International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 1182-1191

"A Blockchain Based Framework for SecureData Sharing Of Medicine Supply Chain in Health Care System"

Vagdevi Kamath M[1], Yaparla Lahari[2], Thejashwini K R[3], Sahana T S[4], Dr GManjula[5]

[1][2][3][4] 8th Sem BE Students, [5] Professor, Department of ISE Dayananda Sagar Academy of Technology and Management, Bengaluru-560082

ABSTRACT

The main issues with drug safety inthe counterfeit medicine supply chain, are to do with how the drugs are initially manufactured. The traceability of right and active pharmaceutical ingredients during actual manufacture is a difficult process, so detecting drugs that do not contain the intended active ingredients can ultimately lead to end consumer patient harm or even death. Block chain's advanced features make it capable of providing a basis for complete traceability of drugs, from manufacturer to end consumer, and the ability to identify counterfeit-drug. This project aims to address the issue of drug safety using Block chain and encrypted QR(quick response) code security.

Any product subject to a sensitive production process and widespread reputational issues are associated with the final product, the benefits of Block-chain are evident. Block-chain is the best fit in those scenarios where privacy protection and data security are the highest priority. Therefore, pharmaceutical supply chain presents a further use case of Block-chain technology.

Date of Submission: 05-06-2022 Date of acceptance: 20-06-2022

I. INTRODUCTION

Pharmaceutical Research & Development is a complex process that takes several years from drug discovery to drug development and regulatory approval. When all the process is done and a standard productis developed, the next challenge formanufacturers is to deliver the productto the intended customer in its original form and to ensure that the customer get the genuine product that is developed by the legitimate manufacturer, not by counterfeiter. But the current Supply Chain Management (SCM) system of pharmaceutical industry is outdated, and doesn't provide visibility and control for manufacturers and regulatory authority over drugs distribution and it cannot withstand the 21st century cyber-security threats. This situation of SCMleads to the production, distribution, and consumption of counterfeit drugs. Counterfeit drugs have created a particularly dangerous public health risk and increasingly keen worldwide issue especially in developing countries.

These counterfeit drugsdirectly and indirectly adversely affect health. Indirectly, these drugs do not contain the dosage or active agent required to kill the disease, that finallycause drug-resistant strains, and then even using the original drugs are useless. More directly, such counterfeits may contain activeingredients, but the amount is too low or too high, or produced in an impure manner that contains toxic ingredients, in this case it can cause very serious health problems. Counterfeit drugs manufacturers sometimes use the brand logo of legitimate manufacturersand make fake products used in daily life, that's less harmful. But in many cases, they affect the drugs for the treatment of cancer, painkillers, cardiovascular disorders, antibiotics, contraceptives and other prescription drugs that can lead to very seriousresults.

Fig 1.1 Counterfeit medicine.

According to the International Anti-Counterfeiting Coalition (IACC),counterfeiting has become one of world’s largest and fast-growing criminal businesses, with an estimated value of more than US$ 600 billion annually. For the prevention of counterfeit drugs, pharmaceutical industry needs an efficient supply chain management system, and the best available solution to develop a perfect SCM system is the Block-chain technology. Block chain is a distributeledger system (firstly introduced by a pseudonym Satoshi Nakamoto in 2008) that has shown widespreadadaptability in recent years and a variety of market sectors sought ways of incorporating its abilities into their operations. Although, so far most of the focus has been on the financial services industry, but now projects in other service-related areas, such as healthcare, energy and legal firms also started using this marvel.

Supply chain security is one aspect that has recently won attention. Any product subject to a sensitive production process and widespread reputational issues are associated with the final product, the benefits of Block-chain are evident. Block-chain is the best fit in those scenarios whereprivacy protection and data security are the highest priority. Therefore, pharmaceutical supply chain presents a further use case of Block-chain technology.

