International Journal of Research in Advent Technology, Special Issue, ICATESM 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Effective use of Digital Ledger to Preserve and Secure Data Packets using Blockchain in IOT Enabled Environment.

[1]Prof. Amit Palve, [2]Mali Chaitali Suresh, [3]Chaudhari Rajashree Daulat, [4]More Priyanka Ravindra , [5]Mahajan Roshni Kishor
[1,2,3,4,5]*Department of Computer Engineering Sandip Foundation (SITRC) Nashik,India*
amit.palve@sitrc.org, chaitalinsk@gmail.com, rajashreechaudhari0210@gmail.com, priyarmore118@gmail.com, roshnimahajan500@gmail.com

Abstract— The Internet Of Things (IoT) is a network of computing devices that contains sensors, actuators, softwares, connectivity and the ability to exchange data through a network automatically without any human interaction. There already are numerous applications for the internet of things in healthcare, but the technology is still growing. While one of the challenges of healthcare IoT is how to manage all of the data it collects, the future of IoT will depend on the ability of healthcare organizations to turn that data into meaningful insights.
The Internet of things is experiencing aggressive growth in research and Industry, but it still under go through Privacy and Security Vulnerabilities. Blockchain provides a decentralized database. This network is actually a chain of computers that must all appreciate an exchange before it can be verified and recorded. The recent increase in reported incidents of surveillance and security crack negotiate users' privacy. In current model the third-parties collect and control huge amounts of personal data. The proposed project consists of a protocol that turns a blockchain into an automated tellers that does not require trust in any third party. A Blockchain is a system for a distributed database of records of all transactions that have been done and shared among participating all nodes. Finally, we discuss possible future expansion to blockchains that provides well-rounded solution for trusted computing problems in society.
Keywords— Blockchain, Threats, IOT, hashing, digital certificate.

1. INTRODUCTION

Internet of Things (IOT):

The internet of things is a network of computing devices that contains sensors, actuators, softwares, connectivity and the ability to exchange data through a network automatically without any human interaction. Embedded with technology, these devices can communicate and interact through an Internet, and they can be remotely monitored and controlled.
The term "Internet of things" was likely originated by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he choose the phrase "Internet for things". At that point, he viewed RFID as necessary to the Internet of things, which would allow computers to handle all individual things.

Application:

A. Consumer Applications:
A growing portion of IoT devices are developed for personal and commercial use, including connected vehicles, wearable technology, home automation, connected health, and gadgets with remote monitoring capabilities.
Ex. Smart home, Elder care etc.

B. Commercial Applications: The Smart Healthcare is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. This led to the formation of a computerized healthcare system, connecting available medical resources and healthcare services. IoT devices can be used to enable emergency notification and health monitoring systems remotely. These health monitoring devices can capable of monitoring blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as electronic wristbands, pacemakers, or advanced hearing aids. Some hospitals already started implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also automatically adjust itself to ensure convenient pressure and support is applied to the patient without the manual interaction of nurses or doctors.

C. Industrial Applications:
The IoT can realize the logical combination of various manufacturing devices equipped with sensing, communication, actuation, identification, processing, and networking capabilities. Based on such a highly unified smart cyber physical space, it provides new opportunity to create whole new business and market opportunities for manufacturing.

Blockchain:

Blockchain technology is used for the creation of a decentralized environment, where the transactions validated cryptographically and data are not under the control of any third party. All transaction ever completed is recorded in an enduring ledger in a valid, secure, transparent and permanent way, with a timestamp and all other details. Blockchain wipe out the need for third party to handling transactions on one's behalf. This implies that the harmony mechanism has to exist in the network itself.

Characteristics of Blockchain:

A. **Decentralization:**
In traditional centralized transaction systems, each transaction needs to be validated through the central trusted agency that is necessarily resulting to the cost and the performance bottlenecks at the central servers. Comparison to the centralized mode, third party is no longer needed in blockchain. Harmony algorithms in blockchain are used to manage data firmness in distributed network.

B. **Emphasis:**
Transactions can be validated instantly and invalid transactions would not be admitted by authentic miners. It is approximately impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be detected instantly.

C. **Invisibility:**
Each and every user can connect with the blockchain with a generated address, which does not expose the real identity of the user.

D. **Logically centralized system:**
There is one commonly allow state and the system behaves like a single computer. Anyone has the freedom to approach a blockchain, to download a copy and play a role in managing the blockchain, so that computer becoming a node. The copy will be actively updated along with every copy on every other node, edits can only be made to the blockchain with general harmony among the existence running a node. The process of adding a new block that containing thousands of transactions to a blockchain, by hash verification procedures, is called as mining. The new block is appended as the last one in blockchain.

