International Journal of Current Engineering and Technology
©2021 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

A Novel Approach for Traceability and Detection of Counterfeit Medicines through Blockchain

Ms.Kajal Bharat Adsul and Prof. S.P.Kosbatwar

Department of Computer Engineering. Smt. Kashibai Navale College of Engineering Pune

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The production and distribution of counterfeit tablets is an urgent and increasingly critical worldwide issue, specially in developing countries. The market cost of pharmaceutical counterfeiting has reached billions of dollars annually. One of the reasons for tablets counterfeiting is the imperfect supply chain device in pharmaceutical industry. Drugs change ownership from manufacturers to wholesaler; distributor and then pharmacist earlier than it reach the customer. In existing supply chain gadget, data isn't always shared between systems, producers don t know what happened to their products, pills regulatory authority has no visibility of the system, recalls are complex and costly, and corporations cannot follow-up patients. In this paper we explain the way to use block-chain generation in pharmaceutical deliver chain to feature traceability, visibility and protection to the drugs deliver device. The proposed gadget may be used in pharmaceutical industry to track the tablets from its manufacturing until its delivery to patient. After using a drug, its effect on patient will be recorded to a database for future statistics. A authorized block-chain could be used for storing transactions and only trusted parties may be allowed to join the community or system and push all the records to blockchain.

Keywords: *Blockchain, traceability, counterfeit medicines, supply chain management, security, pharmaceutical industries.*

Introduction

Pharmaceutical Research Development is a complicated method that takes several years from drug discovery to drug improvement and regulatory approval. When all the process is done and a general product is developed, the next challenge for producers is to deliver the product to the intended patron in its original form and to make certain that the client get the real product this is developed by means of the valid manufacturer, now not via counterfeiter. But the contemporary Supply Chain Management (SCM) machine of pharmaceutical enterprise is outdated, and doesn't offer visibility and control for producers and regulatory authority over capsules distribution and it can't resist the 21st century cyber-security threats. This state of affairs of SCM leads to the production, distribution, and intake of counterfeit tablets. Counterfeit pills have created a specifically risky public fitness danger and increasingly eager worldwide difficulty specifically in developing countries. These counterfeit capsules directly and not directly adversely affect health. Indirectly, these pills do not comprise the dosage or energetic agent required to kill the disease, that finally motive drug-resistant strains, and then even using the original pills are useless. More immediately, such counterfeits may incorporate lively ingredients, but the quantity is simply too low or too high, or produced in an impure way that contains poisonous ingredients, in this case it is able to motive very critical fitness problems. Counterfeit pills producers on occasion use the brand emblem of valid manufacturers and make fake merchandise used in daily life, that's much less harmful. But in many instances they have an effect on the drugs for the remedy of cancer, painkillers, cardiovascular disorders, antibiotics, contraceptives and different pharmaceuticals that can result in very serious results.

According to the International Anti-Counterfeiting Coalition (IACC), counterfeiting has become one among world's largest and fast developing crook businesses, with an predicted cost of more than US dollar 600 billion annually. For the prevention of counterfeit tablets, pharmaceutical enterprise desires an efficient supply chain management device, and the fine available strategy to develop a super SCM device is the Block-chain technology. Block-chain is a distribute ledger system (firstly delivered by way of a pseudonym Satoshi Nakamoto in 2008) that has shown significant adaptability in latest years and plenty of market sectors sought ways of incorporating its capabilities into their operations. Although, to this point most of the focus has been on the financial services industry, but now tasks in other service related areas, inclusive of healthcare, energy and legal corporations also started using this marvel.

Supply chain security is one issue that has recently gained attention. Any product problem to a touchy production method and extensive reputational problems are associated with the final product, the benefits of Block-chain are evident. Block-chain is the satisfactory fit in those scenarios wherein privacy protection and information safety is the best priority.

Therefore pharmaceutical supply chain presents a in addition use case of Block-chain technology.

B. Motivation

- Pharmaceutical organizations face many challenges regarding counterfeit medicines.
- Detecting faux medicines so that it will save public life.