IMPLEMENTATION

Modules

- ❖ Medical Chain Data Storage inBlockchain
- ❖ Drug Safety using Blockchain
- ❖ QR Code Encryption & Decryption
- ❖ System Model

Modules Description

Medical Chain Data Storage inBlockchain

The proposed structure for storage of transaction data, represents the similaritywith Bitcoin transaction data. The each participant will share their public key, hashvalue of previous transaction, encrypted QR (Quick response) code by manufacturer. The QR code consist the details of medicine which is manufactured by pharmaceuticals agency. The transaction of medical chain here is secure and tempered-proof. Illegitimate participant can’t get access to the block of transaction due to public key verification of participant(recipient) and digital signature verificationof sender.

This structure provides the non- repudiation verification using the sendercryptographic signature. The given structure also prevents the double spendingproblem because of QR code. Each transaction of block in blockchain will contain an unique QR code, which cannot be reused by the manufacturer for differentmedicine.

Drug Safety using blockchain

The proposed framework for drug safety using blockchain produces the securechannel for drug safety among various participants like Manufacturer, Distributor,Patient, Hospital, and Regulatory of smart contract, in medicine supply chain. Each transaction data includes manufacturer and its product information, e.g., manufacturer-id1(MID1) has manufactured Drug-ID1 (DRUG1) and Drug-ID2 (DRUG2). This data is known and distributed to all participants in medical chain framework. This structure shows here transparency between the participants.

- In proposed framework,pharmaceuticals organization will manufacture the drug with details such as drug name, location, timestamp, ingredients, usage of drug, and side effect and get authorized by regulatory approved smart contract. Manufacturer generates an encrypted QR (quick response) code for the details and attaches the transaction to the blockchain system.
- If any participants want details of drugs, then public key must be shared by that participant to the manufacturer. Manufacturer will encrypt the QR code and will send back to the participant.
- The QR code will be decrypted by the valid participant by their privatekey.
- The illegitimate user can not accessthe blockchain, only legitimate can access the blockchain using public key.

QR Code Encryption & Decryption

In the QR code encryption &decryption method based on the DES algorithm, the DES encryption &decryption algorithm is used to encrypt thepepper-and-salt region of the QR code image in 64 bits. Then, the unencrypted dates of the white region around the QR are combined with encrypted data of thepepper-and-salt region in the middle of the QR. The data are written in binary digital image format, and then, they are stored as image file. It is the encrypted QR codeimage.

According to the characteristics of QR code image and digital image, as well as the principle of digital image encryption& decryption system in blockchain technology, an effective QR code encryption method which can ensure the high speed and high security is designed inthis project.

System Model

The proposed which is based on private Blockchain technique ,where all the authorities has to get the membership by provider(Regulatory Body) and digital signature by certificate authority.The digital signature will be provided by the certificate authority , hence the participantscan trust on it.

- Transaction between participantswill consist sender public key and digital signature, receiver public key and the information which is sent by sender.
- The shared information between theparticipants will be in encrypted QR code format , which can be onlyaccessed by receiver public key.
- Sender public key will be verified by all the participants of medical chain supply.
- Once the transaction get committedthen it will be distributed to all the participants.

OBJECTIVES

1. Input Design is the process of convertinga user-oriented description of the input intoa computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing inputis to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

Product function

The purpose of the Software Requirements Specification (SRS)document is to maintain all the function andthe specification of the our Application. It contains the description of all the requirements as specified in synopsis.

The main purpose of the document is to maintain the sales calls record made byration centernel spread across the branches, taken order from the Consumer, set remainder to retrieve and set the current andfuture sales record provide Consumer interaction facility which eases the requirements of the Consumers. This system includes the requirements tocomplete a companies interaction with the current and future Consumer; it includes therequest, approval, reimbursement, saleselements.

So instead of paper basedtransaction the system can accomplish automated micro finance activities where the workflow can be easily maintained. And the System is much user friendly as it overcomes the physical appearance of boththe parties and consumes less time in all aspects. And mainly reports can be maintained easily.

In the proposed system will helpthem to manage day to day operation very smoothly It is having different modules to fulfill the requirement of the organization. Proposed system is an online system: so anypersons can browse and register with the application.

