EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Blockchain-Enabled Hyperledger Fabric to Secure Data Transfer Mechanism for Medical Cyber-Physical System: Overview, Issues, and Challenges

P. Vinayasree[1, *], A. Mallikarjuna Reddy[2]

[1, 2] Anurag University, Hyderabad, India

Abstract

This paper proposes a model to address the challenges faced by medical cyber-physical systems (MCPS) by implementing a permissioned blockchain platform. The platform incorporates the unique properties of blockchain into the network of affected systems, including decentralization, transparency, and immutability. The platform also includes a novel technique to secure MCPS through an automated access-control manager. This manager allows users to control who has access to their data, and can be configured to trust a third party if desired. The paper also extends into networked medical device systems, and discusses how the platform can be used to address critical is-sues specific to this field, such as network design. Finally, the paper discusses how various security features can be integrated into ultra-small devices, enhancing the protection of embedded systems. The overall objective of this research is to develop a secure and efficient data transfer mechanism for MCPS. The proposed platform addresses the challenges faced by MCPS by incorporating the unique properties of blockchain.

Keywords: Blockchain technology, cyber-physical system, Data privacy, Data security, Healthcare, IoT

Received on 09 September 2023, accepted on 22 November 2023, published on 30 November 2023

doi: 10.4108/eetpht.9.4518

*Corresponding author. Email: vinayasreecse@cvsr.ac.in

1. Introduction

Cyber-physical systems (CPS) are an architectural paradigm that provides several benefits to the economy and society by combining pervasive sensing and communication technologies. The term "cyber-physical system" (or "cyber-sys") refers to a system that has been specifically built to include cyber components, such as computers and networks, within a traditional physical system or process [1]. These parts are remarkably intertwined, suggesting that the proper operation of one part is crucial to that of the other. Both of these parts are essential to each other's operation. Its fast growth is seen in several fields, such as the energy market, the healthcare industry, the transportation industry, and the IoT (Industrial Internet of Things) [2]. An in-depth study of stability, dependability, robustness, security, and privacy is required before such systems may be designed to be intelligent, efficient, and adaptable. The rapid advancement of enabling technology has, however, made such systems extremely susceptible to serious and far-reaching consequences. Without proper risk management, we risk losing out on the tremendous advantages that come with these developments. Establishing trust among nodes in a distributed system can be a time-consuming and inefficient process; however, blockchain technology has the potential to streamline this process. Being a key component in the CPS landscape, this technology is essential for facilitating decentralization [3]. Figure 1 shows the cyber physical system architecture.

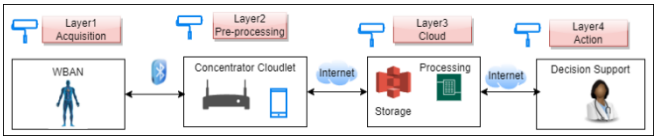

Figure 1. Overview of health care cyber physical system architecture

The medical field generates a massive amount of data, including information about patients' diagnoses, treatments, insurance coverage, personal details, etc. It also contains X-ray, CAT scan, MRI, and other imaging data. There is a significant opportunity for data tampering when information is kept in a cloud service or other centralized repository that is accessed by several parties for diverse purposes.

Table 1.

Paper and Year	Author	Methodology	Challenges
Improvements to the healthcare industry's e-health infrastructure for patient privacy and safety in 2017	Shrestha et al. [11]	This is a mixed method that provides both qualitative with a quantitative approach. This Method provides a means to discover the impacts by high reliability as well as validity. Conducting this method gives quality and the authenticity of the study	Rely on a single point of failure; have inadequate data privacy and security due to poor access controls.
A Blockchain future for internet of things security 2018	Benarjee et al. [12]	This methodology used to apply to enhance IOT Security. It provides data Integrity, transparency, and decentralized control.	Scalability; Low Performance and Speed; High Energy and resources are required for blockchain.
Facilitating the Shift to Patient-Driven Interoperability with Blockchain Technology in Healthcare (2018)	William Gordan et al. [13]	Offer a hand of assistance in the blockchain 's journey to patient-driven Interoperability	Data and Privacy; Data Standardization; Patient Identity Management; Consume More power and computational overhead.
Design and Analysis and Implementation of a security assessment/enhancement platform for cyber physical system 2021	X Ning, et al. [14]	For cyber physical system security, a hardware module is developed to aid in attack detection and mitigation, resulting in reduced or eliminated cps loss.	There is a scarcity of attack prevention and detection strategies.

