International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**6**, pp.**08-14**, June **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

A Hybrid Approach to Health Insurance Fraud Detection Using Machine Learning and Blockchain Smart Contracts

Shilpa Kottapally[1]

[1]Sr. Software Development Engineer, Adjudication - Rxclaim developement Application, CVS Health, 2100 E lake cook road , Buffalo grove Illinois 60047, USA

Corresponding Author: ✉

Received: 20/Apr/2025; **Accepted**: 22/May/2025; **Published**: 30/Jun/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i6.814

Abstract: Since fraudulent activities account for an projected 3- 10% of total healthcare expenses, detecting fraud in healthcare systems is vital. Developed and underdeveloped nations alike are not immune to healthcare fraud. The criminals' goal was to take advantage of the shortcomings of the healthcare system as it stands. Unfortunately, fraud often prevents those who should be able to benefit from universal health coverage, such as individuals with health insurance, from actually receiving it. The purpose of this research was to compile a comprehensive literature review on the topic of health insurance claim fraud detection using ML-techniques. Further, we suggest preventing and detecting healthcare fraud, particularly in claims processing, by utilizing blockchain technology and ML-strategies. In order to sort the initial claims dataset, a decision-tree classification technique is used. In order to identify and stop healthcare fraud, the extracted knowledge is put into an Ethereum blockchain smart contract. Furthermore, our objective is to examine the information gathered from the literature over the last twenty years in order to shed light on topics such as research prospects and obstacles. Several obstacles stand in the way of machine learning's ability to detect healthcare claims fraud. Some of these issues include data inconsistency, privacy worries, a lack of standardized and integrated data, and an insufficient amount of labelled fraudulent cases to train algorithms on. Results from the comparing experiments reveal that the top tool obtains a sensitivity level of 99.09% and a classification accuracy of 98.96%. By using the suggested system, the blockchain smart contract can now detect fraud with a 98.96% accuracy rate.

Keywords: Machine Learning, Blockchain, fraud detection, healthcare claims, AI, insurance claims

1. Introduction

Healthcare claims including fraud, waste, and abuse (FWA) endanger the financial well-being and health of beneficiaries while costing insurers, taxpayers, and the insured billions of dollars. There is a greater opportunity for and danger of fraud due to the expanding complexity of the healthcare system, increasing expenses, and the large number of people enrolling in both public and private healthcare programs [1]. With a 9.7 percent increase from 2020, healthcare expenditure in the United States reached over 4.1 trillion USD in 2021, or 19.7 percent of GDP. [2]. Healthcare claims data is notoriously complex, making fraud detection analysis very difficult. There is a lack of standardization and integration, and the data is often large in size and dimensionality, as well as multi-modal, heterogeneous, and non-stationar. Figure 1 illustrates these difficulties. There are already a lot of problems with using machine learning (ML) models to detect fraudulent activity, and the lack of ground-truth labels for fraud just makes things worse [3].

There is a great chance to improve fraud detection systems with data analytics, thanks to recent advances in data mining and ML approaches, better means for collecting healthcare claims data, and the availability of data repositories. Within the framework of current research, this article investigates the feasibility of using ML to the problem of health insurance fraud detection. We have summarized the existing literature on the subject, addressed the difficulties in detecting this type of fraud, and offered suggestions for further research into healthcare claims fraud detection as our primary contributions [4]. Our analysis of 137 studies published over the last 20 years on the topic of machine learning for healthcare claims fraud detection yielded these findings.

