Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology

P.Hemalatha[a], S.Balaji[b], E.Chandru[c] , Pelleti Pradeep Kumar[d], and D.Saravanan[e]

[a] Assistant Professor, Department of CSE, IFET College of Engineering, Villupuram, India.
[b]Research Student, Department of CSE, IFET College of Engineering, Villupuram, India.
[c]Research Student, Department of CSE, IFET College of Engineering, Villupuram, India.
[d]Research Student, Department of CSE, IFET College of Engineering, Villupuram, India.
[e]Associate Professor, Department of CSE, IFET College of Engineering, Villupuram, India.

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Blockchain and Internet of Things (IoT) technologies are used in many domains, predominantly for electronic-healthcare. Here, IoT devices has the ability to provide real-time sensor data from patients to get processed and analyzed. As a single point of failure, mistrust, data manipulation and tampering, and privacy avoidance may all occur as a result of such a method. Through offering shared computing and storage for IoT data, blockchain can help solve such issues.Maintaining and sharing Medical data is necessary here.If there occurs loss of confidence means it threatens the medical data and loss of integrity creates impact on the life of patient. So, the first objective is to protect the medical records. Also, a central server to the records will pretend the hackers to attack and continuous fetching is difficult.Therefore, combining Blockchain and IoT will be a threat breaker for computerized medical records.

Keywords: Electronic health record (EHR) e-Health signature infrastructure (KSI) Timestamped algorithm Merkle tree Blockchain

1. Introduction

As the number of patients and illnesses continues to climb, health care has become increasingly relevant. It is important to keep track of an individual's medical history in order to accurately address potential health needs. The existing environment ensures that health data is managed and exchanged in a transparent way across different organization. Even if documents are exchanged with other organizations' in a protected way. For avoiding the impacts of privacy, data integrity the proposed work has a new methodology. Maintaining the integrity of medical records is important. As a consequence, documents can only be exchanged where there are properties that are partly dependent on attributes that fit. This is done by using anonymous entry and only sharing common knowledge, followed by using attribute values to distinguish highly protected information.

1.1 Problems with existing data maintenance

Healthcare data management has a range of big problems, including data availability, scalability, and storage performance.

1.1.1 Availability of Data

Healthcare sector places a high priority on data access since it is essential for medical treatment. And in the case of hardware malfunction or user error, uninterrupted data storage and usability is a problem. Errors may also be caused by system failure or storage facility flaws.

1.1.2 Adaptability

The Adaptability of storage of data has an effect on the optimal usage of available storage space as well as the need to add room to store new data. When it comes to cloud setup, the inclusion of additional computing capacity does not have an impact on existing structures. It is critical to ensure scalability in data-intensive systems like electronic health records (EHR) as a consequence of which data can be stored without difficulties.

1.1.3 Accomplishment

The application's total efficiency is influenced by storage performance. This has an effect on the level of patient caring. By giving a faster data storage facility, particular application wouldn't fix these issues since multiple applications need to be monitored in order to perform better.

For avoiding the impacts of privacy, data integrity [3] the proposed work has a new methodology. Blockchain keeps the medical data as non-centralized method and provides a alert when there occurs any unauthorized access to the data.It's found in bitcoin as well as other digital currency schemes. This new technology allows people with digital information to share it with others in a distributed way. Blockchain guarantees data distribution integrity while also providing increased privacy and protection. There is no single point of failure in this situation since data is contained in blocks and distributed as this is the drawback. Additionally, one blockchain version is accessible, which guarantees the information openness by enabling everyone to function anonymously in the network. Since it is private, another version requires for a small number of users to access it. Traditional blockchain's key disadvantages are problems with speed, scalability, and storage space.

In health care, blockchain technology is being used to address security issues. The files are safe because they are stored at cloud that is secured and partitioned by several parties. Each record is allocated to a block, which is then connected to the previous block in a logical manner. As a consequence, there is a relation between the documents, and they are not shattered. The block timestamps are all current. It's easy to verify network transactions with a timestamp. A key-less signature infrastructure framework (for example, [4]) assists in efficiently securing the patient's health record. As a result, it outperforms the current infrastructure, the value of blockchain technologies is illustrated in terms of response time and cost.