Other possible solutions are investigated, including fog computing [4, 5], and mobile edge computing [6]. Another difficulty is dealing with the massive amounts of data generated by medical sensors [7]. The crypto-graphic algorithm [8], the Kalman filter [9], and the chaotic cryptosystem [10] are only a few of the proposed solutions to the security problems. There are some suggestions for managing and storing data [11, 12]. Although cryptographic methods like encryption might help prevent this kind of leak, there is always a danger that sensitive information could get into the wrong hands.

Solutions based on the blockchain are a good fit for this kind of problem. In the healthcare industry, permissioned blockchains, which are accessible exclusively to authorized users rather than the general public, can be used to manage authentication and data transmission with other characteristics [13]. Interplanetary File System (IPFS) is used by blockchain networks; it encrypts files and stores

the hash on the distributed ledger. The internet allows for easy access to the medical records that have been saved utilizing these methods [14]. Cloud data access increases latency and network capacity requirements, and researchers have discovered challenges with scalability, throughput, data volume, and patient privacy [15].

1.1 Motivation

Data exchange is crucial in cancer care, as multidisciplinary committees are formed to diagnose and categories malignancies. On a regular basis, these boards gather together to discuss cancer cases, compare notes, and formulate a plan for the most effective therapy possible. Trusting relationships between entities are essential in such a cooperative setting. Medical professionals aren't the only ones who can join such a group; pharmaceutical companies and research and development labs are often welcomed as well. This may increase the potential for financial and legal repercussions from clinical data breaches such as data leaking, tampering, and fabrication. Sensitive health data obtained by body sensors can be compromised by sophisticated assaults such as ransomware and denial of ser-vice. Therefore, it is essential that an intelligent healthcare system be built upon a foundation that protects the privacy and confidentiality of patient information.
In particular, this paper contributes in the following ways:
• Provide a comprehensive report on the ways in which blockchain technology is being implemented in CPS settings.
• Explain real-world uses for systems that combine cyber and non-cyber components such as communications, sensing, and computing.
• In order to determine if and when distributed ledger technologies like blockchain are appropriate for a given use case, a mathematical model is needed.
The remaining sections of the paper are structured as follows: In Part 2, we will discuss the relevant prior literature and the ways in which it has contributed to the field. In Section 3, we lay out the suggested system architecture and its proto-type model. Section 4 details the system's essential features. In Section 6 we offer the experimental analysis along with some outcomes. We have finished our work and outlined some suggestions for the future in Section 7.

2. Background

A blockchain is a distributed, persistent ledger to which new transactions with timestamps can be added and the results of these transactions are sorted into blocks. Several identical blocks can be built and kept in a decentralized manner, as specified by the blockchain's underlying protocol. One of the most important parts of this protocol is determining how a group of users (called miners) may reach an agreement on the state of the blockchain at any one time [16]. This algorithm makes the conservative assumption that only a small percentage of miners will become malicious or malfunctioning at any particular epoch. Blockchains can have a variety of structures (i.e., public, private, permissioned, and permission-less). The ability to join a blockchain ledger is a key feature of a public blockchain [17]. Typically, they are permission-less systems in which all participants have official status. Access to a private blockchain is restricted to a small set of authorized users. Each node in this instance has been hand-picked after extensive testing. They require special access credentials to join and do not pro-vide all users with the same privileges. Bitcoin is a pioneering permissionless blockchain protocol that continues to gain traction [18]. Every 10 minutes, a random miner is selected to have the privilege of adding a new block to the block-chain. Finding out who and how the next round of transactions will be introduced is the most pressing matter. Two common solutions to this issue are "proof of work" (PoW) and "proof of stake" (PoS). Let's examine the simplest possible scenario, where P1 makes a payment offer to P2. P1 first makes its intent clear, and then uses a cryptographic signature to ensure the integrity of the transaction. The network's miners verify the authenticity of all transactions and digital signatures. Following these procedures, the latest transactions are included in the distributed ledger. A hash, a unique code that incorporates the hash of the prior item in the chain, is used to link each block in the chain to the one before it. Miners are re-quired to do a number of computations to demonstrate their leadership abilities [19]. These computations resolve a problem by fitting a variable-size data set into a fixed-size one. Any given network may use one of these procedures to choose a leader. Many miners race to be the first to solve the challenge and broadcast their answer to the network in Proof of Work (PoW). Further miners check to ensure the accuracy of the completed work. When this is established, the miner automatically becomes the group's leader. This method is computation-ally intensive due to the large number of miners attempting to answer the puzzle concurrently (see figure 2) [20].

