International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E-Ration Distribution System using Blockchain Technology

Dipti Aswar, Shravani Suryawanshi, Vaishnavi Dagade

Professor Computer Engineering, PVPIT Collage, Pune, India
BE Computer Engineering, PVPIT Collage, Pune,India
BE Computer Engineering, PVPIT Collage, Pune,India

DOI: https://doi.org/10.55248/gengpi.4.523.40203

ABSTRACT

Recently, the Public Ration Distribution System structure is one of the prime government commercial schemes. Low economical group and people below scarcity line use this amenities provided by the government. Due to deception appear in a chain, such amenities do not reach to the needy people. This happens because in the existing system all the work done by physically. To computerize or automate this physical job there is no any specific unreasonable technology or tools involved. Due to this, system facing two problems firstly weight of the material that is given to the people may be inaccurate or imprecise and secondly, at the end of the, illegal wrong entries in the inventory of the shop about the amount of the material given to the consumers. In this work we will describe a blockchain technology-based prototype that can be used in a small website. There are presently many fraud activities and corruptions taking place in the food supply schemes present as it sometimes does not reach the poor or the other sections of the society. This paper focuses on developing blockchain prototype that is used to record all the transactions/records and log all these transactions. A simple end-to-end web based app of this kind of the blockchain prototype can be built that has most of the features and functionalities to carry out all kinds of the transactions between the central government, state government, the district office, ration shop/and the customers, are recorded in the system. The user of the system can view the transactions of any part of the public distribution system. The project have some features that is guaranteed to provide the most important aspect that is, the security using the concept of blockchain

Keywords:Blockchain,Ledger,Cryptography,Decentralized,Multi-Chain,Distributed Systems

1.1 Introduction

The world is changing incredibly fast, and we are not all aware of it. Block chain technology and crypto currencies are an irreversible advancement that is disrupting established industries and the ways in which we interact financially. For that reason, I believe understanding and being aware of this block chain wave is incredibly important. The existing systems work as centralized architecture in database system.

- Large data storage at the required of decentralized data storage as well as information system
- The different attack issues in centralized database architectures.
- There are no automatic attack recovery in central data architectures
- The decentralized architecture provides the automatic data recovery from different attacks.

After the analysis of this system we move to develop the decentralized system architecture, and fog computing provide parallel processing in distributed environment

1.2 Problem Statement

In the proposed research work to design and implement a system for Ration Distribution Management data, where user can store all information in single blockchain without any Trusted Third Party (TTP) in distributed computing environment. The system eliminates data integrity, privacy as well as end user discrepancies.

1.3 Goals and objectives

- To design an approach for public ration distribution where system can stores all historical transactional data into block chain manner.
- To develop a custom blockchain for proposed public system, that end user can access and view entire data publically.
- To develop an own smart contract as well custom mining policy to achieve the efficiency into the system.

- To developed a consensus algorithm for proof of validation between P2P decentralized networks, for data security and eliminate different network attacks.
- To explore and validate how proposed system provides, beneficial influence than classical ration distribution system

2. Literature Survey

Smart Contracts [1] Also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate BlockOn IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Blockwheels are especially used to provide access control system for Smart-Devices Transactions located on Smart- Home. Introducing BC technology in IOT, this search again provides some additional security features, however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology can not provide a general form of block-chain solution in case of IOT usage.

According to Ilya Sukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based feature-based encryption scheme, which has dynamic features. Using BlockChain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the siftertext is only transmitted by the blockcon laser. Our system has been tested on prototype smart contracts and tested on IteriumBlockchan platforms.

According to Huehuangenet. Al [4]they offer a blockchain and a MedRec-based approach by enabling encryption and attribute based authentication to enable secure sharing of healthcare data. By applying this approach: 1) The fragmented EHR fragment of all patients can be seen as a complete record and can be safely stored against tampering; 2) The authenticity of patients' EHR can be verified; 3) Flexible and finer access control can be provided and 4) it is possible to maintain a clearedaudit trail.

According to VipulGoyalet. Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE). In our cryptosystem, Cefhettext is labeled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to categorized identification-based encryption (HIBE).

