IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

Implementation towards Blockchain based Healthcare Insurance Fraud Detection

Prerana S Pawar[1], Prof. S. P. Vidhate[2]

P.G. Student, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra India[1]

Assistant Professor, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra, India[2]

ABSTRACT: With the rapid growth of medical costs, the control of medical expenses has been becoming an important task of Health Insurance Department. Traditional medical insurance settlement is paid on a per-service basis, which leads to lots of unreasonable expenses. To cope with this problem, the single-disease payment mechanism has been widely used in recent years. However, the single-disease payment also has a risk of fraud. The insurance industry is a collection of service companies that provide protection services to customers with agreements and agreements from several parties involved. The conventional mechanism of the insurance claim process has the potential to cause fraud and a high risk that will harm the parties involved. On the other hand, block chain is a technology that one of its features is to provide a ledger where insurance companies can transfer insurance claims to an immutable ledger and help eliminate sources of fraud that are common in the insurance industry. The aim of this research is to help reduce fraud and risk for the insurance industry in general. In this work, proposal of a framework to identify fraud of medical insurance based on consortium blockchain and machine learning, which can recognize suspicious medical records automatically to ensure valid implementation on single-disease payment and lighten the work of medical insurance auditors. An explainable model is designed to evaluate the reasonability of disease code for Medicare reimbursement by predicting the probability of a disease according to the chief complaint of a patient. Storage and management process of medical records based on consortium blockchain to ensure the security, immutability, traceability, and auditability of the data is also presented.

KEYWORDS: Healthcare, Insurance Fraud, Machine Learning, AI, Blockchain.

I. INTRODUCTION

A Health insurance (HI) is a contract between the insurance provider and insurance subscriber in which the provider compensates the insurance subscriber's healthcare expenses. The health insurance association of America stated that healthcare insurance covers losses resulting from accidents, healthcare expenses, incapacity, accidental injury, and damage. Insurance subscribers have to pay the premium regularly for this compensation. The insurance provider can be from the The associate editor coordinating the review of this manuscript and approving it for publication was Bo Pu. commercial world or a government body. Nowadays, HI has become a necessity for each individual due to the rising hospitalization and treatment costs and getting income tax rebates. Earlier, the health insurance claim (HIC) process was manual and offline, with many shortcomings, such as insurance subscribers need to visit the insurance office during office hours only to fill out the premium and inquire about the HIC status, which wastes time and money in terms of transportation costs. Health claim records are easily alterable and accessible. So, the chances of fraud occur from the insurance provider, insurance subscriber, and healthcare service provider due to lesser transparency and privacy. It is less cost-effective due to the involvement of the intermediary broker or agent costs. In the digital era, every piece of information is gathered in a digital form, which revolutionizes the HIC worldwide. Following are various benefits of digitization: (i) it provides convenience to the parties involved with HIC. Insurance subscriber does not need to visit the insurance office frequently to purchase an HI and to fill out the premium amount , (ii) communication between insurance subscribers and providers becomes efficient, (iii) it makes auditor's complex and tedious work easy, (iv) any kind of fraudulent behaviour can be easily identified using Artificial Intelligence (AI), (v) it also reduces the human resource cost, and (vi) verification of claims becomes fast using web-generated reports, so insurance subscribers get insurance coverage fast and automatically during any medical emergency. There are many other benefits of the digitization of HIC besides those mentioned above. Despite several benefits of digitized HIC, it faces various challenges, which are described as follows. • Validation of data and model: Insurance providers use a digital business model to determine the premium rate and coverage price. This model is developed by professionals who may be unfamiliar with the rules and specific requirements of HIC, which can make professionals find it