2.1. Blockchain Limitations and Future Directions

This study extensive literature coverage is indicative of the widespread interest in blockchain technology that has developed in recent years. It has the ability to completely transform the way people collaborate and share information since it sets the way for apps that will leverage linked devices in the future. However, it does have a few drawbacks, such as the following:

- The block size and computation time required are too large a fixed point to allow it to scale with the number of linked devices.
- It may necessitate transaction fees or another form of miner incentive in some implementations.

- It is dependent on a small number of powerful actors, such as miners, but is less centralized than the idea of a central bank.

Blockchain participants have high computational and storage demands since they are responsible for keeping the whole ledger and serving as endorsers or miners in the transaction verification process. Because to these restrictions, blockchain technology is not suitable for a very big IoT system with many interconnected devices. To address these concerns, in 2019 the tangle protocol was proposed as a method of ensuring the integrity of IoT-related transactions [23]. It's more suited to solving the needs of the Internet of Things (IoT), including low resource consumption, broad interoperability, billions of nano-transactions, and data integrity, since it's quicker, uses less energy and resources, and is quantum-proof.

3. Hyperledger Fabric

Fabric is a decentralized operating system that permissioned blockchains may use to execute compiled code written in general purpose programming languages (like Go, Java, and Node.js). It skips cryptocurrency in favor of an append-only replicated ledger data structure, allowing for the secure preservation of execution history. In contrast to the standard order execute design used by other blockchain systems such as HLF's preview version [25], Fabric provides an execute-order-validate architecture [24]. The plan is to split off the process of placing an order and having a smart contract (SC) carry it out. When compared to the conventional state machine replication approach [26], this architecture has several advantages: it is more scalable, it makes more generous trust assumptions when validating transactions, it allows for non-deterministic SC to be used, and it allows for modular consensus implementations [28, 29]. The peers in Fabric are responsible for processing transactions and updating the distributed ledger. All network transactions are ordered by the orderers, who also propose new blocks and try to reach consensus. The accumulation of orders received from the ordering service.

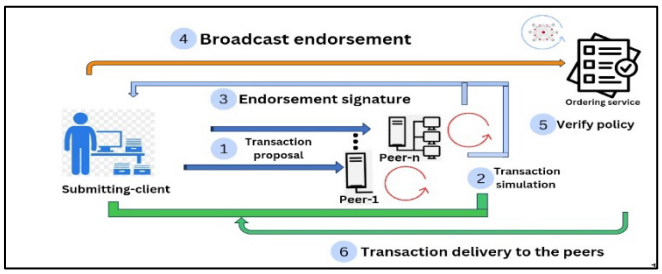

Figure 2. Fabric high level transaction flow

Each node in the network is a committer by default, meaning it receives a batch of transactions from the ordering service in the form of state updates in an ordered fashion and updates the distributed ledger. Each node in the network is responsible for validating new blocks, making any necessary adjustments to its own copy of the ledger, and adding the completed block to the chain. Peers who endorse a transaction are able to attest to its authenticity on behalf of the buyer or seller. An endorser provides the simulated transaction to the client after completing a mock transaction by executing the smart contract (SC; "chain code" in HLF) and appending the results with its crypto signature (known endorsement). Keep in mind that one peer node can play the roles of both endorser and committer.