Hao Wang et Mate Al [6] They offer a secure electronic health record (EHR) system based on special-based crypt ococcurs and blockchan technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity-based signature (IBS) to apply digital signatures. . In order to obtain various functions of ABI, IBE and IBS in crypto, we present a new cryptographic primitive, it is called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES). It simplifies system maintenance and does not require the installation of separate cryptographic system for various security requirements. In addition, we use blockconne techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business.

According to Yan Michalevskyet. Al [7] system introduces the first practical decentralized ABE scheme with proof of policy-hiding. Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This ABB scheme supports results, disputes, and threshold policies, which protect the access policies of those parties that are not authorized to decrypt content. In addition, we handle the receiver's privacy issue. Using our plan with Vector Commitment, we hide a complete set of attributes presented by the individual with the recipient; Just disclose the feature that regulates the authority. Finally, we propose random-polynomial encoding that immerses this scheme in the presence of corrupt officials.

Al [8] they successfully address these issues by offering a clearepolicy feature-based data sharing plan with direct cancellation and keyword search. In the proposed scheme, the non-terminated users' private key is not required to be updated during the cancellation of direct revocation of features. In addition, a keyword search has been realized in our plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in our plan, and therefore, the privacy of users is preserved. Our security and performance analysis show that the proposed plan can deal with security and efficiency concerns in cloud computing.

According to SarmadullahKhanet. Al [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meet those features. The public and private key manufacturers have been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective. To protest against collision attacks, the makers are given secret pseudo-functional work seeds. Comparative analysis shows the efficiency of the proposed approach to existing people.

According to Ruuguet. Al [10] To guarantee the validity of the EHR surrounding the block channel, he has submitted a special-based signature scheme with multiple officials, in which the patient supports the message according to the specifications, but there is no evidence that he does not have any other information. In addition, there are many officers without generating a reliable individual or a central person in order to generate and deliver a public / private key, which avoids the escrow problem and adapt to the mode of data storage distributed in the Block Block. By sharing the secrecy of the secret pseudo-festive festivals in the authorities, this protocol opposed the attack of N-1 affiliated with officials.Under the computational BillineDiffie-Hellman concept, we also formally demonstrate that, in relation to the specialty-signatory's enforceability and complete privacy, this specialty-based signature scheme is safe in random decorative models. Comparison shows the efficiency and qualities among the proposed methods and methods in other studies.

3. Relevant mathematics associated with the Project

A System has represented by a 5-different phases, each phase works with own dependency System S = (Q, ∑, δ, q0, F) where −

- **Q** is a finite set of states.
- ∑ is a finite set of symbols called the alphabet.
- **Δ** is the transition function where δ : Q × ∑ → Q
- **q0** is the initial state from where any input is processed (q0 ∈ Q).
- **F** is a set of final state/states of Q (F ⊆ Q).

All (n) data nodes will return 1 when each have the same blockchain, . Q = initial transactional data with genesis block

∑ **=** {SHA-256, Consensus_Val, Mining**}**

Δ = Validate all server(S1 ⊆ S2⊆ S3⊆ S4) all server validation process

q0 = Initial transaction T[0]

F = {Commit Trans, GetHostoryRecord} **State =>**1 :if all chains are validate or same 0 :if any t(n) server consist the invalid chain

Set dependency

Sys= {Phash, Tdata, Chash}

n

$NodesCh\ ain\ [Nodeid,\ Ch\ ain]\ \sum(GetCh\ ain)$

i=1

Get blcokchain from each node and validate with each other. (1)

4. Algorithm

Algorithm 1 : Hash Generation

Input : Genesis block, Previous hash, data d, Output : Generated hash H according to given data Step 1 : Input data as d

Step 2 : Apply SHA 256 from SHA family

Step 3 : CurrentHash= SHA256(d)

Step 4 : RetrunCurrentHash

Algorithm 2 : Protocol for Peer Verification

Input : User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain], Output : Recover if any chain is invalid else execute current query

Step 1 : User generate the any transaction DDL, DML or DCL query

Step 2 : Get current server blockchain Cchain□ Cnode[Chain]