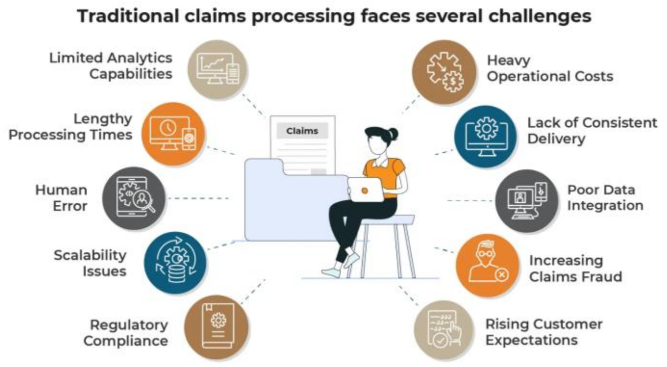


Fig. 1. The challenges in claims processing

In 2008, a mysterious individual or group of individuals known only as Satoshi Nakamoto invented blockchain technology (BC). A long-term fix for the double expenditure issue, it was instituted. Many other industries have begun to adopt blockchain technology after its initial successful implementation in the financial sector. These include healthcare, education, engineering, the IoT, and many more. Swan [5] idealized this extension. Blockchain technology is utilized in several fields to provide security, efficiency, privacy, immutability, accountability, ownership, easy auditability, etc., even though cryptocurrencies are not allowed to be used. As an example, BC technology can be utilized in the health insurance industry to permanently document healthcare treatments, paid claims, and other data pertaining to claims [6]. For instance, in this case, BC does not mandate efficient data security and management for bitcoin transfers or management.

Beneficiaries of high-quality healthcare services, particularly those with health insurance, are particularly vulnerable to healthcare fraud, which is a global problem that impacts both wealthy and developing countries [7]. Insurance companies' operational expenses and premiums paid by policyholders are both inflated due to the massive sums of money lost to fraud on a global scale.

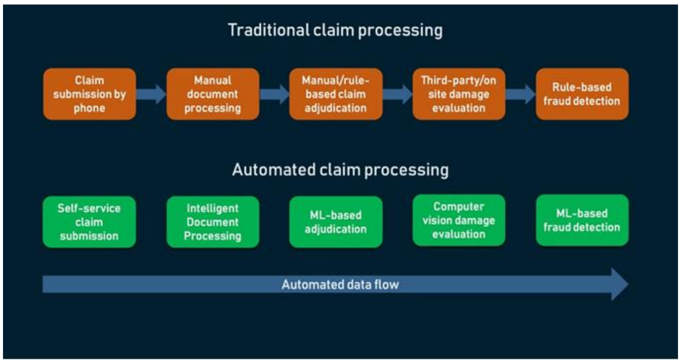

Traditional claim processing
Claim submission by phone
Manual document processing
Manual/rule-based claim adjudication
Third-party/on site damage evaluation
Rule-based fraud detection
Automated claim processing
Self-service claim submission
Intelligent Document Processing
ML-based adjudication
Computer vision damage evaluation
ML-based fraud detection
Automated data flow

Fig.2. Automated Process comparison with tradition process in claims settlement

There are serious concerns about the long-term financial viability of Ghana's National Health Insurance Scheme. Among these dangers is the prevalence of dishonest and fraudulent behavior throughout the claims processing cycle. Because of this, achieving Universal Health Coverage (UHC)—as outlined by the WHO and the UN Sustainable Development Goal 3—has become increasingly challenging for the country's citizens and residents [8]. As a result, this study suggests a method for detecting fraud in a blockchain claims processing system by making use of the smart contract's machine learning expertise. Preventing fraudulent operations by hostile and dissatisfied organizations inside the NHIS claims processing lifecycle is the primary benefit of this study. It will also shield the insurance program from monetary harm caused by exploiting claims processing lifecycle inefficiencies [9].

Only a small number of studies have examined the potential uses of Blockchain Technology in the insurance industry, with most of these studies focusing on Blockchain 3.0 [10]. As a result, this study provides an explanation for why and how modern insurance sub-business operations might benefit from Blockchain Technology. This narrows the focus of the study to the identification of fraud in claims processing and adds to the efforts to expand Blockchain 3.0 to incorporate the insurance industries. Once again, authors of [11] provide a blockchain system that operates in the cloud. This system is designed to store claims data efficiently, process claims rapidly and reimburse healthcare providers. We are confident that their system can be improved when the smart contract is enabled with data-driven decision-making capabilities, but until then, it guarantees transparent interactions among the primary parties. As a result, this work addresses a critical need by enabling the blockchain smart contract to make decisions using the extracted Decision Tree classification rules. The smart contract can use real-time data to identify instances of health insurance claim fraud [12]. We have already established that fraud has infected African national health insurance schemes, robbing them of resources that may have gone toward achieving universal health coverage. Thus, an effective strategy to combat healthcare fraud is required. This work's prototype uses health insurance domain-specific data and advanced Decision Tree classification algorithms to identify and prevent fraud in the blockchain's smart contract.