4. Security and privacy challenges with Cyber-Physical System

The advent of IoT and wearable technologies in recent years has enhanced the quality of patient care by allowing for greater remote patient control. It also helps doctors treat more patients. The term "Remote Patient Management" (RPM) [30] refers to a system that monitors and treats patients outside of the typical hospital or clinic setting (at home, for instance). To begin, we can relax into the natural convenience of patient care. As necessary, patients should be connected with medical professionals. It improves service while decreasing expenses for hospitals. This is the primary motivation for healthcare professionals' pursuit of RPM delivery mechanisms. Health data from wearable devices is transmitted to hospitals or other medical facilities for use in patient monitoring and diagnosis. Wearable healthcare devices are microcontroller-based smart electronics that can be worn as clothing accessories. They don't get in the way, and users may access advanced capabilities like wire-free data transfer, real-time feedback, and alert systems from their computers. These gadgets will offer doctors with critical data, such as patient vitals, blood sugar levels, respiration patterns, etc.

In order to ensure that the data's authenticity is maintained, it is essential that the data not be altered, lost, or corrupted in any way. Patients should have the power to control who has access to their data but should not have the ability to make any changes themselves. Information that is both trustworthy and publicly accessible in the medical field should be easily accessible regardless of specialization [31, 32]. Hence, Medical CPS includes cutting-edge medical technologies and problems, such as complicated embedded systems enabled with communication services that can monitor a patient's body's control and physical features. Such examples are implantable biocompatible devices, robotic prosthetics, and proton therapy machines for treatment. In the event that one of these devices fails or breaks, it can have a serious impact on the health of the patients. Therefore, validating and certifying their proper operation is crucial, while being an arduous undertaking. Several critical infrastructures (CPSs) are currently under investigation after a variety of security flaws were found in

systems. Our research shows that while the services are forthright, they also have an insatiable appetite for knowledge. It is important to note that the same method can be used to address diverse privacy concerns, such as those involving the disclosure of patients' medical records for research purposes, etc. In a word, our solution can protect sensitive information from the following threats to privacy: *Ownership of the Data:* The users retain full control over their own data and are the sole proprietors of the information they generate. Assuming all goes well, the system will correctly identify the users as the genuine and authorized data and service controllers.
Data Transparency and Auditability: Every user has the ability to adjust and regulate the information that are gathered about him or her, in addition to the manner in which those details are made visible to other users. Distributed ledgers are kept of all activity related to the data.
Fine-grained Access Control: The need for several permissions to be provided after registration is a major issue for mobile applications.

4.1 Applications of Blockchain in Healthcare

Blockchain is being used to keep track of records in fields like public health and medical research which uses patient data. The criteria of feasibility, planned capabilities, and compliance [34] may be used to the evaluation of blockchain-based decentralized applications in the healthcare field. Vital for medical records, blockchain's primary advantage is that it leaves no digital footprint when a document is altered or deleted. Blockchain is being used by many countries, including Estonia, to protect health and clinical trial records by tying user access to predetermined levels of permission The final link in the supply chain should be the only one with access to the real-time records, thus bolstering the security of the process. Blockchain has various applications, including data sharing, access control, health records, audit trail management, and the supply chain [35].

4.2 Privacy and security concerns in a cyber-physical system

Since cyber-physical systems are now widely employed in a variety of applications, it is imperative that security concerns associated with these systems be given a very high level of priority. Serious repercussions will result from the compromise of these systems (through numerous security vulnerabilities, assaults) in critical infrastructure [13]. Security countermeasures that integrate well into cyber-physical systems are necessary in the face of such threats. In addition to being challenging, the deployment and maintenance of patches and many other regular upgrades in cyber physical systems and control systems are also problematic. New research issues in MCPS [14] include high assurance software, interoperability, knowledge of context, security and privacy, and certifiability. In conclusion, MCPS allow various researchers, sectors, etc. to move forward by addressing privacy and security issues. Have in mind that it is a major challenge to create a CPS architecture that is both effective and visually appealing. A multi-view, multi-stakeholder, extensible framework is required for early design choices in CPS architecture. There are a number of potential problems that might develop with CPS, including those related to its adaptability, performance, dependability, portability, flexibility, heterogeneity, reliability, maintainability, verification, and compatibility. Thus, some major concerns and difficulties in CPS and MCPS are discussed here.

Flaws in Biometric Capture Systems: CPSs offer a wide range of services to a large user base, making them susceptible to a variety of attacks. Contractors are hired to handle the system's most important functions. As a result, these companies may compromise or get access to customers' biometric and private data.

