing health record was proposed by the authors in [53], in which they have discussed the dilemma between privacy and accessibility of patients' records. They have implemented a framework of blockchain technology integrated with smart contracts. The patient will have the ownership of their data, while the physicians can read it. Furthermore, this whole scenario is controlled by a discovery system, which also keeps an eye on the events of the blockchain. The proposed architecture to access electronic health records (EHRs) ensures data privacy and accessibility [53].

Research by Dias et al. also focuses on the issue of access control of patients' records in blockchain technology. The crucial part of system security—access control - determines what data is available for whom. The authors discus that current systems that share access do not guarantee integrity of data. The authors have proposed a framework that employed consortium blockchain and enables interested parties to access e-Health whilst maintaining integrity. They have designed a state machine for storing the states of access control. The three states are: Access Policy, Individual Authorization State and Record Life Cycle [54].

As the increase in data generated by IoT devices and sensors, logging of transactions is facing a threat. The Griggs et al. have taken a more advanced perspective on patient data by analyzing security concerns of IoT devices used in health data. They have used Ethereum blockchain based protocol, in which IoT sensors communicate with smart contract implemented smart device. That device is responsible for maintaining records of transactions on the blockchain. The proposed design, according to authors would handle security vulnerabilities that were occurring previously [55].

From the previous discussion on existing work done on maintenance of electronic health records (EHRs), electronic medical records (EMRs) and personal health records (PHRs)

on distributed ledger technology, it can be seen that many experts have presented their solutions, protocols, frameworks and architecture to tackle two prime concerns, i.e, privacy and security of stored data. However, as discussed in Section "Background", blockchain technology does not provide feasible solution for scalability. With the advancement in internet of things (IoT), hundreds and thousands of devices are becoming a part of this system. Similar is the scenario in IoT for medical and health related data. For this purpose, the authors, in this research, have proposed a framework in which IOTA Tangle is used as a ledger for storing medical data. They have also used masked authenticated messaging (MAM), a communication protocol. This extension of IOTA tangle enables users to send and receive encrypted data from a wearable device [22].

Similar framework was proposed by Zheng et al.. In this framework, they aim to develop a secure, fee-less, scalable and tamper-resistant health data sharing system over IOTA Tangle. They have also introduced Raspberry Pi as the gateway to share data from sensors in IoT system. They have concluded that this design could solve several of the problems that blockchain-based technologies have faced [56].

An extended framework of [22] was proposed in [23], in which the authors have extended their research. In this research, they have developed a General Data Protection Regulation (GDPR) compliant "Proof-of-Concept" system for health data exchange. They have proposed two designs: one is solely based on public IOTA Tangle, while the other design is based on the combination of public IOTA ledger with InterPlanetary File System (IPFS) cluster. They have done the analysis of both the designs and compared them in terms of data reversal, data linkability, processing time, file size compatibility and overall system complexity. Also, they have taken blood glucose data as the test data for the system [23].

However, the IOTA-based solutions did not consider the security aspects of IoT applications. Furthermore, the calculation of latency while integrating IoT devices with the *Tangle*. Hence, our proposed technology is built on top of the classical IOTA protocols, and majorly focuses on two aspects: latency while Integration of IOTA with IoT devices, and the achievement of security by Setting up a secure communication medium using the masked authenticated messaging protocol.

Background

Blockchain

Blockchain, a type of distributed ledger technology (DLT), has been trending recently since its popular emergence after 2015. Blockchain is a technology that enables moving digital coins or assets from one individual to another. The first application of DLT appeared in 2008 with the development of Bitcoin [57]. It was first proposed by Nakamoto in 2008 and implemented in 2009 [58]. As represented by Fig. 1, a blockchain is a public chain of digital data or blocks [59], usually consisting of transactions. The records are added in chain one after another, and the nodes in the network have their copy of the transactions [60]. There is no central controller and the data on blockchain is tamper-proof [22].

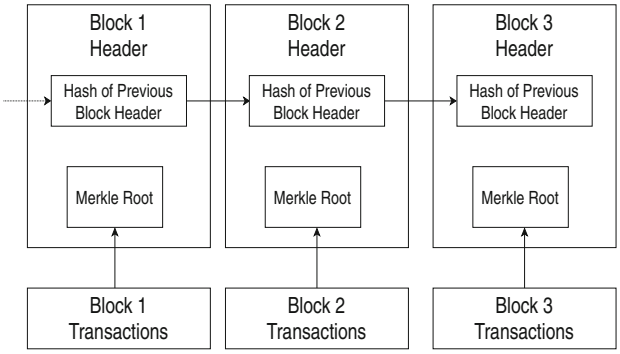


Fig. 1 Simplified blockchain

Table 1 Centralised Database to distributed ledger

Technology	Control
Centralised database	Single entity
Traditional distributed database	Single entity
Distributed ledger technology	Multiple entity

Table 1 illustrates the differences between traditional databases and distributed ledger technologies.

While blockchain does not allow any malicious interference from outside the network, any node, that is present in the network can be suspected to cause malicious changes to previous, historical transactions. This issue of an adverse node is tackled by cryptographic primitives, or one-way hash functions [61].

Transaction

Identical to any distributed or online transaction processing (OLTP) [62] transaction that acts on some data, blockchain transactions are the same. In the blockchain, a transaction represents an exchange of money or assets [63] between two users, and that transaction is stored in a block [64].

Blocks

Figure 2 illustrates the structure of a block in a blockchain network. There are two parts of a block: *block header* and *block body*. The block header consists of:

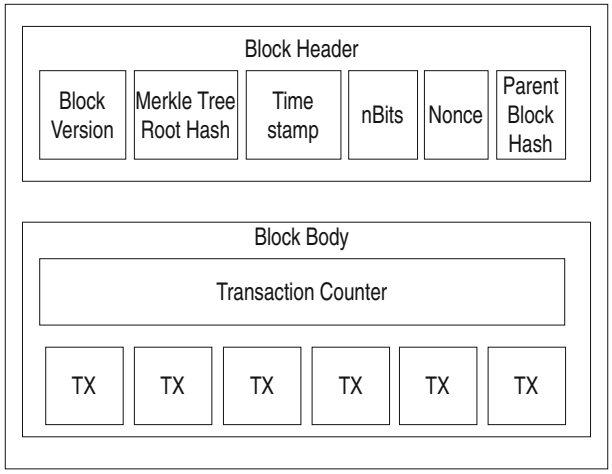


Fig. 2 Block structure

(1) Block version: it indicates which block validation rule to follow
(2) Merkle tree hash: it consists of the hash value of all the transactions in the block
(3) Timestamp: it stores current time in seconds
(4) nBits: target threshold of a valid block hash
(5) nonce: nonce is a 4-byte field. It starts with 0 and increases as the hash increases
(6) Parent block hash: it is a hash value that points to the previous block in the chain

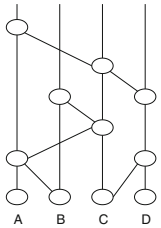
The block body consists of transaction counter and transactions. Block size and size of each transaction determine the maximum number of transactions that a block may contain [65]. The authentication of the transaction is validated using asymmetric cryptography mechanism [66].

Limitations of blockchain

The technological needs of IoT cannot be met by blockchain [67] as it has some limitations which intercept it from being used as a common platform for IoT data.

Transparency The first challenge found in blockchain is *transparency*. Since everything is visible to everyone on blockchain [68–70], open data are considered blockchain's limitation. This becomes very critical in the digital healthcare scenario, where personal medical records are highly sensitive. Although updates made on blockchain are immediately available across the network to all the concerned parties, it raises the following questions: Can all the involved stakeholders in the healthcare scenario be considered controllers of data? How does Article 22 of GDPR, which grants the users protection against automated processing of their information can affect the blockchain?

Fig. 3 An example of Hashgraph



Scalability and speed The second challenge is scalability and speed [19]. Transaction times in Blockchain are often long, which in turn affects the size of the blockchain [71]. For a transaction to be final on the blockchain, it has to wait for 6 blocks to be added to the longest chain [72–75]. This issue of speed and scalability is not suitable for scenarios of medical data in the IoT domain. As the data is generated rapidly in the IoT health domain, using blockchain technology might cause a delay in the processing of that generated data as it is harder to scale due to its consensus method. An optimal blockchain that could balance the scalability is yet to be found.

Transaction fees The third challenge is *transaction fees*. This concept in blockchain that a node needs to pay some fees for the transaction is also a notable drawback. The transaction fees could be financial or it could be toke based. For instance, the transaction could be in the form of a bitcoin, or it could be a gas price. For such a large scenario, a model with high fees will not suffice as. It is certainly not a wise decision to pay higher fees than the data itself. Since the transaction fees are an incentive for the block creators, getting rid of the transaction fees in blockchain structure would not be a suitable decision [28].