Less time consuming.

- Highly secure in datastoring.
- Can avoid intermediatepersons & institutions
- It is more users friendly.

User characteristics

The user of the system will be givena user name and password during login. Once login in to the system user can maintain all the information related to test operations.

Specific constraints

Since the system will be implemented in ASP.NET C# technology, the software will used in any windows platform. Front End is Microsoft VisualStudio .Net 2012. Admin is the user of the system who is going to login the system with the username and password.

General constraints

Hard disk capacity can be variesfrom 30GB to 40 GB. Ram capacity may be512Mb or 1GB. Any person can use the system and any kind of images can be used.

Software Environment

4.1 Features OF. Net

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutralplatform for writing programs thatcan easily and securely interoperate. There's no language barrier with

.NET: there are numerous languagesavailable to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation forcomponents to interact seamlessly,whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

".NET" is also the collective name given to various software components built upon the

.NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET MyServices, and so on).

THE .NET FRAMEWORK

The .NET Framework has two main parts:

1. The Common Language Runtime(CLR).
2. A hierarchical set of class libraries.

The CLR is described as the "execution engine" of .NET. It provides the environment within which programs run. The most important features are Conversion from a low-level assembler-stylelanguage, called Intermediate Language (IL), into code native to theplatform being executed on.

Memory management, notablyincluding garbage collection.

Checking and enforcing security restrictions on the running code.

Loading and executing programs, with version control and other such features.

The following features of the .NET framework are also worthdescription:

Managed Code

The code that targets .NET, and which contains certain extra Information - "metadata" - to describe itself. Whilst both managedand unmanaged code can run in the runtime, only managed code containsthe information that allows the CLR to guarantee, for instance, safe execution and interoperability.

Managed Data

With Managed Code comes Managed Data. CLR provides memory allocation and Deal location facilities, and garbage collection.Some .NET languages use Managed Data by default, such as C#, Visual

Basic.NET and JScript.NET, whereas others, namely C++, do not. Targeting CLR can, depending on the language you're using, impose certain constraints on the features available. As with managed andunmanaged code, one can have both managed and unmanaged data in

.NET applications - data that doesn'tget garbage collected but instead is looked after by unmanaged code.

Common Type System

The CLR uses something called the Common Type System (CTS) to strictly enforce type-safety.This ensures that all classes are compatible with each other, by describing types in a common way. CTS define how types work within the runtime, which enables types in one language to interoperate with types in another language, including cross-language exception handling.As well as ensuring that types are only used in appropriate ways, the runtime also ensures that code doesn't attempt to access memory that hasn't been allocated to it.

Common Language Specification

The CLR provides built-in support for language interoperability.To ensure that you can develop managed code that can be fully used by developers using any programming language, a set oflanguage features and rules for usingthem called the Common Language Specification (CLS) has beendefined. Components that followthese rules and expose only CLS features are considered CLS- compliant.

THE CLASS LIBRARY

.NET provides a single-rooted hierarchy of classes, containing over 7000 types. The root of the namespace is called System; this contains basic types like Byte, Double, Boolean, and String, as wellas Object. All objects derive fromSystem. Object. As well as objects, there are value types. Value types canbe allocated on the stack, which can provide useful flexibility. There are also efficient means of converting value types to object types if andwhen necessary.

The set of classes is pretty comprehensive, providingcollections, file, screen, and network I/O, threading, and so on, as well as XML and database connectivity.

The class library is subdivided into a number of sets (or namespaces), each providing distinct areas of functionality, with dependencies between the namespaces kept to a minimum. **LANGUAGES SUPPORTED BY .NET**

The multi-languagecapability of the .NET Frameworkand Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft'sold favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family.

Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-orientedprogramming language. Thesefeatures include inheritance,interfaces, and overloading, amongothers. Visual Basic also now supports structured exceptionhandling, custom attributes and also supports multi-threading.