Step 3 : For each

n

$NodesCh\ ain\ [Nodeid,\ Ch\ ain]\ \sum(GetCh\ ain)$

```
i=1
End for
Step 4 :Foreach (read I into NodeChain)
If (!.equalsNodeChain[i] with (Cchain)) Flag 1
Else Continue Commit query
Step 5 :if (Flag == 1)
Count = SimilaryNodesBlockchian()
Step 6 :Cacluate the majority of server
Recover invalid blockchin from specific node
Step 7: End if
End for End for
```

Mining Algorithm for valid hash creation

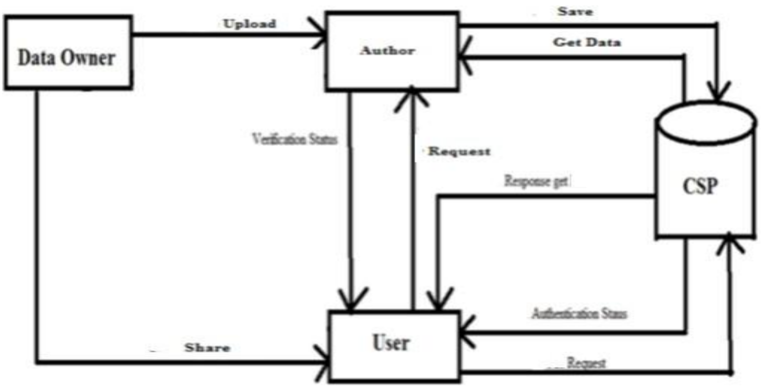
Input : Hash Validation Policy P[], Current Hash Values hash_Val Output : Valid hash

```
Step 1 :System generate the hash_Val for ith transaction using Algorithm 1
Step 2 :if (hash_Val.valid with P[]) Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3 :Return valid hash when flag=1
```

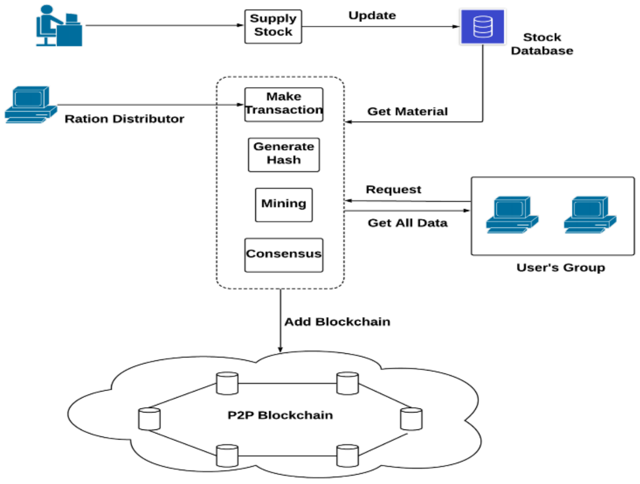
4.4 Outcome

- The proposed mining approach generates the strong hash with minimum difficulties.
- According to mentioned smart system for generate a dynamic transaction can allow to update for entire block.
- It can also detect and prevent various network as well as database attacks

State Diagram



Architectural Design



Implementation Constraints

- We create a multiple ration distribution transactional data and stored all transactional data into multiple data nodes.
- Each node will holds the specific block for each transaction.
- Same block has replace for all nodes, and generates a valid block chain.
- System will retrieve data from all data nodes and commit the transaction, it should be any kind of DDL, DML as well as DCL transactional query.
- If any block chain invalid during the validation of data servers, then system will automatically recover whole blockchain using majority of servers.
- We will address and eliminate the runtime server attacks and recover it using own blockchain.
- System will provide the each transactional validation, for all servers

Project plan

- The waterfall model is a sequential design process, used in software development processes, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of conception, initiation, analysis, design, construction, testing, production/Implementation and maintenance. Waterfall approach was first SDLC Model to be used widely in Software Engineering to ensure success of the project. In the waterfall approach, the whole process of software development is divided into separate phases. In Waterfall model, typically, the outcome of one phase acts as the input for the next phase sequentially. Following is a diagrammatic representation of different phases of waterfall model.