Hashgraph

Hashgraph is a decentralized ledger by Hedera Hashgraph Council [76]. Hashgraph attempts to solve the obstacles of blockchain, such as security, scalability, and performance. Hashgraph is like a blockchain, but it permits the growth of new nodes that link back to the chain of nodes.

This DAG uses the probing technique. It is based on the human mechanism of sharing information: gossip. One network node shares the complete information with other randomly selected nodes in the network. These nodes combine all the information received from several other nodes and add it to the transaction. However, it has only been implemented in a private ledger. Hashgraph uses the BFT algorithm and discards proof-of-work which has increased the overall efficiency. A BFT or Byzantine Fault Tolerance algorithm is a feature of distributed ledgers to reach the consensus on some value. The gossip mechanism of Hashgraph is much faster than blockchain's proof-of-work mechanism and reduces communication barrier [77].

The user has to perform two roles in the Hashgraph. The first role is to submit a new transaction. The second role is to

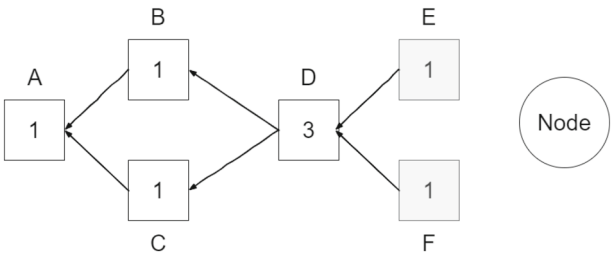


Fig. 4 Transactions in the tangle

randomly select other users or nodes to whom they will share the information [78] Fig. 3 is an example of Hashgraph.

The *Tangle*

After the development of blockchain as the most widely used distributed ledger technology, two major problems appeared. The first one was miners, and the second and most important problem was scalability [28]. To overcome this problem, another distributed technology, known as the *Tangle*, was introduced by Popov [28]. It was created with an intent to solve the problems of post-quantum security, scalability and centralization as well as to focus on the Internet of Things (IoT) [24].

The *Tangle* is a distributed ledger similar to blockchain. It is based on the mathematical concept of Directed Acyclic Graph, or DAG [79]. So the *Tangle* is a graph (the ledger for storing transactions) formed of transactions in a directionally significant way (pointed in one direction). And those transactions can not be cyclic. The tangle is a zero-fee, zero-miner, zero-block [27] technology that has distributed consensus mechanism and uses an algorithm called Markov Chain Monte Carlo (MCMC) as its Proof of Work (PoW) mechanism [28]. Zero-fee means that no monetary transaction fee is required to process the transactions. Zero-miner means that there are no powerful machines like miners in the *Tangle* that would mine the transaction. Instead, it distributes transaction confirmation among all users. Additionally. zero-block implies that it does not have transaction blocks like blockchain. The *Tangle* has transaction bundles that validate the other two transactions which makes it scalable.

Architecture of the *Tangle* platform

The Tangle architecture consists of several layers and components such as the transaction, client nodes, APIs, and network types. The Comnet is the most widely used network that is used for the purpose of testing and development. It is also used in this proposed framework [80].

Another component is the *Tangle* transaction bundle. The basic building block of one transaction comprises a transaction hash, value, confirmation status, tag, address, bundle, nonce, signature message fragment, and address of parent transaction. Additionally, the *Tangle* also has an API that developers can use to test the transactions and for building applications [80].

Components of the *Tangle*

Figure 4 shows how the Tangle transaction works. In the above figure, node A is Genesis. Genesis is the first transaction in the ledger. Unconfirmed transactions at the edge of the graph are called tips. In the above case, node E and node F are the tips.

A **node** is any computer that propagates transactions, also known as a site. The next transaction creates an edge that validates two previous transactions. The edges are created as the new transactions are added. Every new transaction is linked to the first transaction. Every site gets a personal weight [28]. The node must validate two transactions by solving a puzzle. That puzzle is similar to hashcash [81]. The central node in the *Tangle* is called *Coordinator*. This node is responsible for electing the tips to approve. The approved tips are called "Confirmed" transactions. The resultant transaction of the process of approving tips is called "Milestone". This new transaction can now approve two other transactions [24].

In the *Tangle*, the transactions are also capable of carrying the message. They consist of 2673 trytes and can transfer both the message and IOTA tokens [82]. However, since all the transactions are visible to everybody, it is not feasible to share content that requires confidentiality [24].

The *Tangle* is still in "Beta" status. Hence, the rules of tip selection have not been released yet for the public as users with malicious intents and adequate computational power might perform a malicious activity such as double-spending [83].

Table 2 shows the comparison among blockchain, hashgraph and the *Tangle*. From this table, it can be seen that DAG-based DLTs are appropriate for IoT-based mechanisms especially with their lower transaction fees and consensus mechanisms [84]. Furthermore, from the two DAG-based mechanisms. the *Tangle* is more suitable for healthcare scenarios as it offers an extra layer of encryption with the help of its MAM protocol, which is discussed in the next subsection. It is specially designed for IoT scenarios and is immune [28] to quantum attacks. Thus, the *Tangle* is more suitable for e-health implementation as it allows scalability, quantum security, and offline capabilities [85].

Trits and trytes

The *Tangle* system utilizes ternary system (a system with three values) instead of binary system (a system with two values). The ternanry system can be balanced $(-1, 0, 1)$ or unbalanced $(0, 1, 2)$. The tangle utilizes balanced ternary

Table 2 Comparison of DLTs

DLT	Scalability and speed	Transaction fees	Vulnerable to quantum attacks	Copyright	Latency issue
Blockchain	Low	High	Vulnerable	Open source	High
Hashgraph	High	Low	Vulnerable	Patented	Reduced
The *tangle*	High	No cost for validating transactions	Immune	Open source	Low

system with trits instead of bits. Hence, according to numeral system [86]:

$$1\ Byte = 2^8 = 256\ combinations$$
$$1\ Tryte = 3^3 = 27\ combinations$$

The maximum value that a tryte can have is 13 with 27 different combinations. The tryte alphabets in the *Tangle* uses ASCII sequence ranging from A to Z, and starting with number 9. Hence, it is strictly recommended not to use the same address for sending value once it has been used for the transaction [86].

Seeds and addresses

IOTA seeds, addresses, and hashes are trytes that use tryte alphabets. IOTA seed consist of 81 trytes and each tryte has 27 combinations, so IOTA seed has ($27^{81} \approx 8.71 \times 10^{115}$) combinations, while bitcoin has only ($2256 \approx 1.15 \times 10^{77}$) combinations [86]. With this unique seed, IOTA addresses are generated where the first address has 0 key index number, the second address has 1 key index number, and so on [86].

After the address has been created, the security levels ranging from 1 to 3 are assigned. This indicates how long the private key would be in terms of trytes. Security level 1 has 2187 trytes, security level 2 has 4374 trytes and security level 3 has 6561 trytes of private key and signature length. By default, level 2 security is used.

Masked authenticated messaging

Masked authenticated messaging (MAM), a second layer data communication protocol and an experimenting module, enables a node to publish or fetch data over the *Tangle* [87,88]. It was developed by IOTA foundation [24]. The data in MAM is in encrypted forms, as an RSS feed. Messages can be sent anytime over IOTA using MAM. Whenever the message is published using MAM, a channel is created [56]. The message will be received by the node that is subscribed to that MAM channel [87]. Since MAM transactions are stored in the *Tangle*, it contributes to the hashing power in the ledger and maintains data integrity. MAM adds an extra layer of encryption onto the *Tangle*, which enables only the subscribers to decode the encrypted message [24]. Furthermore, MAM provides the possibility for sensors and other IoT Devices to encrypt and data streams before sending it to IOTA Tangle.

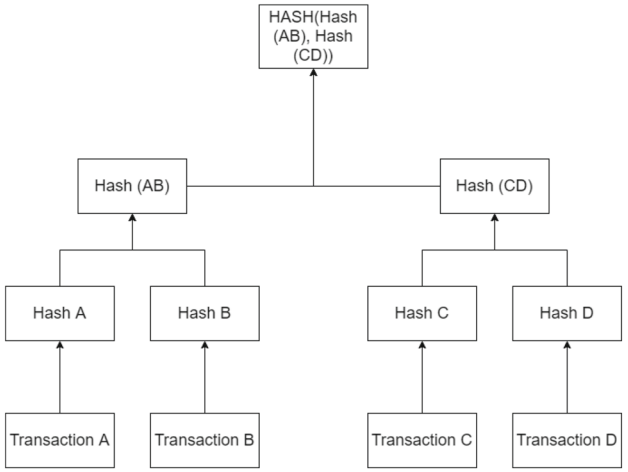


Fig. 5 Merkle hash tree

Since the data in IOTA are decentralized (any node can send a message to any address), there is a risk that a message transaction might contain malicious data sent by any node to hijack the channel. This is where message signing comes in which encrypts the data. The encryption system used by Masked Authenticated Messaging is based on a Merkle Hash Tree (MHT) based signature scheme [56]. The ID of the MAM channel is determined by its root of the Merkle Tree. The next root is referenced by the message in the existing Merkle Tree [87]. It is a type of tree in which the tree is generated bottom-up [89]. The leaves of the Merkle Trees are hashes of the amalgamation of the seed and index number of each leaf, which starts from i = 0 [90].

