ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Iot Based Secure E-Health System in Blockchain Environment

[1] Anitha.A
(ME Computer Science Engineering with specialization in Networks)
Francis Xavier Engineering College of Engineering

Abstract: **- E-Health is a contemporary healthcare practice which is supported by the number of electronic process and communicative elements. Variety of patient data have been managed here that will be transformed to somewhere when it is needed. So that kind of data should be more secure. Blockchain allows having a divide out peer-to-peer network where non-trusting members can communicate with each other without a trusted intervenor, in a falsifiable manner. We then move into the IoT domain and describe how a blockchain-IoT combination that facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices and allows us to automate in a cryptographically verifiable manner several existing, time-consuming workflows. This system proposed that how healthcare data are bind to the combination of blockchain-IoT. The advanced blockchain process not only increases the demands of healthcare growth but also gives the better interaction between users in a secured manner.**

***Keywords*: e-Health, Blockchain technology, IoT, peer to peer transmission.**

I. INTRODUCTION

The main purpose of this e-Health system is to develop the next generation healthcare system with digital service solution to improve patient outcomes, decrease cost and address the complexity of challenging e-Health problems in secured manner with more reliability, flexibility and efficiency[1]. The olden day procedures follow the security process by using password authentication method, wireless sensor method[3] that had been communicated within a small distance or some other patterns which can easily be hacked by professional hackers. So that there is an urgent need to adapt e-Health technological services to meet the demands not only in numbers but also in improvement of social interactive norms. Blockchain technology is introduced here to provide the security, as mentioned above by using trustless network. This is because the parties can transact even though they do not trust each other. Also the blockchain concept use only the peer to peer communication, there is no other way to loss of data during transmission. In blockchain network, heavy use of cryptographic process brings authoritativeness behind all the interaction in the network. Integration of smart contacts and self executing scripts made the blockchain network for proper distribution and heavily automated data. This concept allows IoT to combine with the blockchain network. The main concept behind this system is to use corresponding sensors in healthcare unit to collect the patient data and store that into the cloud. Then the stored data can be getting from the cloud when it is needed. The data will be send to blockchain network for better secures transaction to the corresponding user. The rest of the paper organized as follows, section II describes about the blockchain networktechnology working model that how the blockchain architecture used for transmission. Section III describe about the patient data storage into the cloud by using IoT. Section IV explains, how the blockchain and IoT are combined to form a network in a secured manner. Section V concluding this paper with advantages and their limitations too.

SECTION II

BLOCKCHAIN NETWORK TECHNOLOGY

A. Working of Blockchain

The distributed structure of blockchain is to replicate and shared among the members of the network. This technique[2] has been used over the Bitcoin process to solve the double spending problem. As a result the Bitcoin blockchain houses authoritative ledger of transactions that establishes who own what.

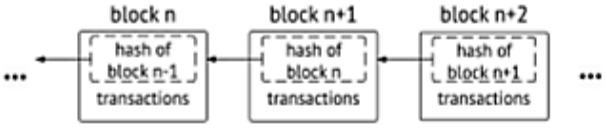

Figure 1: Each block in the chain carries a list of a transactions and a hash to the previous block. The exception to this is the first block of the chain (not pictured), called genesis, which is common to all clients in a blockchain network and has no parent.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

However the blockchain is standing on its own there is no need of cryptocurrency. The data are batched into timestamped blocks in blockchain. Each block references the hash of the block that came before it in which block is identified by its cryptographic hash. This creates a link between the blocks and this is known as chain of blocks or blockchain (Figure: 1). Any node with access to this ordered, back-linked list of blocks can read it and explain about the state of data that is being transformed on the network. If we examine the working of blockchain networkthen we can get a better understanding of blockchain. Blockchain network is a set of nodes or clients which can operate on the same blockchain where the copy of data holds on each node. These network form a peer to peer network where:

- Users interact with a blockchain by using private/public keys which is for the authentication purpose. The signed transaction via the private/public keys is broadcasted by a user's node to its one-hop peers.
- The neighboring peers make sure this incoming transaction is valid before relaying it any further; invalid transactions are discarded. Eventually this transaction is spread across the entire network.
- The transactions that have been collected and validated by the network using the process above during an agreed-upon time interval are ordered and packaged into a timestamped candidate block. This is a process whether the hash is generated over the block's contents or its header, as is the case in Bitcoin for instance, is a design choice. Depending on the implementation, the address can be the public key itself or (usually) a hash of it called mining. The mining node broadcasts this block back to the network.
- The nodes verify that the suggested block (a) contains valid transactions, and (b) references via hash the correct previous block on their chain. If that is the case, they add the block to their chain, and apply the transactions it contains to update their world view. If that is not the case, the proposed block is discarded. This marks the end of a round.