1.2 Related works

Established cryptographic methods that are being used in a cloud setting inspired using blockchain in e-healthcare. The techniques used previously are listed here.

1.2.1 Encryption strategy focused on characteristics and aliases

Article [5] investigates an identity-based encryption scheme for better protection of a particular part of cryptographic data at the end user while still restricting unauthorized access. With the private key, the cloud's access control feature provides access to a portion of encrypted files.Similarly, it is simple to apply encryption with various attributes to ensure the privacy of data stored in the cloud in a distributed setting by implementing the identity-based encryption scheme.

Here [6] proposes (MA-ABE) that lets any entity to be an administrate by generating a key that also aids in the dissemination of private keys. Since each variable can come from a separate jurisdiction, security is a major restriction in this scheme.The dual encryption method is used, which helps to preserve the system's integrity by using bi-linear principles. [7] uses the ABE protocol as management framework for data collected. [8] suggests a user revocation system based on identity.Instead of placing the data load on a single proxy server, this scheme distributes it across a wide number of users, reducing computing overhead. As a result, the proposed design significantly increases the efficiency of the current ABE programme.

There are some technological problems with the ABE method. Blockchain is included in the architecture to fix the limitations. Here, the token-based framework is used. The tokens are often used to measure attribute-based ownership. Many authorities carry out these activities in a distributed way.

The data is not leaked and is stored and accessed in compliance with the permissions. Content control is often required by the hierarchical IBE.

1.2.2 Hierarchical encryption technique

In article [10], offering forwarding protection has particular necessary. By the suggested scheme, when a new user reaches the protected system, they will enter. As a consequence, encryption is guaranteed when the individual enters. This makes the task of generating hidden keys much easier.Role-based programmes are used to protect various functions that have been identified in the scheme.

Multiple hierarchy identity-based encryption is a recently suggested scheme that focuses on protected information transactions between institutions. The private key is also used for decryption. As a result, the suggested system assigns tasks to various people, who are given access depending on their roles. A single user can have several responsibilities, each of which defines their level of access. Some organizations can appear to have several functions, which adds an extra layer of protection to the system. As a result, the new scheme is ID-based scheme with several functions and encryption.

Initially, a cipher-text-policy attribute-based encryption scheme was developed to provide stability. However, it did not address the issue of multi-level hierarchy implementations in fields such as medicine. The current scheme has many significant defects, including high cost, encryption time, and decryption time. To solve the problem, a encryption scheme [11] was introduced as a way-up to CP-ABE, incorporating specified mechanism. Protection is guaranteed in the proposed framework due to the use of bi-linear Diffie-Hellman. The suggested scheme also guarantees low storage and computing costs, allowing encryption and decryption both simple and affordable.

1.2.3 Architectures of Healthcare

As healthcare is growing fastly, necessitating a variety of efficient systems to efficiently handle it. The patient could be tracked using an Internet of Things (IoT) device that links the sensor to the web[27],[28]. By this concept, the proposed scheme employs the pathway to provide a variety of resources such as storing, mining the data, processing, allowing for the effective use of information. A smarter e-health in article [12] is suggested, which improves healthcare tracking while still conserving resources. Sensor network, pathway for health care, and numerous big-data servers are also part of the planned infrastructure.These modules provide data storage as well as data protection. The proposed healthcare portal scheme tackles the issues of scalability and interoperability, as well as reliability.

As a result of the use of mobile devices, health treatment is tracked, and procedures for handling and preserving different health criteria are established.

The system of data protection by alerting was defined in the paper [14] which was published previously. The data gathered by sensors is analyzed and put to good use. A mobile application , an IoT portal, a bridge, and medical equipment are also part of the proposed system. As a result of the use of IoT,there will be assurance for protection of health data.