Figure 5 shows the formation of the Merkle tree for transactions A, B, C, and D. Hash is the cryptographic hash function. The last node in the tree is called a leaf. A One-Time Signature (OTS) scheme is used to enable faster signing. Each leaf in the Merkle tree is an OTS scheme.

MAM stores its data in the form of a bundle. Figure 6 shows the structure of the MAM bundle, which consists of two sections: Signature and MAM. The signature section is concerned with validity checking. MAM section contains

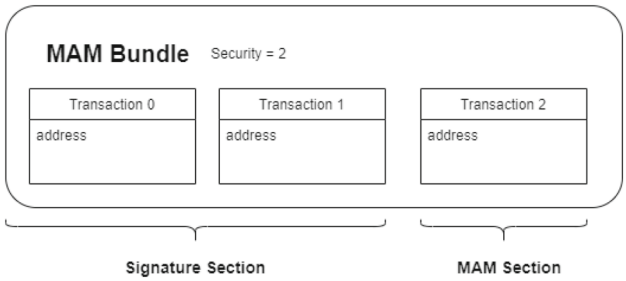


Fig. 6 MAM bundle

Table 3 MAM privacy modes. A hash function is used to generate private key from user's seed

Mode	Channel ID	Decryption key	Authorization key
Public	CK	CK	–
Private	H(CK)	CK	–
Restricted	H(AK ‖ CK)	CK + AK	AK

the actual message [90]. In this figure, the security level is 2. Hence, the first two transactions, transaction 0 and transaction 1 contain the Merkle Tree signature. Transaction 1 contains the actual message.

Figure 6 shows MAM bundle with two transactions in detail. As it can be seen from the figure the MAM bundle consists of information about siblings of the leaf as well as branch index.

MAM has three different privacy and encryption modes [90]. They are:

Public In this mode, the address transaction is the Merkle tree's root [56] and that address serves as both the channel ID and channel key [22]. Any node can fetch this message and decode it using the transaction's address. This type of mode can be used for public announcements mostly [87].

Private In this mode, the address of the transaction is the channel ID. It is encrypted and not meant for the public, i.e, it can not be decrypted by any node. A node must be provided with root to encrypt the stream [87].

Restricted In this mode, an authorization key, also known as *side key* [56], is concatenated with the channel key [22]. It is like a private MAM with an authorization key on top of it [87]. It allows the publisher of MAM message to revoke the access anytime [56]. The message broadcaster has the authority to revoke access anytime by altering the authorization key, which disables the subscriber from receiving future broadcasts [22].

Table 3 [22] shows three modes of privacy in MAM. It also shows the control visibility and access to channels. CH stands for channel key and AK stands for authentication key.

MAM works on two main functions: publish and fetch. To publish the data on MAM stream, first, the *root* of the tree needs to be generated. In public mode, the address of the tree is the hash of its root, i.e *address* = *hash(root)*. After that, the message that is to be posted is converted into *trytes* and stored as a *message*. It also contains the *address* to the next generation, known as *next root*. *Branch index* and *Siblings* are also calculated. The combination of message, nextRoot, branch_index and Siblings is then encrypted with *root* (in Public mode) or *sideKey* (in Restricted mode). To fetch the data from MAM, *root* (in Public mode), or *root* and *sideKey* (in Restricted mode) is required. The *address* is calculated from *root*. After that, the MAM section is decrypted. From decrypted data, *message, nextRoot, branch_index, Siblings* is received [90].

Thus, masked authenticated messaging provides a fine layer of data integrity and access control management which could be beneficial in many IOTA use cases.

The next section elaborates the setup and evaluation process carried out to test several key performance parameters of the *Tangle* and discusses the obtained results.

The proposed scheme

Discussion

The proposed framework is a "Proof-of-Concept" of the research objectives. This framework stores medical data on IOTA *Tangle* in encrypted form, which provides complete privacy and security to the stored data. The sharing of data over IOTA *Tangle* is done using Masked Authenticated Messaging (MAM) which also provides different modes with different levels of security. Sample health data are collected using a simple android application, which has been designed using Google Fit API [91]. A web interface has also been designed to enable concerned entities to view health data. The android phone is used because Google Fit API can be utilized easily for the purpose of health data. The implementation could also work for a phone with any other OS, provided that the health apps allow utilization of their APIs.

The proposed framework is a simple design at the initial level to demonstrate the deployment of IOTA Tangle and MAM while collecting real-time health data from the application. This has been done for the basic understanding of research.

Two main roles are designated in the system. The roles are publisher and fetcher. The publisher can be any individual who wishes to publish their health data from their smart device. The fetcher is any healthcare personnel that intends to view the published data. A user can be a publisher and fetcher at the same time.

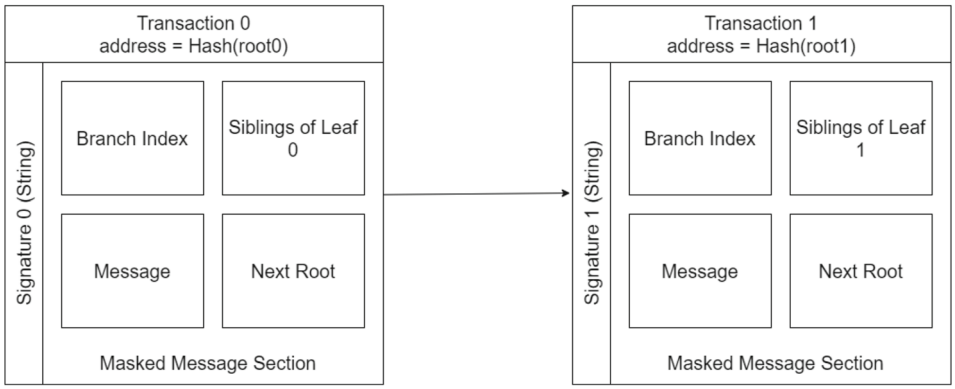


Fig. 7 MAM bundle with two transactions

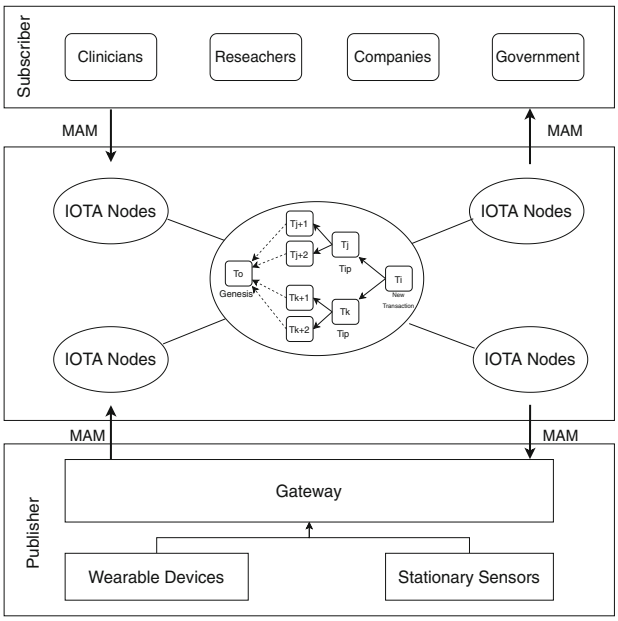


Fig. 8 Proposed architecture

The implementation of the proposed framework presents a proof of concept of sending data securely from a smart device to IOTA Tangle, which is done via gateway. However, for publishing the data to IOTA Tangle from smart devices such as smartphones, smart watches and smart fitness monitoring devices the proposed setting has to be adapted as per the technical requirements of these devices. For this purpose, a computer or Raspberry Pi [92] can be used as a gateway layer.

Research questions The system was designed with the following questions in mind:

(1) Do the users have control of their health data in the existing healthcare systems?
(2) Do the existing healthcare systems provide GDPR compliance over the health data?
(3) What are the optimal solutions for providing privacy and security in medical and e-Health applications
(4) Is the health data that is shared over secure and private?
(5) Can the concerned entities view the health data with a user's permission?

Identification of software requirements Before the development of the framework, thorough research was carried out and several IOTA libraries were tested. Several different libraries were existing on the IOTA Foundation's website for the implementation of IOTA like C library, Go library, Java library, JavaScript library, and Python library. However, the MAM package was included in the JavaScript library. For this purpose, the JavaScript library was chosen for the implementation of MAM on IOTA Tangle. Out of three modes of MAM, the restricted mode was chosen as it enables the user to revoke access anytime they want to.

After the identification of the language, the next important step was to identify the code editor. VS Code editor was found to be a suitable choice. Another important step was to decide the choice of the operating system for mobile applications. For this step, the android operating system was chosen which has to work in conjunction with Google Fit [93] and Google Fit API.

