A DETAILED REVIEW ON USE OF IOT AND BLOCKCHAIN IN HEALTH CARE

Illa Singh, Assistant Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

A rapid surge in medical big data has led to a new and unavoidable fact about our healthcare: Medical care is now an integral aspect of our lives. Using IoT-based wearable technologies, healthcare practitioners are streamlining the diagnostic and treatment process. Most recently, we've seen the networked use of billions of sensors, gadgets, and cars. Many such technologies—remote patient monitoring—are used in the current practise of medical treatment and care. However, the use of these technologies has both privacy and security dangers. Health data privacy and security concerns may be caused by a delay in therapeutic progress, resulting in even worse patient outcomes. We suggest the use of a blockchain to store and manage healthcare large data, and make it accessible for study. Even while blockchains are computationally costly, consume a considerable amount of bandwidth, and are therefore not ideal for most resource-constrained IoT devices aimed for smart cities, these digital currencies have other benefits. We tackle the aforementioned difficulties using blockchain IoT devices in our project. A new model of modified blockchain frameworks is proposed to meet the specific needs of IoT devices, such as providing increased privacy and security for the devices while being able to provide access to the information for other purposes on the network. We use some more complex cryptographic primitives to achieve these extra privacy and security aspects in our architecture. By using these ideas, businesses may build more secure and anonymous IoT application data and transactions over a blockchain-based network.

KEYWORDS: IOT, Blockchain, Healthcare, Information Technology.

INTRODUCTION

As the number of individuals seeking medical treatment grows, it becomes more difficult for people to find primary-care physicians or caretakers. Using IoT and wearable devices, the quality of health care has been enhanced, allowing for remote patient monitoring. Additionally, it enables doctors to handle a greater number of patients. providing monitoring and treatment for patients who are away from a clinical environment (in the home as an example). Convenience of service is firstly provided by the fundamental functionality of the design. Patients may keep in touch with their doctors if they are needed. Reducing medical expenditures and improving treatment is a byproduct of the use of healthcare resources more efficiently. RPM provides a huge benefit to the population, hence suppliers are using different ways to give it to the public. RPM is based on the idea of using a smartphone with internet access and an RPM application to collect health data, as well as to monitor the machine, and then transmitting the data to smart contracts. Wearable devices and the Internet of Things are critical in RPM, as well as in Smart City development. Patient health data, such as heart rate, temperature, and breathing rate, are gathered by

wearable devices and then sent to medical institutions where they're used to monitor and diagnose health problems and provide therapy. This kind of setup allows for the creation of a Big Data scenario since all the patient data is being examined and shared.

Clothing and accessories equipped with micro-controllers are wearable electronic devices that may be implanted into the fabric. These kind of tools may be placed unobtrusively, have simple user interfaces, and include useful features like wireless data transfer, real-time feedback, and notifications embedded into the product.

IOT IN HELATHCARE

In this study, we use Refs. [3–8] to identify and elaborate on the major motivations for our own exploration of blockchain in healthcare. Since Bitcoin was first implemented in Ref. [1], new applications of the underlying technology are almost limitless. Blockchain has been attempted in a variety of other applications, with the most well-known being within the financial sector [9–14]. One may easily envisage the many possible uses of this technology in healthcare, smart cities, and the Internet of Things.

In [15], an introduction of blockchain's capabilities in drug development was given. Irving and Holden tried this using a clinical trial design in which previously documented result switching has been shown. The organisations found that using blockchain for their low-cost, independently verifiable audit methods has proven to be successful. Ref. [2] has shown us that lightweight digital signature methods are an excellent alternative to traditional ones, and that we should employ them in our research.