C. Objectives

- To protect public fitness and to prevent and combat counterfeit capsules at national, local levels through the measures provided on this convention and protocol.
- To formulate a commonplace and coordinated technique towards the elimination of the counterfeit tablets, and the development of not unusual definitions, information resources and tools.
- To identify counterfeit drugs.
- To discover the consciousness of the fake medication issue which requires an expanding security level for the appropriation of lawful pharmaceutical items.

Review of Literature

In this paper, author advise Gcoin blockchain because the base of the information flow of medicine to create transparent drug transaction information. Additionally, the law model of the drug deliver chain may be altered from the inspection and examination best model to the surveillance internet version, and each unit that is involved in the drug deliver chain would be able to participate concurrently to save you counterfeit pills and to shield public health, including patients. With Gcoin blockchain, the governance version of the drug deliver chain could shift from regulating (handiest through government audits) to surveillance net (via each player who entails the supply chain).[1]

In this, the writer uses the net which is facilitating the trade by using imparting counterfeiters with a huge purchaser base and limited risks. The dark internet within it allows for nameless transactions between manufacturer, distributor and consumer. While some on-line pharmacies are legitimate, there are a developing quantity of those which can be unverified which sell dangerous counterfeit products. Both the packaging and medication are becoming increasingly sophisticated, making it hard for customers and regulation enforcement to perceive them without chemical analysis. Counterfeit batches have additionally been detected in hooked up legal trade routes wherein they may be able to, if undetected, become in high street pharmacies and hospitals. Multiple groups have installation global operations to dismantle the alternate but that is a complex and evolving trouble that with out sizable modifications to law may by no means be fully.[2]

The author propose a scientific records sharing and safety scheme based on the Hospital's private blockchain to improve the electronic health system of the hospital. Firstly, the scheme can satisfy diverse security properties such as decentralization, openness, and tamper resistance. A dependable mechanism is created for the docs to keep medical records or get admission to the historical statistics of patients while assembly privacy preservation. Furthermore, a symptoms-matching mechanism is given among patients. It lets in sufferers who get the same symptoms to behavior mutual authentication and create a session key for their future verbal exchange approximately the illness. The proposed scheme is implemented through the use of PBC and OpenSSL libraries. Finally, the safety and overall performance evaluation of the proposed scheme is given.[3]

The authors affords a systematic mapping study to be able to map out all applicable research on SCM based on BCT. The paper took a survey on other blockchain programs in SCM that want additional investigation, such as agricultural deliver chain, protection of additive manufacturing, product ownership control, common-pool useful resource control, buying and supply control, supply chain great control, supply chain performance measurements. Nevertheless, many of the proposed frameworks-based totally answers lack actual performance evaluation on the economic context.[4]

According to this paper, the writer suggest an progressive blockchain-primarily based IIoT structure to help construct a greater steady and dependable IIoT device. By reading the shortcomings of the prevailing IIoT structure and the benefits of the Blockchain technology. We decompose and reorganize the authentic IIoT structure to shape a new, multi-center, partially decentralized structure. Thus, the proposed structure represents a good sized development of the original architecture, which presents a new route for the IIoT development.[5]

In this the author advise a blockchain enabled efficient facts collection and secure sharing scheme combining Ethereum blockchain and deep reinforcement learning (DRL) to create a dependable and secure environment. In this scheme, DRL is used to obtain the maximum amount of collected records, and the blockchain generation is used to make certain protection and reliability of statistics sharing. Extensive simulation results show that the proposed scheme can provide higher protection level and stronger resistance to assault than a traditional database based information sharing scheme for different levels/varieties of attacks.[6]

The author describes about the data sharing and collaboration through cloud service carriers is a stronghold with the increasing advancement of current technologies driving today's society. In this paper we design a information sharing model between cloud service companies the usage of the blockchain. By imposing the proposed model, cloud service providers will be able to securely reap information provenance and auditing while sharing clinical data among different cloud service providers in addition to entities which includes research and medical institutions with out any hazard on records privacy.[7]