1. Requirement Gathering and analysis: All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification doc.

2. System Design: The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture.

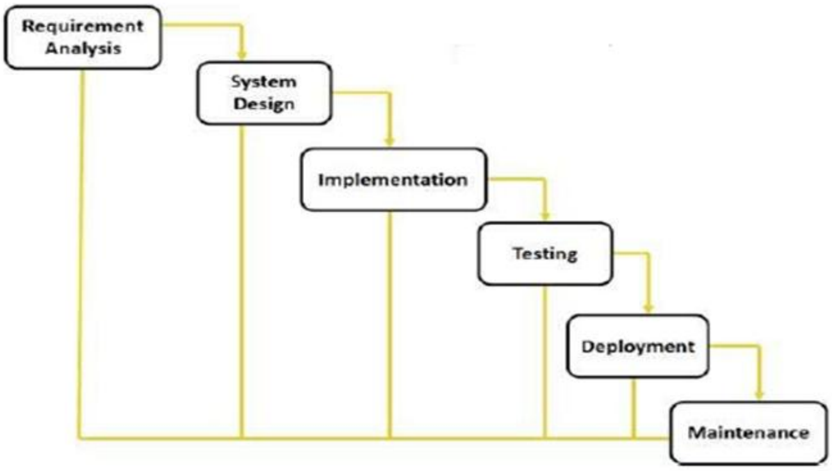


Fig.5.1 Project plan

3. Implementation: With inputs from system design, the system is first developedin small programs called units, which are integrated in the next phase.Each unit is developed and tested for its functionality which is referred toas Unit Testing.

4. Integration and Testing: All the units developed in the implementationphase are integrated into a system after testing of each unit. Post integrationthe entire system is tested for any faults and failures.

5. Deployment of system: Once the functional and nonfunctional testing isdone, the product is deployed in the customer environment or released intothe market.

6. Maintenance: There are some issues which come up in the client environment.To fix those issues patches are released. Also to enhance the productsome better versions are released. Maintenance is done to deliver thesechanges in the customer environment.

All these phases are cascaded to each other in which progress is seen as flowingsteadily downwards (like a waterfall) through the phases. The next phase isstarted only after the defined set of goals are achieved for previous phase and it issigned off, so the name"Waterfall Model". In this model phases do not overlap.

Risk Management w.r.t. NP Hard analysis

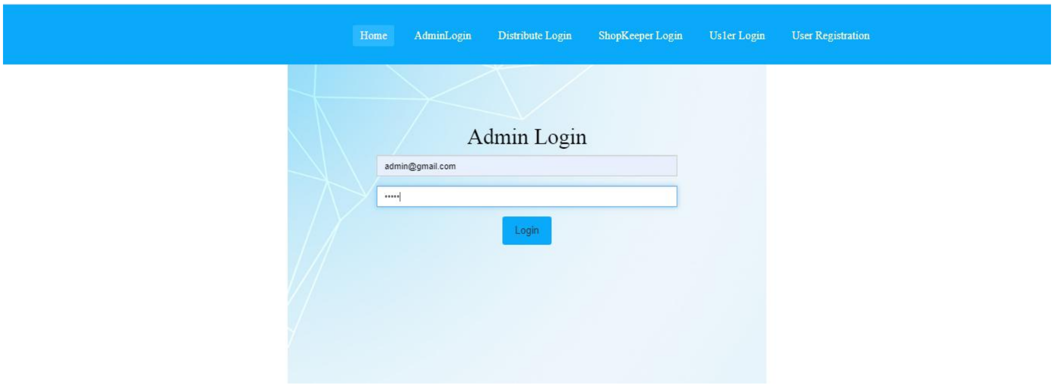
- Risk is a possibility of loss or injury. Risk management is the identification assessment and prioritization of risks followed by coordinated and economical application of resources to minimize and control that would probability and impact of unfortunate events or to maximize the realization of opportunities. Risk can come from uncertainty in financial markets, project failures (at any phase in design, development, production and sustainment life cycles), legal liabilities, credit risks, accidents, natural causes and disasters as well deliberate attack from an advisory of uncertain and unpredictable cause. Using risk management techniques we alleviate the harm or laws n software project or risk cannot be avoid but by perform in risk management we can attempt to ensure that right risks are taken at right time. Risk taking is essential to progress and failure is often key part of learning.

