Convergence of Blockchain, IoMT, AI for Healthcare Platform Framework

Ms. Vibhuti Awastl
vibhutiawasthi28@gma

Dr.Nikhil Karande,
nikhilkarande18@gmail.com

Dr. Sumit Bhattacharjee
bsumit021@gmail.com

Abstract: *This paper proposes the work of creating a healthcare platform framework which integrates Blockchain, Internet of Medical Things(IoMT) and Artificial Intelligence(AI) which covers applications raging from collecting medical records, analyzing it and maintaining security of it. These applications will eventually enable remote patient monitoring particularly during virus outbreaks thus protecting frontline healthcare professionals by reducing the risk of contracting diseases. Also it enhances the reach of healthcare to people. Further it helps detect and predict future diseases.*

Blockchain which is a distributed hyperledger will help in secure handling of data. IoMT will help collecting data and process it on the fly. AI will help in long term prediction and analytics of data.

Convergence of these technologies in a healthcare platform poses technical challenges which this work intends to address. Right from interoperability to protocol mismatches all sorts of challenges occur while integration. The work proposes a solution to address these problems and provide a user friendly, cost effective solution to healthcare professionals and in the larger interest of patients and society.

Keywords-keyboards; Internet of Medical Things(IoMT), Artificial Intelligence(AI) , Blockchain,healthcare platform, edge computing, fog computing, interoperability.

1. INTRODUCTION

Why IoT in healthcare?

The IoT has broad application in the field of medical care as well as health care. It has potential to provide ascend to numerous medical services and applications like remote or distant health monitoring, information tracking, improved drug usage, device, emergency care, healthcare charting etc. The IoT has a variety of application area which includes health care. The modern health care is becoming sophisticated and redesigned by the IoT revolution. Promising technological, economic, and social prospects promote the revolution in IoT. The IoT is likely to enable a range of healthcare solutions. In the context of healthcare, service and application cannot be differentiated objectively and both are interdependent. So, both IoT services and IoT applications ought to have closer attention[1].

Why Blockchain in healthcare?

A key initiative taken by Government of India in response to Prime Minister Narendra Modi's "Digital India" move is the formation of Internet of Things (IoT) ecosystem for smart healthcare. Any security flaw occurring during authentication with a centralized environment affects the connectivity of devices in the network and the transaction of data in IoT. As a solution, Blockchain technology emerges to use in IoT network for the betterment. The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems. In IoMT environment, a private Blockchain network is created containing all the participants of a hospital including doctors, lab technicians, patients and clinical laboratories etc., There exists no necessity to carry the report by the patients during every visit, as the data is already available in the network. The data is completely decentralized to avoid failure, data loss and to provide faster recovery. Whenever a change is attempted by a third person in the database, a notification is sent to all the members of the group. Since this is a private Blockchain, it requires an additional level of authentication. Whenever any new person requires being a part of the network a document for proof is provided. The data is transparent, so any modification done by any member of the group will get notified to

everyone. An additional level security can be provided for data transfer based upon the mutually agreed security parameter and any modification in database is accepted upon approval of all members[2].

Why Artificial intelligence in healthcare?

Artificial intelligence is the most vital area which can be explored more and more in this field. Healthcare robots are being used today but it will be used more in near future than today. To be futuristic, It may seem that, there will be a 50% increase in the use of robots by 2020. In fact, these robots perform simple, automated tasks such as delivering medications, food and lab results. Internet of medical things (IoMT) devices can also directly feed data into larger AI-driven healthcare analytics systems. These systems can diagnose heart disease, and detect blood infections and even certain types of cancer. These IoMT devices are being more improved and will be able to diagnose more diseases in future. Next-generation IoT devices will bring intelligent services as part of their offering, allowing for real-time data which enables some actions to be executed by the device if necessary, and then send back data to the patient and their clinical teams[3].