The web API was designed using Node.js running on a machine with Windows 10, having Intel Core i3, a 3.76 GHz processor, and 4 GB RAM.

Proposed design

The proposed framework addresses the research question. The model was designed by keeping those questions in mind. Figure 9 shows the working of the "Proof-of-Concept".

Detailed architecture and prototype of the proposed framework is shown in Figs. 8 and 9.

The application was designed for the android smartphone which fetches data from the Google Fit application using Google Fit API. This customized application for smartphones allows the user to send their health data such as calories, heart points, and the number of steps to a remote server. In this case, Firebase [94] serves as a remote server. The data is then fetched from a remote server and published to IOTA Tangle.

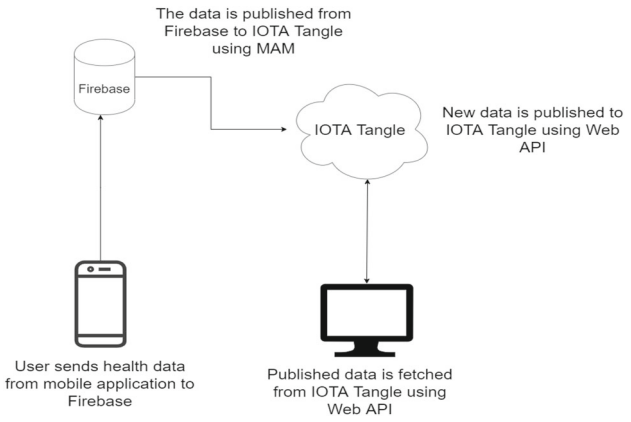


Fig. 9 Proposed framework

In this framework, the android smartphone is a part of the sensing layer. The computer system (running the web interfaces) plays the role of a gateway. For security, the user's health data is published using MAM restricted mode.

To subscribe to that published data, the concerned entity only needs to know the address of the channel and an authentication key (also known as a secret key). This is shared by the user using QR code [95]. The QR code is generated consisting of the user's channel's address and authentication key. The advantage of using restricted mode is that user has an authority to revoke access anytime they want to.

Extended scheme

An extended scheme was designed to refine the experiment and evaluate the results. Few changes were made to the existing scheme which includes the addition of Raspberry Pi 3B+ to the architecture as a master node. Additionally, the latency tests were carried out on the latest Comnet.

The IoT device (Raspberry Pi 3B+), in this scenario, sends data to the *Tangle*. Since Raspberry Pi is capable of processing data from the sensors attached to them and then sending this data to the Hornet node or Comnet Node WiFi for attaching it to the *Tangle*, it acts as a master node. However, other IoT devices such as sensors are not capable of doing the same. Hence, they can forward the data to the gateway layer via Bluetooth or WiFi, or Arduino serial communication protocol.

Setup and arrangement of hardware

The setup and arrangement of extended scheme was refined on the basis of existing framework. The modified scheme can be seen in the Fig. 11. For the purpose of experimentation, a Raspberry Pi has also been added to the architecture. It is not only capable of sending data to the *Tangle*, it can also server as a gateway layer for the devices that are not capable of performing transactions on Hornet.

System and Software Specifications For the extended experiments, some modifications were made to the current archi-

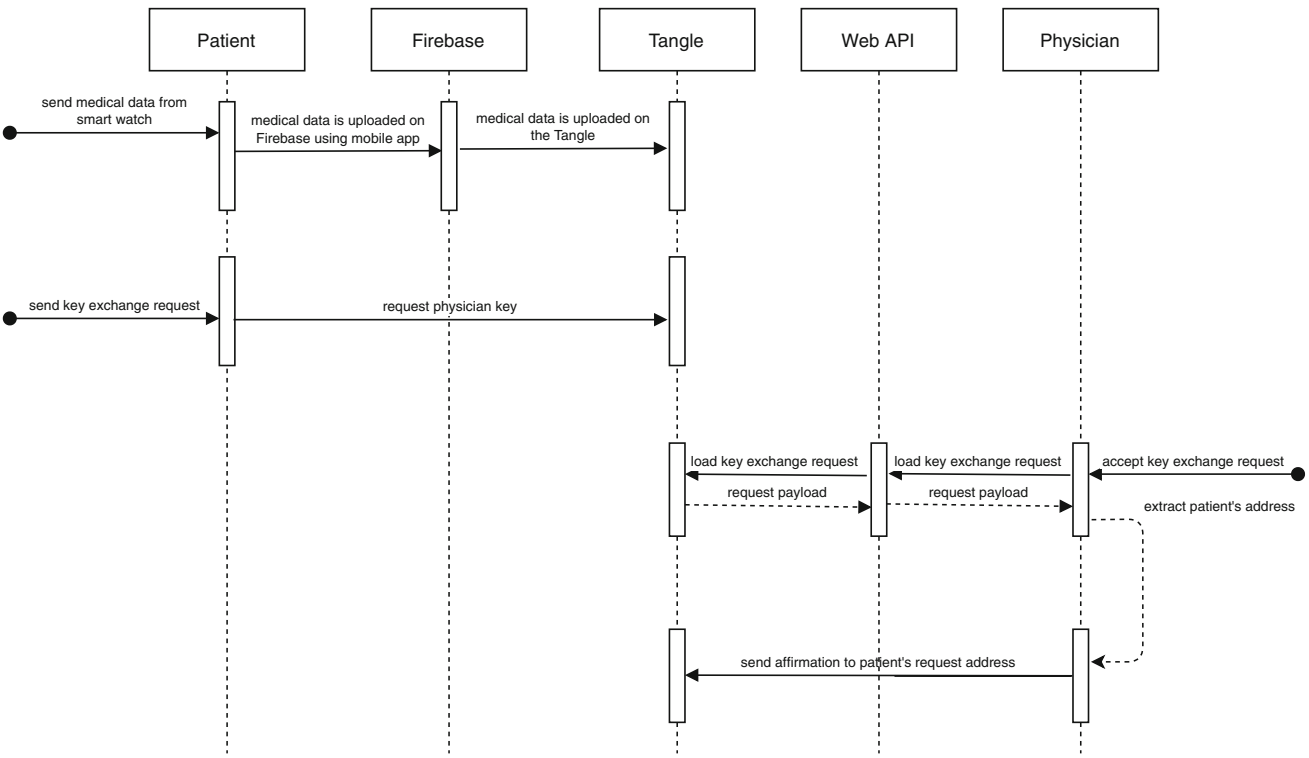


Fig. 10 Steps for the remote key exchange in the proposed system

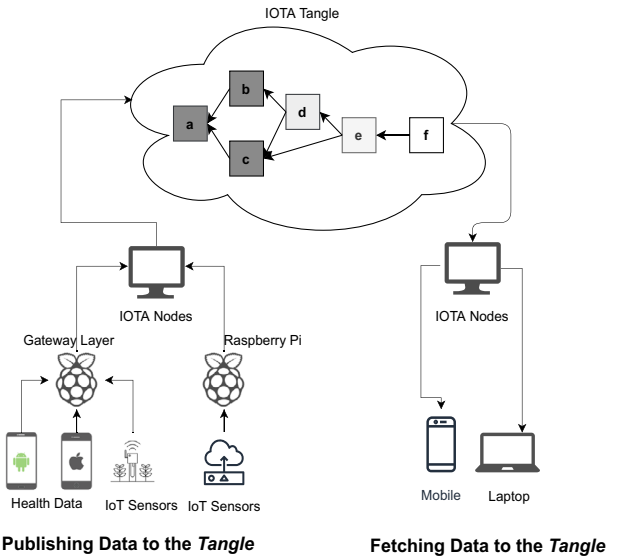


Fig. 11 Extended framework

Table 4 System and software specifications

Purpose	Name of Software and version
Node End-Point	Ubuntu 20.04.3, 8 GB RAM, 512 GB SSD
Browser	Google Chrome
IDE	Visual Studio Code
Language used for development	JavaScript
IoT device used	Raspberry Pi 3B+

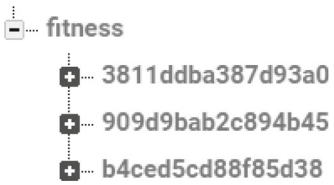


Fig. 12 Device information stored by device Id

tecture. Two new nodes were setup. One was connected to Comnet, and the other one was Hornet running in a Docker container. Table 4 shows the system specifications of the revised architecture.

Method

In the feasibility study of this proposed framework, the data was broadcasted using MAM protocol in restricted mode. This test was carried out on 5 android smartphones with different android versions. However, all of the versions were above android 5.0. This test was carried out for approximately 10 days.