The authors of this paper demonstrates an technique for handling clinical records, providing auditability, interoperability and accessibility via a complete log. Designed for file flexibility and granularity, MedRec permits patient information sharing and incentives for clinical researchers to maintain the gadget. We sit up for formalizing an on boarding manner for scientific studies "miners", and exploring mining statistics economics. In the close to future, we intend to perform user studies to evaluate the feasibility of the machine and to gauge patient and issuer interest.[8]

In this paper, the author describes approximately the Blockchain that offers numerous opportunities for usage within the healthcare sector, e.G. In public health control, user-oriented medical research primarily based on personal affected person statistics in addition to drug counterfeiting. The immense ability of this generation indicates up wherever, until now, a depended on third party was vital for the agreement of marketplace services. With Blockchain, direct transactions suddenly emerge as possible, whereby a critical actor, who managed the information, earned commission or maybe intervened in a censoring fashion, may be
eliminated.[9]

In this, the author introduce an extensible Unique Patient Identifier System that can ensure a unique ID for a patient to go across hospitals anywhere. It is a distributive system and has the gain in scalability, overall performance, and simplicity. This enables us to control the challenge in phases, and reaping the return-on-investment continually inside the entire process. Although this paper provides the technical ground for a complete implementation, a set of comprehensive hospital business techniques and regulations that helps the management of Unique Patient Identifier should accompany this solution that allows you to attain the general enterprise objective. This includes right procedures for the medical crew and administrative body of workers to query and become aware of the patient's identity, as well as the splitting and merging of Unique Patient Identifier through the registration office.[10]

Proposed Methodology

The blockchain is beneficial in keeping tune of the complete production chain of the drug. Each new transactions brought to a block is immutable and time stamped this means that that the information can not be tampered with. Companies can either have a public or a private blockchain. On those blockchains, the corporations may have a allotted ledger shared some of the events involved inside the manufacturing and distribution of the drug. Moreover, access is only limited depending on records sharing contract between the 2 parties. Through blockchain, we are able to get the whole trail of the drug. Each time the drug actions from an entity to another, the records is stored on the blockchain which makes it easy to track the drug and wipe off counterfeits from the shelves. As a end result the blockchain generation will assist with two foremost issues: first, it will allow organizations to tune their merchandise down the deliver chain, creating an airtight circuit, impermeable to counterfeit merchandise. Second, it's going to also permit stakeholders, and specifically labs, to take action a posteriori in case of a trouble by identifying the exact place of their drugs. Advantages:

- End-to-end traceability of healthcare products.
- Reduced loss related to counterfeit drugs.
- Enhancing the trust and transparency between each and every module connected in the block chain.
- Using blockchain, in the supply chain can allow us to identify the location of that products.
- Detection of counterfeit drugs is very helpful in order to save the public lives.

Modules:

In this different modules are used:

Module 1:

Manufacturer: Manufacturer will register and login to the system by using valid credentials. After that manufacturer will add the products in its database. They also generate the QR code in the products.

Module 2:

Supplier: Supplier will register and login to the system by using valid username and password. Supplier will view the product list and if want then they can place the order of that drugs by scanning the QR code.

Module 3:

Pharmacist: Pharmacist will also register and login to the system with valid credentials. Pharmacist view the patients request and also view the available products list and if want then they can place the order of that drugs by scanning the QR code.

Module 4:

Patients: Patient will register and login to the system using valid username and password. Patient place its order buy the drugs and at last logout from the system.

A. ArchitectureExplanation:

In this framework, first we are login to the framework by utilizing OTP. After login to the framework we are going to view our profile, Manufacturer will manufacture the drugs and apply QR code to that after that supplier will buy that and scan the QR code and then from supplier pharmacist will order that drugs also scan the QR code. Then user can view the medicines list if user want any medicine then they can place the order and buy that medicine. At last logout from the system. In this system all the modules will connected will each other through the blockchain to maintain the trust and transparency throughout the whole system process.