1.2.4 Present blockchain architecture

Blockchain technology ensures data integrity and availability. An architecture called Prov-chain is implemented to aid data collection, validation in article [15]. Prov-chain is needed to protect confidential healthcare data, ensuring that health care is more reliable. The Merkle tree arrangement in a blockchain-based framework provides logs and assists in data maintenance while preserving anonymity. A timestamp definition is used to verify the records, which aids in the handling of the blockchain.

1.2.5 Med Rec prototype

A decentralized approach to EHR management has previously been suggested [16]. Patients can conveniently view their medical records through providers through the proposed scheme. It also aids in protecting patient data integrity, data management, and sharing. The proposed decentralized architecture often aids in the analysis of blockchain's use in health care and study. It will be available as open source in the future so that it can be more developed. Pseudonym-Based Encryption with Separate Authorities (PBEDA) is a privacy-preserving method suggested in [21], which succeeds privacy by blockchain. The method allows for the review of health records as well as the checking of critical details in the EHR system. The protection is maintained by using the ECC methodology. To ensure security programmes, MIRACL security software are used.

This dissertation [22] focuses on IoT-based health-care techniques and also seeks to provide assisted housing for the elderly. This paper explains numerous IoT-based strategies that assist in the medical field, referred to as IoHT. Middleware is mandated to be an essential component of IoT solutions, according to the draught IoT middleware architecture [23]. In addition, IoT-based strategies are discussed, as well as the problems that come with them. In [24], a cloud-based architecture is proposed, which aids e-healthcare networks in successfully handling medical data and makes data transmission simpler.As a result, the proposed system saves costs while retaining confidentiality and honesty. The Discrete Wavelet Transform is used in [25] to improve the system's security. To reduce the queue, a genetic algorithm is used, and encrypted keys are used for better cloud transmission. CoT (Cloud of Things) [26] is a modern phenomenon that combines the internet of things with cloud computing.

2 Proposed system

2.1 Signature Infrastructure

Unlike standard public key infrastructure strategies[17, 18], which rely on asymmetric keying scheme the KSI uses a hash value to provide authentication to the user who accesses it. Signatures are created with the aid of cores, gateways, and aggregators. The KSI aims to validate data by ensuring data security, integrity, and safety. Blockchain was created to address the shortcomings of KSI.

2.2 About Block chain

It is a distributed public framework that primarily keeps transaction details public [19] and stable. The Blockchain has the advantage of it has no pre-defined links and can manage cases when a trusted party becomes malicious, reducing vulnerability and increasing the system's robustness. Public, consortium-based corporate, and entirely private are the three main distinctions of blockchain. Block headers and blocks, as well as the Merkle tree, are components of blockchain.

2.2.1 Blocks and Block header

The blockchain has the block header which holds the hash signature as well as the previous block header's value. The data to be transacted is stored in each cube. The information could be changed if needed. The exchange takes place inside the blocks in a safe manner. In the blockchain, new blocks can be inserted at any time.

2.2.2 Merkle tree

Merkle Tree is the combination of a mathematical derived file known as hash and other file formed at the same instance. Cryptographic links are used to increment the number of files produced or updated at a given time, with the first roots hash being created and used as evidence of each file's contribution.

2.2.3 Pros of Proposed Method

The key advantage of proposed method is that the rules may be updated and the data present in the blockchain can be adjusted if required. The probability of attack is greatly reduced thanks to decentralised architecture [20]. Private blockchain, as compared to public blockchain, will be stable and effective, with and stronger authentication quicker processing.

2.3 KSI with blockchain

The technology of KSI blockchain offers protection, confidentiality, and data integrity. The information is digitally and processed signed on KSI blockchain. The data is then checked for signing with the signed period at some stage in the future. Since KSI does not have any keys like the public crypt scheme, it cannot be hacked. A hash is used by KSI to help maintain the system's security.

The following are some of the special characteristics of the KSI blockchain:

a) It is a offline component, based on real-time entity since it runs without the use of a network link.
b) The data does not need to be maintained by a third party, because it is extremely scalable.
c) Data can be checked right after it has been transmitted, which ensures the principle of data availability..

