Secure and Anonymous IoT Data Sharing Platform based on Blockchain using Proxy Re-Encryption

Dr.K.Chandramohan[1] B.Mathimila[2]
[1]VP & Professor [2]Research Scholar
[1,2]Department of Computer Science and Engineering
[1,2]Gnanamani College of Technology, Namakkal, India

Abstract— Data is central to the Internet of Things (IoT) ecosystem. With billions of devices connected, utmost of the current IoT systems are using centralized pall- grounded data participating systems, which will be delicate to gauge up to meet the demands of unborn IoT systems. The involvement of such a third- party service provider requires also trust from both the detector proprietor and detector data stoner. Also, freights need to be paid for their services. To attack both the scalability and trust issues and to automatize the payments, this paper presents a blockchain- grounded business for sharing of the IoT data. We also use a deputyre-encryption scheme for transferring the data securely and anonymously, from data patron to the consumer. The system stores the IoT data in pall storehouse after encryption. To partake the collected IoT data, the system establishes runtime dynamic smart contracts between the detector and data consumer without the involvement of a trusted third- party. It also uses a veritably effective deputyre-encryption scheme which allows that the data is only visible by the proprietor and the person present in the smart contract. This new combination of smart contracts with deputyre-encryption provides an effective, fast and secure platform for storing, trading and managing detector data. The proposed system is enforced using out-the-shelf IoT detectors and computer bias. We also dissect the performance of our mongrel system by using thepermission-less Ethereum blockchain and compare it to the IBM Hyperledger Fabric, a permissioned blockchain.

Keywords: IoT, Data Sharing Platform, Blockchain

I. Introduction

The Internet of Things (IoT) is an arising technology which has great specialized, social, and profitable significance. Current prognostications for the impact of IoT are veritably emotional. Data is central to the IoT paradigm. IoT data is collected to serve numerous different types of operations similar as smart home, smart megacity, wearable, healthcare, smart grid, independent vehicles, smart granges, diligence and manufacturing, and retail sector (3). Thus, multitudinous miscellaneous detectors live to measure a variety of parameters. The collected data from these IoT detectors can be useful for different stakeholders. For case, air quality measures are of interest to governmental associations, operation inventors and occupants of the applicable spaces. Still, numerous challenges arise when organizing this data sharing as these IoT bias, which are generally resource-constrained, bear effective mechanisms to guarantee the data integrity and to enable proper processing and security (4). Due to the large number of IoT bias, scalable deployment, and conservation costs (3) should also be taken into account. Presently, nearly all the detector systems use centralized pall-grounded results to partake detector data with different stakeholders. IoT manufactures frequently use these third-party pall service providers for storehouse, access control or indeed enforcing their business intelligence services (5). In that case, both data directors and consumers have to trust the third- party service provider and also need to pay some figure for their services. In addition, it's demanded to establish an agreement between the data directors and consumers about the pricing and the quantum of data participated. Also, these agreements can be indeed established without the concurrence of the IoT detector (6). Utmost of these agreements are stationary and takes significant time and administration to be established. For case, the detector data consumer has to pay the correct quantum or buy a subscription to pierce data, which requires the involvement of other trusted parties similar as banks. It'll affect in a significant increase in time before the factual data sharing can be realized. On the other hand, the responsibility of the detector data is also an important issue to bear in mind. Untrusted or third- party realities can alter information according to their own interests, so the information they give might not be fully dependable (8). Data consumers need to be sure that the information handed by IoT bias and by other external realities, similar as data directors, has not been tampered or altered in any way. Therefore, the current centralized armature model in IoT systems doesn't give any result for enhancing trust and will also struggle to gauge up to meet the demands of unborn IoT systems. In order to further monetize from the detector data, deals are used in the business. The open thrusting price transaction is conceivably the most common form of transaction in use moment. Utmost of the online transaction platforms that presently live are grounded on one centralized driver. They calculate on personal and unrestricted software (9). As a result of this centralization, these deals frequently warrant translucency and stab have no way to insure the legality of an advanced shot.

