IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FORTIFIED-CHAIN: A BLOCKCHAIN-BASED FRAMEWORK FOR SECURITY AND PRIVACY-ASSURED INTERNET OF MEDICAL THINGS WITH EFFECTIVE ACCESS CONTROL

Vidyashree Biradar, Dr Sridevi Hosmani

[1]Students, Dept. of Computer Science Engineering, Sharnbasva University Engineering and technology(Exclusive for Women), Kalaburgi,,India

[4]Asst.Professor,Dept.ofComputerScienceEngineering,Sharnbasva University Engineering and technology(Exclusive for Women), Kalaburgi,,India

ABSTRACT: The rapid developments in the Internet of Medical Things (IoMT) help the smart healthcare systems to deliver more sophisticated real-time services. At the same time, IoMT also raises many privacy and security issues. Also, the heterogeneous nature of these devices makes it challenging to develop a common security standard solution. Furthermore, the existing cloud-centric IoMT healthcare systems depend on cloud computing for electrical health records (EHR) and medical services, which is not suggestible for a decentralized IoMT healthcare system. In this article, we have proposed a blockchain-based novel architecture that provides a decentralized EHR and smart-contract-based service automation without compromising with the system security and privacy. In this architecture, we have introduced the hybrid computing paradigm with the blockchain-based distributed data storage system to overcome blockchain-based cloud-centric IoMT healthcare system drawbacks, such as high latency, high storage cost, and single point of failure. A decentralized selective ring-based access control mechanism is introduced along with device authentication and patient records anonymity algorithms to improve the proposed system's security capabilities. We have evaluated the latency and cost effectiveness of data sharing on the proposed system using Blockchain. Also, we conducted a logical system analysis, which reveals that our architecture-based security and privacy mechanisms are capable of fulfilling the requirements of decentralized IoMT smart healthcare systems. Experimental analysis proves that our fortified-chain-based H-CPS needs insignificant storage and has a response time in the order of milliseconds as compared to traditional centralized H-CPS while providing decentralized automated access control, security, and privacy

1.INTRODUCTION

The Internet of medical things (IoMT) is an integrated embedded system of software, hardware, network access, and sensor/actuators [1, 2]. As these systems are more sophisticated and interfere with critical healthcare operations, due to which it raises many security and privacy issues. However, IoMT technology revolves at a greater speed, yet majority of devices are resource-constrained and limits us from considering the high-end mechanism for security and privacy perspectives. Regardless of having multiple protocols and standards for IoMT ecosystems, it lacks in security and privacy issues [3].

In addition, the classical cloud-centric healthcare systems have inherent problems like a single point failure, lack of transparency, low level of contover personal data, and high latency. Because of less availability of medical service professionals, the healthcare industry is unable to provide critical healthcare services to large number of patients [4] during pandemic time. These particular technical challenges are achievable with the help of a perfect combination of protocols, mechanisms, and enhanced system architecture. The remote patient monitoring system (RPMS) helps the healthcare service providers to eliminate unnecessary engagement of professionals in regular consultancy and provides more time for understanding the patient's health issues to improve the patient health status. It is suggestible to have a parallel supporting system to automate primary healthcare services to handle pandemics with limited healthcare professionals.

A cloud-centric H-CPS architecture is illustrated in Fig. 1, where the patient's data is transferred to a cloud for data processing and analysis [5]. However, this model is not a suitable option for patient-centric time-critical healthcare systems [6] which requires low latency. Moreover, they are vulnerable to single point of failure and Denial of Service attacks (DoS) attack that leads to service unavailability. As a result, healthcare service providers migrate to a decentralized community managed frameworks. These are more patient-centric and provides transparent healthcare services on decentralized architectures. Present cloud-centric IoMT healthcare architecture models guarantees event traceability, security and low cost maintenance. However, it still lacks in privacy, transparency, data ownership, and community control mechanism. To overcome these important issues, the new generation systems utilize robust advanced technologies like blockchain, distributed data storage systems (DDSS), and hybrid computing. The blockchain technology is a decentralized distributed ledger system which provides smart-contracts, and exhibits traceability, transparency in digital asset management [7].