Cost Estimation

- The information can be specified in the form of: Object points
- Function points
- Line of source code
- For this project the sizing information in the form of lines of source code is used.
- Equation for calculating the efforts:
- E = a(KLOC)b
- a = 3
- b = 1:14
- for the project the KLOC 4.5

- E = 3(2 : 5)2 : 12
- E = 10:40 personal month

Screen shots

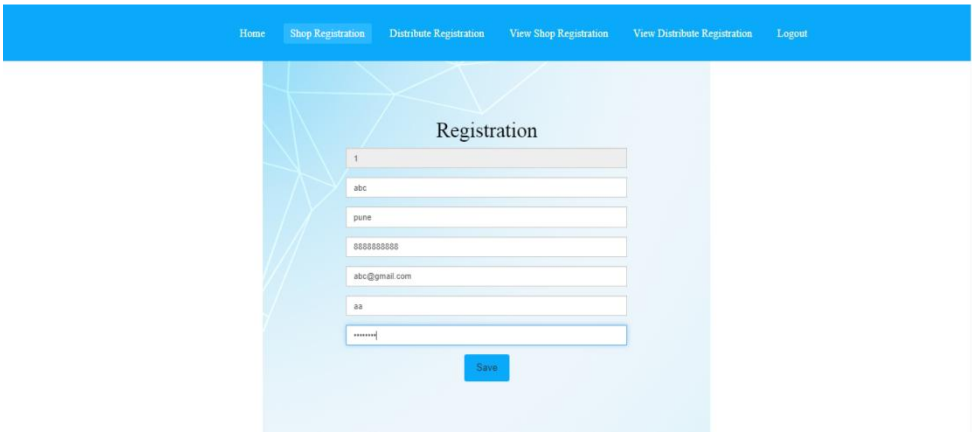


Admin Login

admin@gmail.com

•••••

Figure 6.1: Admin Login Page



Registration

1

abc

pune

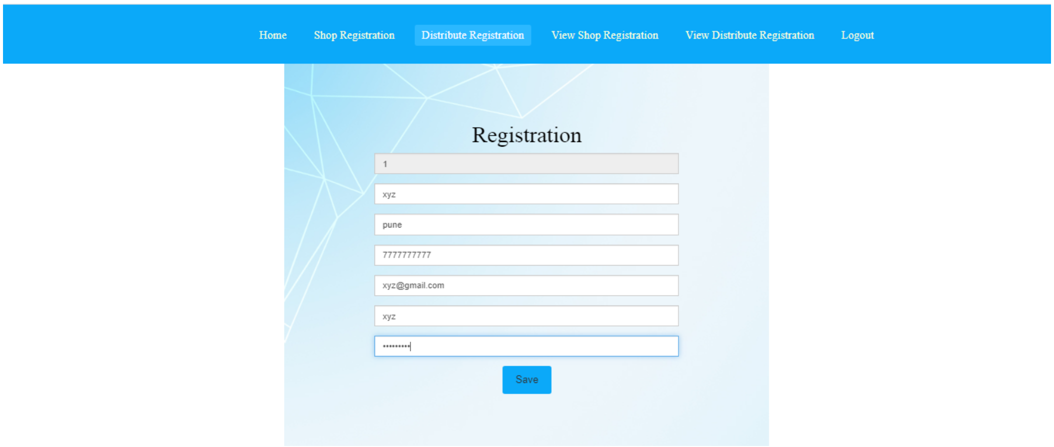
8888888888

abc@gmail.com

aa

••••••••

Figure 6.2: Admin Add Shop Register Page