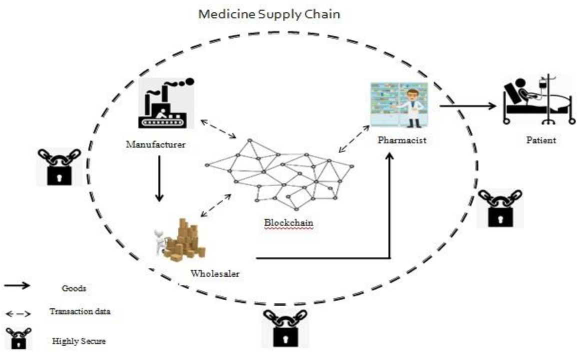

Fig. 1. Proposed System Architecture

B. Algorithms

Hybrid Approach:

In this we are going to increase the security and time efficiency by using algorithms i.e. Block-chain Algorithm (Cryptography algorithm).

The main purpose of using public-key cryptography for the blockchain is to create a secure digital reference about the identity of a user. Secure digital references about who is who, and who owns what, are the basis for P2P transactions. Public-key cryptography allows proving one's identity with a set of cryptographic keys: a private key and a public key.

Secure Hash Algorithms:

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. Secure hash Algorithm is a set of cryptographic hash functions developed by US-National Security Agency(NSA).

SHA – 256 algorithm is used in blockchain to get a constant hash of 256 bits every time. This algorithm is also a part of encryption technology.SHA-256 is a cryptographic hash function that takes an input of a random size and produces an output of a fixed size. Hash functions are powerful because they are 'one-way'. What this is means is, it is possible for anyone to use a hash function to produce an output when given an input; however, it is impossible to use the output of the hash function to reconstruct its given input.

Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.SHA is used to ensure that data has not been modified. SHA accomplishes this by computing a cryptographic function and any change to a given piece of data will result in a different hash value. As a result, differing hash values are key to determining if data has been altered. SHA-256 is used to improve security and privacy.

SHA-256 functions in the manner of MD5: The message to be hashed is first padded with its length in such a way that the result is a multiple of 512 bits long, and then parsed into 512-bit message blocks M(1) ; M(2) ;::::;M(N) The message blocks are processed one at a time: Beginning with a fixed initial hash value H(0) , sequentially compute H(i) = H(i1) + CM(i) (H(i1)); where C is the SHA-256 compression function and + means word-wise mod 232 addition. H(N) is the hash of M.

Advanced Encryption Standard:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java Operation of AES:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

1) Input:
2) 128 bit /192 bit/256 bit input(0,1) 3)secret key(128 bit)+plain text(128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6)Xor state block (i/p)
7)Final round:10,12,14
8)Each round consists:sub byte, shift byte, mix columns, add round key.
9)Output:
10)cipher text(128 bit)

C. Mathematical Model

1. Mathematical equation:

The algorithm implemented in this project is describe as: Initialization: password,key,time,salt:string time *←− get time input ←−* (*password*) *key ←− salt + time* Encryption: *Ciphertext ←− AESEncrypt*(*password,key*) *output*(*ciphertext*) Decryption:

```
$key \longleftarrow salt - time$
$forasmuchtolerancegiventime$
$if key = get\_time$
$key \longleftarrow salt + time$
$plaintext \longleftarrow AESDecrypt(ciphertext, key)$
$endif$
$endfor$
$output(plaintext)$
```

Result and Discussion

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i5-6700HQ CPU @ 2.60GHz, 16GB memory, Windows 7, MySQl Server 5.1 and Jdk 1.8.

In our system, We compared the proposed and existing system through the number of fake drug detected. The overall accuracy of proposed technique is enhanced as compared to existing techniques. So our proposed system accuracy is better than existing system. So this works gives better results as compare to existing method.

A. Results and Performance

Number of Test Case Prioritization selection:

S.No	Algorithm	No. of drugs	Rate of drug counts	Results
01	Proposed System	30	28	85%
02	Existing System	30	24	70%

Conclusion

The objectives for the research have been met. There is a bunch of example approaches using machine learning presented from the different aspects of the software testing.