2. LITURATURE SURVEY

The paper [1] consists of the state-of-art of the existing blockchain protocols designed for the Internet of Things networks. It has an overview of application domains of blockchain technologies in IoT. It has a classification of threat models that are considered by Blockchain protocols in IoT networks, into five main categories namely identity based attacks, manipulation based attacks, cryptanalytic attacks, reputation-based attacks and service based attacks. In a similar paper [2] the security and privacy issues in Iot applications and systems have been presented. It contains the limitations of IoT devices in battery and computing resources, the possible solutions for battery life extension and lightweight computing. The last part of the work analyzed the security issues and solutions in four layers, including the perception layer, network layer, transport layer and application layer.[3] has an introduction to the primary design of a distributed secure data storage system targeted for the internet of things. This allows for fine-grained access control and sharing of time-series sensor data of various IoT applications.

As the complexity of power systems increase due to the evolution of power grids, decentralized transitive-energy IoT systems are emerging to tackle this complexity. The paper [4] describe privacy preserving Energy tractions, innovative solutions for anonymous energy trading within a transitive microgrid. According to [5], in the plethora of blockchain based applications and experiments, faith on the longevity of blockchain technology, is increasing. Scalability and consensus algorithms are areas of growing research in order to make blockchain more adaptable to businesses of large scale. The public Blockchain also provides an opportunity of mining interesting patterns of cryptcurrency usage, user behaviors and monetary networks across the globe. Paper [6] has an exhaustive analysis the security protocols and mechanisms available to protect communications on the IoT. It addresses existing research proposals and challenges providing opportunities for future research work in the area. It summarizes the main characteristics of the mechanisms and proposals analyzed throughout the survey, together with its operational operational layer and the security properties and functionalities supported.

Users should own and control their data without compromising security or limiting companies' and authorities' ability to provide personalized services. The proposed platform enables this by combing a blockchain, repurposed as an access control moderator, with an off blockchain storage solution. Users are not required to trust any third party and are always aware of the data that is being collected about them and how it is used. In addition , the blockchain recognizes the users as the owners of their personal data. Companies, in turn, can focus on utilizing data without being overly concerned about properly securing and compartmentalizing them. Finally paper [7] contained several possible future extensions for blockchains that could harness into well-rounded solution for trusted computing problems in society.

The paper [8] presents a comprehensive overview on blockchain. It first gives an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. It describes typical consensus algorithms used in blockchain and comparison of protocols in different respects. It also lists some challenges and problems that would hinder blockchain development and summarize some existing approaches for solving these problems.

3. METHODOLOGY

The main aim of this project is to provide security to healthcare data using blockchain. Initially the temperature data is collected through temperature sensors. This data is stored in the table which contains the patient details which is stored on the cloud. The data stored on cloud is in encrypted format. We have used MD5 algorithm for encryption of the data. After being encrypted we provide unique key to each record using KDD algorithm. The data is uploaded on cloud using REST API through the controller. The table consists of all static fields and only one dynamic field i.e. temperature

value. The patient records must be accessible on the web application as and when required. The temperature value changes dynamically and hence can be seen on the web application as per the updated temperature.

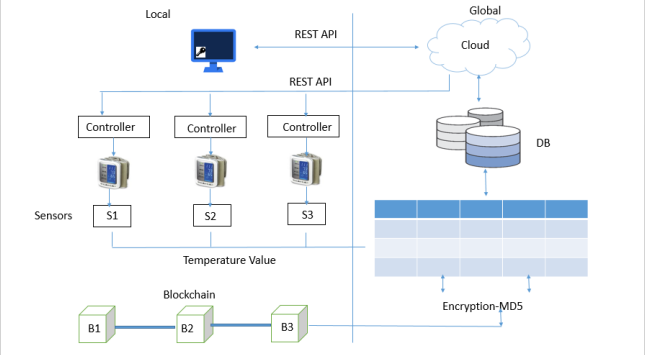

Fig.1: Healthcare System Architecture

As represented in above system architecture Sender send their personal information to distributed network where numbers of systems are connected with network and they encrypted the sender information using appropriate algorithm. In distributed network all system are connected to each other's and when sender send any information then all system get one copy of that information, if any intruder is present in our network & they manipulate the data it will understand immediately. The main task of distributed network is maintain the security of data packet and after that create the block of data and the block are connected with another block to form a "BlockChain". Now a days with an ongoing increase in patient numbers, healthcare providers have to maintain more and more health data on a regular support. As the information increases each year, it becomes tough for hospitals and clinics to process and store information.