The core of our offering is an innovative approach for detecting and preventing fraud that leverages blockchain technology and machine learning algorithms. We offer a flexible framework that can be easily updated to incorporate new data as it becomes available, and a machine learning method that can transform domain-specific data into knowledge is also available. This study's findings extend Swan's [13] vision of Blockchain 3.0 to encompass the insurance industry. Improvements in privacy, authenticity, integrity, and non-repudiation are all brought about by Blockchain technology. We integrate the framework into the system that processes health insurance claims and use the retrieved machine learning decision rules. Due to the fact that healthcare fraud is a global issue that causes millions of dollars in lost revenue, the health insurance case was examined [14].

Following is the structure of this work. The second section delves into the relevant literature, while the third introduces the ideas and early definitions of blockchain and ML. The procedures used to accomplish the goals and the experimental design are detailed in Section 4. In Section 4, we cover the findings and analysis of the machine learning experiments that went into building the Blockchain fraud detection system. The study concludes in Section 5, which discusses its breadth and potential opportunities.

2. Related Works

In what follows, we'll take a look at the current landscape of healthcare claim automation R&D, touching on key technologies, processes, and the impact they have on efficiency and accuracy. Claims processing workflows can be optimized with the use of AI, ML, robotic process automation (RPA), and blockchain technology, according to various research.

2.1. AI and ML in Claims Processing

The implementation of AI and ML has greatly improved the accuracy and efficiency of claims processing. Finding trends in healthcare claims data can aid in early fraud identification and processing error reduction, according to research by [15]. AI-driven solutions can also assist with this. To aid in decision-making, AI-powered algorithms are beginning to analyze trends in past claims, predict abnormal activity, and organize claim information based on measured patterns. The requirement for human verification was eradicated in 92% of cases when a model based on deep learning was used to automate claim approvals [16]. Furthermore, there has been research into enhancing claim adjudication information procedures through the application of reinforcement learning techniques [17]. The healthcare industry and health insurance firms both benefit from these developments since they increase efficiency while decreasing operational expenses. Nevertheless, there are a number of challenges that necessitate additional development, including data privacy and biased AI models.

2.2. RPA for Claims Processing

In the healthcare claims processing industry, RPA has demonstrated to be an effective tool for automating mundane but necessary processes, such as data entry, claims validation, and payment processing. According to a recent study conducted by [18], RPA based systems have commoditized the information in the systems and removed some of the tedious tasks from them. This has enhanced and accelerated the claim processing time because they no longer require constant human participation.

When we integrate AI models with RPA, we can increase processing efficiency by more than 40%, according to a related study in [19]. Using bot-based automation, insurance companies may process tickets in bulk without compromising accuracy. Still, problems with system compatibility mean that RPA-driven automation frameworks can't always communicate with older healthcare systems (as mentioned in [20]). Furthermore, despite the benefits, initial setup costs and employees resisting automation still hinder widespread adoption.

2.3. Blockchain for Secure and Transparent Claims Processing

Blockchain for Healthcare Claims Processing: A Step Towards Data Science Claims Settlement Process Utilizing Blockchain Technology. We promise real-time verification and 0% processing delays in our blockchain-based smart contracts, which automate and manage claim settlements with third parties. Research evaluates our claims and intentions in this regard. Researchers suggest a blockchain-based decentralized claims processing system in [21] that would allow for the secure sharing of encrypted patient and claim data across all parties involved, so doing away with the need for duplicate verifications. Additionally, blockchain protects data and claims from illegal alterations due to its immutable nature. On the other hand, scalability and regulatory concerns have emerged as roadblocks to widespread blockchain use in healthcare, as highlighted in [22]. One area of focus for industry-wide standardization efforts is FBL's high computing costs and quantity of available data.