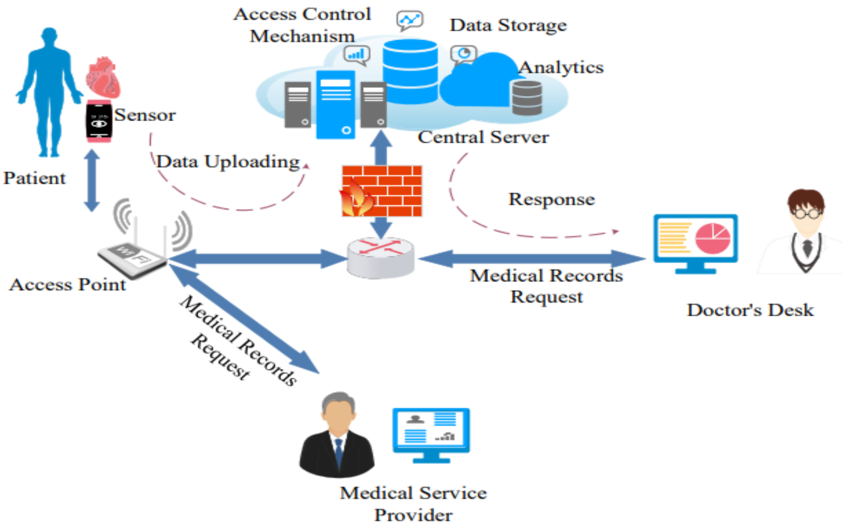


Fig: Overview of a Smart Healthcare System or Healthcare Cyber-Physical Systems (H-CPS).

The transactions in blockchain are represented as blocks linked together to form a chain of blocks. If one block or transaction is forced to alter, then we need to change the entire chain header information of that blockchain. The transaction integrity is maintained by using Merkel tree mechanism. However, use of blockchain technology for IoMT or H-CPS is not straightforward due to several deficiencies in the original blockchain, such as lack of scalability and high computational demand [8].

The smart-contracts automates event-driven actions without intervention of a third party to provide a cost-effective automation solutions [9]. In order to mitigate large data storage problem of blockchain, we have adopted a distributed data storage system (DDSS) named as InterPlanetary File System (IPFS) [10]. The chosen DDSS provides a content-centric peer-to-peer faster data sharing. It uses data caching and file versioning to maintain multiple documents with same name. However, when a large size file is uploaded to DDSS, it breaks the file into multiple objects of 256kb and connects all these objects to an empty object to retrieve the complete file using Distributed Hash Tables (DHTs) [11]. Another major issue is high latency in real-time data utilization. A proposed novel hybrid computing model focuses on low latency and real time data utilization by combining the edge and cloud computing topologies [12]. However, sending critical data to cloud for data processing and analysis requires high bandwidth and 24/7 connectivity which offers high latency and cost [13]. On the other hand, edge computing provides computational capability at the edge of the network to reduce the latency and eliminates the high bandwidth cost. Therefore, in our work we have designed hybrid model to gain benefits from both the technologies

2.RELATED WORK

Blockchain technology in healthcare: The revolution starts here

The authors of this paper[25] presented Blockchain technology has shown its considerable adaptability in recent years as a variety of market sectors sought ways of incorporating its abilities into their operations. While so far most of the focus has been on the financial services industry, several projects in other service related areas such as healthcare show this is beginning to change. Numerous starting points for Blockchain technology in the healthcare industry are the focus of this report. With examples for public healthcare management, user-oriented medical research and drug counterfeiting in the pharmaceutical sector, this report aims to illustrate possible influences, goals and potentials connected to this disruptive technology.