Note that this is a repeating process.

B. Transferring Digital Assetson a Blockchain:

In the case of Bitcoin, new Bitcoin are introduced into the network with every mined block: The mining node includes a so-called coin base transaction in the block of transactions it broadcasts to the network. This coin base transaction has no inputs and rewards the mining node with a predetermined (by the network) amount of bitcoins. The key thing to keep in mind is this: if you have a set of users (a) who want to trade digital tokens, and (b) have agreed on how these tokens are generated, then a blockchain network is an ideal tool to use both for exchanging these tokens, and tracking who has what. No middleman is needed to facilitate the exchanges cause every node on the network runs the necessary checks and reaches consensus on the accepted result. Asset tracking comes out-of-the-box since every node has access to the agreed set of cryptographically verifiable transactions on the blockchain.

SECTION III

IoT AND CLOUD DATA EXTRACTION

A. IoT- based E-Health Systems Architecture Elements:

Architecture is one of the major design constraints across IoT-based E-Health systems [4]. In general, we categorize the healthcare architecture into two types such as distributed and cloud-based architectures. We do not provide any information on centralized architecture because the EHR's are distributed in nature. It is distributed across multiple entities such as hospital, patients, doctors and research analysts for various purposes. This makes the application of centralized architecture inappropriate among IoT-based E-Health systems.

Distributed Architecture:

The distributed architecture consists of a set of servers connected together, and each has its own functionalities and appears as a single system. This type of architecture supports IoT-based E-Health systems as the EHR's are highly distributed in nature. In a distributed architecture a network of computer work together and achieves a common goal. This type of architecture is most suitable for clinical and hospital management systems. The patient health information's from the local hospitals are collected and stored across the distributed servers. The data stored on the distributed servers are then processed and analyzed for research and medication purposes through the central server. The drawback of this type of architecture is that it is not much suitable for real-time health monitoring systems. In a performance aspect, distributed architecture supports speed-up and lacks at scale up measures. Also, its performance degrades when dealing with huge amount of complex data. This is due to the reason that it supports only the horizontal scaling and fails to deal with vertical scaleup.

B. Cloud based Architecture:

In a cloud-based architecture there exists a trusted cloud service provider or a central authority (CA). It makes use of the public, private and hybrid cloud infrastructures. In cloud-based architectures, the patient's health

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

information's are monitored through the body area networks (BAN). The body sensors are projected in and around the patient's body through the wearable smart devices. The patient's health information's are monitored through the body sensors and sent to the cloud server for storage purposes. The patients can also track their health information's through the mobile devices. The Health service provider establishes the Service Level Agreement (SLA) with the patient's and manages EHR's across the cloud server. The cloud service provider (CSP) provides the health care services across the cloud computing environment. The CSP stores and manages EHR over the cloud computing infrastructure. Once the data is stored into the cloud server, the CSP imposes access policies and shares it with a trusted group of users. The user can gain access to the data only when the CSP defined access policy matches with the user data access policy. In general, there exist two different approaches such as patient-centric and non-patient centric approach. In a patient centered approach, the patient's defines the access policies and shares the data. This approach becomes inefficient when dealing with emergency situations. Thus the proposed system introduces the CSP centered approach, where the Cloud Service Provider (CSP) specifies the data access policies and acts as the entire responsibility for health data management processes. Also, the cloud-based architecture remains to be the most suitable solution for the IoT-based E-Health systems as it can handle large and complex EHR in an efficient manner. An overview of IoT-based E-Health System security is given in figure 2.