Visual Basic .NET is also CLScompliant, which means that any CLS-compliant language can use theclasses, objects, and components youcreate in Visual Basic .NET.

Managed Extensions for C++ and attributed programming are just someof the enhancements made to the C++ language. Managed Extensions simplify the task of migrating existing C++ applications to the new .NET Framework.

C# is Microsoft's new language. It's a C-style language that is essentially "C++ for Rapid Application Development". Unlike otherlanguages, its specification is just thegrammar of the language. It has no standard library of its own, and instead has been designed with the intention of using the .NET libraries as its own.

Microsoft Visual J# .NET provides the easiest transition for Java- language developers into the world ofXML Web Services and dramaticallyimproves the interoperability of Java-language programs with existing software written in a variety of otherprogramming languages.

Active State has created Visual Perl and Visual Python, which enable .NET-aware applications to be built in either Perl or Python. Both products can be integrated into the Visual Studio .NET environment. Visual Perl includes support forActive State's Perl Dev Kit.

Other languages for which .NET compilers are available include

- FORTRAN
- COBOL
- Eiffel

STRUCTURED EXCEPTION HANDLING

C#.NET supportsstructured handling, which enables us to detect and remove errors at runtime. In C#.NET, we need to use Try…Catch…Finallystatements to create exceptionhandlers. Using Try…Catch…Finally statements, we can create robust and effective exception handlers to improve the performance of our application.

THE .NET FRAMEWORK

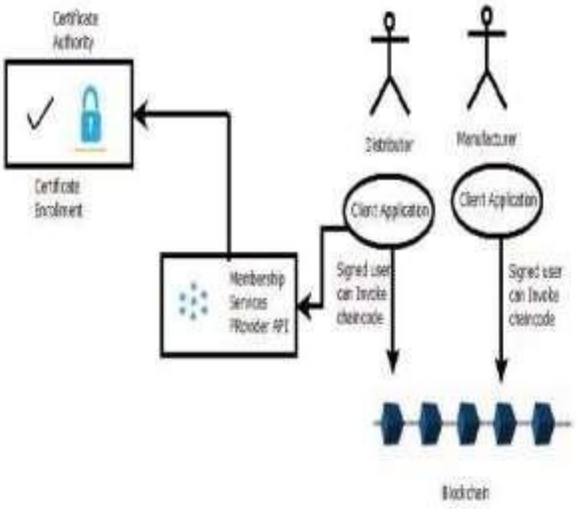
The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet.

OBJECTIVES OF. NETFRAMEWORK

1. To provide a consistent object- oriented programmingenvironment whether object codesis stored and executed locally on Internet-distributed, or executedremotely.
2. To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
3. Eliminates the performance problems.

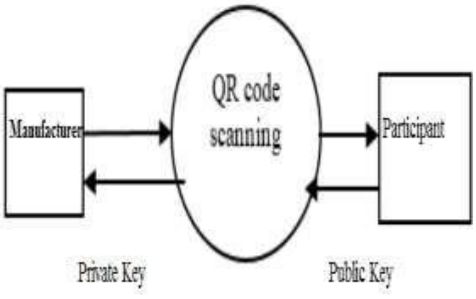
There are different types of application, such as Windows- based applications and Web- based applications.

SYSTEM DESIGN
SYSTEM ARCHITECTURE:

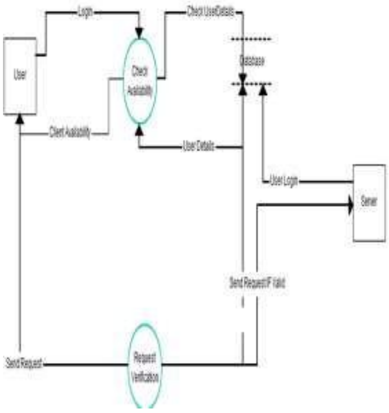


DATA FLOW DIAGRAM:

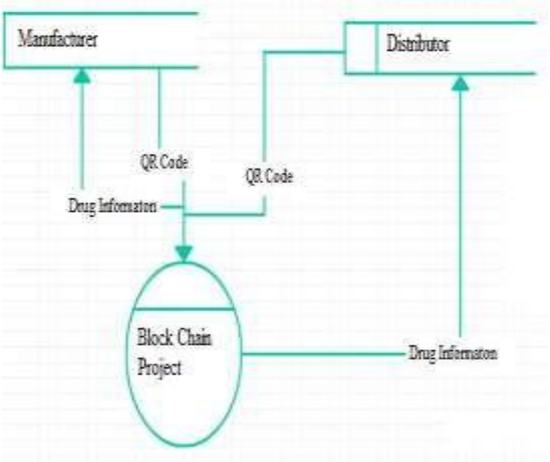
1. The DFD is also called as bubble chart. It is a simple graphical formalism that canbe used to represent a system in terms of input data to the system, various processingcarried out on this data, and theoutput data is generated by thissystem.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components.These components are the system process, the data used by the process, an external entity that interacts with thesystem and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations.It is a graphical technique thatdepicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may bepartitioned into levels that represent increasinginformation flow and functional detail.

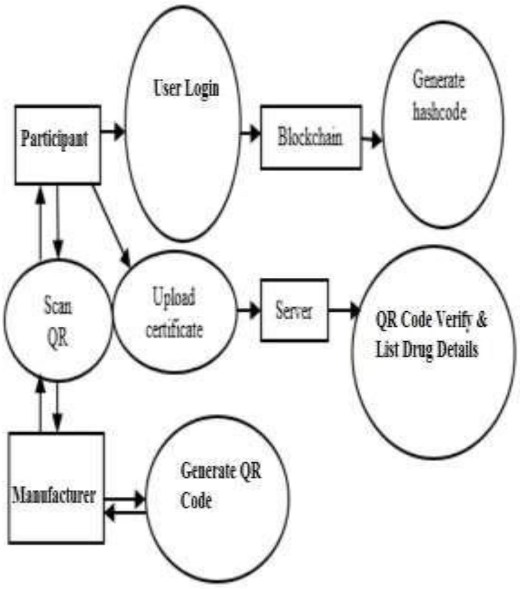


Level 0



Level 1





Level 2

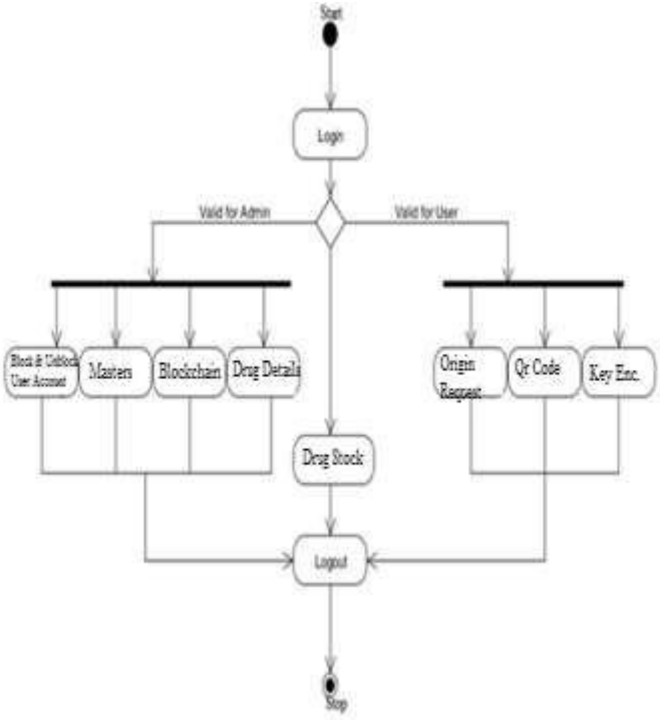
GOALS:

The Primary goals in thedesign of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility andspecialization mechanisms toextend the core concepts.
3. Be independent of particularprogramming languages and development process.
4. Provide a formal basis for understanding the modelinglanguage.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration andconcurrency. In the Unified Modeling Language, activity diagrams can be used to describe thebusiness and operational step-by-stepworkflows of components in a system. An activity diagram shows the overall flow of control.