MEDICAL DATA

With relation to medical data, there have already been several data breaches and data losses (16,17). Hackers will look for health information since it may include sensitive information like credit card numbers and social security numbers. Health information management is a crucial component when it comes to medical record ownership. A variety of records—such as reports, photos, videos, and raw data—are included inside each record. Depending on the systems that are in use by the particular provider, these components might also appear in various forms. To preserve the integrity of these documents, it is very critical. To preserve the integrity of the data, contingencies must be in place. Since patient data should be protected, the ability to access that data should be regulated. However, the patients should not be allowed to modify the data either. Consistent and accessible records should be maintained [18,19].

We have seen outstanding work by Wu and Ota in reference [20–23] in the context of Smart Cities and Big Data. As they can concentrate on how IoT, Smart Cities, and the consequent Big Data are all critical components moving ahead, they've really been able to zero in on how they would include these IoT, Smart City, and Big Data features into their Smart City strategy. Our cryptanalysis of ARX cyphers and other security techniques [24–30] has already begun.

SECURITY ISSUE

In RPM systems, the security and data transfer effectiveness are the primary concerns. The key motive for healthcare providers is to keep healthcare data safe from hackers. Due to the growing focus on healthcare, hackers have shifted their sights to healthcare. As an example, medical gadgets and health data have been increasingly often targeted by cyber-attacks in the recent decade. Blockchain, on the other hand, is particularly good for the healthcare system because of the fact that users cannot remove or alter data once it is input. But, in its original form, blockchain technology is not a complete answer [31].

CONCLUSION

One of the biggest concerns when it comes to privacy and security in the Internet of Things (IoT) is how to protect people's data. Due to the shortage of resources affecting IoT, conventional security solutions are unable to provide enough protection. We designed our architecture to tackle most of the security and privacy concerns while taking into consideration the scarcity of resources inherent with IoT. We developed a patient-centric access control system that takes use of lightweight cryptographic primitives including private keys, public keys, blockchains, and others to provide a safe and confidential medical record access control [32]. We also used open questions to help avoid different assaults such as Distributed Denial of Service (DDoS), attack modification, and so on. This, however, becomes an issue when dealing with resource limits with IoT.

REFERENCES

1. Aazam, M., & Huh, E.-N. (2015). Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In X. F. E. T. P. J. H. Takizawa M. Barolli L. (Ed.), *Proceedings - International Conference on Advanced Information Networking and Applications, AINA* (Vols. 2015-April, pp. 687–694). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AINA.2015.254

2. Akyildiz, I. F., Pierobon, M., Balasubramaniam, S., & Koucheryavy, Y. (2015). The internet of Bio-Nano things. *IEEE Communications Magazine*, *53*(3), 32–40. https://doi.org/10.1109/MCOM.2015.7060516

3. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access*, *5*, 26521–26544. https://doi.org/10.1109/ACCESS.2017.2775180

4. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal*, *2*(6), 515–526. https://doi.org/10.1109/JIOT.2015.2417684

5. Chen, M., Wan, J., & Li, F. (2012). Machine-to-machine communications: Architectures, standards and applications. *KSII Transactions on Internet and Information Systems*, *6*(2), 480–497. https://doi.org/10.3837/tiis.2012.02.002

6. Doukas, C., & Maglogiannis, I. (2012). Bringing IoT and cloud computing towards pervasive healthcare. *Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012*, 922–926. https://doi.org/10.1109/IMIS.2012.26

7. Fan, Y. J., Yin, Y. H., Xu, L. D., Zeng, Y., & Wu, F. (2014). IoT-based smart rehabilitation system. *IEEE Transactions on Industrial Informatics*, *10*(2), 1568–1577. https://doi.org/10.1109/TII.2014.2302583

8. Gope, P., & Hwang, T. (2016). BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. *IEEE Sensors Journal*, *16*(5), 1368–1376. https://doi.org/10.1109/JSEN.2015.2502401

9. Gravina, R., Alinia, P., Ghasemzadeh, H., & Fortino, G. (2017). Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges. *Information Fusion*, *35*, 1339–1351. https://doi.org/10.1016/j.inffus.2016.09.005