2.4 Blockchain risks

Many companies face a number of risks when implementing blockchain technologies. Strategic danger, information technology risk, organisational and IT risk, market stability, provider risk, main management risk, data confidentiality, and compliance risk are the most often experienced threats. As a result, businesses should be able to deal with these challenges and adopt a high degree of risk control.

2.4.1 Blockchain risks and its types

There are three risk: standard, smart contract, and value transfer.

(i)Standard risks

Strategic risk includes the point at which the organisation plans to implement blockchain technologies, the network of which the users may be members, and the shortcomings of the goods being built on the current framework. Since blockchain technology shortens the time it takes for business processes to complete, the business continuity strategy should ensure a quick solution. While protection for transacting records is provided by blockchain technology, it doesn’t provide encryption for individual accounts.Another issue to consider is how to integrate this emerging technology with existing technologies, as well as how to maintain and improve metrics like transparency and scalability.

(ii) Smart contract risks

Company operations, regulatory disputes, and various financial information are also linked with the blockchain, that operates in Oracle database. As a result, any threatening to Oracle foundation would cause a major problem.

(iii)Value transfer risks

The blockchain technology main feature of that there is no authority at the central and the architecture is decentralised as a result, value can be transferred freely between different peers. To take advantage of blockchain technologies, these threats must be successfully handled.

3 Proposed framework for encrypting the e-healthcare by blockchain and KSI

The proposed architecture assists in the safe storing of medical records. The suggested structure in Fig. 1 depicts a set of measures to safeguard health data protection and honesty. If a doctor wants to treat a patient he/she needs to provide their own ID as well as the patient's private key when demanding health details. The local databases consist of information which was provided by the doctor. Additionally, the person's authority for control is checked in the Access control List using the given ID (ACL). After the user has been authenticated, KSI processes is used to sign the data in order to guarantee digital integrity.In the suggested system, an portal at the initial stage that serves as an aggregator to search and a centre helps to guarantee privacy and data protection. Additionally, the data is sent to the blockchain to be analysed for further authentication..Each patient's healthcare data is stored in the blockchain as a block.

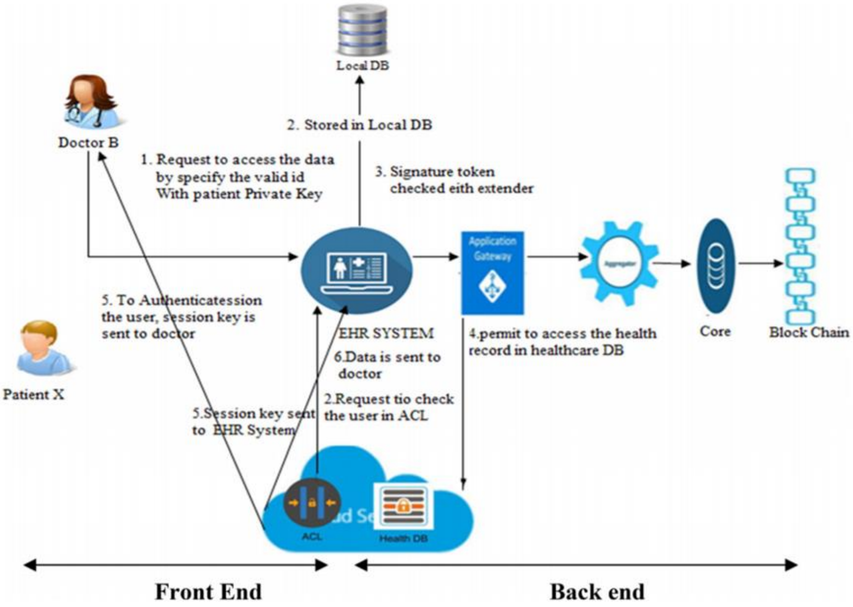

Local DB
2. Stored in Local DB
Doctor B
1. Request to access the data by specify the valid id With patient Private Key
3. Signature token checked eith extender
Application Gateway
Aggregator
Core
Block Chain
5. To Authenticatession the user, session key is sent to doctor
EHR SYSTEM
6.Data is sent to doctor
4.permit to access the health record in healthcare DB
Patient X
5.Session key sent to EHR System
2.Request tio check the user in ACL
ACL
Health DB
Front End
Back end