Registration

1

xyz

pune

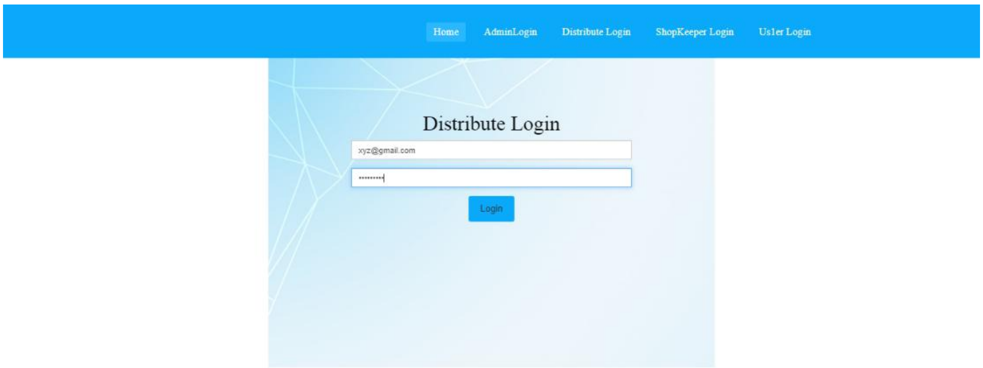
7777777777

xyz@gmail.com

xyz

•••••••••

Figure 6.3: Admin Add Distributes Register Page

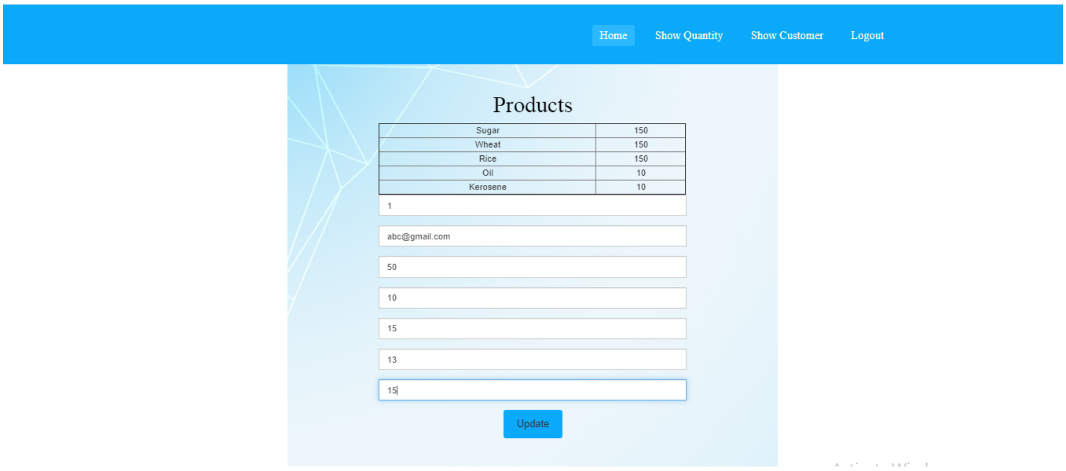


Distribute Login

xyz@gmail.com

•••••••••

Figure 6.4: Distributes Login Page



Products

Sugar	150
Wheat	150
Rice	150
Oil	10
Kerosene	10

1

abc@gmail.com

50

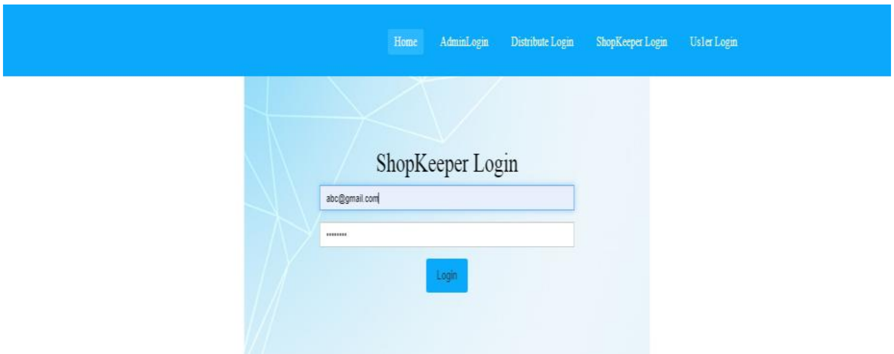
10

15

13

15

Figure 6.5: Distributes Add Product Page

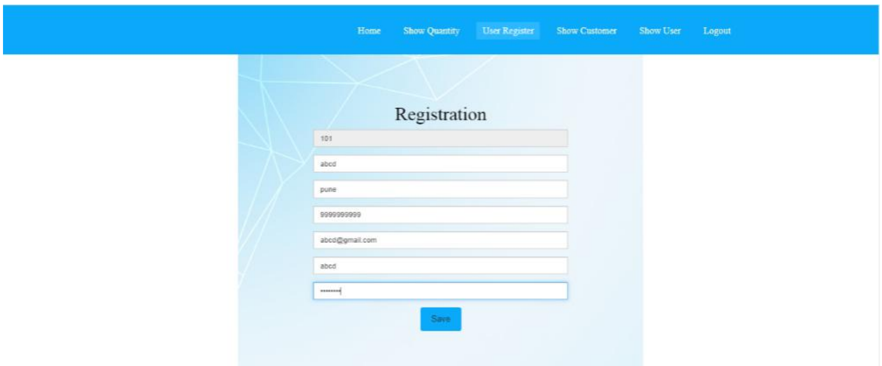


ShopKeeper Login

abc@gmail.com

••••••••

Figure 6.6: Shop Login Page



Registration

101

abcd

pune

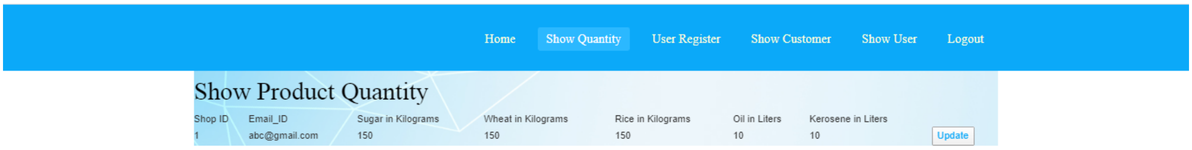