2. LITERATURE SURVEY

Healthcare system plays a vital role in our day to day life especially for old age people. In the recent days, a hospital visit by an old aged person has become a customary one. The hospital system requires the patient to do a lot of tests just to make sure that they are perfectly fit. The records needs to be maintained properly else the tests which were performed should be done repeatedly which ultimately results in wastage of money and the health of the patient. The main objective of any healthcare management system is to provide high quality service to the patients. But this has become a very tedious one because of the ardent rules and laws imposed by the government and the hospital management[4]. One cannot always ensure that the service provided by the provider is always satisfactory. Sometimes the patient and the hospital cannot have a direct contact rather they go through an intermediate person. That person cannot be relied upon all the time. Sometimes if money is going to be the motive of the person, then his main objective will be making money and not on providing a quality healthcare service. The crucial part of any healthcare management system is patients' medical record. This data is distributes among many systems and hence makes the process of accessing the data very difficult. Proper exchanging of the information is also not done properly in the current system. This creates a big gap which needs to be filled out by making use of proper mechanisms. The healthcare organizations store the reports of the tests and other procedures locally in the respective hospital servers. This might be easy from the hospital point of view. But they face a very serious flaw from the patients' view since they need to perform the tests again and again if they are not satisfied with the diagnosis and the treatment given by the hospital. This is really a time consuming procedure for the patient. The doctors also face issues if they are not able to diagnose the disease properly because of missing data in the reports. The maintenance of the records is also a very expensive procedure for a hospital management. Any healthcare system ultimately keeps patient health management as a priority and focusses on providing quality health services. But providing these become extremely arduous and lengthy with several regulations and laws being imposed. There is a huge gap between the payers and providers which is a major setback in providing quality health service. To make matters worse, there exists a dependency on the intermediaries in the supply chain. Data about the patients is critical and these are scattered across systems and this makes the data inaccessible and not handily available. The absence of a smooth process management renders this 316 K. Anitha Kumari et al. existing healthcare system incomplete. It can also not handle information exchange which makes it inadequate and in need of huge changes. The healthcare organizations still make use of outdated systems which house patient data. They can cover the functionality of storing the patient data locally but makes life difficult for medical practitioners during the time of diagnosis. It would be time consuming and tedious from patient perspective as well. This considerably increases the cost of maintenance of these businesses. The healthcare system thus obviously needs a better system to deliver appropriate patient care and high quality health care. But these organizations are wary of the huge misuse of data that could cause lot of trouble because of any breach. So there is always a need of the system which takes care of the flaws discussed above but at the same time should take care of two major issues: money and security. Small hospitals will not be having enough revenue to invest in servers to maintain the records. On the other

hand multispecialty hospitals have enough money to buy servers but sometimes they are not able to provide quality service to the patients. This is because when any security breach in the security premise, the data are prone to leakage and there won't be any privacy to the patients 'data. Some of the issues face by the current scenario is: • Part of the data available in the servers is either missing or erroneous. • Proper recording of the reports are not done properly. Sometimes the entry might be made by a newbie who does not have any prior experience. • Apart from identifying a breach in the system, the recovery cost is costly and may increase in future. In the current healthcare system faces many issues and they need a system which performs better. For example, a pharmaceutical company might have patented a new medicine. Initially the cost might be little bit higher. So some fraudulent companies which want to make money might produce similar medicine with similar name and appearance and release the same into the market at a very low cost. People tend to be get attracted by such product as they do not want to spend money on a similar costly product. This results in a very big loss to the company. Many do not find this as a very dangerous issue[5]. Counterfeiting the drugs is an important issue to be taken care of. Unless and until there is no problem arising, the fraudulent company goes on with the production. If in case a massive death rate occurs in a particular, after consuming the fraudulent medicine, there the issue starts. The authorized manufacturer of the medicine might face some legal issues. If the supply is tracked properly, then these kinds of issues might be eradicated to a considerable extent.

As of December 2018, a survey revealed the following:

• These fraudulent activities take place mostly in China and India.

• According to Word Heath Organisation, either the drugs contain wrong components or it contains wrong composition of the components.

• A total of 200 billion dollars is involved in this per year 12 Securing Internet of Medical Things.

• Out of this, a major portion of income comes through the ales of the drugs through internet. • This involves a coverage of 30% of the rugs sold worldwide. It is not the fact that simply manufacturing fake medicine is illegal. This in turn might result in many other serious issues [5]. The patients may buy such fake medicines unknowingly. No proper guarantee can be given that the medicines might cure the diseases in all the cases. Sometimes taking a contaminated or wrong medicine for a prolonged period might result in many serious ailments. This is because the companies do not mix the ingredient in proper proportions. The way in which these medicines are administered to the patients might differ from one company to another. Also this results in a huge loss to the nations' revenue.