Figure. 1 Framework for healthcare data

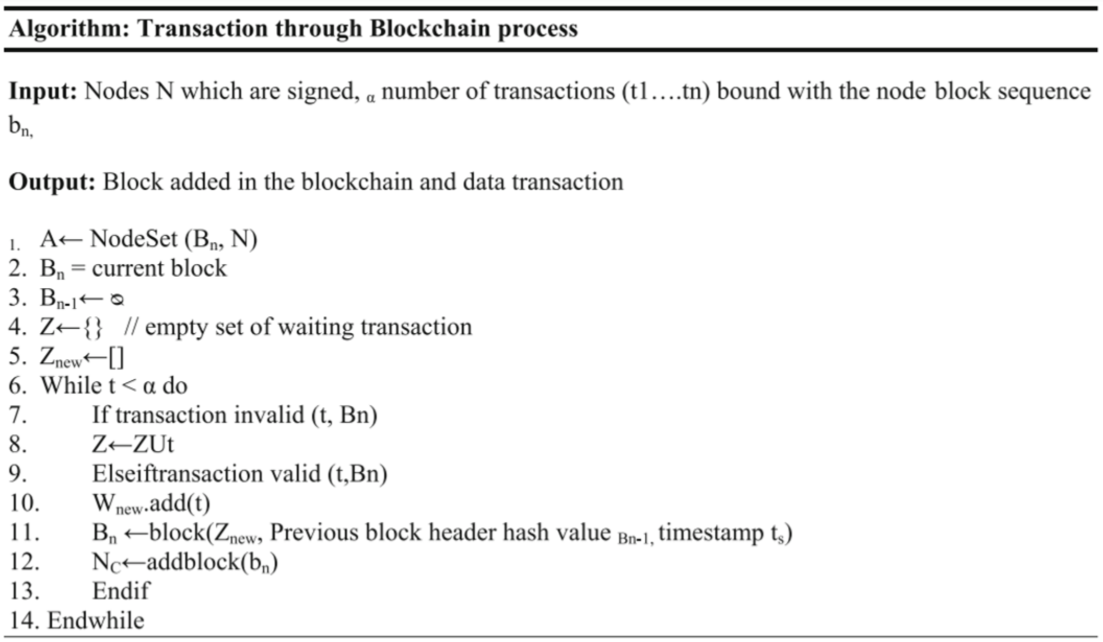
The confidentiality of the data is maintained to a significant degree in the proposed system by using digital signatures and the blockchain methodology. Requesting authorization to view the health record from the health archive is the next step. As a result, a session key is given to give the doctor access to the EHR. This key authenticates the patient and grants access to the data. To maintain data confidentiality, a set of authentication levels are used. The following segment explains how blockchain can be used to guarantee data integrity.

The front-end of the EHR system is where the members of the medicinal process communicate with it. Doctors and patients seek access to their EHR documents in order to inquire about their medical knowledge. The consumer must first be approved by the EHR system's database. To ensure this, the user information on the access list is double-checked. If the value fits, the customer is granted access to the record at the stage at which he has been granted access.

The back-end method includes protecting healthcare records leveraging infrastructure and blockchain technologies to ensure the data is maintained without issue.The data is then sent to the programme portal, which verifies that it complies with the specifications. The data is then provided to an aggregator to be clustered for effective storage. Furthermore, for a more effective storing and retrieval operation, the data is processed using blockchain technologies.

The first and only tool to verify data integrity is Blockchain with KSI. Loss of accuracy of healthcare documents can result in the death of a patient. The KSI is designed to authenticate and validate the credibility of medical documents. Then, to ensure the confidentiality of patient records, signature infrastructure and blockchain are added. Without the support of reputable authorities, blockchain provides secure authentication.