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

challenging to measure the impact of new variables used in the models. In web-based HIC, data is collected from various social media platforms that may be no 100% accurate and outdated for validating the digital business model. The subscriber does not provide the data generated from the social media platform to the insurance provider. The insurance subscriber does not have a chance to correct this social media platform data, which may be used to determine the premium rate. • Lack of talent: Developing web-based HIC needs a group of skilled people because it is dependent on complex algorithms and mathematical skills. Lack of talent leads to the insurance sector becoming expensive. • Fraud detection system: Every insurance plan, including HI, is vulnerable to fraud. Every year, HI provider firms lose revenue due to fraudulent claims. Insurance firms hike premiums to maintain profit, which impacts legitimate insurers. It is assessed that fraudsters approximately take fifteen percent of the taxpayer's money, which is utilized to finance government-assisted Medicare. So, this is necessary for national authorities to develop systems for detecting fraudulent cases and payments. HI fraud is a severe offence that affects people and the nation's money and time. As a result, a good fraud detection system is necessary for lowering costs and enhancing the security of healthcare. HI fraud is increasing daily, which is a concern for the nation's insurance subscribers and providers. As there is no option for a HI fraud penalty, the number of fraudulent cases is increasing as a rapid rate. • Connecting to outdated computer system: Insurance providers need to replace legacy computer systems or customize their systems to interface with new technologies. However, such technologies increase the back-end cost for the insurance provider, but provides security against the HIC fraud. Legacy computer systems was developed around satisfying regulatory requirements rather than enhancing the subscriber's experience. • Privacy of HI subscriber's data: The insurance providers expanded the use of subscriber's data, which raises concerns about its security and privacy. It cannot be possible for an insurance subscriber to know exactly what or when data is collected and how data is being used. So, insurance subscriber does not provide explicit consent to the insurance provider, and insurance subscriber loses control over their personal information. So, the identity threat is a big issue in which insiders can misuse the insurance subscriber's identities to get insurance coverage. • Security of HI system: Digitization in HI raises various security concerns such as ransomware attacks, phishing attacks, Distributed Denial of Service (DDoS) attacks, replay attacks, and many more. Cybercrime affects the HIC industry from both internal and external sources, including the third parties. HIC data is stored in various systems, and it is interlinked between systems which causes authentication and authorization problems. Insurance firms lose lots of revenue and reputation due to the compromised security of the HI system.

Paper is organized as follows. Section I gives brief introduction to the topic; Section II describes survey done to understand the problem and detect the underlying problem in system. The diagram represents the step of the process with blockchain. After transaction, how process takes place is given in Section III. Finally, Section V presents conclusion.

II. RELATED WORK

1. Electronic Health Record's Security and Access Control Using Blockchain and IPFS

An electronic health record (EHR) typically contains sensitive medical records, personal information, doctors' provided prescription, and other physical histories of a patient. This digital approach remodeled the health sector while increasing privacy concerns and possibility of security breaches. This paper proposes an EHR system based on blockchain, interplanetary file system (IPFS), and cryptographic functions and includes features like secure access control having accountability, transparency, immutability of data in a cost-efficient patient centered architecture which is free from third-party interruption. Here, we divided data into two categories and three types of participants who are verified with digital certificates are granted permission by the patients and then they can access data. Finally, we build and investigate a simple implementation to analyze the cost of the system and propose some approaches to optimize it.

2. Introduction to Blockchain and Its Application in Smart Healthcare System

The blockchain technology has been into existence since 1991. A group of researchers had an aim for themselves, as they tried to solve the problem of tampering essential digital documents particularly, by the means of timestamping. However, when it comes to a break-through, it was done by Satoshi Nakamoto in the year 2009. He used this technology for the purpose of creating digital cryptocurrency bitcoin. Since then, fields in which it has been applied has increased manifold. However, before diving into the endless applications that it offers us, it is essential that we understand all the basics and features of this technology. Blockchain is said to have a peer-to-peer network which is decentralized and has ledger that is distributed to everyone that is a part of that network. Also, blockchain networks are

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

open to anyone to become a part of and start availing the various benefits. Every block in the blockchain stores essential information that corresponds to the transactions that take place, pertaining to various use cases.

3. Comparative Analysis Performance of Na¨ive Bayes and K-NN Using Confusion Matrix and AUC To Predict Insurance Fraud

The fraud allegedly started when customer submits a policy issuance for the elderly insured with a low sum insured so that the premium is also low. The insured's health condition at that time may not be good but it is not explained in the insurance application letter. To increase the sum insured, the policy is usually added with additional coverage. Fraud claim creates big loss for insurance company since the company has to pay the claim that they should not pay. Insurance company need to have a mechanism to avoid the fraud claim. From this research, it is expected to find the best methodology to be able to predict the potential of insurance claim fraud early when customers apply for policy issuance so that additional checks can be carried out for suspected submissions. The initial data available for this research is 14,778 claim records with attributes are: the date of claim submission, policy effective date, sum assured, type of claim, cause of claim, province and fraud. In order to get the best methodology on the accuracy and performance aspect to fulfil the expectation, two methodologies (Na¨ive Bayes and K-NN) are compared. Both Naive Bayes and K-NN methods are used with a comparison of training data and testing data is 80:20. Several combinations were performed for each of these methods.

4. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: Analysis, Architecture, and Future Prospects

Health insurance and its several benefits can face many security, privacy, and fraud issues.For the past few years, fraud has been a sensitive issue in the health insurance domain as it incurs high losses for individuals, private firms, and governments. So, it is essential for national authorities and private firms to develop systems to detect fraudulent cases and payments. A high volume of health insurance data in electronic form is generated, which is highly sensitive and attracts malicious users. Motivated by these facts, we present a systematic survey for Artificial Intelligence (AI) and blockchain-enabled secure health insurance fraud detection in this paper. This paper presents a taxonomy of various security issues in health insurance. We proposed a blockchain and AI-based secure and intelligent system to detect health insurance fraud. Then, a case study related to health insurance fraud is presented.

5. Fraud Detection in Insurance Claim System: A Review Insurance fraud has existed since the inception of insurance companies.

These are a wide range of crimes that go undiscovered and cost the insurance business billions of dollars each year. Due to economic growth, increased awareness, and stronger distribution channels, the Indian insurance business is predicted to reach US$280 billion by 2020. India is ranked 10th in terms of gross premiums earned for life insurance and 15th for non-life insurance products. For that reason, wen're introducing a blockchain-based framework for enabling secure transactions and data exchange among various interacting agents in the insurance network. Blockchain is a distributed peer-to-peer technology that allows for the safe, immutable, and transparent validation of healthcare claims. Also, discuss how blockchain and smart contracts can be used together to improve organizational operations. More particularly, it will show how these technologies can be utilized to create a system that prevents certain types of fraud in the areas of vehicle, health-care, and life insurance claims, among others. In this review will discuss about types of Fraud Detection in Insurance Claim System and its classification based on different machine learning methods. Also gives the future direction for Fraud Detection in Insurance Claim System.

6. Blockchain technology for Fraud Detection and Risk Prevention in Insurance Industry

The insurance industry is a collection of service companies that provide protection services to customers with agreements and agreements from several parties involved. The conventional mechanism of the insurance claim process has the potential to cause fraud and a high risk that will harm the parties involved. On the other hand, block chain is a technology that one of its features is to provide a ledger where insurance companies can transfer insurance claims to an immutable ledger and help eliminate sources of fraud that are common in the insurance industry. The aim of this research is to help reduce fraud and risk for the insurance industry in general. The research method uses a qualitative approach through observation of the mechanisms and business processes in insurance companies, especially those related to the claim process, to identify existing problems. Literature studies are used to find alternative solutions with information technology. The result of this research is a block chain model to reduce fraud and risk for the insurance industry in general.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

III. METHODOLOGY

A. System Architecture

The healthcare industry is constantly reforming and adopting new shapes with respect to technological evolutions and transition. It is necessary to maintain and monitor the patient's record without any ambiguity. Quality healthcare services have to be provided to users. Because of the growing technology, it is necessary to build a system in which the data is secured and maintained accurately. Due to the lack of traceability in the data transaction and the records, there have been several problems in the healthcare system.

