Blockchain Based Healthcare Insurance Fraud Detection

Ms. Pratiksha Pansare
Department Of Computer Eng.
Sharadchandra Pawar College
Of Engineering. Dumberwadi
Otur, Pune,India

Prof.Monika Rokade
Department Of Computer Eng.
Sharadchandra Pawar College
Of Engineering Dumberwadi
Otur, Pune,India

Prof. Sunil Khatal
HOD,Department Of Computer Eng.
Sharadchandra Pawar College
Of Enginering Dumberwadi
Otur, Pune,India

ABSTRACT: With the rapid growth of medical costs, the control of medical expenses has been be coming 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 in surance industry is a collection of service companies that provide protection services to customers with agreements and agreements from several parties involved. The conven tional 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 technol ogy 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 iden tify fraud of medical insurance based on consortium blockchain and machine learning, which can recognize suspicious medical records automatically to ensure valid implemen tation 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

Health insurance (HI) is a contract between the insurance provider and insurance subscriber in which the provider compensates the insurance subscriber's healthcare ex penses. Health insurance has become an essential part of people's lives as the number of health issues increases. Healthcare emergencies can be troublesome for people who can't afford huge expenses. Health insurance helps people cover healthcare services expenses in case of a medical emergency and provides financial backup against indebtedness risk. 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. To detect health insurance fraud, a blockchain and AI-based secure and intelligent system is proposed .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. The framework to identify fraud of medical insurance based on consortium blockchain and machine learning. To recognize suspicious medical records automatically to ensure valid Implementation on single-disease payment and lighten the work of medical insurance auditor

Consists of twelve chapters which gives step by step implementation of system "blockchain based healthcare insurance fraud detection". The covers basic introduction about the system. It also states the objectives and motivation for the system.

It includes literature review through tech nologies which earlier researchers have stated. The contains the requirement analysis for the system such as software needed and hardware needed for the project. The chapter emphasis on design of system. The system architecture, DFD diagrams and UML diagrams are discussed in the chapter. The discusses about implementation and methodology about the system. The discusses Partial results and Testing strategy.

I. LITERATURE SURVEY

According to [1] a 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.

According to [2] an blockchain technology has been into existence since 1991. A group of re searchers 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 breakthrough, 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.

According to [3] an fraud allegedly started when customer submits a policy issuance for the el derly 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 ad ditional 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.

According to [4] an 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 insur ance 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.

According to [5] 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 intro ducing a blockchain-based framework for enabling secure transactions and data ex change among various interacting agents in the insurance network.

According to [6] The insurance industry is a collection of service companies that provide protec tion services to customers with agreements and agreements from several parties involved. The conventional mechanism of the insurance claim process has the po tential 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.

According to [7] The blockchain's basic technology, the consensus algorithm, determines which nodes have the right to record transactions and enables them to swiftly agree on the information included in a block. This ensures the consistency and security of the data while also improving the blockchain's computational efficiency.A consensus mechanism is a protocol that brings all nodes of a distributed blockchain network into agreement on a single data set. They act as the verification standards through which each blockchain transaction gets approved. In the blockchain, a consensus mechanism is a system that validates a transaction and marks it as authentic.

According to [8] AI in insurance fraud detection uses advanced algorithms and machine learning technologies to excel at analyzing extensive datasets, including policyholder details, insurance claims, and historical trends. Having AI bots in insurance processes streamlines data collection, extraction, and analysis, enhancing the speed and accuracy of identifying suspicious activities associated with insurance fraud. Let's explore in detail how AI in insurance fraud detection helps insurers. Identifying and halting insurance claim fraud quickly and efficiently is a top priority for insurers.

II. OVERVIEW OF BLOCKCHAIN

Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. Blockchain is an invention that was initially designed for the digital currency Bit coin as it lets digital information to be distributed and secures it. However, the technology world has now found it useful in far more applications than this.To describe simply, the Blockchain is a distributed ledger of similar information records called blocks. This ledger is continually growing, and all the blocks are linked by cryptography[9]. The information that is held by a Blockchain is a shared and continually updated database. One of the strong positives of the Blockchain that makes it so secure is that this database is not stored or centralised in one

single location. It is hosted by millions of computers on the chain so there are several copies of the ledger and consequently, it will take a tremendous amount of computing power to hack into the chain and corrupt the records. In theory the amount of computing power needed to perform a hack can be devised but practically this is impossible.[8]
The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority.

Fraud detection
Fraud detection is a process that detects and prevents fraudsters from obtaining money or property through false means. It is a set of activities undertaken to detect and block the attempt of fraudsters from obtaining money or property fraudulently. Fraud detection is prevalent across banking, insurance, medical, government, and public sectors, as well as in law enforcement agencies. Fraudulent activities include money laundering, cyber attacks, fraudulent banking claims, forged bank checks, identity theft, and many such illegal practices. As a result, organizations implement modern fraud detection and prevention technologies and risk management strategies to combat growing fraudulent transactions across diverse platforms. These techniques apply adaptive and predictive analytics machine learning) to create a fraud risk score along with real-time monitoring of fraudulent events. This allows continuous monitoring of transactions and crimes in real-time. It also helps decipher new and sophisticated preventive measures via automation.