10. Gupta, H., Vahid Dastjerdi, A., Ghosh, S. K., & Buyya, R. (2017). iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Software - Practice and Experience*, *47*(9), 1275–1296. https://doi.org/10.1002/spe.2509

11. Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., & Andreescu, S. (2015). Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. In P. I. Chou W. Maglio P.P. (Ed.), *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015* (pp. 285–292). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SCC.2015.47

12. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Z. L.-J. Bahsoon R. (Ed.), *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015* (pp. 21–28). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SERVICES.2015.12

13. Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications*, *98*, 27–42. https://doi.org/10.1016/j.jnca.2017.09.002

14. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access*, *3*, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

15. Mainetti, L., Patrono, L., & Vilei, A. (2011). Evolution of wireless sensor networks towards the Internet of Things: A survey. *2011 International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2011*, 16–21. https://www.scopus.com/inward/record.uri?eid=2-s2.0-81455142290&partnerID=40&md5=8089ed723b1c1056c9a6ae8fa767fa4f

16. Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems. *IEEE Internet of Things Journal*, *4*(1), 269–283.

https://doi.org/10.1109/JIOT.2017.2647881

17. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal*, *13*(10), 3711–3720. https://doi.org/10.1109/JSEN.2013.2277656

18. Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, *1*(3), 217–253. https://doi.org/10.3390/jsan1030217

19. Vermesan, O., & Friess, P. (2014). Internet of things applications: From research and innovation to market deployment. In *Internet of Things Applications: From Research and Innovation to Market Deployment*. River Publishers. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071892740&partnerID=40&md5=4221011e71133c5d1e9ee09f13de191c

20. Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Xu, L. D., Kao-Walter, S., Chen, Q., & Zheng, L.-R. (2014). A Health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Transactions on Industrial Informatics*, *10*(4), 2180–2191. https://doi.org/10.1109/TII.2014.2307795

21. Yang, T., Xie, D., Li, Z., & Zhu, H. (2017). Recent advances in wearable tactile sensors: Materials, sensing mechanisms, and device performance. *Materials Science and Engineering R: Reports*, *115*, 1–37. https://doi.org/10.1016/j.mser.2017.02.001

22. YIN, Y., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, *1*, 3–13. https://doi.org/10.1016/j.jii.2016.03.004

23. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

24. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

25. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., & Anderson, J. (2002). Wireless sensor networks for habitat monitoring. In S. K. M. Raghavendra C.S. (Ed.), *Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications* (pp. 88–97). Association for Computing Machinery (ACM). https://doi.org/10.1145/570748.570751

26. Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á. (2004). The flooding time synchronization protocol. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems*, 39–49. https://www.scopus.com/inward/record.uri?eid=2-s2.0-27644533289&partnerID=40&md5=6c6eb8ef24c305da9d864706607cdca6

27. Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems*, 95–107. https://doi.org/10.1145/1031495.1031508

28. Polastre, J., Szewczyk, R., & Culler, D. (2005). Telos: Enabling ultra-low power wireless research. *2005 4th International Symposium on Information Processing in Sensor Networks, IPSN 2005*, *2005*, 364–369. https://doi.org/10.1109/IPSN.2005.1440950

29. Stoppa, M., & Chiolerio, A. (2014). Wearable electronics and smart textiles: A critical review. *Sensors (Switzerland)*, *14*(7), 11957–11992. https://doi.org/10.3390/s140711957

30. Timmer, B., Olthuis, W., & Van Den Berg, A. (2005). Ammonia sensors and their applications - A review. *Sensors and Actuators, B: Chemical*, *107*(2), 666–677. https://doi.org/10.1016/j.snb.2004.11.054

31. Van Dam, T., & Langendoen, K. (2003). An adaptive energy-efficient MAC protocol for wireless sensor networks. *SenSys'03: Proceedings of the First International Conference on Embedded Networked Sensor Systems*, 171–180. https://doi.org/10.1145/958491.958512