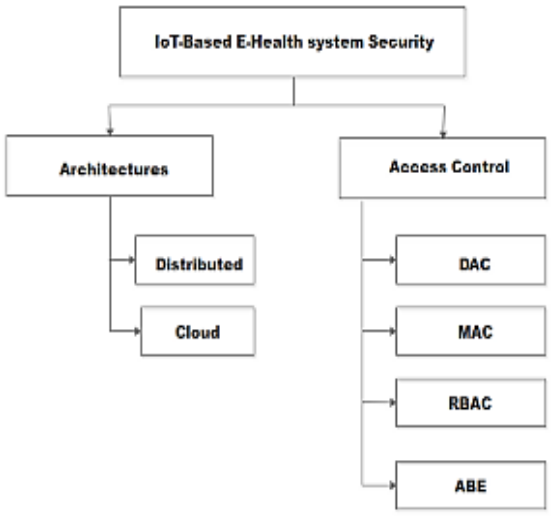

Figure 2: Overview of IoT-Based E-Health System Security

SECTION IV

BLOCKCHAINS AND IoT

In[6], the authors make the case for a shift towards a decentralized architecture for the ever-expanding IoT device ecosystem to be sustainable. From the manufacturer's side, the current centralized model has a high maintenance cost – consider the distribution of software updates to millions of devices for years after they have been long discontinued. From the consumer's side, there is a justified [7] lack of a trust in devices that ''phone home'' in the background and a need for a ''security through transparency'' approach. These issues can be solved with a scalable, trustless peer-to-peer model that can operate transparently and distribute data securely; the authors correctly point out that a blockchain provides an elegant solution to this problem. Consider the following setup to get an understanding of how this could work. All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network. The devices either ship with the smart contract's address baked into their blockchain client, or they find out about it via a discovery service.They can then query the contract, findoutaboutthenewfirmware,andrequestitbyitshashvia a distributed peer-to-peer filesystem such as IPFS [8] [9]. The first requests for this file will be served by the manufacturer's own node (also taking part into the network),but after the binary has propagated to enough nodes [10], the manufacter's node can stop serving it. Assuming the devices are configured so as to share the binary they got, a device that joins the network long after the manufacturer has stopped participating in it, can still retrieve the soughtafter firmware update and be assured that it is the right file. This all happens automatically, without any user interaction.

Architectural concept:

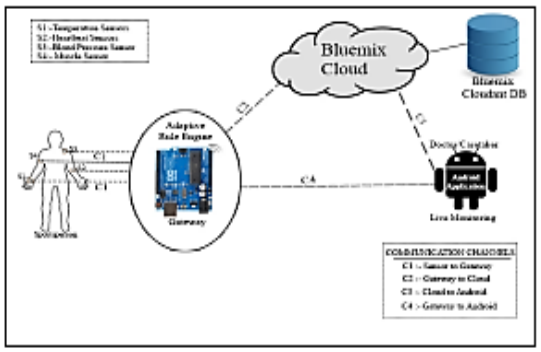

Figure 3: IoT with cloud interaction

Several architectural designs have been proposed in IoT based health care systems[5] [12] [13], but most of them are not that efficient in their security aspects and in data handling process. Recently few architectures [14] [15] have been introduced that are focused mainly on securing sensor data using some cryptographic algorithms. In this paper, we propose different schemeto protect any IoT based system and the network communications in it. In our system, we propose an architecture (Figure: 3) which is based on a secure gateway [11] [16] which drives the entire system. The secure gateway is implemented here using ArduinoMKRzero microcontroller board. To collect the body parameters of a sports person, we use temperature, heartbeat/pulse, muscle and blood pressure sensors. Sensors will collect the data and communicate with the gateway using a pre-shared key. This pre-shared key can be specified during the device configuration time itself. The gateway will then analyze the received data using an adaptive rule engine for any abnormalities in it. In case of any abnormalities detected, this will get notified to the monitoring device through a fast and secure channel which is enabled using a new key exchange scheme based on LEACH protocol. Gateway then transfers the data to cloud storage for future reference. The channel between the gateway and cloud is enabled using modified HIP-DEX protocol. End users (doctor/physio/any authorized person) can frequently monitor the health statistics of the sports person using an Android application. Communication between the end-user device and the cloud is again secured using modified HIP-DEX protocol.