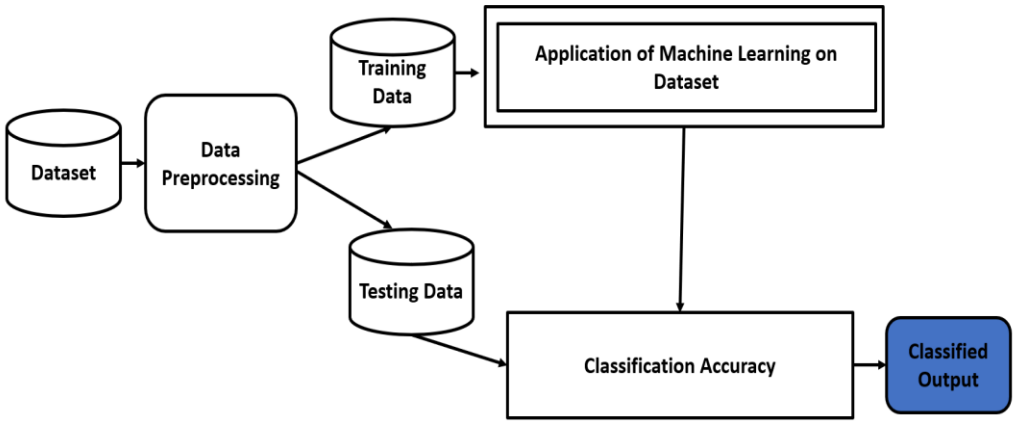


Figure: System Architecture

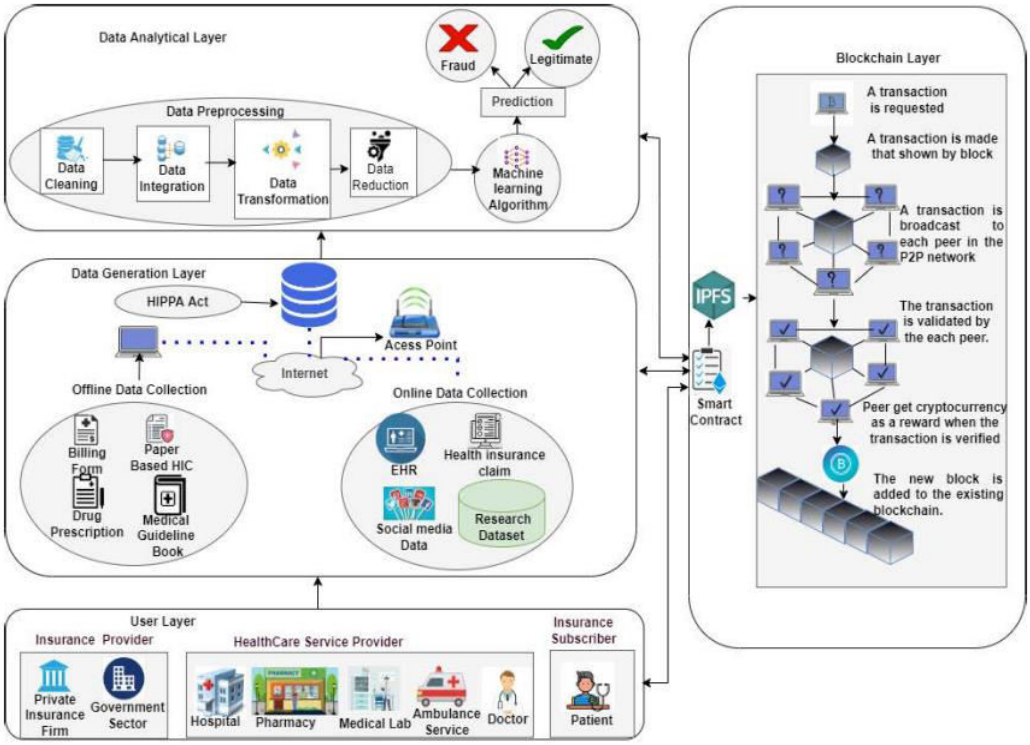


Figure: Whole Structure

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

B. Modules

1) User
- The user or patient registers for insurance.
- The user creates the profile.

2) Blockchain
- The claim is added to bock.
- The block is validated.
- The block is added to chain.

3) Insurance Fraud Detection
- The claim is tested after training is done with dataset.
- The claim is classified.
- The fraud is detected.

The Figure Sequence Diagram gives overview of all the activities implemented in the system.

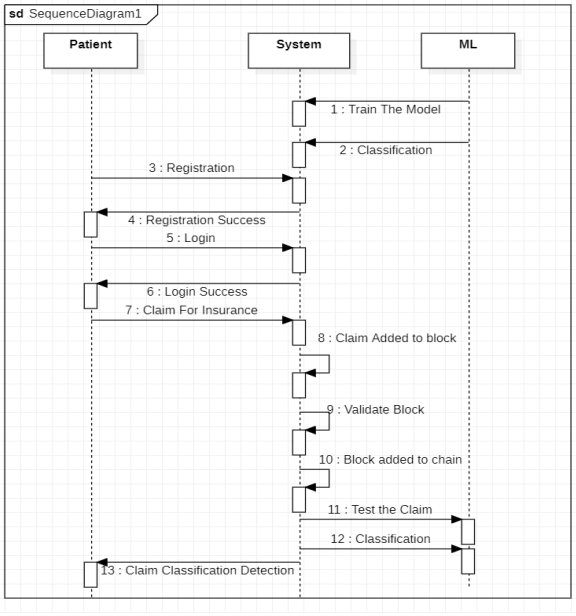


Figure: Sequence Diagram

C. Algorithm

1) Support Vector Machine (SVM)

SVM (Support vector machine) is one popular algorithm used for many classification problems.\\

• It is one of the supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier.