2.4. NLP for Claims Adjudication

Automating claims adjudication from unstructured medical records into structured information is one of the main functions of NLP. There are no major coding mistakes when using NLP algorithms to automatically categorize claims according to medical diagnoses and procedures [23]. The NLP Underwriting: A different study, the one cited in [18], sheds light on chatbots powered by NLP that manage queries connected to claims, providing clients with great convenience and protecting them from administrative tasks. On top of that, a small number of articles [24] brought up NLP models that use a machine learning method to identify discrepancies in patient records and prevent false claims. On the other hand, research in [25] shows that current NLP models aren't always reproducible when applied to medical documentation because of linguistic difficulties; this is because these models depend on vast training datasets to achieve strong prediction performance.

Despite the fact that these innovations are substantially bettering the processing of healthcare claims, researchers have also found obstacles such as problems with integration, data privacy, and interoperability. Standardized data exchange protocols and well-established cybersecurity standards could be useful in addressing these challenges, according to the authors [26]. There are still some obstacles to overcome when implementing ML for claims processing, even with current developments. Difficulties with data privacy, model interpretability, and regulatory compliance are some of the obstacles to broad adoption. Stakeholder trust must be preserved by making sure ML-driven fraud detection systems are fair and transparent. Good data governance frameworks and AI methods that are easy to understand are necessary to overcome these obstacles.

3. Proposed Methodology

In order to get the classification results, the ML classification task was run and compared to the benchmark. This took place prior to the smart contract's decision rules being extracted.

Description of dataset and preprocessing

The classification rules module's domain knowledge is generated in this study using an original dataset that is specific to the domain. The data mining project made use of a dataset of 1323 instances and 7 attributes (label inclusive). Of the seven characteristics, six were nominal and one was numerical.

Following screening and payment to service providers, the National Health Insurance Scheme provided the data. The medicine 1–5 system is based on the current manual claims filing and processing technique, which limits service providers to administering no more than five drugs. Due to its initial submission to the scheme by the service providers, subsequent auditing by the fulfilling and vetting officials, and the appropriate payment of genuine amounts, the dataset is considered an absolute depiction of reality.

The data was preprocessed to guarantee that the scheme and patients' privacy were fully protected. With that in mind, in order to guarantee k-Anonymity, all identifiers were eliminated. In accordance with [27], the NHIS-identified diseases and drugs were used to preprocess the data. As an example, several drugs are known to cure malaria and infections, such as Artemether + Lumefantrine and Amoxicillin, respectively. Hence, all the medications were altered for their use. The most commonly prescribed medications are pain relievers, infection treatments, and malaria medications, in that order, according to preliminary data analysis.

Blockchain based ML development environment

The data mining simulations in this paper were executed using the exceptional computational and graphical capabilities of WEKA version 3.6. To prevent data mining results from being statistically skewed, the simulation used 10-Fold Cross Validation unless otherwise stated. It is essential to utilize the classifiers with their default configuration files to ensure reproducibility in machine learning research. Once again, the blockchain fraud detection and prevention system was developed using the Remix IDE. This smart contract was tested with MetaMask and JavaScript VM. In figure 3, we can see the suggested model.