II. Proposed System

To break the issues, the decentralized and agreement- driven blockchain technology and the underpinning cryptographic processes behind it can offer an interesting volition. Therefore, we propose a new armature that uses blockchain in combination with a pall service provider for the trading of the detector data. We also propose a deputy reencryption scheme to insure the confidentiality and integrity of the data. The advantage of using blockchain to vend the detector measures with different realities is that the corresponding fiscal deals are automatically managed through the agreed smart contract, stored on the blockchain. We also present a smart contract- grounded open thrusting shot transaction for dealing the IoT data on competitive prices. Accordingly, compared to the current IoT platforms where the data is stored in a pall- grounded structure, there's no need for homemade verification of the payments and the predefined conditions. Also, controversies on these aspects are fully avoided. To the stylish of our knowledge, our offer is the first to use a mongrel armature of combining blockchain with pall storehouse to break this particular issue of participating data. Also, we bandy the different aspects of the perpetration of the proposed scheme. On the one hand, we propose a veritably effective deputyre-encryption scheme to be used as the security medium and how it allows that the data is only visible by the proprietor and the person present in the smart contract. On the other hand, we bandy the practical points similar as the use of a smart contract, the storehouse of data and the communication between the pall garçon provider and the blockchain. In order to corroborate the viability of the offer, a prototype perpetration of the mongrel armature and deputyre-encryption scheme is done on a test bed. We used off-the-shelf bias and a marketable pall service provider for the prototype perpetration. Also, a detailed performance analysis is handed to demonstrate the scalability and performance criteria of the approach. To validate the conception of our result, perpetration of the scheme in this paper was done using a public Ethereum blockchain i.e. Rinkeby Test Network (10) and latterly on permissioned IBM Hyperledger Fabric. To further understand these blockchain platforms, we compare their separate performances and deals costs and also bandy their limitations in the end. The conference paper published before proposed the introductory ProxyRe-Encryption Scheme and included perpetration only on private Ethereum network without performance or security analysis.

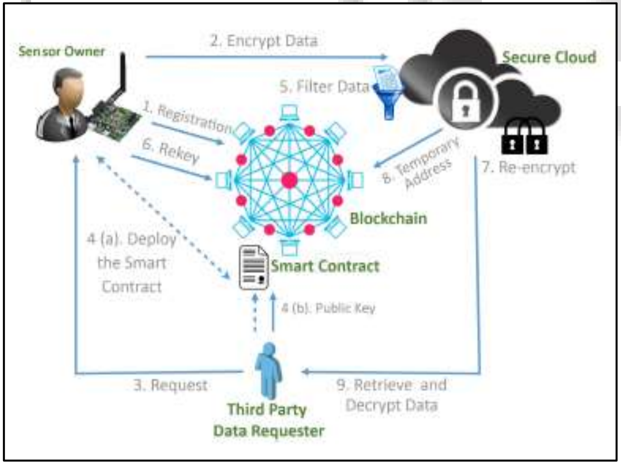


Fig. 1: Proposed Architecture

III. METHODOLOGY

A. Blockchain

A blockchain is a continually evolving, tamper-apparent, participated digital tally (11). It holds the records of the deals similar as the exchange of means or data between the peers in a public or private peer-to- peer network. The tally is participated, replicated, and accompanied among the member bumps in the network. This tally holds the records permanently in a successional chain of cryptographic hash-linked blocks. Without the involvement of a central authority or third- party middleman, the party bumps in the blockchain network govern and agree by agreement on the updates to the records in the tally. These records can not be altered or reversed unless the change is agreed by all members of the network in a posterior sale. Consensus mechanisms in blockchains offer the benefits of a consolidated and harmonious dataset with reduced crimes, nearreal- time reference data, and the inflexibility for actors tochange the descriptions of the means they enjoy (12). Also, .none of the sharing members enjoy the source of originfor information contained in the participated tally. The blockchainleads to increased trust and integrity in the inflow of transactioninformation among the sharing bumps (12).