Types of Fraud Detection
This Techniques in Computers Fraud detection generally involves data analysis-based techniques. These techniques are broadly categorized as statistical data analysis techniques and artificial intelligence or AI-based techniques.
1. Statistical parameter calculation: Statistical parameter calculation refers to the calculation of various statistical parameters such as averages, quantiles, performance metrics, and probability distributions for fraud-related data collected during the data capturing process.
2. Regression analysis: Regression analysis allows you to examine the relationship between two or more variables of interest. It also estimates the relationship between independent and dependent variables. This helps understand and identify relationships between several fraud variables, which further helps in predicting future fraudulent activities. These predictions are based on the usage patterns of fraud variables in a potentially fraudulent use case.
3. Probability distributions and models: In this technique, models and probability distributions of various business fraudulent activities are mapped, either in terms of different parameters or probability distributions.
4. Data matching : Data matching is used to compare two sets of collected data (fraud data). The process can be carried out either based on algorithms or programmed loops. In addition, data matching is used to remove duplicate records and identify links between two data sets for marketing, security, or other purposes.

III. Proposed 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

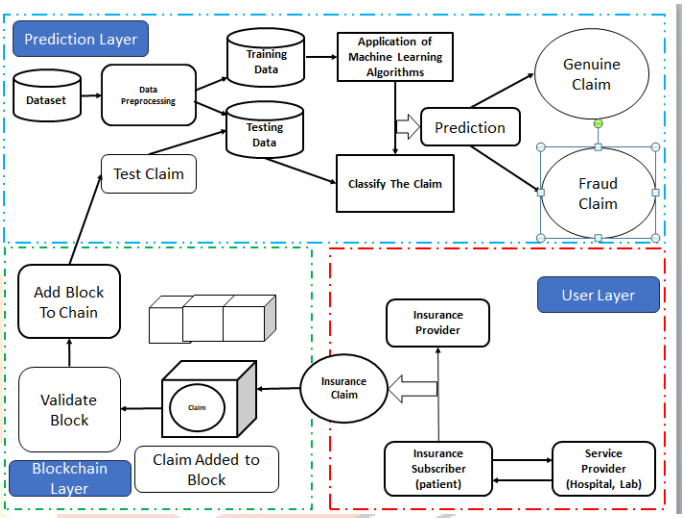

Figure 1: Proposed System Architecture

The system is designed with three layers.
1) User Layer:
The layer includes the insurance subscriber i.e., Patient. Patient gets the service from service providers such as labs, hospitals.The subscriber claims the service charges to insurance provider.

2) Block Chain Layer:
The insurance claim is same as smart contarct. The claim is added to block.The block is validated .The block is added to chain.

3) Prediction Layer:
The dataset is preprocessed and trained.
The claim is tested with trained data using the machine learning algorithm. The claim is classified and prediction is done whether the claim is fraud or genuine.

IV. System Implementation

1. User: The user or patient registers for insurance.The user creates the profile.
2. Blockchain: The claim is added to block. and 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.
4. 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.

5. 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.

V. 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

VI. CONCLUSION

This Study evolving blockchain technology is expected to affect technological ad vancements 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. More over, there is a record of each and transactions and modifications done within the network.

VII. 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 Com munication 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¨ıve 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 Preven tion in Insurance Industry. Y. Guo and C. Liang, ''Blockchain application and outlook in the banking 802 industry,'' Financial Innov., vol. 2, no. 1, pp. 1–12, 2016. 803

[7] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, ''A review on consensus 799 algorithm of blockchain,'' in Proc. IEEE Int. Conf. Syst., Man, Cybern. 800 (SMC), Oct. 2017, pp. 2567–2572

[8] Y. Guo and C. Liang, ''Blockchain application and outlook in the banking 802 industry,'' Financial Innov., vol. 2, no. 1, pp. 1–12, 2016

[9] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, ''Blockchain technology 804 and its relationships to sustainable supply chain management,'' Int. J. Prod. 805 Res., vol. 57, no. 7, pp. 2117–2135, 2019.

[10] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, ''Internet of Things, 807 blockchain and shared economy applications,'' Proc. Comput. Sci., vol. 98, 808 pp. 461–466, Sep. 2016.

[11] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, ‘‘A lightweight blockchain- 810 based iot identity management approach,’’ Future Internet, vol. 13, no. 2, 811 p. 24, 2021

[12] W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: 813 Facilitating the transition to patient-driven interoperability,’’ Comput. 814 Struct. Biotechnol. J., vol. 16, pp. 224–230, Jan. 2018.

[13] P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, ‘‘Managing lifelong learn- 816 ing records through blockchain,’’ Res. Pract. Technol. Enhanced Learn., 817 vol. 14, no. 1, pp. 1–19, 2019.

[14] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decen- 819 tralized Bus. Rev., p. 21260, Oct. 2008.

[15] D. R. Garrison, E-Learning in the 21st Century: A Community of Inquiry 821 Framework for Research and Practice. Evanston, IL, USA: Routledge, 822 2016.

[16] A. Grech and A. F. Camilleri, Blockchain in Education. Luxembourg, U.K.: 824 Publications Office of the European Union, 2017