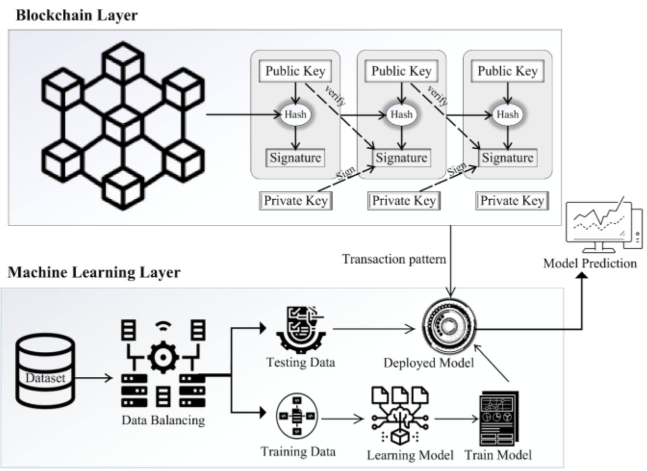


Fig. 3

Decision Tree Classification Algorithm

Many different versions of the Decision-Tree (DT) method are used in machine learning. We employed J48, ADTree, BFTree, and REPTree, which stands for Reduced Error Pruning. A network of nodes with logical connections is the building block of the Decision Tree classification method. Each terminal node represents a categorization, while the nodes themselves represent options from a set of possible values. In addition to being highly good predictors, decision trees provide an explicit concept description of a dataset. The states that decision tree algorithms begin at the root node, do attribute testing, and then classify data along the branch of the tree that corresponds to the attribute value. The process continues until the next terminal node is reached. The splitting approach divides each node in half and then uses the result to determine the impurity level. Two of the most used criteria for decision tree splitting are the Gini Index and the Information Gain.

Performance metrices

The suggested blockchain-based decision tree is tested in a simulated environment running on an Intel i5 processor, 128 GB of RAM, Windows 10, and Python 3.4. The model's performance is assessed using recall, accuracy, f1-score, and precision, which are determined by the following equations: (1) to (4).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

$$Recall = \frac{TP}{TP+FN} \tag{2}$$

$$F1 - Score = \frac{2TP}{2TP+FP+FN} \tag{3}$$

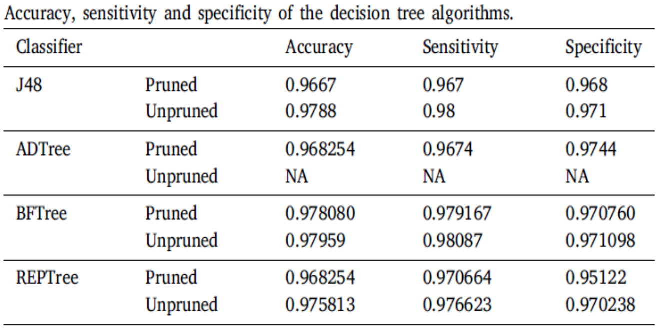
$$Precision = \frac{TP}{TP+FP} \tag{4}$$

Where TP denotes True Positive, FN represents False Negative, FP demonstrates False Positive, and TN indicates True Negative.

4. Results and Discussions

This section details the planned integrations into the blockchain-based fraud detection and prevention system, as well as the outcomes of the machine learning experiments and model performances. We showcase the abstracted system and the criteria for classification that were extracted.

Table 1. Performance Analysis of the proposed model



Accuracy, sensitivity and specificity of the decision tree algorithms.

Classifier		Accuracy	Sensitivity	Specificity
J48	Pruned	0.9667	0.967	0.968
	Unpruned	0.9788	0.98	0.971
ADTree	Pruned	0.968254	0.9674	0.9744
	Unpruned	NA	NA	NA
BFTree	Pruned	0.978080	0.979167	0.970760
	Unpruned	0.97959	0.98087	0.971098
REPTree	Pruned	0.968254	0.970664	0.95122
	Unpruned	0.975813	0.976623	0.970238

Based on the results of Eqs. (1)–(4), Table 1 displays the specificity, sensitivity, F1, and accuracy of both the pruned and unpruned DT models. Results for accuracy(0.9667), sensitivity(0.967), and specificity (0.968) were all attained by the trimmed J48 DT. In a similar vein, the unpruned J48 DT achieved sensitivity values of 0.97, specificity of 0.97, and accuracy of 0.98. Once more, the accuracy, sensitivity, and specificity values were 0.97, 0.96, and 0.97 for the pruned ADTree, respectively. The opposite was true with ADTree. The accuracy, sensitivity, and specificity values for pruned and unpruned BFTree were 0.98 and 0.97, respectively. Both the pruned and unpruned versions of REPTree achieved respectable results in terms of accuracy (0.96 and 0.97, respectively), sensitivity (0.97 and 0.97), and specificity (0.95 and 0.97, respectively). Table 4 and Figure 4 show that the sensitivity and accuracy were greater in the unpruned BFTree model. In contrast, the pruned ADTree achieved the greatest specificity.