B. Ethereum

Ethereum blockchain was introduced by Vitalik Buterin (13) in late 2013 and addressed several limitations faced by the Bitcoin network. It incontinently came the alternate most common public blockchain. The Ethereum state consists of accounts, where each account has a 20-byte address and state transitions. Block generation time on Ethereum is dropped to 13 seconds and so is the size of the block. The implicit exercises of Ethereum are described as token systems, fiscal derivations, identity and character systems, train storehouse, insurance, pall computing, vaticination requests,etc. (13). In Ethereum" Gas"is a abecedarian unit for calculation. Each sale requires a certain quantum of calculation and the" Gas Limit"states the maximum number of computational way the sale is allowed to consume. The usual price is 1 gas per existent computational step plus the fixed fresh price for reading and writing to the data area. Ethereumo_ers a smart contract functionality through the Ethereum virtual machine (EVM) running on the distributed bumps. Smart contracts are restated into the EVM law and also executed by the bumps (14). Smart contracts on Ethereum are"Turing-complete", meaning it supports a broader set of instructions, including circles. Ethereum as a platform is suitable for the allocation of commemoratives. 3.3 Hyperledger Fabric Hyperledger Fabric (17) is a distributed tally by IBM and Linux foundation. Its modular armature delivers a high degree of confidentiality, resiliency, inflexibility, and scalability. The Hyperledger design was started in 2015 and launched inmid-2017. The Hyperledger Fabric is a private and permissioned blockchain, in which individualities of all the actors are known. It's designed to support the pluggable perpetration of different factors to support complications that live across ecosystems. Fabric supports modular agreement protocols, which allows the system to knitter to particular use cases and trust models. Hyperledger Fabric can store data in multiple formats, and it's also the first blockchain system that runs distributed operations written in standard, general- purpose programming languages, without systemic reliance on a native cryptocurrency.

IV. OVERALL RESULTS AND TEST LABORS

1) Detectors

An IoT detector knot labeled as detector proprietor in Figure 1 is a computing device that connects to the blockchain network and can capture and transmit data. It interacts with (a) Pall storehouse, to save and recoup the translated detector data from the database . (b) Blockchain, to perform smart contract deals and manage the electronic portmanteau.

2) Panhandler

The stoner knot is labeled as a third- party panhandler in Figure 1. It can be seen as a software agent acting on behalf of the stoner for specifying the conditions and type of detector data to be queried. It manages cryptographic keys of the stoner demanded for there-encryption scheme. The stoner knot also acts as the blockchain knot and manages all the fiscal associated deals related to the stonere.g. transferring commemoratives to IoT detector or bidding for the data.

3) Pall Garçon

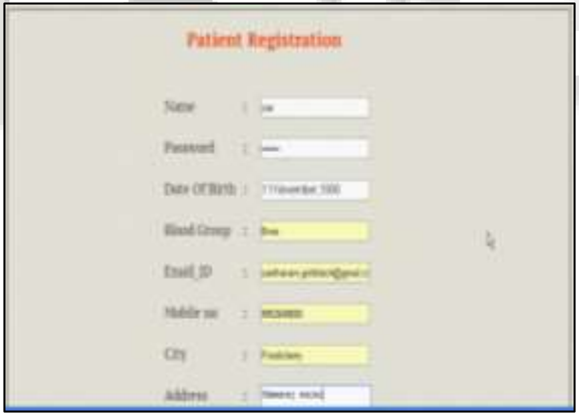
The pall storehouse knot stores the translated detector data coming from the IoT gateway and it also entertains the stoner request by returning the records that match the third- party panhandler specified criteria. The pall garçon also runs a blockchain knot and connects to the network to do deals and maintain a dupe of the tally.

4) Blockchain

A known and trusted operation shares and synchronizes sale data across multiple bumps. It interacts with all the realities in the system and logs those relations in the form of deals. Smart contracts only live in the blockchain environment and are used for penetrating blockchain external data. The smart contract manages the fiscal sale costs and checks the matching conditions (e.g. Data Position) related to the data.

5) Market Place Blockchain

Grounded or decentralized commerce are peer-topeer networks that directly connect consumers and directors without any interposers. IoT Data fromdi_erent sources can be vended and bought on this platform. Then show some sample labors for medical records to distributed multiple cases usings blockchain technologies.



Patient Registration

Name :

Password :

Date Of Birth :

Blood Group :

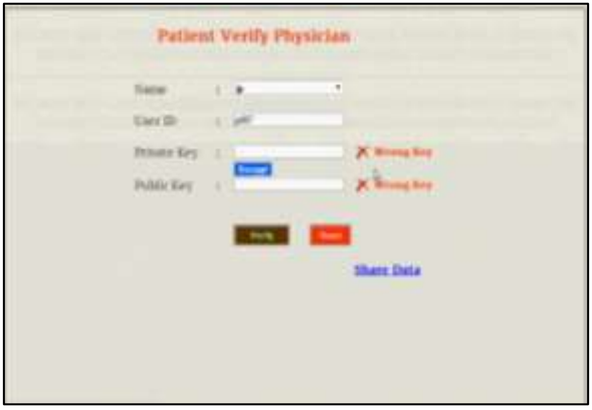
Email_ID :