Design of cold chain application framework (CCAF) based on IOT and cloud

The authors of this paper[27] a smart cold chain application framework (SCCAF) based on Cloud and IOT (Internet of Things) techniques. The purpose of SCCAF is to provide PaaS (Platform as a Service) and IaaS (Infra as a Service) to users who want to develop and apply cold chain management systems with low cost and in short time. Also, SCCAF enables users to use any type of IOT devices such as RFID tags, WSN sensor nodes, BLE (Bluetooth Low Energy) sensor nodes and so on. We define common components by generalizing function of existing cold chain management systems, and design SCCAF based on Hadoop and Spark to store the large amount of data stream on salable storage and process stream data to detect events and assess risks in cold chain.

Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly,

The authors of this paper[28] unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U^6 HCS)

The outcomes in this paper are (i)A systematic investigation of the current IoMT, Block Chain and Cloud Storage in Health Care;(ii) Explore the challenges and necessities for the confluence of Block Chain (BC), Internet of Medical Things (IoMT), Cloud Computing (CC);(iii)Formulate the requirements necessary for the real-time remote Health Care of one-to-one care structure, which, supports the vital functions that are critical to the Patient Centric Health Care;(iv) Design and develop a novel BC IoMT U6 HCS (Block Chain based Internet of Medical Thin

Applications of Ensuring Security and Privacy Using Block Chain with IoT for Health Record

The authors of this paper [29] the healthcare system has key security and privacy requirements when considered like an enterprise, such as safeguarding patients' medical records from unwanted access, protected drug tracking, secure connection with transportation such as ambulances, and secure and smart e-health surveillance. With suitable security measures, block chain has brought novel concepts in security and safety of medical data, and it may reconcile the discrepancy among sharing data and confidentiality. We combine the strengths of both block chain and cloud computing in this research to provide a confidentiality method for block chain and IoT. This strategy incorporates IoT and delivers IoT services to block chain nodes; in the meantime, it gathers, examines, operates, and preserves in the identity validation for health information. Interaction and addresses the inadequate computing capabilities of some block chain nodes in order to confirm data validity and feasibility. The proposed approach is efficient, as demonstrated by the simulation experiment. It can preserve and verify the integrity of medical data while also addressing issues such as high computer complexity, data exchange, and privacy protection.