• An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible.

Input: D dataset, on-demand features, aggregation-based features

Output: Classification of Application

2) SHA256:

SHA-256 (256 bit) is part of SHA-2 set of cryptographic hash functions, designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). A hash function is an algorithm that transforms (hashes) an arbitrary set of data elements, such as a text file, into a single fixed length value (the hash). The computed hash value may then be used to verify the integrity of copies of the original data without providing any means to derive said original data. Irreversible, a hash value may be freely distributed, stored and used for comparative purposes. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor.

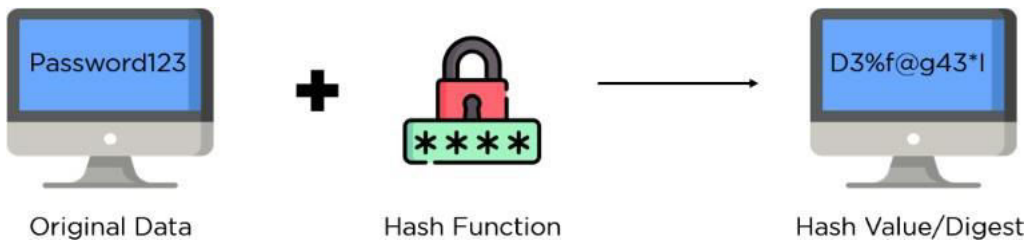


Fig. 2. SHA256

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

D. Mathematical Model

Let S be the whole System,

S = {I, P, O}

I = Input

P = Procedure

O = Output

I = {I0, I1}

I0 = Insurance details

I1 = Insurance Claim

P ={P0, P1, P2, P3,P4}

P0 = claim for insurance

P1 = claim added to block

P2 = Validate block

P3 = Block added to claim

P4 = Testing the claim

O = {O0, O1}

O0 = Detect Insurance Fraud

IV. RESULTS AND DISCUSSIONS

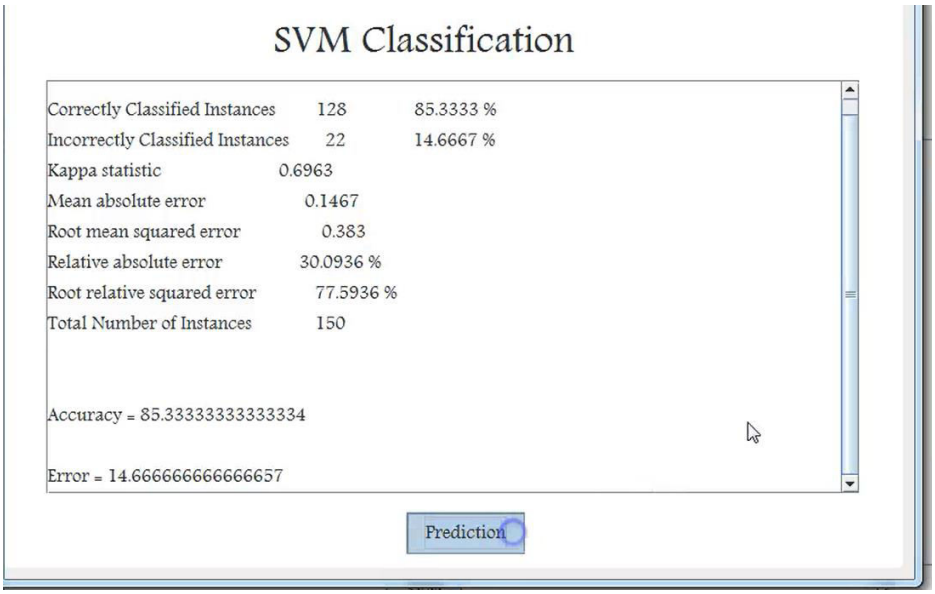
Load Dataset For Fraud Insurance

Clustered Data

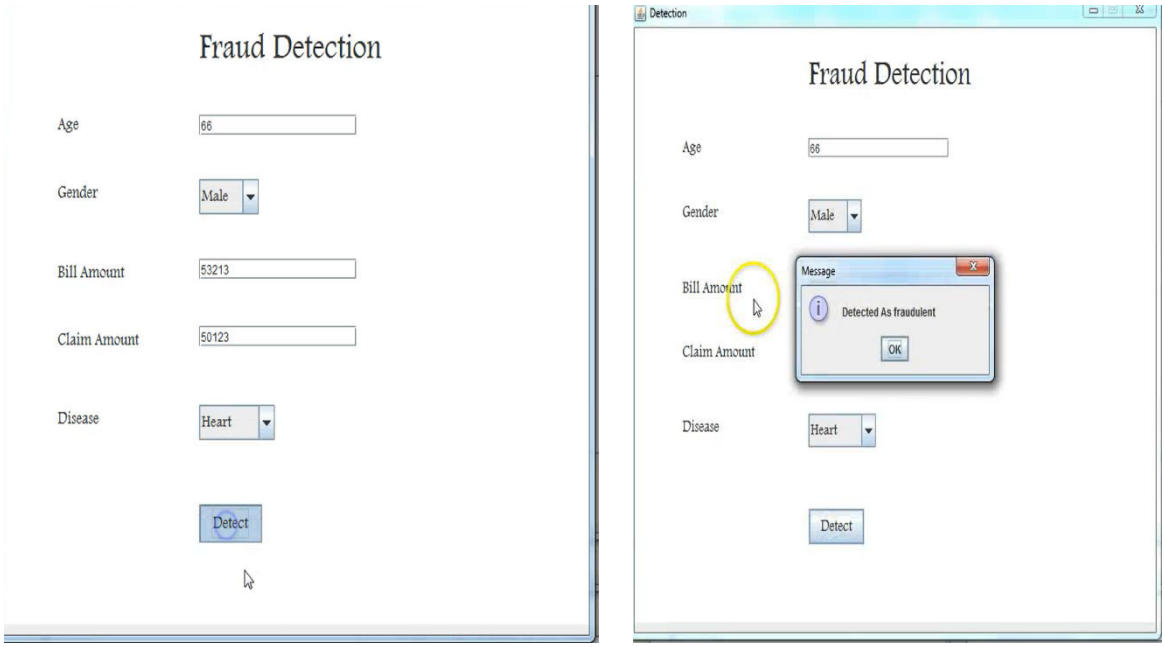
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |



Classification With SVM



Fraudulent Detection

V. CONCLUSION

Although evolving blockchain technology is expected to affect technological advancements in future, its capabilities seem especially appropriate for the pharmaceutical and healthcare industries and their complex data-sharing requirements. The findings and results shows that, the use of blockchain in storing health information can be effectively secured by having