Mobile no :

City :

Address :

Fig. 2: Patient Registration



Patient Verify Physician

Name :

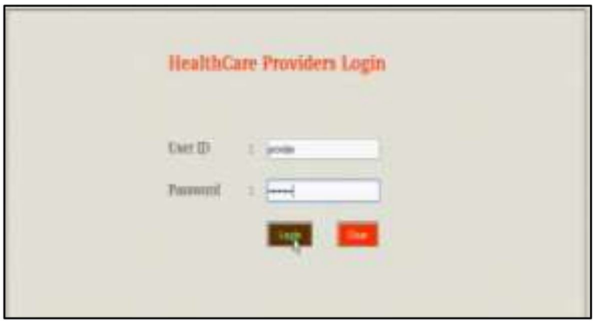
User ID :

Private Key : ✗ Wrong Key

Public Key : ✗ Wrong Key

Share Data

Fig. 3: Patient verify doctors



HealthCare Providers Login

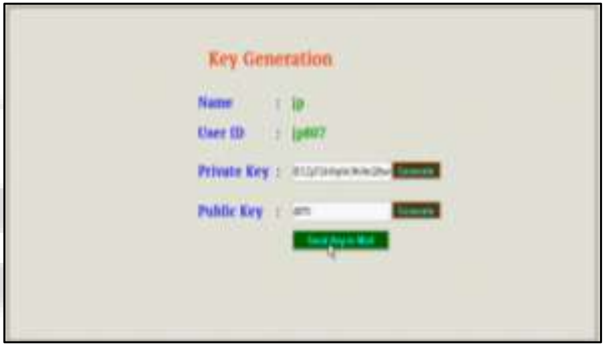
User ID : provider

Password :

Fig. 4: Healthcare Login

User ID

Fig. 5: User verify from Healthcare provider



Key Generation

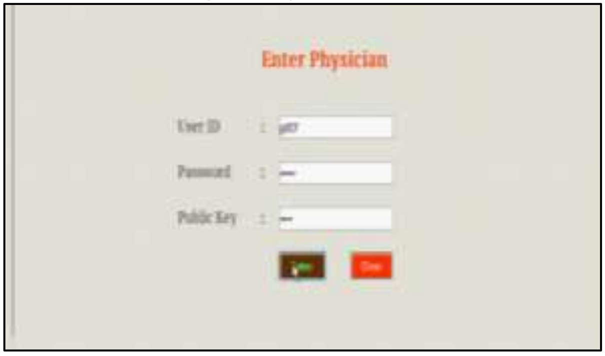
Name : jp

User ID : jp007

Private Key :

Public Key :

Fig. 6: Key Generation



Enter Physician

User ID :

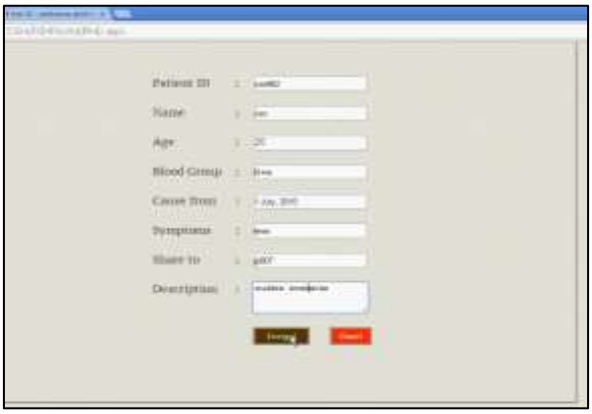
Password :

Public Key :

Fig. 7: Physician Login

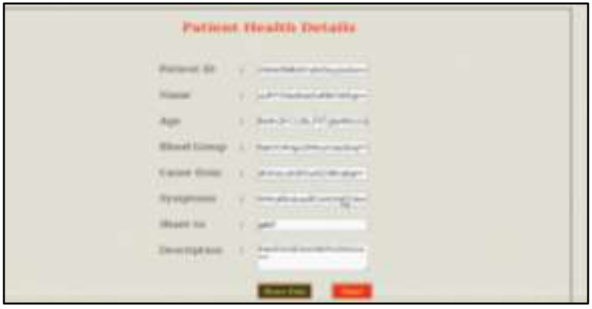
Authorization Key

Fig. 8: Physician received key from Healthcare Provider



Patient ID : [illegible]
Name : [illegible]
Age : [illegible]
Blood Group : [illegible]
Cause from : [illegible]
Symptoms : [illegible]
Share to : [illegible]
Description : [illegible]