3.METHODOLOGY

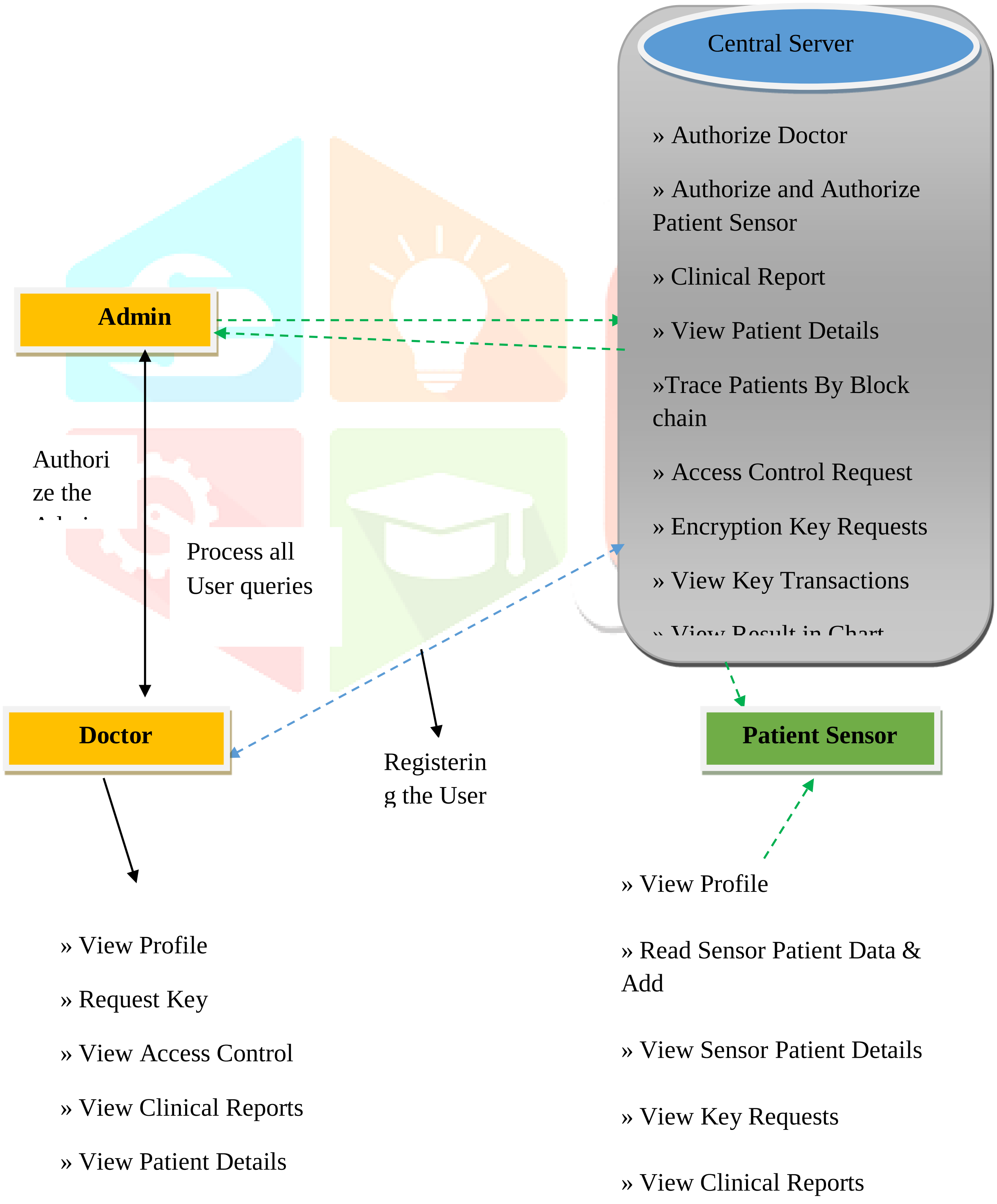
Central Server: In this module, the Server login by using valid user name and password. After login successful he can do some operations such as Authorize Doctor, Authorize Sensor Patient, Clinical Report, View Patient Details, Access Control Request, Encryption Key Requests, View Key Transactions, and View Result in Chart

View and Authorize Users : In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Sensor Patient: In this module, there are n numbers of sensor patient are present. Owner should register before doing any operations. Once patient registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful Owner will do some operations like View Profile, Add Patient Details, View Patient Details, View Key Requests, and View Clinical Reports.

Doctor: In this module, there are n numbers of doctors are present. Doctor User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Request

Key, View Access Control, View Clinical Reports, and View Patient Details.



Organization of Fortified-Chain In this paper, we have proposed a novel architecture and cryptography methods for IoMT-based to provide data privacy, security, traceability, low latency, low storage cost and availability

Our proposed architectural model is divided into three layers for easy system implementation and management. The first layer has data generators or IoT sensors like heart beat sensor, temperature sensor, etc. The second layer represents novel hybrid computing paradigm which combines the edge and cloud paradigms to gain benefits from both technologies. The third layer is data consumers layer which consists of actuators like smart insulin, caretaker robot, smart beds, etc. The system layer view is represented in the, In our proposed work, we suggested Datagram Transport Layer Security (DTLS) protocol which ensures the secure communication between these three layers.