Consider the scenario where users or patients intend to share their health data with physicians or any other medical

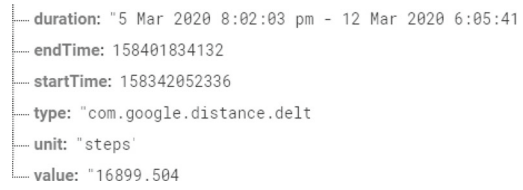


Fig. 13 Stored data in JSON format

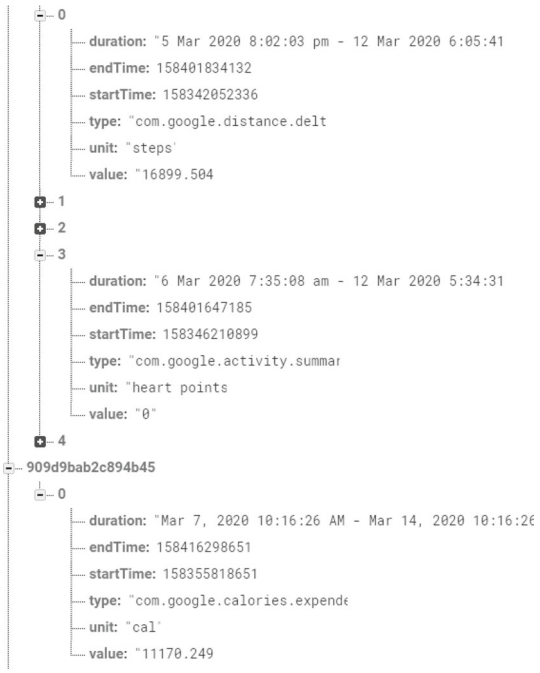


Fig. 14 Only the data that is shared by the user is fetched from Google Fit using Google Fit API and stored in Firebase

entity. For this, they will have to publish the data to Firebase first.

Figure 12 shows the storage of health data by device number. The data is stored in JSON format in Firebase, unlike relational databases, where data is stored in tabular form.

Figure 13 shows the JSON string. From Fig. 14, it can be seen that the user had control over what data they intend to share. The first device (device number: 3811ddba387d93a0) has shared its calories, number of steps as well as heart points.

But, the second device (device number: 909d9bab2c894b45) has only shared calories.

This also highlights the right of access (mentioned in GDPR) of the person to whom the data relates. This data is then published to IOTA Tangle using a Web API. OpenSSL protocol is used to ensure the safety of the seed. To check whether the data has been published to IOTA Tangle or not, IOTA MAM Explorer is used.

After publishing the data, a QR code is generated consisting of *address* and *side key* as shown in Fig. 15. Now, that patient can share the QR code with their physician to give them access to view their data.

YJTVJNTLIRASUOKNQBZAQJMKIUJYNDKDFR
LQRANZXKHUNTYNZNKICTDROLRCQPSABF
MFBLBQLFUGXIJTZVERYSECRETKEY

Fig. 15 Address and secret key shared using QR code

Similarly, published data can be fetched from IOTA tangle using the developed web API.

IOTA Devnet [96] was used to publish and fetch data from IOTA Tangle. At the beginning of the research, IOTA Devnet was supported by IOTA Foundation. However, it no longer supports Devnet and has switched to Comnet, so the system was also switched to Comnet. The Node.js [97] scripts for publishing and fetching data from IOTA Tangle using MAM are available [98,99].

Evaluation

This section describes the setup used to append the transaction to the *Tangle*. It also describes the preliminary results of this experiment. This study will provide the basis to discuss the practicability of implementing healthcare applications on IOTA.

Setup

A basic setup consisting of a public node was created to evaluate the transaction time in the *Tangle*. The public node at https://nodes.thetangle.org:443 (Node A), was hosted in Ashburn, USA. And a private node (Node B) was hosted in North Virginia, USA.

The hardware employed to test the trials of the public node is a 2 core i3 CPU running at 2.40 GHz, with a 4 GB RAM and 500 GB SSD disk for storage. The private node has been set up as an E2 instance using Amazon AWS [100].

The official IOTA Python API PyOTA [101] is used to add transactions with a payload of different lengths and their transaction writing time is assessed. An IOTA transaction has a payload length of 2187 trytes. If the payload size in a transaction exceeds 2187 trytes, then the transaction is segmented into two and then added to the *Tangle*. For this research, two payloads of different lengths were considered: *m* with 1399 trytes and *n* with 2373 trytes.

Two different scenarios, appending transactions and appending masked authenticated messages, have been considered. Their details are given below:

(1) *Append transactions to the Tangle:* For this scenario, the tests were conducted in two phases. First, the overall delay of adding these transactions to the Tangle was calculated with 100 trials. After that, again for a set of 100 trials, the delay measurement was partitioned into "tip selection", "attach to tangle" and "broadcast" operations.

(2) *Append MAMs to the Tangle:* The test was conducted for a set of 100 trials measuring the delay of appending MAMs to the Tangle partitioned in terms of "encoding", "broadcast" and "get message" operations.

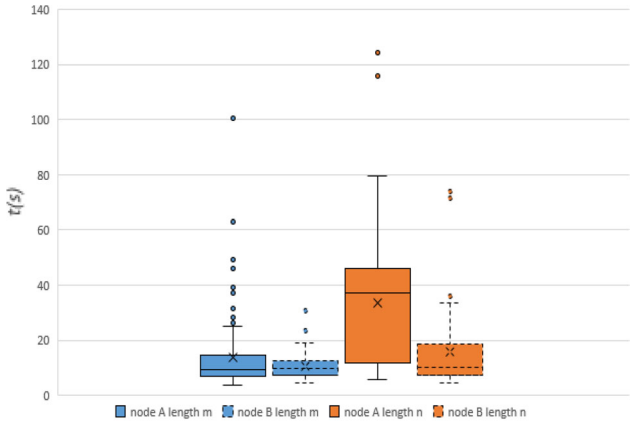


Fig. 16 Time distribution for attaching message *m* and *n* and of sizes 1399 and 2373 trytes respectively for node A and node B

Results

In this section, the results are arranged according to the above-discussed scenarios: append transactions and append MAMs.

Append transactions to the tangle

Figure 16 is a box-and-whisker plot to show the global delay in attaching the transaction to the *Tangle*. It can be seen that message of size *n* has a higher median delay for both nodes (A and B) probably because the message has been segmented into two transactions. For the same reason, i.e the size of trytes, there is less median delay for the message of size *m*.

It can be seen that the private node, node B, has exhibited a clear improved performance timing for both the messages, *m* and *n*. This is probably due to the reduced load in transaction requests that the private node, node B, experiences.

There are some transaction maximum outliers in Fig. 16. The attachment delay can have multiple causes. The most likely cause is the highly challenging "proof-of-work".

To get a deeper understanding of the delay in attaching transactions to the *Tangle*, this procedure is divided into three operations: "tip selection", "attach to tangle" and "broadcast". The first step decides which two transactions are to be approved. It is done by running the tip selection algorithm twice. The second operation carries out some "proof-of-work". This operation has a high variance because

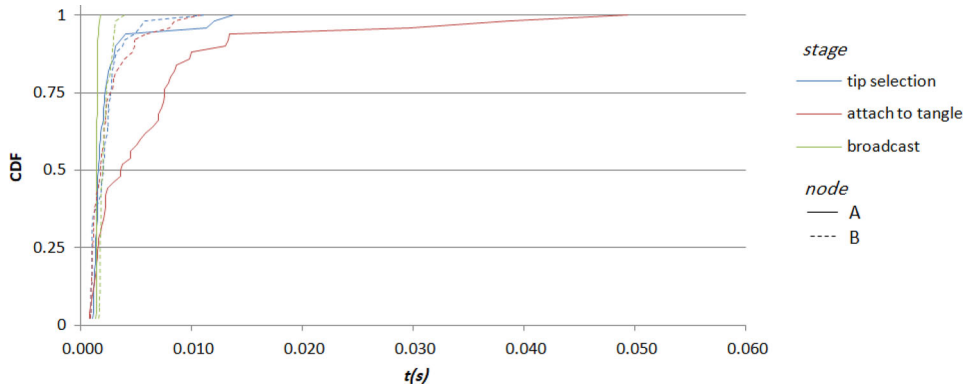


Fig. 17 CDF of the latency taken when appending message *m* of size 1399 trytes to the *Tangle* using public node A and private node B

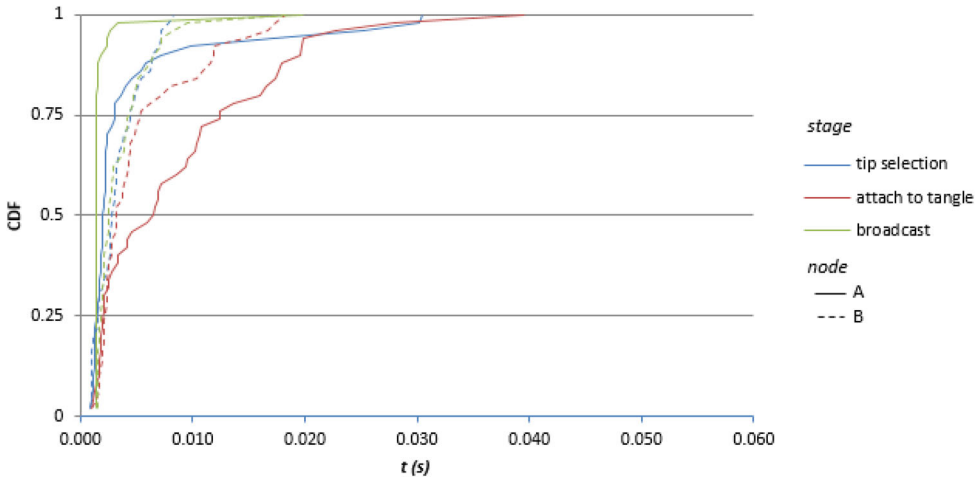


Fig. 18 CDF of the latency taken when appending message *n* of size 2373 trytes to the *Tangle* using public node A and private node B

the randomness of finding a suitable nonce requires time. In the last operation, the transaction is broadcasted to the network. The cumulative distribution functions (CDF)of the latency experienced in these operations for messages *m* and *n* is demonstrated in Figs. 17 and 18.