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentiumi3 2.4 GHz.
- Hard Disk : 500 GB.
- Floppy Drive : 1.44 Mb.

- Monitor : 15 VGAColour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : -Windows 7 and Above.
- Coding Language :ASP.NET, C#
- Data Base : MS SQLSERVER 2008
- Framework : VisualStudio 2012

An SRS is basically anorganization's understanding (in writing) ofa customer or potential client's system requirements and dependencies at aparticular point in time (usually) prior to any actual design or development work. It'sa two-way insurance policy that assures thatboth the client and the organization understand the other's requirements from that perspective at a given point in time.

The SRS document itself states in precise and explicit language those functions and capabilities a software system (i.e., a software application, an ecommerceWeb site, and so on) must provide, as well as states any required constraints by whichthe system must abide. The SRS also functions as a blueprint for completing a project with as little cost growth as possible. The SRS is often referred to as the"parent" document because all subsequent project management documents, such as design specifications, statements of work, software architecture specifications, testingand validation plans, and documentationplans, are related to it.

It's important to note that an SRS contains functional and nonfunctional requirements only; it doesn't offer design suggestions, possible solutions to technology or business issues, or any otherinformation other than what the development team understands the customer's system requirements to be.

User Interfaces

An authenticated user of the system can use the system for item request, ration delivery and managing the consumer details.

Hardware interfaces

The Hardware Interfaces of the system are handled by the Windows Operating System. Further, core-2duo or higher processor with minimum 2GB random access memories and minimum of 40GB hard disk memory is recommended. No hardware dependent code will bewritten in the project.

Software interfaces

Coding Language used in our work is ASP .NET. Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NETFramework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate. Front end is Microsoft visual studio .net 2008 and Operating system is windows XP professional

Communication constraints

Communication constraints are notapplicable for our work.

Functional Requirement:

This project has been developed using ASP.Net as the front-end tool and MS SQL Server as back-end tool. C# is used for interfacing ASP.Net and MS SQL Server. ADO.Net Technology is used for managing application with the server and the database.

Non-functional Requirement

The efficiency is always been an issue in thisapplication development. This is no longer a critical issue in the proposed method. The application supports to logo detection & recognition.

Usability

The application which we are developing is going to be used by people who require to categories the documents based on the logo detection. The application also provides user friendly Graphical User Interface (GUI) with minimum user inputs.

Efficiency

Our application takes less time to accomplish a particular task once it is activated such as logo detection & recognition.

Dependency

The application provides its services once activated and it is more dependability while account number is detected.

Reliability:

The application that we are developing isdesigned to set of services as expected by theuser.

SYSTEM ANALYSIS

EXISTING SYSTEM:

The counterfeiting of medicines causes the serious threat to the society. The counterfeited medicines make an adverse effect on the health of the people and also causerevenue loss to the legitimate medicinemanufacturing organizations.

In the recent years, several anti-counterfeiting techniques have been proposed. However, most of the existing schemes are not secure and are prone to various attack such as replay, man-in-the-middle attack. Although conventional technologies, such as RFID, barcode scanning, and mobile technology, have been applied for tracking and tracing of medicines, counterfeit medicine is stillsignificantly high.

Counterfeiting of various products creates problem to different manufacturing industries and it causesserious threat to pharmaceuticalsproducts. This threatens the public health and also causes revenue loss to the legitimate manufacturing organizations. The International Chamber of Commerce of Geneva reported that the annual sales of counterfeit products in the world amounts to U.S.$ 650 billion.

DISADVANTAGES OF EXISTINGSYSTEM:

- The counterfeiting of medicines causes the serious threat to the society.
- The existing schemes are not secureand are prone to various attack suchas replay, man-in-the-middle attack.