Millions of dollars are involved in this sector. Also there will be recession in this area as the companies do not need so many employees. Blockchain can be used here to solve this problem [6–11]. Another persistent difficulty in today's healthcare system is Health Information Exchange. Even though many fraudulent companies make money out of this business, the one who is directly affected is the patient. They actually do not have any idea about what is happening in the background. The details about the patient are leaked out and sometimes they are sold out for research purpose. They don't have any idea about what data is stored, where it gets stored, how it gets stored and who stores it. The mere presence of technologies and cutting edge gadgets in the healthcare facilities does not provide means of collection, analysis and seamless data exchange. Thus, today's healthcare system needs a system that is efficient in terms of both economy and usage, smooth in functioning and also transparent. All this paved way for the introduction of a technology in the healthcare system, the Blockchain.

Patient health data management is difficult because of two main issues in the healthcare industry[12].

• First, each patient is unique therefore there can be no such thing as a common disease or common treatment strategy. So what works on a patient might not work on the other and vice versa due to inter-individual variability. Hence, there is a need to access the complete medical records in order to adapt the treatment and provide personalised care. All in all, healthcare is becoming more and more patient-centred and thus more and more specific ad patient data oriented.

• Second, sharing information among the medical community is a major challenge. Even today, doctors use social networks to communicate and share patient data. Medical data is sensitive and should always go through secured networks when revealed. The lack of any sort of secure structure to share data is an important obstacle for scientific advancements. Though medical

records are kept in very different locations without having a common database sounds secure, this derails scientific advances since only on allowing the researchers to access the data there 318 K. Anitha Kumari et al. can be a heavy contribution to scientific advances worldwide especially when it comes to rare diseases or minorities.

3. ORIGINAL CONTRIBUTIONS TO THE PAPER

The work of this paper intends to create a healthcare platform framework which integrates Blockchain, Internet of Medical Things(IoMT) and Artificial Intelligence(AI) which covers applications namely collecting medical records and analyzing it and maintaining security of it. These applications will eventually enable remote patient monitoring particularly during virus outbreaks thus protecting frontline healthcare professionals by reducing the risk of contracting diseases. Also it enhances the reach of healthcare to people. Further it helps detect and predict future diseases.

4. SYSTEM DESIGN

Figure 1. A workflow of blockchain-based healthcare applications.

The workflow is composed of four main layers including healthcare raw data, blockchain technology, healthcare application, and stakeholders.

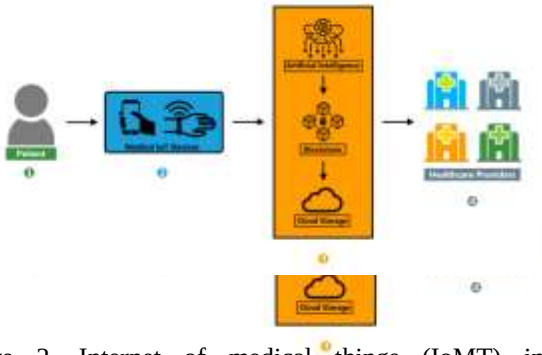

Figure 2. Internet of medical things (IoMT) in blockchain.

The following sections elaborate mostly on the progress in healthcare IoT and smart medical devices in the AI arena. Figure 3 is an illustration of IoMT in blockchain.

• Step-1: In the realm of IoMT, the patient is the source of all data.

• Step-2: Medical IoT devices are normally either attached closely or remotely monitoring patients' body, consequently, generating large volume of data.

• Step-3: Data generated in step-2 are stored on blocks or on the cloud storage. AI will help blockchain to create intelligent virtual agents, which in turn can create new ledgers automatically. In case of sensitive medical data, where security is the first priority, decentralized AI system could help block chain to reach highest security [135].

• Step-4: Healthcare providers are the end users who seek access for a safe and sound care delivery which is authorized by the owner.