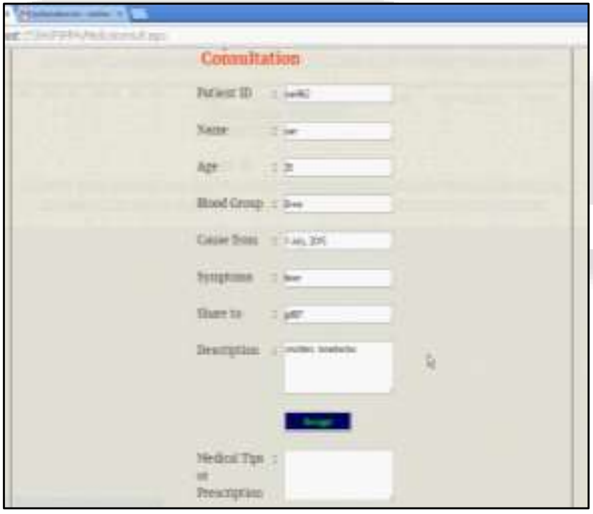
Fig. 9: Patient share data to doctor



Patient Health Details

Patient ID : [illegible]
Name : [illegible]
Age : [illegible]
Blood Group : [illegible]
Cause from : [illegible]
Symptoms : [illegible]
Share to : [illegible]
Description : [illegible]

Fig. 10: Doctor recived request(Encrypt) from patient



Consultation

Patient ID : [illegible]
Name : [illegible]
Age : [illegible]
Blood Group : [illegible]
Cause from : [illegible]
Symptoms : [illegible]
Share to : [illegible]
Description : [illegible]
Medical Tips or Prescription :

Fig. 11: Doctor send suggestion after recived request from patients

V. CONCLUSION

In this paper, we've proposed a blockchain grounded trading platform with the combination of a shearing free deputy reencryption scheme to insure secure transfer of the detector data to the stoner. We've also validated the evidence of conception model on a public Ethereum testbed and private Hyperledger Fabric. We demonstrated the practicality of the system design using on-the-shelf laptops, jeer pis and amazon managed blockchain. Also, our trials and analysis corroborate that digging deputyre-encryption scheme with blockchain enables a secure platform for trading and sharing of the detector data. The use of blockchain does increase the detention but it keeps a record of all the commerce between the realities and eliminates a need for a trusted third party. Our frame provides an effective, fast and secure platform for storing, trading and managing of. detector data.

REFERENCES

[1] R. Taylor, D. Baron, D. Schmidt, The world in 2025-predictions for the next ten years, in: Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT), 2015 10th International, IEEE, 2015, pp. 192–195.

[2] N. Suryadevara, S. Mukhopadhyay, Internet of things: A review and future perspective, Reliance (2018).

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys & Tutorials 17 (2015) 2347–2376.

[4] M. Liyanage, A. Braeken, P. Kumar, M. Ylianttila, IoT Security: Advances in Authentication, John Wiley & Sons, 2020.

[5] L. Hou, S. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, W. Xiang, Internet of things cloud: architecture and implementation, IEEE Communications Magazine 54 (2016) 32–39.

[6] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future generation computer systems 29 (2013) 1645–1660.

[7] E. Karafili, E. C. Lupu, Enabling data sharing in contextual environments: Policy representation and analysis, in: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, ACM, 2017, pp. 231–238.

[8] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with iot. challenges and opportunities, Future Generation Computer Systems 88 (2018) 173–190.

[9] "domraider whitepaper", Accessed: 29.04.2019. URL: https: //s3-eu-west .amazonaws.com/domraider/domraider/ DomRaider+ICO+Whitepaper+EN.pdf.

[10] "rinkeby testnet", Accessed: 05.09.2020. URL: https://www. rinkeby.io/.

[11] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and iot integration: A systematic survey, Sensors 18 (2018) 2575.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: Big Data (BigData Congress), 2017 IEEE International Congress on, IEEE, 2017, pp. 557–564.