It can be seen that the major delay caused when appending transaction to the *Tangle* is due to the "attach to tangle" operation corresponding to the "proof of work" which is carried out in each transaction. The second reason for the delay is the "tip selection". The broadcast operation is approximately 1 s and thus insignificant as compared to other delay contributions.

While comparing Figs. 17 and 18, an expected behaviour is revealed: the "proof of work" for messages of size *n* exhibit delay as compared to messages of size *m*. For example, 80% of the transactions of size *m* for private node B experience the "attach-to-tangle" delay below 10 ms, while the same is true for 25% of the transactions of size n for the same node.

Append MAMs to the tangle

MAM transactions are different from normal transactions on the *Tangle*. In a MAM transaction, the data is encrypted before attaching it to the *Tangle*. So, attaching a MAM transaction includes three stages: "encoding", "broadcast" and "get message". The first stage is the encryption of the message with its secret key. The second stage is attaching the message to the tangle and broadcasting it. The last stage corresponds to fetching a MAM message.

The latency CDF for all three stages can be seen in Fig. 19. As the graph suggests, the "broadcast" stage is the prime contributor to the overall delay. This behavior is expected as a small amount of proof-of-work is included in this stage and it is a random process. The second contributor is the "get message" stage. The "encoding" stage has a negligible jitter and exhibits delays of 0.8 to 1 s.

Extended evaluations

The evaluation setup has been extended for 500 transactions instead of 100 transactions. Furthermore, two nodes are used to test transactions. However, the payload has been kept same for both the nodes i.e. 1399 trytes. Additionally, the similar operation of appending transactions to the *Tangle* was carried out with the set of new nodes.

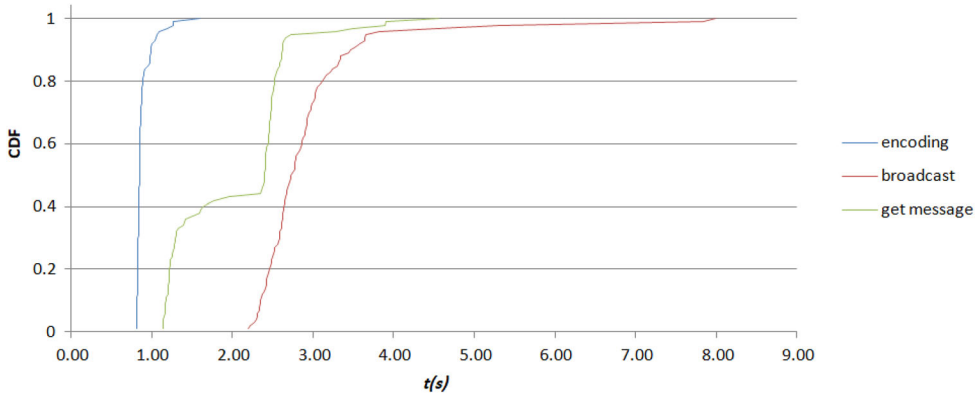


Fig. 19 CDF of the latency taken when appending transaction using masked authenticated messaging protocol

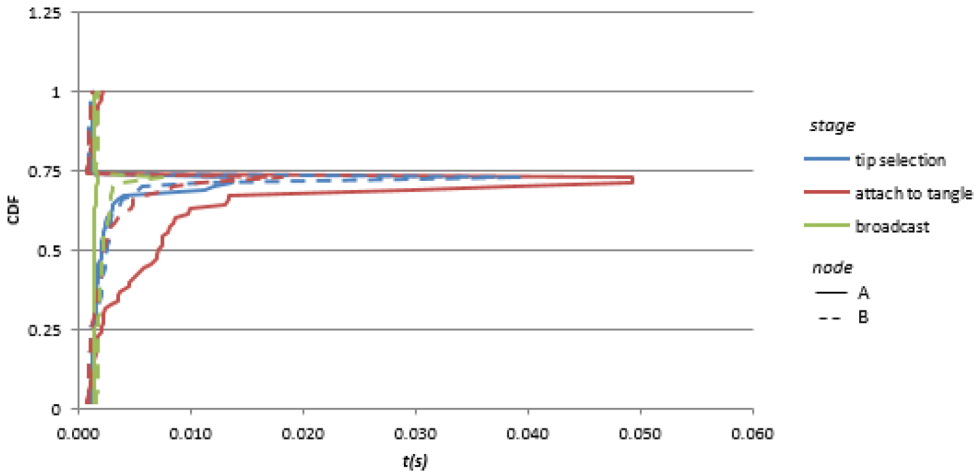


Fig. 20 CDF of the latency taken when appending transaction using message *m* on the *Tangle* using Hornet and Comnet nodes

Figure 20 shows the latency of attaching the transaction on IOTA Tangle using the latest nodes, each performing 500 transactions on the *Tangle*.

Discussion

The above-observed data shows that the transmission of a transaction in the *Tangle* can be achieved with a relatively low delay as compared to blockchain technologies. The above-observed implementation leverages medical applications with the benefits of IOTA technology.

At the current stage of the *Tangle*, many of the transactions were not immediately confirmed by the *Coordinator*. Many of them took a long time to get confirmed, which might represent a security risk, such as double-spending. This risk can be evaded using MAM.

MAM is an extension module that allows the storage, retrieval, and sharing of authenticated and encrypted data on-demand. It relies on distributed nodes and the data is distributed. Due to this reason, there is no central target for data leaks or cyber-attacks. Another important point is that this is the implementation of MAM in restricted mode, which gives users authority and agency to define the level of control over their data. The user can change the authorization key and disable future transactions for the past subscribers.

The tests were carried out on the current MAM library and it was observed that the overall delay of attaching the transaction is probably influenced by a small amount of "proof-of-work", which has randomness associated with it. This current library is not optimized for healthcare scenarios and it needs to be improved. The "proof-of-work" implementation can be made further efficient to run more effectively. Another important factor to delay is network latency, but this issue is out of the scope for this research.

MAM channels were found to be more efficient in storing, managing and sharing IoT data due to scalability which makes it a suitable protocol for healthcare IoT as well as industrial IoT.

Security analysis

The *Tangle*, similar to the blockchain network, is secure, scalable, resilient, and robust as its foundation is laid upon the cryptographic fundamentals. To further improve the security and encryption mechanism, MAM [87] protocol is used to encrypt the data stream on the *Tangle*. The restricted mode

in this protocol allows the data to be decrypted only if the private key is shared by the sender with the receiver.

The *Tangle* is known for its security features, hence making it suitable for several applications. It offers tamper-proof solutions and helps in attaining the security requirements such as confidentiality, authorization, availability, and integrity. This section discusses the security requirements and how these requirements are achieved by the *Tangle*.

Confidentiality Confidentiality is one of the most important requirements of security. The *Tangle* offers confidentiality by providing encryption to the data. All the information that is stored on the ledger, or communicated between nodes is encrypted. An extra layer of encryption is also provided using the MAM protocol. For the current scenario of the proposed framework, MAM protocol is used in restricted mode, thus only enabling the authorized users to communicate with the data. Therefore, data confidentiality is well maintained using the *Tangle*.

Authorization Another critical factor in an e-health system is the authorization of the data. The patient has the access to their health data and they have complete authority over it. For example, in the proposed healthcare system, only the user must share the data with the required medical person.

Availability Availability is another important security requirement. This requirement is facilitated by the *Tangle*. The nodes are always available and the transaction can take place at any time. The significant feature of the *Tangle* is decentralization which eradicates the single point of failure from the system.

Integrity The *Tangle* also offers this security feature in addition to the features mentioned above. The ledger has built-in integrity as it is immutable and tamper-proof. The information that has been stored there can not be changed or deleted. Hence, the integrity of the system is maintained using this distributed ledger.