5. HEALTHCARE DATA MANAGEMENT IN BLOCKCHAIN

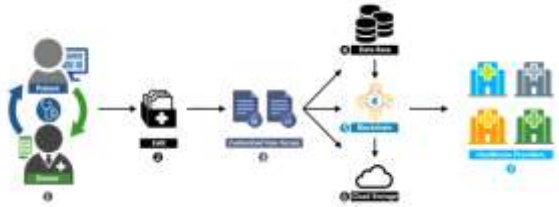

Figure 3. Healthcare data management in blockchain.

Step-1: Primary data is generated by the interaction between a patient and their doctors and specialists. This data consists of medical history, current problem and other physiological information.
• Step-2: An EHR is created for each patient using the primary data collected in the first step. Other medical information such as those generated from nursing care, medical imaging, and drug history are also included in EHR.
• Step-3: Individual patient who has the ownership of sensitive EHR, and customized access control is given only to the owner of this property. Parties who want to access such valuable information must request permission which is forwarded to the EHR owner, and the owner will decide to whom access will be granted.
• Step-4, 5, and 6: These three steps are part of the core of the whole process including database, the blockchain, and cloud storage. Database and cloud storage store the records in a distributed manner and a blockchain provides extreme privacy to ensure customized authentic user access.
• Step-7: Healthcare providers such as ad hoc clinic, community care center, hospitals are the end user who wants to get access for a safe and sound care delivery which will be authorized by the owner. For example, no matter where you are treated in the globe, your health record will be available and accessible on your phone and validated through a distributed ledger such as blockchain, to which healthcare providers would continue to add to over time.

Convergence of these technologies is proposed and challenges will be encountered and solved in the platform to be designed.

Blockchain technology, Artificial Intelligence, and the Internet of Things are brought innovation to the digital world in all aspects. They have the potential to come together and create new business models such as machines that will act as their profit centers. This integration will increase the development of auto business models dramatic way.

The convergence between these technologies will be as follows:

IoT collects and renders healthcare information in the form of data.

Blockchain technology stores healthcare data securely and improves transparency.

AI helps to find multiple patterns based on healthcare data and helps to optimize processes.

Referring to design, AI, IoT, and blockchain are complements, and their integration can deliver the maximum potential all of them have. It will be very productive for the automation and data management in healthcare [17].

The implementation of IoT at a large scale means that there is coordination between billions of devices through data management. According to recent researches, there will be more than 50 billion devices in 2025. So, monitoring them will be a critical task for large organizations. Hence there is a need to integrate blockchain solutions with IoT to reduce problems in this industry.The integration of blockchain with IoT will allow every device with a public key, and it can send encrypted messages to other devices and also receive responses against them. Therefore, it becomes clear that devices have control over their identity. In addition to this, the device can create history and reputed regularly being tracked by blockchain[18].

Blockchain and AI are aiming to reshape multiple industries. Both of them bring a lot of benefits and challenges along with them. The logical combination of these technologies will bring useful outcomes for every industry. Blockchain decentralizes AI processes like data, analytics, and models to offer trust and confidence that end-users need to rely on AI-based business operations.Machines are producing a huge amount of data, and it becomes difficult to make this data invulnerable to hackers. AI models integrated with blockchain solutions strengthen solutions protocols and makes processing faster. Additionally, emerging blockchain technologies use AI to create autonomous organizations and marketplaces that minimize costs and enhance accessibility[18].

Blockchain has the potential to build a connection with AI and IoT because blockchain brings missing trust for both these technologies. When technologies become successful to achieve the trust of multiple communities, they reach the next level. Therefore, the integration of IoT, AI, and Blockchain technology will increase the trust in data at a broad level. The increase in the trust will convince everyone to adopt IoT and AI without any fear. It will take the digital world into a new era where everything will be smart and autonomous[19].

IoT, AI, and blockchain bring outstanding benefits for security, transparency, immutability, and automation of the business process. Furthermore, the integration of blockchain technology with them adds trust to their

usability. It will make data management more efficient by boosting privacy, security, and standardization of data. If you want to enhance users' interest in your product or service, then add blockchain with AI and IoT[20-25]

6. CONCLUSION

In this paper , we have discussed convergence challenges in combining AI, IoMT and blockchain technology in the field of healthcare. The main problem that we believe it needs attention from researchers is how the blockchain will operate in tandem with AI, IoMT in complex and diverse communication and analytic environments and systems. The IoMT delivery system will be using communication networks owned by different service providers with different data access control policies. For the blockchain technology to work in such an environment, we need research that investigates blockchain mechanisms that promote single global access policy for the whole network. Furthermore, since the network consists of nodes and computers that are spatially separated, there is a need for synchronization mechanisms to identify the order of block additions. We also suggest further research on innovative solutions that promote blockchain as a service that allows various parties (networks, devices, users, etc.) of the IoMT paradigm to access basic coherent blockchain infrastructures in healthcare systems.