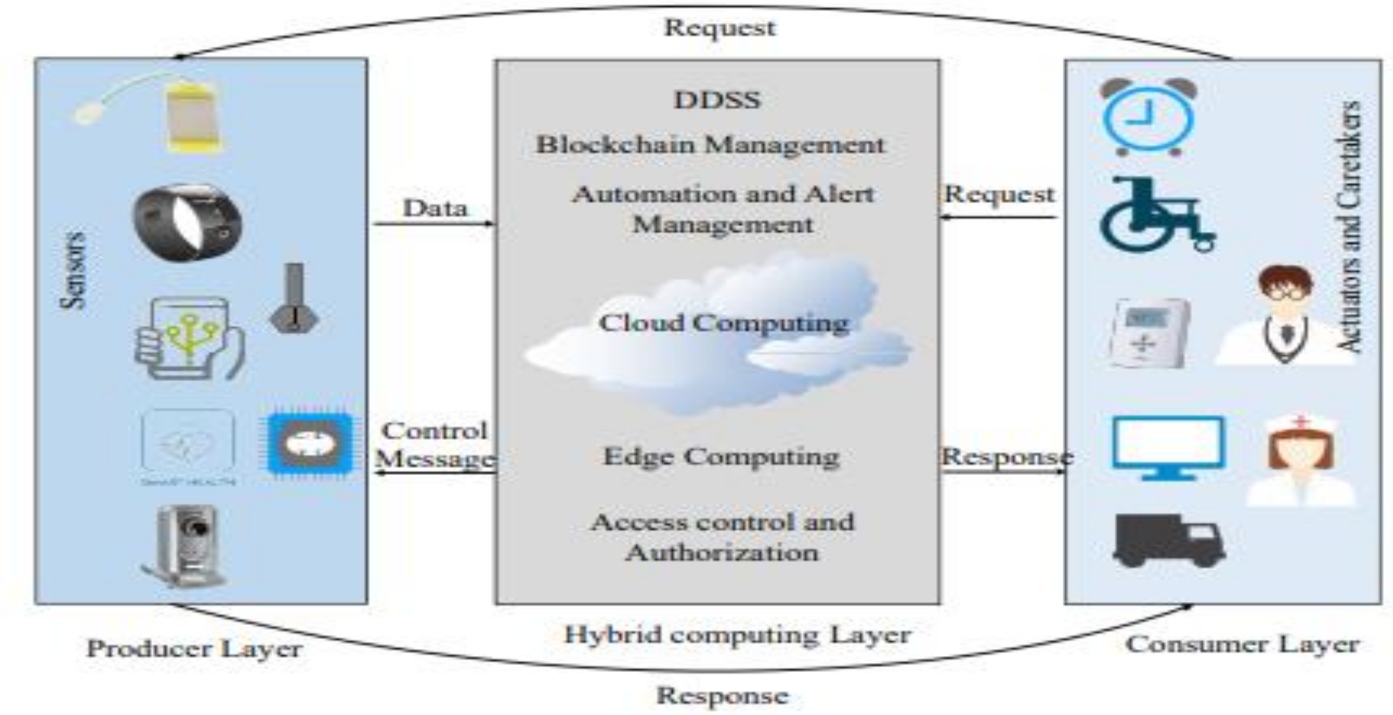


Fig: Fortified-Chain in a Layered view.

In addition, we have also introduced three cryptography mechanisms in the form of algorithms to deliver system level privacy and security. Likewise, we combined blockchain technology and DDSS to achieve a decentralized EHRs transparent system. Our proposed model maintains a public ledger for each medical record and critical event to provide traceability. Moreover, system specific smart-contracts help medical professionals to perform event-based automation activities without human interference

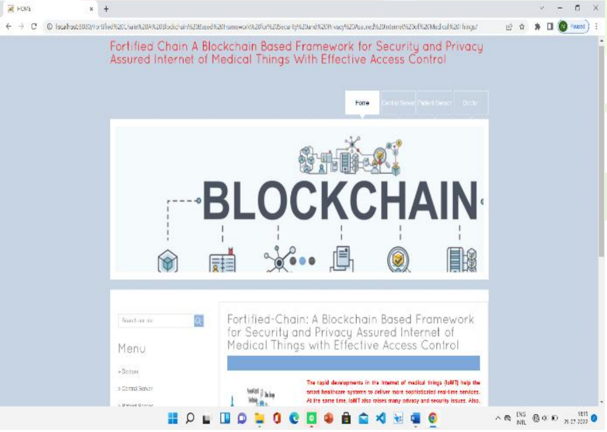
The sensor generated patient medical raw data is appended with additional information and encrypted with respective edge computer public key before it transfer to consumer layer. At the middle layer, hybrid computing performs the data processing and analysis followed by decision making. Moreover, it performs tasks related to data storage, access controlling, and anonymity along with blockchain based DDSS management. Also, the hybrid computing layer takes care of smart-contract creation and deployment. In the consumer layer, the actuators and terminals perform events defined by a specific smart-contract. In this paper, we have illustrated all Fortified-Chain functions and algorithms in an abstract format. The following sub sections give a detailed view of the three layers.