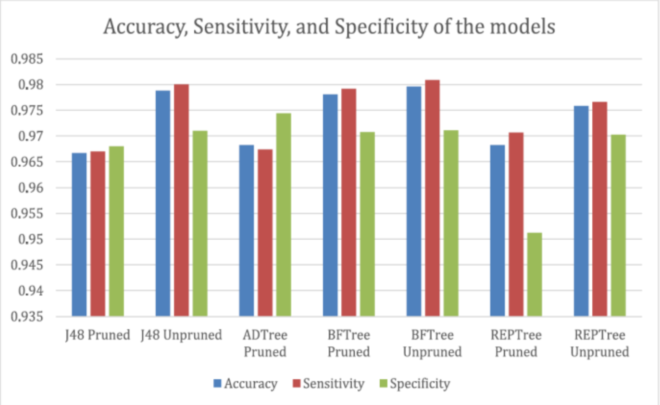


Fig.4. Performance comparison of the proposed models

In order to identify and stop healthcare fraud, this study used decision tree classification methods and blockchain technology. Blockchain technology completely eliminates the need to rely on the faith of healthcare providers (claimants) by adding a layer of decentralization, accountability, auditability, etc. to current centralized claims processing systems. Additionally, the blockchain smart contract is able to detect and prevent sense fraud using domain specific data thanks to the decision tree categorization rules, which enable data-driven decision-making. All things considered, this study adds to the growing body of evidence that blockchain 3.0 [1,60] is beginning to encompass in the insurance industry. This study offers a fresh method for preventing healthcare fraud by combining decision tree classification rules with the blockchain smart contract, which is in contrast to previous attempts and proposals to reduce healthcare fraud. The integration of fraud detection and prevention smart contracts represents a sea change in healthcare fraud prevention systems, ushering in a new era of highly efficient claims processing for insurance schemes across the world, including those in Africa.

Data management and predictive models rely on reliability, and as shown in Table 1, the unpruned BFTree produced the best results with a specificity of 99.09% and an accuracy of 98.96%. On the other hand, a specificity of 98.44% was reached using the ADTree classifier. What this means is that the extracted and applied BFTree classification rules may detect fraudulent claims with an accuracy of over 99% once they are adopted. All of the tested DTs had excellent outcomes for RMSE, MAE, and Kappa statistics.

There are eight distinct parts to the system's high-level abstraction: the Machine Learning Algorithm, the Decision-Making Module, the Data Entry Console, the Data Collection Module, the Blockchain Ledger, WorldState, and the Rejection Logs. In the first part, you can utilize whatever ML algorithm you like. Whitebox computing methods, such as Decision Tree [63,64], are what we recommend instead. The second component involves creating or extracting knowledge from the machine learning experiments, which is subsequently used in the smart contract that is built on the blockchain.

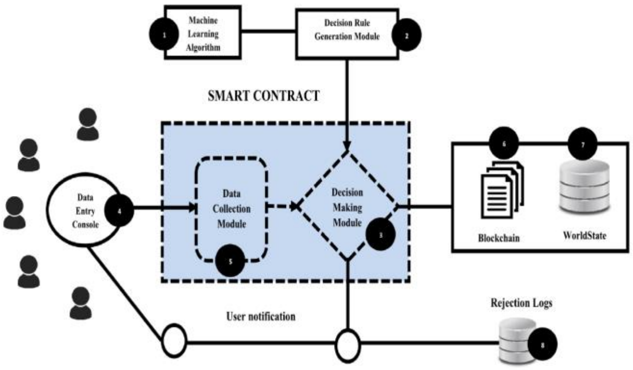


Fig.5. Blockchain based prevention system.

Since steps 1 and 2 are executed externally to the Ethereum smart contract, impartial testing and code are required. African health insurance programs now have a more efficient and cost-effective solution thanks to the suggested system's successful deployment after domain-specific data was used. It can, however, be rewritten to fit other schemes all around the globe and in other areas. Figure 5 will display the blockchain-based process.