Stored or collected data: Presents a significant chance for data leakage by private entities. Through the CPS network, a large number of private individuals are participating in the full sequence of registration and data generation procedures. As a result, it's crucial to assess the integrity and accountability of the participants/users.

Cryptographic techniques: Public network security and commercially available cryptographic products provide security for CPS infrastructures. Using these approaches dramatically increases the likelihood of confidential data being lost, disrupted, observed on, monitored, or hacked.

5. Proposed Solutions to the MCPS for Building Affordable, Accurate, reliable and innovative approach

The affordable, accurate, reliable, and innovative permissioned Blockchain Technology has been proposed for secure healthcare cyber physical system. The proposed framework involves obtaining the patient data from the medical sensors through IoT gateway. The collected data from the patients are secured using permissioned blockchain and stored in the cloud. The data accessor (doctors) requests the miner to access the patient data, which is stored in the cloud, the miner check the authentication of the doctors if authenticated miner provides the access to the data.

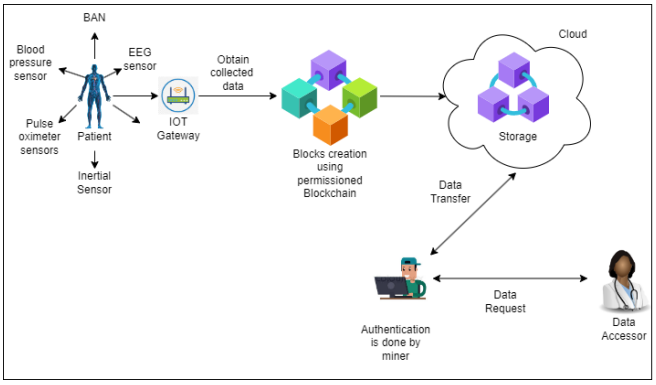

Figure 3. Proposed block diagram

The permissioned blockchain's high-level architecture is depicted in Figure 3. Here, when a transaction is requested, a data structure is broadcast to all nodes in the network so that they can keep track of the collection of transactions. Before any new blocks are added to the blockchain, all the nodes verify the previous ones. Verifying blocks results in a financial incentive for participating nodes.

In a similar vein, when a new node is added to the blockchain network, it is provided with a full copy of the blockchain. Whenever a new block has been added to the blockchain, the information is shared around all of the nodes that are currently active in the network. After that, every node verifies the block to ensure the information contained within it is accurate. If everything checks out, the block will be added to the local blockchain on each node.

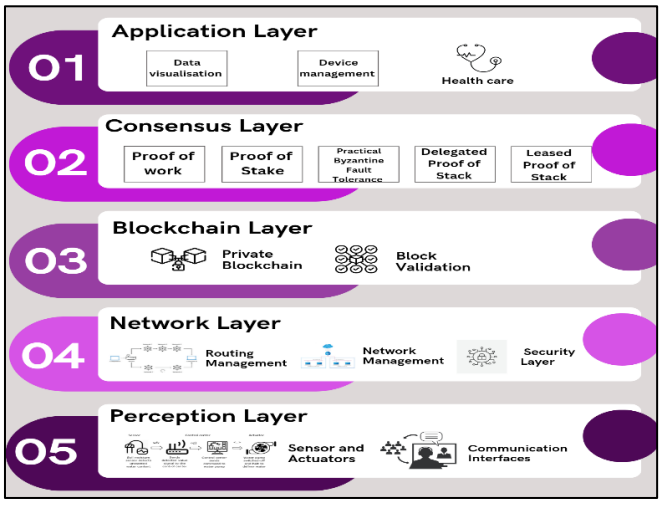

Figure 4. Fabric high level transaction flow

- *Affordable:* Light weight digital signature was utilized for low-powered devices, and light weight ring signature was used in addition to digital signature to protect user anonymity at a low cost.
- *Accurate:* employs a pair of symmetric encryption algorithms, one for the data and one for the key, to foil any attempts at tampering or hacking.
- *Trustworthy:* Information is received without corruption, loss, or deletion.
- *Innovative:* In order to simplify things, we created an MCPS-based overlay network, which involves splitting networks up into multiple clusters (instead than using a proof of work mechanism or a single chain of blocks).
- *Innovation:* Our method is more efficient than existing models and frameworks in establishing appropriate security requirements and protecting user privacy in medical cyber physical systems.