1) Data Producer Layer: The layer performs device registration and secure patient data transfer to the respective edge computer in a fixed time intervals. As, majority of IoT sensors are primarily resource constraint devices, hence, our architecture eliminates blockchain and DDSS operations overhead using edge devices as proxy for constrain devices. Due to this, the essential resources of the sensors is only used for patient data operations to provide long uninterrupted services. In our proposed system, the sensors generate patient's raw medical data (Datraw) and appends with supplementary information like service identity, device identity, digital signature, raw data hash value and time-stamp..

2) Hybrid Computing Layer: A hybrid computing is distributed computing topology that brings computational and storage capability near to the data source along with robust features of cloud computing. In our proposed work majority of the critical operations of the system is performed by the edge computing topology where as cloud computing provides necessary additional and backup services. In this layer, the data received from sensors is decrypted and validated before data processing and analysis.

3) Data Consumer Layer: This layer consists of actuators, service provider terminals, emergency alerting systems etc. The nodes act as per the decisions received from the hybrid computing layer. Simultaneously, hospital level edge computer monitors and alerts node operational status like online or offline in a frequent time intervals to hybrid computing for smoother system operation.

4.EXPERIMENTAL RESULTS



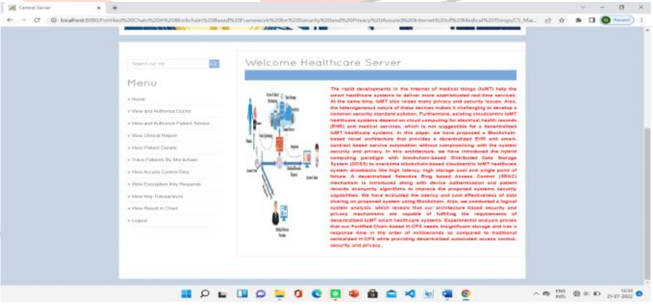
Fortified Chain A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things With Effective Access Control

Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control

The rapid developments in the Internet of medical things (IoMT) help the smart healthcare systems to deliver more sophisticated real-time services. At the same time, IoMT also raises many privacy and security issues. Also,

Fig: Home Page

Our project has been start its operation in the home page, home page contains the login pages of central server, patient sensor and doctors

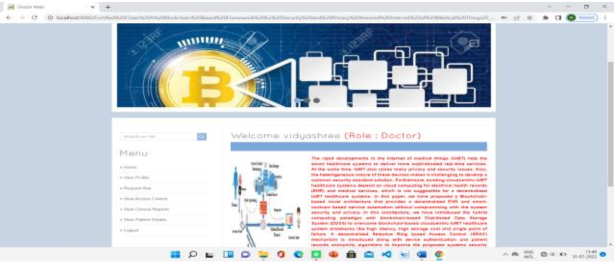

Central Server
Search our site
Menu
» Home
» View and Authorize Doctor
» View and Authorize Patient Sensor
» View Clinical Report
» View Patient Details
» Trace Patients By Blockchain
» View Access Control Req
» View Encryption Key Requests
» View Key Transactions
» View Result in Chart
» Logout