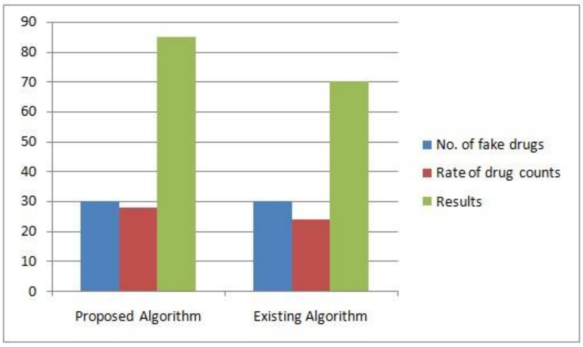

Fig. 2. Comparison graph according to drugs count and accuracy

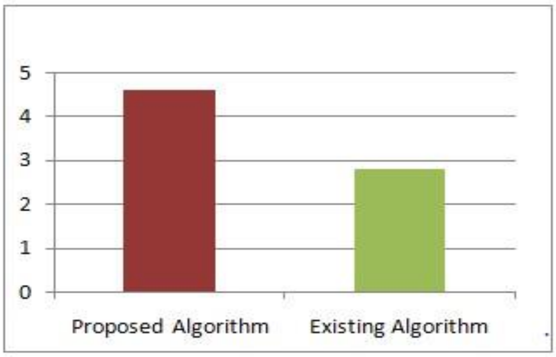

Fig. 3. Algorithms Comparison

These researches answer the question how AI implementations could serve the testing. In the beginning of starting this research it was unclear what would the findings be and what kind of document would this be in the end. The scope and data in the document prove that the field of AI testing has grown rapidly during the last few years and there actually was much more information available that was assumed in the beginning.At present the framework in this examination we have proposed a novel established system for the association of Test case prioritization methods utilizing Fuzzy Logic, for the variety of experiment prioritization strategy dependent on three components: necessity inclusion, endeavors and, intricacy. This exertion is an adjournment of recently proposed combination composition for experiment prioritization strategies. Prioritizing check instances will limit the time, attempt and value of testing and uncover maximum faults inside the software. The current days of manual and automated UI testing gradually become ineffective when contrasted with an MLbased solution. Deployment of this work would unquestionably prove to be extraordinary decline in the testers' time and effort complexity.

Acknowledgment

The authors would like to thank the researchers as well as publishers for making their resources available and for their guidance. We are thankful to the authorities of University of Pune and concern members of CPGCON 2020 conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1]. Jen-Hung Tseng, Yen-Chih Liao, Bin Chong and Shih-wei Liao,"Governance on the Drug Supply Chain via Gcoin Blockchain", International Journal of Environment Research and Public Health, MDPI, 2018.

[2]. Andrew O'Hagan, April Garlington, "Counterfeit drugs and the online pharmaceutical trade, a threat to public

safety", Forensic Research Criminology International Journal, Volume 6 Issue 3 – 2018.

[3]. Xiaoguang Liu, Ziqing Wang, ChunhuaJin, Fagen Li, And Gaoping Li, "A Blockchain-based Medical Data Sharing and Protection Scheme", IEEE Access (Volume: 7), 2019.

[4]. YounessTribis, Abdelali El Bouchti, Houssine Bouayad, "Supply Chain Management based on Blockchain: A Systematic Mapping Study", MATEC Web of Conferences (2018).

[5]. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory",IEEE Transactions on Industrial Informatics Volume: 15 , June 2019.

[6]. Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning", IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019.

[7]. X. Qi, B. S. Emmanuel, O. Kwame, G. Jianbin, D. Xiaojiang And G. Mohsen, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, 2017.

[8]. Asaph, E. Ariel, V. Thiago and L. Andrew, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2nd International Conference on Open and Big Data, Cambridge, MA, 02139, USA, 2016.

[9]. M. Mettler, "Blockchain Technology in Healthcare: The Rovolution Starts Here," in IEEE 18th International 12 Conference on e-Health Networking, Applications and Services, Healthcom, 2016.

[10]. C. Edward, L. Ying, Z. Jia and L. Yang, "Healthcare services across China – on implementing an extensible universally unique patient identifier system," International Journal of Healthcare Management , pp.1-7, 2017.