6. Conclusion

MCPS is becoming more important and will be an important part of the connected digital eco-system in the near future. Despite its many benefits, MCPS is increasingly at risk due to rising worries about electronic health records (EHR). Since more and more people are coming to rely on MCPS to supply EHR data sets, privacy and security concerns are anticipated to increase as a result of this trend. The study proposes enabling MCPS with blockchain technology so as to take use of the characteristics of a blockchain. In contrast to bitcoin's public and unchangeable ecosystem, the MCPS would prefer a permissions-based blockchain with encrypted data transfers. This study suggests using multichain enterprise [19] blockchain as a way to reach this goal, since it offers both safe storage and permission control at the bare thread level. In a secure environment, patients would be able to control who has access to their electronic health records. While in this work we suggest a blockchain-enabled MCPS model and provide a proof of concept using a simplified example, there are still many other avenues to explore. In the present paper, blockchain and cloud services have been used to store data sets. In any case, blockchain technologies like IPFS [20, 21] can make this storage even more decentralized. The actual potential of blockchain will be realized if decentralization is extended to storage in a variety of blockchain-enabled applications. Furthermore, blockchain capabilities can be scaled to much larger levels with the use of artificial intelligence [22]. Hence, while our study has established a proof of concept on a limited scale model, there are certain to be obstacles in a particular real time situation, as mentioned in Sect. 4, that must be handled before the full potential of decentralized via blockchain can be achieved.