Welcome Healthcare Server

The rapid developments in the Internet of medical things (IoMT) help the smart healthcare systems to deliver more sophisticated real-time services. At the same time, IoMT also raises many privacy and security issues. Also, the heterogeneous nature of these devices makes it challenging to develop a common security standard solution. Furthermore, existing cloudcentric IoMT healthcare systems depend on cloud computing for electrical health records (EHR) and medical services, which is not suggestible for a decentralized IoMT healthcare systems. In this paper, we have proposed a Blockchain-based novel architecture that provides a decentralized EHR and smart-contract based service automation without compromising with the system security and privacy. In this architecture, we have introduced the hybrid computing paradigm with blockchain-based Distributed Data Storage System (DDSS) to overcome blockchain-based cloudcentric IoMT healthcare system drawbacks like high latency, high storage cost and single point of failure. A decentralized Selective Ring based Access Control (SRAC) mechanism is introduced along with device authentication and patient records anonymity algorithms to improve the proposed systems security capabilities. We have evaluated the latency and cost effectiveness of data sharing on proposed system using Blockchain. Also, we conducted a logical system analysis, which reveals that our architecture based security and privacy mechanisms are capable of fulfilling the requirements of decentralized IoMT smart healthcare systems. Experimental analysis proves that our Fortified-Chain based H-CPS needs insignificant storage and has a response time in the order of milliseconds as compared to traditional centralized H-CPS while providing decentralized automated access control, security, and privacy.

Fig :Overview Of Central Server Page

After server login by using valid user name and password. After login successful he can do some operations such as Authorize Doctor, Authorize Sensor Patient, Clinical Report, View Patient Details, Access Control Request, Encryption Key Requests, View Key Transactions, and View Result in Chart



Welcome vidyashree (Role : Doctor)

The rapid developments in the Internet of medical things (IoMT) help the smart healthcare systems to deliver more sophisticated real-time services. At the same time, IoMT also raises many privacy and security issues. Also, the heterogeneous nature of these devices makes it challenging to develop a common security standard solution. Furthermore, existing cloudcentric IoMT healthcare systems depend on cloud computing for electrical health records (EHR) and medical services, which is not suggestible for a decentralized IoMT healthcare systems. In this paper, we have proposed a Blockchain-based novel architecture that provides a decentralized EHR and smart-contract based service automation without compromising with the system security and privacy. In this architecture, we have introduced the hybrid computing paradigm with blockchain-based Distributed Data Storage System (DDSS) to overcome blockchain-based cloudcentric IoMT healthcare system drawbacks like high latency, high storage cost and single point of failure. A decentralized Selective Ring based Access Control (SRAC) mechanism is introduced along with device authentication and patient records anonymity algorithms to improve the proposed systems security

Fig: Overview Of Doctor Page

After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Request Key, View Access Control, View Clinical Reports, and View Patient Details.

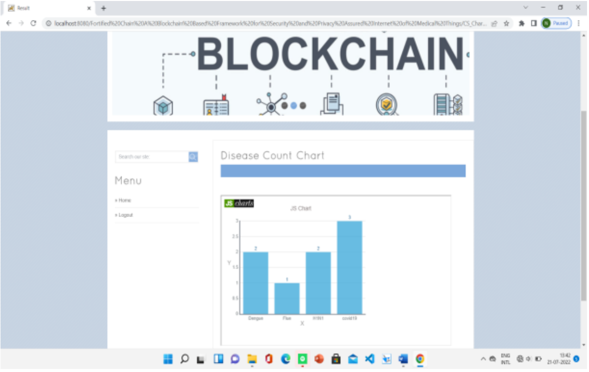


Fig: Result chart

In this resulting page we are predicting result by view the graph page

CONCLUSION

In this work, we have elucidated a novel approach to solve the problems related to latency, data security, privacy, anonymity, and traceability in decentralized IoMT based smart healthcare systems. Moreover, it showcases the leverage blockchain, DDSS, and hybrid computing to deliver architecture level solutions to the discussed issues. The system level traceability is achieved through blockchain-based tamper-proof public ledgers. The SRAC and other proposed cryptography techniques assure the medical data security and privacy. On the other hand, smart contract automates the medical emergency alerting and primary medical services. Simultaneously, the proposed architecture provides a platform for different stakeholders in the healthcare industry to make digital agreements. In the logical analysis, our system exhibited expected functionalities like low latency in data sharing for critical situations. In the future work, we will explore the techniques to leverage the intelligence to our system by using AI/ML technology. Our focus will be on future generation critical patient monitoring and assisting system framework requirements to deal with different types of pandemics. Aim of our future work is to provide a robust system to enhance healthcare services capability along with quality of services (QoS). Moreover, we will develop a full level prototype with all the proposed capabilities in real time scenario. In addition, the future work will be able to detect and alert all stake holders about prepandemic identifications related to a particular area in real time.