Conclusion and future work

In this study, a distinctive model with zero-fee, zero-miner, and zero-block was proposed for the storage and sharing of health-related information securely and privately. This research has evaluated and discussed the chief performance parameters of the transaction on the *Tangle* as well as masked authenticated messaging (MAM) Protocol. Another main factor of this research is masked authenticated messaging (MAM) protocol which allows for smooth and secure transactions over the *Tangle*. This will aid in privacy and security support for medical data with minor latency overhead. MAM module has also enabled the user to exercise authority over access control of data. However, it has room for further improvements. The research can also be seen as a possible solution to overcome the many challenges of blockchain technologies for the healthcare sector, enable remote monitoring, and pilot healthcare into the digital age.

The research does not end here. Another version of this healthcare system can be implemented using random access authenticated Messaging (RAAM) [102] which allows for random access in the channel stream, rather than sequential access as in MAM.

One more similar work that can be carried out is addressing the patients in emergency and critical conditions where patients are not in a position to share their QR Code or publish their recent data to the *Tangle*. They may either be unconscious or unable to access their data at a given time. For this purpose, other facets of biometric identity solutions, such as retina and voice scans, can be explored. This idea was also proposed for future work by [22,103].

The proposed framework can be further modified to adjust with wearable devices and sensors and can be used in other health and fitness domains such as sports and rehabilitation. Environmental sensors can also be included to monitor the environment around patients. These different data can be published to the *Tangle* with different MAM modes. It could be a new direction for the future work [56]. Future work can also be focused on extending the trial count from 100 to a larger set to verify, authenticate and endorse the performance parameters of the *Tangle* [24].

Declarations

Conflicts of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Hammi B, Khatoun R, Zeadally S,Fayad A, Khoukhi L Internet of things (iot) technologies for smart cities, IET Networks 7. https://doi.org/10.1049/iet-net.2017.0163
2. Samih H (2019) Smart cities and internet of things. J Inf Technol Case Appl Res pp 1–10. https://doi.org/10.1080/15228053.2019.1587572

3. Rajab H, Cinkler T (2018). Iot based smart cities. https://doi.org/10.1109/ISNCC.2018.8530997
4. Tao F, Zuo Y, Da Xu L, Zhang L (2014) Iot-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Trans Industr Inf 10(2):1547–1557
5. Cheng J, Chen W, Tao F, Lin C-L (2018) Industrial iot in 5g environment towards smart manufacturing, Journal of Industrial Information. Integration 10:10–19
6. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (iot): a vision, architectural elements, and future directions. Fut Gen Comput Syst 29(7):1645–1660, including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services and Cloud Computing and Scientific Applications - Big Data, Scalable Analytics, and Beyond. https://doi.org/10.1016/j.future.2013.01.010
7. Alansari Z, Soomro S, Belgaum MR, Shamshirband S (2010) The rise of internet of things (iot) in big healthcare data: review and open research issues. arXiv:1904.09270. https://doi.org/10.1007/978-981-10-6875-1_66
8. Bashshur R, Shannon G, Krupinski E, Grigsby J (2012) Sustaining and realizing the promise of telemedicine, Telemedicine journal and e-health: the official journal of the American Telemedicine Association 19. https://doi.org/10.1089/tmj.2012.0282
9. Eysenbach G (2001) What is e-health? J Med Internet Res 3(2):e20. https://doi.org/10.2196/jmir.3.2.e20
10. Zheng X, Rodríguez-Monroy C (2015) The development of intelligent healthcare in China. Telemed e-Health 21:443–448. https://doi.org/10.1089/tmj.2014.0102
11. Fatehi F, Wootton R (2012) Telemedicine, telehealth or e-health? A bibliometric analysis of the trends in the use of these terms. J Telemed Telecare 18. https://doi.org/10.1258/jtt.2012.GTH108
12. Hwang YH (2015) Iot security & privacy: threats and challenges. In: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, IoTPTS'15, association for computing machinery, New York, NY. https://doi.org/10.1145/2732209.2732216
13. Dabbagh M, Rayes A (2017) Internet of things security and privacy, pp 195–223. https://doi.org/10.1007/978-3-319-44860-2_8
14. Peterson KJ, Deeduvanu R, Kanjamala P, Mayo K (2016) A blockchain-based approach to health information exchange networks
15. Chacko A, Hayajneh T (2018) Security and privacy issues with iot in healthcare. EAI Endorsed Trans Pervasive Health Technol 4:155079. https://doi.org/10.4108/eai.13-7-2018.155079
16. Butt S, Diaz-Martinez J, Jamal T, Ali A, De la Hoz E, Shoaib M (2019) Iot smart health security threats. https://doi.org/10.1109/ICCSA.2019.000-8
17. Sadek I, Rehman SU, Codjo J, Abdulrazak B (2019) Privacy and security of iot based healthcare systems: Concerns, solutions, and recommendations. In: Pagán J, Mokhtari M, Aloulou H, Abdulrazak B, Cabrera MF (eds) How AI impacts urban living and public health. Springer, Cham, pp 3–17
18. Regulation (eu) (2016) 2016/679 of the European parliament and of the council, [Online; accessed March 07, 2020]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
19. Kuo T-T, Kim H, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24:1211–1220. https://doi.org/10.1093/jamia/ocx068
20. Angraal S, Krumholz H, Schulz W (2017) Blockchain technology: applications in health care. Circ Cardiovasc Qual Outcomes 10:e003800. https://doi.org/10.1161/CIRCOUTCOMES.117.003800
21. Gordon WJ, Catalini C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability, computational and structural. Biotechnol J 16:224–230. https://doi.org/10.1016/j.csbj.2018.06.003. http://www.sciencedirect.com/science/article/pii/S200103701830028X
22. Brogan J, Baskaran I, Ramachandran N (2018) Authenticating health activity data using distributed ledger technologies, computational and structural. Biotechnol J 16:257–266. https://doi.org/10.1016/j.csbj.2018.06.004. http://www.sciencedirect.com/science/article/pii/S2001037018300345
23. Hawig D, Zhou C, Fuhrhop S, Fialho AS, Ramachandran N (2019) Designing a distributed ledger technology system for interoperable and general data protection regulation-compliant health data exchange: A use case in blood glucose data. J Med Internet Res 21(6):e13665
24. Bartolomeu P, Vieira E, Ferreira J (2018) Iota feasibility and perspectives for enabling vehicular applications 1–7. https://doi.org/10.1109/GLOCOMW.2018.8644201
25. Gropper A (2016) Powering the physician-patient relationship with hie of one blockchain health
26. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management, pp 25–30. https://doi.org/10.1109/OBD.2016.11
27. Biradar DMN (2018) Iota-next generation block chain. Int J Eng Comput Sci 7 23823–23826. https://doi.org/10.18535/ijecs/v7i4.05
28. Popov S (2015) The tangle
29. Oh H, Rizo C, Enkin M, Jadad A (2005) What is ehealth (3): a systematic review of published definitions. J Med Internet Res 7:e1. https://doi.org/10.2196/jmir.7.1.e1
30. Pagliari C, Sloan D, Gregor P, Sullivan F, Detmer D, Kahan J, Oortwijn W, Macgillivray S (2005) What is ehealth (4): a scoping exercise to map the field. J Med Internet Res 7:e9. https://doi.org/10.2196/jmir.7.1.e9
31. WHO (2020) World health organization, Retrieved from https://www.who.int/ [Online; accessed April 20, 2020]
32. WHO (2020) ehealth at who, Retrieved from https://www.who.int/ehealth/about/en/ [Online; accessed April 20, 2020]
33. Sahama T, Simpson L, Lane B (2013) Security and privacy in ehealth: Is it possible? pp 249–253. https://doi.org/10.1109/HealthCom.2013.6720676
34. Acheson ED (1964) Oxford record linkage study. A central file of morbidity and mortality records for a pilot population. Br J Prevent Soc Med 18:8–13
35. Fahy E, Hardikar R, Fox A, Mackay S (2014) Quality of patient health information on the internet: reviewing a complex and evolving landscape. Aust Med J 7:24–28. https://doi.org/10.4066/AMJ.2014.1900
36. Marks P (2014) Hacked to death
37. Plante T, Urrea B, MacFarlane Z, Blumenthal R, Miller E, Appel L, Martin S (2016) Validation of the instant blood pressure smartphone app. JAMA Int Med. https://doi.org/10.1001/jamainternmed.2016.0157
38. Hekler E, Buman M, Grieco L, Rosenberger M, Winter S, Haskell W, King A (2015) Validation of physical activity tracking via android smartphones compared to actigraph accelerometer: laboratory-based and free-living validation studies. JMIR Mhealth Uhealth 3:e36. https://doi.org/10.2196/mhealth.3505
39. Haque ME, Ahsan MA, Rahman F, Islam A, EmdadulHaque M (2019) The challenges of ehealth implementation in developing countries: a literature review
40. Gardiyawasam Pussewalage H, Oleshchuk V (2016) Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions. Int J Inf Manag 36:1161–1173. https://doi.org/10.1016/j.ijinfomgt.2016.07.006
41. Ghazvini A, Shukur Z Security challenges and success factors of electronic healthcare system. Procedia Technol. https://doi.org/10.1016/j.protcy.2013.12.183