References

1. Kumar, A., Chatterjee, K. A lightweight blockchain-based framework for medical cyber-physical system. J Supercomput (2023). https://doi.org/10.1007/s11227-023-05133-2.
2. Tiwari, A., Batra, U. (2022). Medical Cyber-Physical Systems Enabled with Permissioned Blockchain. In: Singh, M., Tyagi, V., Gupta, P.K., Flusser, J., Ören, T. (eds) Advances in Computing and Data Sciences. ICACDS 2022. Communications in Computer and Information Science, vol 1614. Springer, Cham. https://doi.org/10.1007/978-3-031-12641-3_7
3. Murala, D.K., Panda, S.K., Sahoo, S.K. (2023). Securing Electronic Health Record System in Cloud Environment Using Blockchain Technology. In: Panda, S.K., Mishra, V., Dash, S.P., Pani, A.K. (eds) Recent Advances in Blockchain Technology. Intelligent Systems Reference Library, vol 237. Springer, Cham. https://doi.org/10.1007/978-3-031-22835-3_4
4. Aluvalu R, Kumaran V. N. S, Thirumalaisamy M, Basheer S, Ali aldhahri E, Selvarajan S. 2023. Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. PeerJ Computer Science 9:e1308.
5. Nanda, S.K., Panda, S.K. & Dash, M. Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-14846-8
6. Sabella, R., Shamsunder, S., Albrecht, S., Bovensiepen, D.: Guest editorial: networks for cyber-physical systems and industry 4.0. IEEE Commun. Mag. 59(8), 12 (2021). https://doi.org/10.1109/MCOM.2021.9530505.
7. El Hamdi, S., Abouabdellah, A., Oudani, M.: Industry 4.0: fundamentals and main challenges. In: 2019 International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA), pp. 1–5 (2019). https://doi.org/10.1109/LOGISTIQUA.2019.8907280.
8. Sokolsky, O.: Medical cyber-physical systems. In: 2011 18th IEEE International Conference and Workshops on Engineering of Computer-Based Systems, p. 2 (2011). https://doi.org/10.1109/ECBS.2011.40.
9. H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 9, pp. 2499-2505, Sept. 2020, doi: 10.1109/JBHI.2020.2973467.
10. N. M. Shrestha1 , Abeer Alsadoon1 , P.W.C. Prasad1 , L. Hourany1 , A. Elchouemi2 1 School of Computing and Mathematics, Charles Sturt University, Sydney, Australia 2 Hewlett Packard Enterprise. Enhanced e-Health Framework for Security and Privacy in Healthcare System.
11. Mandrita Banerjee a, Junghee Lee a, Kim-Kwang Raymond Choo b,a,* A blockchain future for internet of things security: a position paper.
12. William J. Gordon, Christian Catalini. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.
13. Xirong Ning and Jin Jiang, Fellow, IEEE. Design, Analysis and Implementation of a Security Assessment/Enhancement Platform for Cyber-Physical Systems, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 18, NO. 2, FEBRUARY 2022
14. Keshta, I., Odeh, A.: Security and privacy of electronic health records: concerns and challenges. Egypt. Inform. J. 22(2), 177–183 (2021). https://doi.org/10.1016/j.eij.2020.07.003.
15. Milne, A.J., Beckmann, A., Kumar. P.: Cyber-physical trust systems driven by blockchain. IEEE Access 8, 66423–66437 (2020). https://doi.org/10.1109/ACCESS.2020.2984675.
16. Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical Cyber Physical Systems and Its Issues, Procedia Computer Science, Volume 165, 2019, Pages 647-655.
17. Egala, B.S.; Priyanka, S.; Pradhan, A.K. SHPI: Smart Healthcare System for Patients in ICU using IoT. In Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 16–19 December 2019; pp. 1–6.
18. Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach. IEEE Trans. Netw. Sci. Eng. 2022, 9, 271–281.
19. Zhang, J.; Wu, M. Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine. Electronics 2020, 9, 1746.
20. Gordon, W.J.; Catalini, C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. 2018, 16, 224–230.
21. F. Chen et al., "Medical Cyber–Physical Systems: A Solution to Smart Health and the State of the Art," in IEEE Transactions on Computational Social Systems, vol. 9, no. 5, pp. 1359-1386, Oct. 2022, doi: 10.1109/TCSS.2021.3122807.
22. Sudeepthi Govathoti, A Mallikarjuna Reddy, Deepthi Kamidi , G BalaKrishna, Sri Silpa Padmanabhuni, Pradeepini Gera, Data Augmentation Techniques on Chilly Plants to Classify Healthy and Bacterial Blight Disease Leaves, Article Published in International Journal of Advanced Computer Science and Applications(IJACSA), Volume 13 Issue 6, 2022.
23. Mallikarjuna A. Reddy, Sudheer K. Reddy, Santhosh C.N. Kumar and Srinivasa K. Reddy, Leveraging bio-maximum inverse rank method for iris and palm recognition. International Journal of Biometrics, Published Online:July 11, 2022
24. Padmaja Grandhe; A.Mallikarjuna Reddy; Kavyasri Chillapalli; Kavya Koppera; Manasa Thambabathula; L P Reddy Surasani, Improving The Hiding Capacity of Image Steganography with Stego-Analysis. IEEE International Conference,2023
25. A. Mallikarjuna Reddy, K. S. Reddy, An Efficient Multilevel Thresholding Scheme for Heart Image Segmentation Using a Hybrid Generalized Adversarial Network, Hindawi, 2022
26. Dey, N., Ashour, A.S., Shi, F. et al. Medical cyber-physical systems: A survey. J Med Syst 42, 74 (2018). https://doi.org/10.1007/s10916-018-0921-x.
27. Y. Zhang, D. Zheng and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control", IEEE Internet Things J., vol. 5, no. 3, pp. 2130-2145, Jun 2018.
28. H. Sukhwani, N. Wang, K. S. Trivedi and A. Rindos, "Performance Modeling of Hyperledger Fabric

(Permissioned Blockchain Network)," 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2018, pp. 1-8, doi: 10.1109/NCA.2018.8548070.
29. X. Wang, A. Zhang, X. Xie, and X. Ye, "Secure-aware and privacy-preserving electronic health record searching in cloud environment," International Journal of Communication Systems, vol. 32, no. 8, article e3925, 2019.
30. Gia Nhu Nguyen, Nin Ho Le Viet, Mohamed Elhoseny, K. Shankar, B.B. Gupta, Ahmed A. Abd El-Latif, Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model, Journal of Parallel and Distributed Computing, Volume. 153, 2021, Pages 150-160.
31. Panda, S.K., Satapathy, S.C. Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. Pers Ubiquit Comput (2021). https://doi.org/10.1007/s00779-021-01588-3
32. Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C. (Eds.), Springer, Blockchain Technology: Applications and Challenges, Editors: Intelligent Systems Reference Library. https://doi.org/10.1007/978-3-030-69395-4