REFERENCES

[1] Y. Sun, F. P. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," IEEE Access, vol. 7, pp. 183 339–183 355, 2019.

[2] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 388–397, 2019.

[3] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2702– 2733, 2019.

[4] T. Tekeste, H. Saleh, B. Mohammad, and M. Ismail, IoT for Healthcare: Ultra Low Power ECG Processing System for IoT Devices. Cham: Springer International Publishing, 2019, pp. 7–12.
[5] Y. Zhang, M. Qiu, C. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data," IEEE Systems Journal, vol. 11, no. 1, pp. 88–95, 2017.
[6] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "BeCome: Blockchain-Enabled Computation Offloading for IoT in Mobile Edge Computing," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4187–4195, 2020.
[7] S. Biswas, K. Sharif, F. Li, and S. P. Mohanty, "Blockchain for E-Healthcare Systems: Easier Said Than Done," IEEE Computer, vol. 53, no. 7, pp. 57–67, 2020.
[8] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2343–2355, 2020.
[9] E. Bhaskara Santhosh, S. Priyanka, and A. K. Pradhan, "SHPI: Smart Healthcare System for Patients in ICU using IoT," in Advanced Networks and Telecommunications Systems, 2019, pp. 1–6.
[10] T. M. Fernandez-Caram ´ es and P. Fraga-Lamas, "A Re- ´ view on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32 979–33 001, 2018.
[11] F. Klemm, S. Girdzijauskas, J. Le Boudec, and K. Aberer, "On routing in distributed hash tables," in Seventh IEEE International Conference on Peer-to-Peer Computing, 2007, pp. 113–122.
[12] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. L. Tan, "BLOCKBENCH: A Framework for Analyzing Private Blockchains," in Proceedings of the ACM International Conference on Management of Data, 2017, p. 1085–1100.
[13] M. H. Ghahramani, M. Zhou, and C. T. Hon, "Toward cloud computing QoS architecture: analysis of cloud systems and cloud services," IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 1, pp. 6–18, 2017.
[14] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," IEEE Access, vol. 6, pp. 53 698–53 708, 2018.
[15] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[16] Y. Zhang, D. He, and K.-K. R. Choo, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT," Wireless Communications and Mobile Computing, vol. 2018, pp. 1–9, 2018.
[17] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," IEEE Access, vol. 7, pp. 66 792–66 806, 2019.
[18] S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," IEEE Access, vol. 6, pp. 38 437–38 450, 2018. [19] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2019. [20] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs," in Proc. IEEE International Conference on Internet of Things (iThings), 2018, pp. 1027–1034. [21] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, 2018.[22] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," IEEE Access, vol. 5, pp. 25 408–25 420, 2017.
[23] A. H. Sodhro, Z. Luo, A. K. Sangaiah, and S. W. Baik, "Mobile edge computing based QoS optimization in medical healthcare applications," International Journal of Information Management, vol. 45, p. 308–318, 2019.
[24] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming, 2015, pp. 217–222.

[25] ***Blockchain technology in healthcare: The revolution starts here*** 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)

[26] ***Drugledger: A practical blockchain system for drug traceability and regulation***2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

[27] ***Design of cold chain application framework (CCAF) based on IOT and cloud*** 2015 8th International Conference on u- and e-Service, Science and Technology (UNESST)

[28] **Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly** IEEE Access (Volume: 8)

[29] Blockchain: The Next Direction of Digital Payment in Drug Purchase Applications of Ensuring Security and Privacy Using Block Chain with IoT for Health Recordhttps://www.researchgate.net/publication/361644820_Blockchain_The_Next_Direction_of_Digital_Payment_in_Drug_Purchase