42. Coppolino L, D'Antonio S, Mazzeo G, Romano L (2017) Cloud security: emerging threats and current solutions. Comput Electr Eng 59:126–140. https://doi.org/10.1016/j.compeleceng.2016.03.004. http://www.sciencedirect.com/science/article/pii/S0045790616300544
43. U. D. of Health, H. Services (2013) Federal register, Retrieved from https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf
44. Domínguez Mayo F. J, Escalona M, Mejías M, Aragón G, Garcia-Garcia J, Torres J, Enríquez J (2015) A strategic study about quality characteristics in e-health systems based on a systematic literature review. Sci World J 2015:1–11. https://doi.org/10.1155/2015/863591
45. Scholl M, Stine K, Hash J, Bowen P, Johnson A, Dancy Smith C, Steinberg DI (2013) An introductory resource guide for implementing the health insurance portability and accountability act (hipaa) security rule. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
46. Bleikertz S, Schunter M, Probst C, Pendarakis D, Eriksson K (2010) Security audits of multi-tier virtual infrastructures in public infrastructure clouds, pp 93–102. https://doi.org/10.1145/1866835.1866853
47. Grobauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE Secur Privacy 9(2):50–57
48. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat M, Rodrigues J (2019) Bheem: a blockchain-based framework for securing electronic health records. https://doi.org/10.1109/GLOCOMW.2018.8644088
49. Badr S, Gomaa IA, Abd-Elrahman E (2018) Multi-tier blockchain framework for iot-ehrs systems. In: EUSPN/ICTH
50. Radanovic I, Likic R (2018) Opportunities for use of blockchain technology in medicine. Appl Health Econ Health Policy 16. https://doi.org/10.1007/s40258-018-0412-8
51. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F (2017) Secure and trustable electronic medical records sharing using blockchain, AMIA Annual Symposium proceedings. AMIA Sympos 2017:650–659
52. Rifi N, Rachkidi EE, Agoulmine N, Taher NC (2017) Towards using blockchain technology for ehealth data access management. In: 2017 Fourth international conference on advances in biomedical engineering (ICABME), pp 1–4
53. da Conceição AF, da Silva FSC, Rocha V, Locoro A, Barguil JM. Eletronic health records using blockchain technology. arXiv:1804.10078
54. Dias J. P, Ferreira H. S, Martins A(2018) A blockchain-based scheme for access control in e-health scenarios, in: SoCPaR
55. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42:1–7
56. Zheng X, Sun S, Mukkamala RR, Vatrapu R, Ordieres-Meré J (2019) Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. J Med Internet Res 21(6):e13583. https://doi.org/10.2196/13583
57. Decker C, Wattenhofer R (2013) Information propagation in the bitcoin network. IEEE 1–10
58. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system, Bitcoin
59. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies. Network Security 2016(8):4 10.1016/S1353-4858(16)30074-5. http://www.sciencedirect.com/science/article/pii/S1353485816300745
60. Walport M (2016) Distributed ledger technology: Beyond block-chain, Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
61. Al-Kuwari S, Davenport J, Bradford R (2011) Cryptographic hash functions: Recent design trends and security notions., IACR Cryptology ePrint Archive 2011 565
62. Wikipedia contributors, Online transaction processing — Wikipedia, the free encyclopedia, https://en.wikipedia.org/w/index.php?title=Online_transaction_processing&oldid=945154394, [Online; accessed 14-April-2020] (2020)
63. Sultan K, Ruhi U, Lakhani R (2018) Conceptualizing blockchains: Characteristics & applications
64. Gupta S, Sadoghi M Blockchain transaction processing https://doi.org/10.1007/978-3-319-63962-8_333-1
65. Zheng Z, Xie S, Dai H.-N, Chen X, Wang H An overview of blockchain technology: Architecture, consensus, and future trends, 2017. https://doi.org/10.1109/BigDataCongress.2017.85
66. NRI, Survey on blockchain technologies and related services fy2015 report, 2016, online. https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf
67. Evans D (2011) How the next evolution of the internet is changing everything
68. Greenspan D. G (2015) Multichain private blockchain, [Online; accessed March 07, 2020]. https://www.multichain.com/download/MultiChain-White-Paper.pdf
69. Filippi P. D (2016) The interplay between decentralization and privacy: The case of blockchain technologies
70. Möser M (2013) Anonymity of bitcoin transactions an analysis of mixing services
71. Confirmed transactions per day, [Online; accessed March 12, 2020]. https://www.blockchain.com/charts/n-transactions
72. Mamoshina P, Ojomoko L, Yanovich Y, Ostrovski A, Botezatu A, Prikhodko P, Izumchenko E, Aliper A, Romantsov K, Zhebrak A, Ogu I, Zhavoronkov A (2018) Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9:5665–5690. https://doi.org/10.18632/oncotarget.22345
73. Ethereum, [Online; accessed March 12, 2020]. https://ethereum.org/developers/
74. Iota blog, [Online; accessed March 12, 2020]. https://www.iota.org/research/meet-the-tangle
75. Bitcoin confirmation, [Online; accessed March 12, 2020]. https://en.bitcoin.it/wiki/Confirmation
76. Baird L The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance[Online; accessed September 30, 2020]
77. Schueffel P Alternative distributed ledger technologies blockchain vs. tangle vs. hashgraph - a high-level overview and comparison -, SSRN Electronic Journal https://doi.org/10.2139/ssrn.3144241
78. N. El Ioini, C. Pahl, A Review of Distributed Ledger Technologies: Confederated International Conferences: CoopIS, C&TC, and ODBASE (2018) Valletta, Malta, October 22–26, 2018. Proceedings, Part II 2018:277–288. https://doi.org/10.1007/978-3-030-02671-4_16
79. Bu G, Hana W, Potop-Butucaru M Metamorphic iota (07 2019)
80. Akhtar M. M, Rizvi D. R, Ahad M. A, Kanhere S. S, Amjad M, Coviello G Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy, Sensors 21 (13). https://doi.org/10.3390/s21134354 URL https://www.mdpi.com/1424-8220/21/13/4354
81. Back A Hashcash - a denial of service counter-measure
82. Lamtzidis O, Pettas D, Gialelis J (2019) A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture. Applied System Innovation 2:30. https://doi.org/10.3390/asi2030030
83. Wikipedia contributors, Double-spending — Wikipedia, the free encyclopedia, [Online; accessed 29-April-2020] (2020).

https://en.wikipedia.org/w/index.php?title=Double-spending&oldid=944880185
84. Cao B, Li Y, Zhang L, Zhang L, Mumtaz S, Zhou Z, Peng M (2019) When internet of things meets blockchain: Challenges in distributed consensus. IEEE Network 33(6):133–139
85. Alsbou'i T, Qin Y, Hill R (2019) Towards a scalable iota tangle-based distributed intelligence approach for the internet of things
86. MobiFish, Trit & tryte (2021). https://www.mobilefish.com/download/iota/trits_trytes_part2.pdf
87. Handy P (2017) Introducing masked authenticated messaging, https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e
88. IOTA, Masked authenticated messaging, https://github.com/iotaledger/mam.client.js/ (2020)
89. Merkle R (1989) A certified digital signature 435:218–238. https://doi.org/10.1007/0-387-34805-0_21
90. ABmushi, Iota: Mam eloquently explained (2018). https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413
91. The google fit sdk, [Online; accessed March 07, 2020]. https://developers.google.com/fit
92. Raspberry pi, [Online; accessed March 07, 2020]. https://www.raspberrypi.org/
93. Google fit, [Online; accessed March 07, 2020]. https://www.google.com/fit/
94. Firebase, [Online; accessed March 07, 2020]. https://firebase.google.com/
95. Qr code, [Online; accessed March 07, 2020]. https://en.wikipedia.org/wiki/QR_code
96. Devnet, [Online; accessed March 07, 2020]. https://devnet.thetangle.org/nodes
97. Node.js, [Online; accessed March 07, 2020]. https://nodejs.org/en/
98. Mam, [Online; accessed March 07, 2020]. https://github.com/iotaledger/MAM
99. Mam wrapper, [Online; accessed March 07, 2020]. https://github.com/iotaledger/mam.client.js/
100. Amazon, Amazon web services, https://aws.amazon.com/ (2020)
101. IOTA, Pyota: The iota python api library, https://github.com/iotaledger/iota.py (2020)
102. Lamberti R (2018) Random access authenticated messaging - an alternative messaging protocol for iota . https://blog.usejournal.com/random-access-authenticated-messaging-45a5f40f2532
103. Smart health it (2020). https://smarthealthit.org/