References

[1] Panesar, A. *Machine Learning and AI for Healthcare: Big Data for Improved Health Outcomes*; Springer: Emeryville, CA, USA, 2019.

[2] Frost, J.H.; Massagli, M.P. Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another's data. *J. Med. Internet Res.***2008**, *10*, e15.

[3] Castaldo, L.; Cinque, V. Blockchain-based logging for the cross-border exchange of ehealth data in europe. In *International ISCIS Security Workshop*; Springer: Cham, Switzerland, 2018; pp. 46–56.

[4] Hien, D.T.T.; Hien, D.H.; Pham, V.H. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. In Proceedings of the ACM Ninth International Symposium on Information and Communication Technology, Danang City, Vietnam, 6–7 December 2018; pp. 200–207.

[5] Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.

[6] Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**.

[7] Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136.

[8] Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, *42*, 147.

[9] Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**,*9*, 1207.

[10] Vo, H.T.; Kundu, A.; Mohania, M.K. *Research Directions in Blockchain Data Management and Analytics*; EDBT: Lisbon, Portugal, 2018; pp. 445–448.

[11] Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gen. Comput. Syst.* **2019**, *91*, 527–535.

[12] Genestier, P.; Zouarhi, S.; Limeux, P.; Excoffier, D.; Prola, A.; Sandon, S.; Temerson, J.M. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *J. Int. Soc. Telemed. eHealth* **2017**, *5*, GKR-e24.

[13] Zhang, R.; Liu, L. Security models and requirements for healthcare application clouds. In Proceedings of the 2010 IEEE 3rd International Conference on cloud Computing,

Miami, FL, USA, 5–10 July 2010; pp. 268–275

[14] Bahga, A.; Madisetti, V.K. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inform.* **2013**, *17*, 894–906.

[15] Batty, M. (2016). How Can Big Data Be Used in Urban Planning? http://www.alexandrinepress.co.uk/planning-with-big-data

[16] Bronson, K., & Knezevic, I. (2016). Big Data in food and agriculture. *Big Data & Society*, *3*(1),2053951716648174

[17] Catalini, C., Gans, J. S. (2017). "Some Simple Economics of the Blockchain". *MIT Sloan School Working Paper:* 5191–16.

[18] Epstein, J. (2017).When blockchain meets big data, the payoff will be huge. https://venturebeat.com/2017/07/30/when-blockchain-meets-big-data-the-payoff-will-be-huge/

[19] Rabah, K. (2017b). Challenges & Opportunities for Blockchain Powered Healthcare Systems: *A Review*. *Mara res. j. med. health sci*., Vol. 1. No. 1. Pages 45 – 52

[20] Rabah, K. (2017c). Challenges & Opportunities of Implementing Blockchain Security & Privacy. *Mara International Journal of Computer Science & Information Security*, Vol. 1, No. 1, Pages 1 – 11

[21] Rabah, K. (2018). Overview of Distributed Ledger Technology: *A Review*, *Realm International Journal of Information Security* Vol. 1, No. 1, pp. 1 - 9

[22] Walsh, S. (2017). Blockchain, IoT, AI Will Converge in Healthcare, https://www.rtinsights.com/blockchain-iot-ai-will-converge-in-healthcare/

[23] Rabah, K. (2018). Convergence of AI, IoT, Big Data and Blockchain: *A Review*. *The Lake Institute Journal*; Vol. 1, No. 1, Pages 1 - 18

[24] Internet of Medical Things (IoMT)—The Future of Healthcare. Available online: https://igniteoutsourcing.com/healthcare/internet-of-medical-things-iomt-examples/ (accessed on 20 March 2021)

[25] Kuo, T.T.; Ohno-Machado, L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. *arXiv* **2018**, arXiv:1802.01746.