□ Counterfeit medicine is stillsignificantly high.
□ Counterfeiting of various products creates problem to different manufacturing industries.
□ This threatens the public health andalso causes revenue loss to the legitimate manufacturing organizations.

PROPOSED SYSTEM:

We have proposed Medical chain storage using permissioned blockchain andhow counterfeit drugs will be tracked. It produces the secure channel for drug safetyamong various participants like Manufacturer, Distributor, Patient, Hospital, and Regulatory of smart contract,in medicine supply chain. As shown in Figure-2, each transaction data includes manufacturer and its product information, e.g., manufacturer-id1(MID1) has manufactured Drug-ID1 (DRUG1) and Drug-ID2 (DRUG2). This data is known and distributed to all participants in medicalchain framework. This structure shows heretransparency between the participants.

The following steps are involved for drug safety
1. In proposed framework, pharmaceuticals organization will manufacture the drug with details such as drug name, location, timestamp, ingredients, usage of drug, and side
effect and get authorized by regulatory approved smart contract. Manufacturergeneratesan encrypted QR (quick response)code for the details and attaches thetransaction to the blockchain system.
2. If any participants want details ofdrugs, then public key must be shared by that participant to the manufacturer.
Manufacturer will encrypt the QR code andwill send back to the participant.
3. The QR code will be decryptedby the valid participant by their private key.

Advantages Of Proposed System

□ This project aims at, trying to detectthe fake medicine for the safety purpose
□ and for saving the patient’s life.
□ The mentioned framework can provide drug security as well as authenticity of
□ manufacturer.
□ This helps in gym industry inidentifying fake supplements, where these
□ supplements are widely spread.
□ This can be used in pharmaceutical shop, where pharmacist can sell
□ Authenticated product.

II. CONCLUSION

□ The proposed Framework represent blockchain based secure infrastructure for medical chain supply among valid participants. The mentioned framework can provide drug security as well as authenticity of manufacturer. TheCurrent medical chain framework is working on third-party trust which is not very secure for the drug safety. The proposed methodology based on PKI and digital signature which can prevent from replay and man-in-middle attack.

REFERENCES

[1]. L. Paull, S. Saeedi, M. Seto, and H. Li, “AUV navigation and localization: A review,” IEEE J. Ocean. Eng., vol. 39, no. 1, pp. 131–149, Jan. 2013.

[2]. S. Chatzicristofis et al., “TheNOPTILUS project: Autonomous multi- AUV navigation for exploration of unknownenvironments,” in Proc. IFACWorkshop NGCUV, 2012, vol. 3, pp. 373–380.

[3]. M. Stojanovic and J. Preisig,“Underwater acoustic Communication channels:Propagation models and statistical characterization,” IEEE Commun.Mag., vol. 47, no. 1, pp. 84–89, Jan.2009.

[4]. G. Han, J. Jiang, L. Shu, Y. Xu, and F. Wang, “Localization algorithms of underwater wireless sensor networks: A survey,”Sensors, vol. 12, no. 2, pp. 2026–2061, 2012.

[5]. M. Erol-Kantarci, H. T. Mouftah, and S. Oktug, “A survey of architectures and localization techniques for underwater acoustic sensor networks,” IEEE Commun. Surveys Tuts., vol. 13, no. 3, pp. 487–502, 3rd Quart. 2011.

[6]. H. Jamali-Rad, H. Ramezani,and G. Leus, “Sparsity-aware multisource RSS localization,” Signal Process., vol. 101, pp. 174– 191, Aug. 2014.

[7]. E. Engineering and C. Science, “Reliable Identification of Counterfeit Medicine UsingCamera Equipped Mobile PhonesSaif ur Rehman, Raihan Ur Rasool, M. Sohaib Ayub, Saeed Ullah, AatifKamal, Qasim M. Rajpoot, and Zahid Anwar,” pp. 273–279.

[8]. M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, “Secure Authentication Scheme for Medicine Anti-CounterfeitingSystem in IoT Environment,” IEEEInternet Things J., vol. 4, no. 5, pp. 1634–1646, 2017.