Data managed by medical organizations includes:

- Patient health information (PHI)
- Electronic health records
- Data collected from IoT devices or monitoring systems
- Medical insurance claims.

4. CONCLUSION

In this work, we have proposed a unique model for future IoT-based healthcare systems, which can be applied to both general systems and systems that monitor specific conditions. We then presented a thorough and systematic overview of the state-of-the-art works relating to each component of the proposed model. Several wearable, non-intrusive sensors were presented and analysed, with particular focus on those monitoring temperature. Recent works utilizing cloud technologies for data storage were presented, and showed that cloud is the best means for storing and organizing big data in healthcare. It is also shown by several works that significantly better data processing can be performed in the cloud than can be performed by wearable devices with their limited resources. The most significant drawback of using cloud is that it introduces security risks, and as such we presented several works focused on improving security in the cloud. It was found that access control policies and encryption can significantly enhance security, but that no known standard is suitable for immediate application into a wearable, IoT-based healthcare system. Based on our analysis of state-of-the-art technologies in the fields of wearable sensors, communications standards, and cloud technology, we identified several significant areas for future research.

REFERENCES

[1] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Member,IEEE, Abdelouahid Derhab,Leandros Maglaras,Senior Member,IEEE, Helge Janicke,"Blockchain Technologies for the Internet of Things:Research Issues and Challenges",IEEE,24 Jun 2018,Page No:-1-14

[2] Yuchen Yang,Longfei Wu,Guisheng Yin,Lijie Li*, and Hongbin Zhao,"A Survey on security and Privacy Issues in Internet of Things",IEEE,Page No:-1-10.

[3] Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi. Simon Duquennoy,"Towards Blockchain-based Auditable Storage and Sharing of IoT Data",IEEE,!4 Nov 2017,Page No:-1-6.

[4] Aron Laszka,Abhishek Dubey,Michel Walker,Doug Schmidt,"Providing Privacy,Safety and security in IoT based Transactive energy systems using distributed ledger",IEEE,27 Sept 2017,Page No:-1-8.

[5] Supriya Thakur Aras,Vrushali Kulkarni,"Blockchain and it's Applications-A detailed Survey",International journal of computer applications,3 Dec 2017,Page No:-1-7.

[6] Jorge Granjal,Edmundo Monterio,Jorge Sa Silva,"Security for Internet of Things:A survey of Existing protocols and open Research issues",IEEE,2015,Page No:-1-25.

[7] Guy Zyskand,Oz Nathan,Alex Peterland,"Decentralyzing privacy: Using Blockchain to protect Personal data",IEEE,2015Page No:-1-5.

[8] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, "An overview of blockchain technology: Architechture,consesus, And Future Trends",Conference Paper,june 2017,Page no:-1-9.

[9] D.Miorandi,S.Sicari,F.DePellegrini,"Internet of things: vision, applications and research challenges",Ad Hoc Netw,vol 10, no.7,Page No. 1497-1516, Sept 2012.

[10] M.Swan, "Blockchain:Blueprint for a new economy", 1st ed , Oreilly Media, Jan 2015.

[11] S.Nakamoto,Bitcoin:A peer-to-peer electronic cash system,2008.

[12] F. Tian,"An agri-food supply chain praceabily system for china based on RFID and blockchain Technology",IEEE,June 2016.

[13] T.M. Fernandez-Carames and P.Fraga-Lamas,"A Reviw on the use of Blockchain For the Internet Of Things",IEEE,Access,Page No:-.1-23 May 2018.

[14] M.Ali,J.Neilson,R.Shea,and M.J.Freedman,"Blockstack:A global naming and storage system secured by blockchain",in Proc. Annual Technical Conference,Page No:-181-194,June 2016.

[15] Q.Wang, B.Qin,J.Hu, and F.Xiao,"Preserving Transaction Privacy in Bitcoin",Future.Gener.Comput.Syst,Sept 2017.
[16] Y.He,H.Li,X.Cheng,Y.Liu,C.Yang,and L.Sun,"A blockchain based truthful insentive mechanism for Distributes P2P Applications ",IEEE Access,Page No:-1-1,2018.
[17] J.Gu,B.Sun,X.Du,J.Wang,Y.Zhuang, and Z.Wang,"Consortiun Blockchain Based Malware Detection In Moble Devices",IEEE Access,Vol.6,Page No:-12118-12128,2018.
[18] Jon.Evans. Bitcoin 2.0:Sidechain and etherium and zerocash,oh my!,2014.
[19] G.Foroglou and A.L.Tsilidou,"Further applications of the Blockchain",2015.
[20] G.Maxwell,"Coinjoin :Bitcoin Privacy for the real world", in Post on Bitcoin Forum,2013.