SECTION V

CONCLUSION

As we have proposed, the combination of blockchainsandIoTcanbeprettypowerful.Blockchainsgiveus resilient, truly distributed peer-to-peer systems and the ability to interact with peers in a trustless, auditable manner. Smart contracts allow us to automate complex multi-step processes. The devices in the IoT ecosystem are the points of contact with the physical world. When all of them are combined we get to automate time-consuming workflows in new and uniqueways,achievingcryptographicverifiability,aswellas significant cost and time savings in the process. Webelievethatthecontinuedintegrationofblockchainsin the IoT domain will cause significant transformations across several industries, bringing about new business models and having us reconsider how existing systems and processes are implemented. The opening of accountable treatment records and insurance billing records sets new cost-effective analysis and place them directly into the hands of the public. Our solution provides auditable e-Health records while preserving patient privacy and security. Medical researchers are open to access the vast e-Health blocks, while government and regulatory agencies are given additional identifiers for audit and conformance purposes. The large number of developers as well as the high interest levels in the industry will eventually push the blockchain technology into a well-accepted mode of operation into the e-Health territory. Our solution is a good attempt to further improve efficiency and reliability as inherently derived from the nature of blockchains. With computational logics to be embedded to the e-Health blockchains, additional personalized medicine is enabled by the complete and consistent data blocks available for all service providers involved.

REFERENCES

1. W. Liu, T. Mundie, U. Krieger, S.S.Zhu, Advanced Block-Chain Architecture for e-Health Systems, 2017 19th International Conference on E-health Networking, Application & Services.

2. KonstantinosChristidis andMichealDevetsikiotis, Blockchains and Smart Contracts for the Internet of Things, Special Section on the Plethora of Research in Internet of Things (IoT).

3. An Advanced Wireless Sensor Network for Health Monitoring, G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, R. Stoleru, S. Lin, and J.A. Stankovic Department of Computer Science, University of Virginia.

4. G.S.Tamizharasi, ParveenSultanah H, Balamurugan B, IoT-Based E-Health System Security: A Vision Archictecture Elements and Future Directions, International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

5. Highly Secure and Efficient Architectural Model for IoT Based Health Care Systems Binu P. K., Karun Thomas, Nithin P. Varghese, @ 2017 IEEE.

6. P. Brody and V. Pureswaran, ‘‘Device democracy: Saving the future of the Internet of Things,’’ IBM Institute for Business Value, Tech. Rep., Sep. 2014. [Online].

7. J. Angwin. (2015). Own a Vizio Smart TV? It’s Watching You.

8. J. Benet. IPFS—Content Addressed, Versioned, P2P File System (DRAFT3), accessed on Mar. 15, 2016.

9. IPFS—Content Addressed, Versioned, P2P File System, accessed on Mar. 15, 2016.

10. J.Benet.(2015). Replicationon IPFS — OrtheBacking-UpContentModel.

11. I. Nikolaevisjiy, D. Korzun and A. Gurtov, "Security for Medical Sensor Networks in Mobile Health Systems," IEEE Int. Symposium on a World of Wireless, Mobile and Multimedia Networks 2014.

12. M. F. A. Rasid et al., "Embedded gateway services for Internet of Things applications in ubiquitous healthcare," 2014 2ndInt. Conf. Commun Technol. ICoICT 2014, pp. 145-148, 2014.

13. M. P. R. S. Kiran, P. Rajalakshmi, K. Bharadwaj and A. Acharyya, "Adaptive rule engine based IoT enable remote health care data acquisition and smart transmission system," 2014 IEEE World Forum Interne Things, WF-IoT 2014, pp.253-258, 2014.

14. SriramSankaran, "Lightweight Security Framework for IoTs using Identity based Cryptography," 2016 Int. Conf. on Advance in Computing, Communications and Informatics (ICACCI), 2016, pp. 880-886, 2016.

15. SriramSankaran, Ramalingam Sridhar, "Modeling and Analysis of Routing in IoT Networks," 2015 Intl. Conf. on Computing and Network Communications (CoCoNet'15), 2015, pp. 649-655, 2015.

16. Lakshmi Mohan, M. K. Jinesh, K. Bipin, P. Harikrishnan and ShijuSathyadevan, "Implementation of Scatternet in an Intelligent IoT Gateway," Adv. Int. system and Compt. 338, 2015.