5. Conclusions and Future Works

The global community is aware of the consequences of healthcare fraud, but the problem persists. The plethora of public studies and figures provide indisputable proof. It is impossible to exaggerate the revolutionary potential of blockchain technology to provide contemporary solutions. Due to the massive annual losses caused by fraud, the most critical issue is the immediate requirement for a novel approach to the processing of health insurance claims. Using domain data and machine learning to predict the probability of fraudulent claims, this study develops and tests a blockchain-based system that suggests a new, secure, data-driven approach to processing and submitting health insurance claims. The proposed system was able to classify the claims data with an accuracy of approximately 98%, according to the machine learning trials. Classification errors of approximately 2% will apply to future claims in a similar vein. Adopting the proposed approach will have an impact on costs, but when weighed against the yearly amounts lost to fraud around the world, the advantages outweigh the costs. Claims processing will be more secure, efficient, and data integrity will be high after moving from the centralized system to the decentralized Blockchain-based system, and the fight against fraud will be much stronger as a result. Future work can explore integrating federated learning to enhance data privacy across institutions and improve model generalization. Additionally, leveraging advanced blockchain consensus mechanisms can ensure faster and more secure fraud validation in real time.

Data Availability
No

Conflict of interest
No

Funding source
No

Author's contribution
Concept design, methodology, results and analysis, simulations, writing and reviewing and experimental design is done by S K.

Acknowledgment
NA

References

[1] Kapadiya, K., Ramoliya, F., Gohil, K., Patel, U., Gupta, R., Tanwar, S., Rodrigues, J.J., Alqahtani, F. and Tolba, A., "*Blockchain-assisted healthcare insurance fraud detection framework using ensemble learning*". Computers and Electrical Engineering, *122*, pp.**109898, 2025.**

[2] Amponsah, A.A., Adekoya, A.F. and Weyori, B.A.,. "*A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology*". Decision Analytics Journal, *4*, pp.**100122, 2022.**

[3] Mohammed, M.A., Boujelben, M. and Abid, M., "*A novel approach for fraud detection in blockchain-based healthcare networks using machine learning*", Future Internet, Vol.**15**, Issue.**8**, pp.**250**, **2023**.

[4] Kaafarani, R., Ismail, L. and Zahwe, O., "*Automatic Recommender System of Development Platforms for Smart Contract–Based Health Care Insurance Fraud Detection Solutions: Taxonomy and Performance Evaluation*". Journal of Medical Internet Research, *26*, pp.**e50730, 2024.**

[5] Kaafarani, R., Ismail, L. and Zahwe, O. "*An adaptive decision-making approach for better selection of blockchain platform for health insurance frauds detection with smart contracts: development and performance evaluation*". Procedia Computer Science, *220*, pp.**470-477, 2023.**

[6] Zhang, G., Zhang, X., Bilal, M., Dou, W., Xu, X. and Rodrigues, J.J., "*Identifying fraud in medical insurance based on blockchain and deep learning*". Future Generation Computer Systems, *130*, pp.**140-154, 2022**.

[7] Aziz, R.M., Mahto, R., Goel, K., Das, A., Kumar, P. and Saxena, A., "*Modified genetic algorithm with deep learning for fraud transactions of ethereum smart contract*". Applied Sciences, Vol.**13**, Issue.**2**, pp.**697, 2023.**

[8] Selvamuthu, C.M., Lavaraju, B. and Sundaram, A., October. "*A Novel Approach of Streamlining Claims Processing and Fraud Prevention in Health Insurance through Blockchain Technology*". In *2024* 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC*)*, pp.**611-618, 2024.**

[9] Kapadiya, K., Patel, U., Gupta, R., Alshehri, M.D., Tanwar, S., Sharma, G. and Bokoro, P.N., "*Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects*". IEEE Access, *10*, pp.**79606-79627, 2022.**

[10] Raad, A., Ofoghi, R. and Mahdavi, G., "*Fraud detection in supplementary health insurance based on smart contract in blockchain network*". Journal of Mathematics and Modeling in Finance, pp.**33-56, 2024.**

[11] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T.T., Assam, M., Ghadi, Y.Y. and Mohamed, H.G., "*Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning*". Sensors, Vol.**23**, Issue.**18**, pp.**7740, 2023.**