The KSI enables a person to demonstrate when health data are first entered into the blockchain. The signed data is stored so that the signature time, signing party, and data accuracy can be checked later. KSI is nothing but it is server-based signature that is distinct from traditional signatures. Merkle hash tree and root hash is used to validate record timestamp and integrity and are among the server layers in the KSI.



Algorithm: Transaction through Blockchain process

Input: Nodes N which are signed, $_\alpha$ number of transactions (t1….tn) bound with the node block sequence $b_{n,}$

Output: Block added in the blockchain and data transaction

```
A← NodeSet ($B_n$, N)
$B_n$ = current block
$B_{n-1}$← ∅
Z←{}   // empty set of waiting transaction
$Z_{new}$←[]
While t < α do
    If transaction invalid (t, Bn)
    Z←ZUt
    Elseiftransaction valid (t,Bn)
    $W_{new}$.add(t)
    $B_n$ ←block($Z_{new}$, Previous block header hash value $_{Bn-1,}$ timestamp $t_s$)
    $N_C$←addblock($b_n$)
    Endif
Endwhile
```

The user sends the KSI server a signed hash key or value of the document and a signature token is received as evidence of the time of signature, signing entity, and data integrity. To build a signature token, no keys are needed. The document hash is received by a gateway, which aggregates the hash values and forwards them to the next available server via an aggregator. Finally, the blockchain stores the root hash value.

At the top of the KSI, there is an extra publishing layer called the blockchain. KSI tests the consistency of the data and analyses the result, which is then stored in the blockchain, by using the hash function. Root hash is distributed once a month in the newspaper to prevent regular publishing [10]. The ledger grows in size as the number of transactions grows. The hash path is saved with the text so that it can be quickly checked for its accuracy and timestamp. If the frequency of the deal is uncertain, evidence of work isn't the right solution.

4 Results and discussion

Data type	Avg time (s)	File transfer size (KB)
Creation of Block	0.652	1.05
Updating of Block	0.485	1.04
Sharing of Block	0.493	1.07

Deletion of Block	0.676	1.07

Apache JMeter was used to test the proposed framework's performance. Due to cost, file size, and time taken, file storage, replication, and adjustment in the cloud in the form of blocks incur overhead.The response time for standard cloud data storage is measured using current schemes. For the planned cloud computing, the file size of the data and its subsequent response time are portrayed. The block chain-based technology takes less time than the current systems, as seen in this contrast.

Table 1 Overhead for data storage and retrieval process from the blockchain (time perspective)

5 Conclusion

The paper discussed how Blockchain and IoT technologies can be leveraged to improve e-Healthcare systems and services. We also proposed an improved IoT-based blockchain e-healthcare framework i.e. IoT-Health IoT-based blockchain framework for accessing, managing e-healthcare EHR data, in a manner that is highly more trusted, secure, transparent, and efficient.