data over multiple machines which are supervised and authorized by distributed community in preference to centralized approach. This method provides a way for everyone in the party to view and verify data that is added and modified. Moreover, there is a record of each and transactions and modifications done within the network. The performance of middleware to parse and transform medical health data is fast and there is not much observable delay to load that processed data into blockchain

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106037 |

REFERENCES

1. Ali, M., Ahmed, S., Hossain, M.I., Alim Al Islam, A.B.M. and Noor, J., 2023. Electronic Health Record's Security and Access Control Using Blockchain and IPFS. In Proceedings of Seventh International Congress on Information and Communication Technology (pp. 493-505). Springer, Singapore.
2. Gupta, S., Sharma, H.K. and Kapoor, M., 2023. Introduction to Blockchain and Its Application in Smart Healthcare System. In Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT) (pp. 55-65). Springer, Cham.
3. Triyono, G. and Ginting, D., 2022. Comparative Analysis Performance of Na¨ive Bayes and K-NN Using Confusion Matrix and AUC To Predict Insurance Fraud.JURNAL MEDIA INFORMATIKA BUDIDARMA, 6(4), pp.2293-2300.
4. Kapadiya, K., Patel, U., Gupta, R., Alshehri, M.D., Tanwar, S., Sharma, G. and Bokoro, P.N., 2022. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. IEEE Access, 10, pp.79606-79627.
5. S. Vyas and S. Serasiya, "Fraud Detection in Insurance Claim System: A Review," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 922-927, doi: 10.1109/ICAIS53314.2022.9742984.
6. Hiererra, S.E., Toyib, R., Djajasinga, N.D., El Hasan, S.S., Haryadi, R.N. and Muhammad, R.N., Blockchain technology for Fraud Detection and Risk Prevention in Insurance Industry.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details