[12] Elhence, A., Goyal, A., Chamola, V. and Sikdar, B., "*A blockchain and ML-based framework for fast and cost-effective health insurance industry operations*". IEEE Transactions on Computational Social Systems, Vol.**10**, Issue.**4**, pp.**1642-1653, 2022.**

[13] Pranto, T.H., Hasib, K.T.A.M., Rahman, T., Haque, A.B., Islam, A.N. and Rahman, R.M., "*Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach*". IEEE Access, *10*, pp.**87115-87134, 2022.**

[14] Chakraborty, A., Singh, G., Sirvastava, V. and Dhondiyal, S.A., November. "*Blockchain-Enhanced Adversarial Machine Learning for Fraud Detection and Claims Automation in the Insurance Sector*". In 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), pp.**80-86, 2024.**

[15] Diyasi, S., Ghosh, A. and Dey, D., "*Enhancing Blockchain Transaction Security: A Hybrid Machine Learning Approach for Fraud Detection*". International Journal on Smart & Sustainable Intelligent Computing, Vol.**2**, Issue.**1**, pp.**14-30, 2025.**

[16] Soner, S., Litoriya, R. and Pandey, P., "*Combining blockchain and machine learning in healthcare and health informatics: An exploratory study*." In Blockchain applications for healthcare informatics, pp.**117-135, 2022.**

[17] Jena, S.K., Kumar, B., Mohanty, B., Singhal, A. and Barik, R.C., "*An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry*". Decision Analytics Journal, *10*, pp.**100411, 2024.**

[18] Hisham, S., Makhtar, M. and Aziz, A.A., "*Anomaly detection in smart contracts based on optimal relevance hybrid features analysis in the Ethereum blockchain employing ensemble learning*". International Journal of Advanced Technology and Engineering Exploration, Vol.**10**, Issue.**109**, pp.**1552, 2023.**

[19] Mackey, T.K., Miyachi, K., Fung, D., Qian, S. and Short, J., "*Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework*". Journal of medical Internet research, Vol.**22**, Issue.**9**, pp.**e18623, 2020.**

[20] Banoth, Shobhan, and K. Madhavi. "*A Novel Deep Learning Framework for Credit Card Fraud Detection*." 13th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE, **2024**.

[21] Yallamelli, A.R.G., Ganesan, T., Devarajan, M.V., Mamidala, V., Yalla, R.M.K. and Sambas, A., "*AI and Blockchain in Predictive Healthcare: Transforming Insurance, Billing, and Security Using Smart Contracts and Cryptography*". Springer Natural Letters, Vol.**2024**, Issue.**3**, pp.**34-56, 2024.**

[22] Chidambaranathan, S. and Geetha, R., "*Deep learning enabled blockchain based electronic heathcare data attack detection for smart health systems*". Measurement: Sensors, *31*, pp.**100959**, **2024**.

[23] Anjaneyulu, Gudla, et al. "*A Hybrid Optimization Deep Learning Frame Work for Efficient Stock Market Forecasting*." International Conference on Advanced Computing Technologies (ICoACT). IEEE, **2025**.

[24] Dey, R., Roy, A., Akter, J., Mishra, A. and Sarkar, M., "*AI-driven machine learning for fraud detection and risk management in US healthcare billing and insurance*". Journal of Computer Science and Technology Studies, Vol.**7**, Issue.**1**, pp.**188-198, 2025.**

[25] Prabanand, S.C. and Thanabal, M.S., "*Advanced financial security system using smart contract in private ethereum consortium blockchain with hybrid optimization strategy*." Scientific Reports, Vol.**15**, Issue.**1**, pp.**6764, 2025.**

[26] Shanmughan, G.D., Silpa, S.K. and Jayamohan, S., February. "*Empowering fraud detection in medical insurance: Comparative study of deep learning models"*. In *AIP Conference Proceedings*, Vol.**3237**, No.**1**, pp.**060045, 2025.**

[27] Banoth, S. and Yadala, S., December. *"A Hybrid Deep Learning Framework for Stock Price Forecasting with Sentimental Analysis".* In *2024* 13th International Conference on System Modeling & Advancement in Research Trends (SMART), pp.**467-471**, **2024**.