References

1. *Herlihy M, Moir M (2016) Enhancing accountability and trust in distributed ledgers. arXiv preprint arXiv:1606.07490*
2. *Zou J, Wang Y, Orgun MA (2016, June) A dispute arbitration protocol based on a peer-to-peer service contract management scheme. In: 2016 IEEE international conference on web services (ICWS). IEEE, pp 41–48*
3. *Bhattacharjya A, Zhong X, Wang J (2016, March) Strong, efficient and reliable personal messaging peer to peer architecture based on Hybrid RSA. In: Proceedings of the international conference on internet of things and cloud computing. ACM, p 46*
4. *Fisher J, Sanchez MH (2016) Authentication and verification of digital data utilizing blockchain technology. U.S. Patent Application 15/083,238*
5. *Goyal V, Pandey O, Sahai A, Waters B (2006, October) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and communications security. ACM, pp 89–98*
6. *Lewko A, Waters B (2011, May) Decentralizing attribute-based encryption. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 568–588*
7. *Horva´th M (2015, January) Attribute-based encryption optimized for cloud computing. In: International conference on current trends in theory and practice of informatics. Springer, Berlin, pp 566–577*
8. *Nimje AR, Gaikwad VT, Datir HN (2013) Attribute-based encryption techniques in cloud computing security: an overview. Int J Comput Trends Technol 4:2231*
9. *Hengartner U, Steenkiste P (2005) Exploiting hierarchical identity-based encryption for access control to pervasive computing information. In: SECURECOMM'05: Proceedings of the of the first international conference on security and privacy for emerging areas in comm, Networks, pp 384–396*
10. *Joye M, Neven G (2009) Forward-secure hierarchical IBE with applications to broadcast encryption. Ident Based Cryptogr 2:100*
11. *Wang S, Zhou J, Liu JK, Yu J, Chen J, Xie W (2016) An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Tran Inf ForensSecur 11(6):1265–1277*
12. *Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, Tenhunen H (2015, January) Smart e-health gateway: bringing intelligence to internet-of-things based ubiquitous healthcare systems. In: 2015 12th annual IEEE consumer communications and networking conference (CCNC). IEEE, pp 826–834*
13. *Begam S, Praveen H (2016) U-healthcare and IoT. Int J Comput Sci Mobile Comput 5(8):138–142*
14. *Rajput DS, Gour R (2017) An IoT framework for healthcare monitoring system. LAP LAMBERT Academic Publishing, Cambridge*
15. *Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L (2017, May). Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing. IEEE Press, pp 468–477*

16. *Ekblaw A, Azaria A, Halamka JD, Lippman A (2016) A case study for blockchain in healthcare: ''MedRec'' prototype for electronic health records and medical research data. Proc IEEE Open Big Data Conf 13:13*
17. *Bos JW, Halderman JA, Heninger N, Moore J, Naehrig M, Wustrow E (2014, March) Elliptic curve cryptography in practice. In: International conference on financial cryptography and data security. Springer, Berlin, pp 157–175*
18. *Xia J, Taveira J, Nunes M, Lingli D, Huang R, Cruz R (2016) Peer-to-peer streaming tracker protocol (PPSTP), No. RFC 7846*
19. *Yeh LY, Huang YL, Joseph AD, Shieh SW, Tsaur WJ (2012) A batch-authenticated and key agreement framework for p2p-based online social networks. IEEE Trans Veh Technol 61(4):1907–1924*
20. *Wang X, Xu S (2012, May) A secure access control scheme based on group for peer to peer network. In: 2012 International conference on systems and informatics (ICSAI). IEEE, pp 1507–1511*
21. *Badra S, Gomaab I, Abd-Elrahmanb E (2018) Multi-tier Blockchain framework for IoT-EHRs systems. Int Conf Emerg Ubiquitous Syst Pervasive Netw 141:159–166*
22. *Rodrigues JJ, Segundo DBDR, Junqueira HA, Sabino MH, Prince RM, Al-Muhtadi J, De Albuquerque VHC (2018) Enabling technologies for the internet of health things. IEEE Access 6:13129–13141*
23. *da Cruz MAA, Rodrigues JJPC, Al-Muhtadi J, Korotaev VV, de Albuquerque VHC (2018) A reference model for internet of things middleware. IEEE Internet Things J 5(2):871–883*
24. *Balamurugan B, Krishna PV, Kumar NS, Rajyalakshmi GV (2015) An efficient framework for health system based on hybrid cloud with ABE-outsourced decryption. In: Artificial intelligence and evolutionary algorithms in engineering systems. Springer, New Delhi, pp 41–49*
25. *Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JMR de Albuquerque VHC (2018) A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cogn Syst Res 52:1–11*
26. *Mahmoud MM, Rodrigues JJ, Ahmed SH, Shah SC, Al-Muhtadi JF, Korotaev VV, De Albuquerque VHC (2018) Enabling technologies on cloud of things for smart healthcare. IEEE Access 6:31950–31967*
27. *Hemalatha, P., Matilda, S.,Smart Digital Parenting Using Internet of Things,ICSNS 2018 - Proceedings of IEEE International Conference on Soft-Computing and Network Security, 2018, 8573622*
28. *Hemalatha, P., Dhanalakshmi, K, Development of IOT enabled voice recognition robotic guide dog for visually impaired people to enhance the guiding and interacting experience, Journal of Advanced Research in Dynamical and Control Systems, 2017, 9, pp. 262–272.*
29. *D. Jayakumar; Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; D. Saravanan; R. Parthiban; S. Usharani. "Certain Investigation On Monitoring The Load Of Short Distance Orienteering Sports On Campus Based On Embedded System Acceleration Sensor". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2477-2494.*
30. *R. Parthiban; S. Usharani; D. Saravanan; D. Jayakumar; Dr.U. Palani; Dr.D. StalinDavid; D. Raghuraman. "Prognosis Of Chronic Kidney Disease (Ckd) Using Hybrid Filter Wrapper Embedded Feature Selection Method". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2511-2530.*
31. *Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; R. Parthiban; S. Usharani; D. Jayakumar; D. Saravanan. "An Energy-Efficient Trust Based Secure Data Scheme In Wireless Sensor Networks". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2495-2510.*
32. *Dr. D. Stalin David; R. Parthiban; D. Jayakumar; S. Usharani; D. RaghuRaman; D. Saravanan; Dr.U. Palani. "Medical Wireless Sensor Network Coverage And Clinical Application Of Mri Liver Disease Diagnosis". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2559-2571.*
33. *D.Raghu Raman; D. Saravanan; R. Parthiban; Dr.U. Palani; Dr.D.Stalin David; S. Usharani; D. Jayakumar. "A Study On Application Of Various Artificial Intelligence Techniques On Internet Of Things". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2531-2557.*