9999999999

abcd@gmail.com

abcd

••••••••

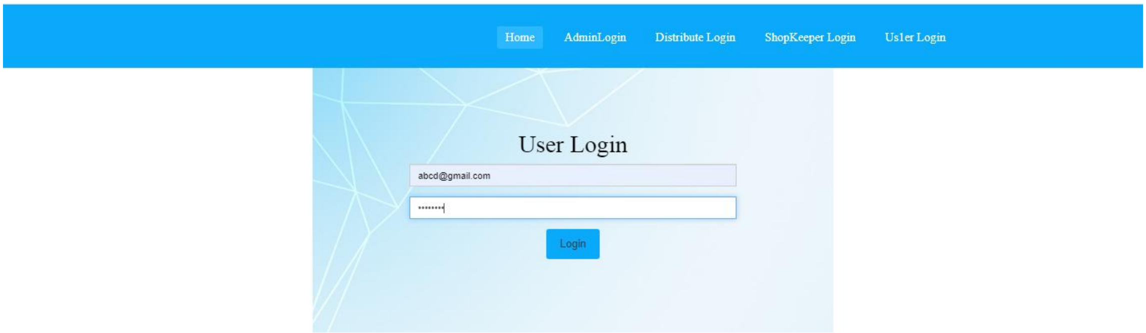
Figure 6.7: Shop Add Register Page



Show Product Quantity

Shop ID	Email_ID	Sugar in Kilograms	Wheat in Kilograms	Rice in Kilograms	Oil in Liters	Kerosene in Liters
1	abc@gmail.com	150	150	150	10	10

Figure 6.8 Shop Update Product Page

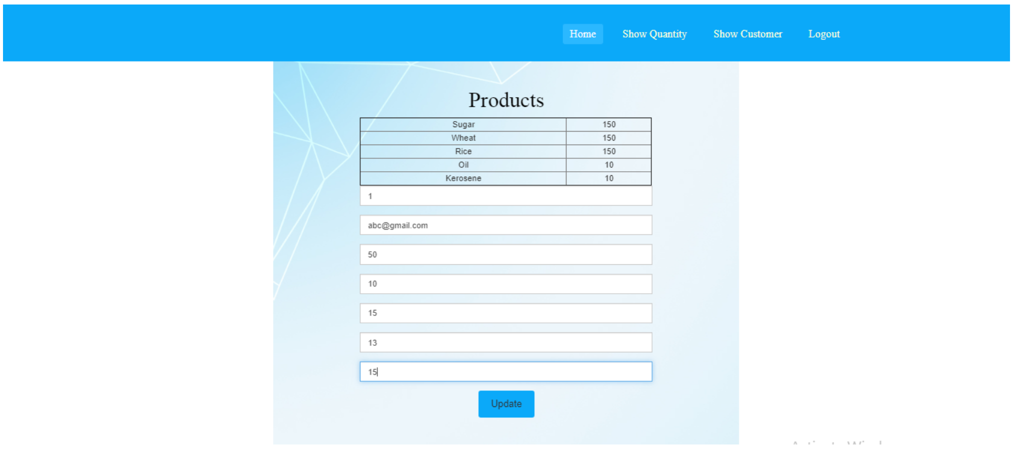


User Login

abcd@gmail.com

••••••••

Figure 6.10: User Login Page



Products

Sugar	150
Wheat	150
Rice	150
Oil	10
Kerosene	10

1

abc@gmail.com

50

10

15

13

15

Figure 6.11: User Get Product Page

Installation and un-installation

Major Tasks in the Dissertation stages are:

Task 1 - Download and install jdk 1.7.0 or higher for windows 7 configuration

Task 2 - Download and install Eclipse Juno which is compatible jdk 1.7

Task 3 – Download and Install MySQL 5.1 and create database and tables, also download and install HeidiSQL for database GUI purpose.

Task 4 - Run Eclipse and create Workspace and provide workspace name

Task 5 - Import Java project Import the source code from the source code directory into workspace

Task 6 - Set up database connectivity. Using JDBC and MYSQL bridge drivers

Task 7 – First go to project properties using right click on project in Eclipse, select Run Tab, and set main class for first execution.

Task 8 - Finally run Java Program- Run Java program through Eclipse

Conclusion

There are many research directions in applying Blockchain technology to the real estate transaction due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many real estate transaction use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating an interoperable ecosystem using the Blockchain technology while balancing critical security and confidentiality concerns in real estate transaction. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in real estate transaction is also needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility). In some cases, a new Blockchain network may be more suitable than the existing Blockchains; therefore, another direction may be investigating extensions of an existing Blockchain or creating a real estate transaction Blockchain that exclusively provides real estate transaction services. Blockchain technology should prevent the insecurity and injustice that are part of these land registries. The shared ledger technology should bring trust. Will this truly be the case? And will it be possible to replace well-functioning Land Registration systems that are not corrupt and are kept and managed the proper way, Will a blockchain-based system be less complicated and less expensive than the current well-functioning Land Registration systems its big question.

REFERENCES

1. “Smart Contracts,” http://searchcompliance.techtarget.com/definition/ smart-contract, 2017, [Online; accessed 4-Dec- 2017]
2. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchainin internet of things: Challenges and Solutions,”arXiv:1608.05187 [cs], 2016. [Online].Available:http://arxiv.org/abs/1608.05187%5Cnhttp://www.arxiv.org/pdf/1608.05187.pd
3. Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian. IEEE, 2018.
4. Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data." Proceedings of the Norwegian Information Security Conference. 2017.
5. Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.
6. Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.
7. Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.
8. Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.
9. Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.
10. Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.
11. Ouaddah, Aafaf, Anas AbouElkalam, and AbdellahAitOuahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things." Security and Communication Networks 9.18 (2016): 5943-5964.
12. Kiviharju, Mikko. "Enforcing Role-Based Access Control with Attribute-Based Cryptography in MLS Environments."
13. He, Qingsu, et al. "A privacy-preserving Internet of Things device management scheme based on blockchain." International Journal of Distributed Sensor Networks 14.11 (2018): 1550147718808750.
14. Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2017.
15. Wu, Axin, et al. "Efficient and privacy-preserving traceable attribute-based encryption in blockchain." Annals of Telecommunications (2019): 1-11.
16. Sui, Zhimei, et al. "An Encrypted Database with Enforced Access Control and Blockchain Validation."
17. Wang, Shangping, Lisha Yao, and Yaling Zhang. "Attribute-based encryption scheme with multi-keyword search and supporting attribute revocation in cloud storage." PloS one13.10 (2018): e0205675.

18. Zhang, Yinghui, et al. "Anonymous attribute-based proxy re-encryption for access control in cloud computing." Security and Communication Networks 9.14 (2016): 2397-2411.

19. Robert H. Deng, Yinghui, et al. "Outsourcing service fair payment based on blockchain and its applications in cloud computing." IEEE Transactions on Services Computing (2018).

20. Alam, Masoom, et al. "Secure policy execution using reusable garbled circuit in the cloud." Future Generation Computer Systems 87 (2018): 488-501.

21. Zhang, Yunru, Debiao He, and Kim-Kwang Raymond Choo. "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT." Wireless Communications and Mobile Computing 2018 (2018).