34. *D.Saravanan; Dr.D.Stalin David; S.Usharani; D.Raghuraman; D.Jayakumar; Dr.U.Palani; R.Parthiban. "An Energy Efficient Traffic-Less Channel Scheduling Based Data Transmission In Wireless Networks". European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5704-5722.*
35. *S. Usharani; D.Jayakumar; Dr.U.Palani; D.Raghuraman; R.Parthiban; D.Saravanan; Dr.D.Stalin David. "Industrialized Service Innovation Platform Based On 5g Network And Machine Learning". European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5684-5703.*
36. *D Saravanan, R Bhavya, GI Archanaa, D Karthika, R Subban," Research on Detection of Mycobacterium Tuberculosis from Microscopic Sputum Smear Images Using Image Segmentation", 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).*
37. *R.Parthiban, Dr.K.Santhosh Kumar, Dr.R.Sathya, D.Saravanan," A Secure Data Transmission And Effective Heart Disease Monitoring Scheme Using Mecc And Dlmnn In The Cloud With The Help Of Iot", International Journal of Grid and Distributed Computing, ISSN: 2005 – 4262, Vol. 13, No. 2, (2020), pp. 834 – 856.*
38. *R.Bhavya, G.I.Archanaa, D.Karthika, D.Saravanan," Reflex Recognition of Tb Via Shade Duplicate Separation Built on Geometric Routine", International Journal of Pure and Applied Mathematics 119 (14), 831-836.*
39. *Dr.A.Senthil Kumar, Dr.G.Suresh, Dr.S.Lekashri, Mr.L.Ganesh Babu, Dr. R.Manikandan. (2021). Smart Agriculture System With E – Carbage Using Iot. International Journal of Modern Agriculture, 10(01), 928 - 931. Retrieved from http://www.modern-journals.com/index.php/ijma/article/view/690*
40. *Dr.G.Suresh, Dr.A.Senthil Kumar, Dr.S.Lekashri, Dr.R.Manikandan. (2021). Efficient Crop Yield Recommendation System Using Machine Learning For Digital Farming. International Journal of Modern Agriculture, 10(01), 906 - 914. Retrieved from http://www.modern-journals.com/index.php/ijma/article/view/688*