International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Insurance Fraud Detection Using Novel Machine Learning Technique

M. Sathya[1,*], Dr. B. Balakumar[2]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: The ultimate focus of the insurance agency is the management of financial risks, since it includes a sizable amount of daily transactions. It is mandatory for the insurance industry to develop the capability of identifying the fraudulent activities with increased accuracy in order to minimize the excessive unwarranted loss due to claim leakage. Initially, many fraud detecting techniques has been introduced and it relies on the heuristics around fraud indicators, also on the checklist prepared about frauds. However, the above mentioned traditional techniques highly relies on the manual intervention. Therefore, for eliminating the above mentioned issues, the insurance companies are looking towards machine learning based fraud detection techniques. In this paper, initially a block chain technique is presented as a secure network by the insurance agencies to detect, store and share different customer informations. Then, a hybrid classifier called eRFSVM, which entails Random Forest (RF) and Support Vector Machine (SVM) algorithm is used for classifying the insurance frauds. Additionally, to analyse the working of the proposed work, it is implemented in Python software.

***Keywords*:** *Insurance Fraud, Block chain technique, RF classifier, SVM classifier, Hybrid ERFSVM classifier.*

1. Introduction

The insurance agencies are robbed of a considerable share of their expected gain owing to the issue of claim leakage. Fraudulent claims are an alarming and expensive problem for insurance firms, potentially resulting in the loss of billions of dollars in annual unwarranted costs for the sector. Exaggerating or fabricating the circumstances are common tactics used by insurance fraudsters to support their false claims. Earlier, the calculation of premium rates for policy approval, which guarantees reasonable levels of payoffs without jeopardising the financial stability of the company was generally left to mathematicians. Moreover, the conventional fraud detection techniques are erroneous, time-consuming, expensive and complex, since they are highly dependent on special investigation agencies and expert analysis. The Association of Certified Fraud Examiners (ACFE) defines fraud as an act of deceit or mistake committed by a person or an institution even after being perfectly aware about its negative consequences [1, 2]. There are several types of insurance frauds, among which the Healthcare frauds [3-5] and automobile frauds [6, 7] are more frequent in occurrence. Healthcare fraud occurs whenever a group of persons, or a person, or a business intentionally conceals or makes false claims about the extent of the medical treatment service or medical treatment provided in a way that leads to unlawful payments being made. About 18% of personal injury and 21% of bodily injury claiming full refund are underhanded and deceptive in nature. Automobile insurance fraud is the practice of deceiving an insurance provider by requesting financial assistance for vehicle theft or damage using fabricated credentials [8]. In order to counteract the enormous fraudulent pay-outs made by auto insurance companies, rates have been raised significantly, which a negative impact on the competitiveness and service quality has provided by insurance corporations. Therefore, devising a prompt and effective fraud detection solution is instrumental in prevention of unnecessary loss of money. The big datasets that are appropriate for detection of fraud came in to existence after the digitization of insurance and banking sector [9].

The world is moving towards complete digitization, and many organisations have recently started considering the integration of block chain technology into their operational workflows. Numerous sectors have recently invested time and resources learning about the potential of block chain and the impact of its adoption [10]. This technique was primarily introduced for Bitcoin applications to enable peer-to-peer transfer of electronic cash in the absence of a centralised trusted system and prevent the problem of double payment [11, 12]. The Blockchain 1.0 came in to existence in the year 2009 and the first generation technique featured hardcoded special-purpose protocols that concentrates chiefly on digital currency while also serving potentially dangerous public players. In 2014, the Blockchain 2.0 came in to existence

[1] *Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India.*
[2] *Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India.*
** Corresponding Author Email: 46msathya@gmail.com*

and it focusses on creative application of smart contracts in variety of fields. Hyperledger projects are the base of Blockchain 3.0 and it was introduced in the year 2017. The development of extensive amount of systems in the fields of finance, certification and logistics took place during the second generation [13, 14]. A blockchain based solution is proposed in this work for insurance agencies to ensure digital security and quicker processing. In case of the insurance industry, the Blockchain technique is a relatively newer approach and the several advantages of applying Blockchain technique in the field of insurance is given in Fig. 1.

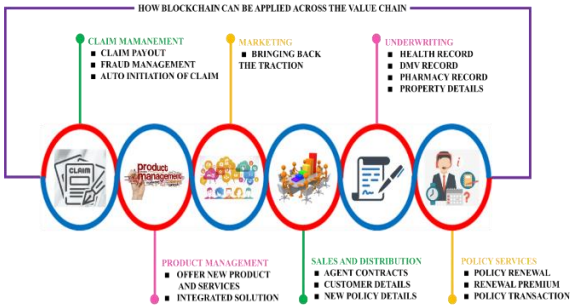

Fig. 1. Benefits of block chain in insurance sector

Blockchain has the ability to resolve some of the major issues troubling the insurance sector today, including effective fraud detection, product innovation and decreased operational expenses. Additionally, combining the Blockchain with a machine learning technology increases its effectiveness and intelligence. So, in order to classify the insurance frauds, the machine learning technique of SVM [15-17] is considered. The working of the SVM is further improved by integrating it with the RF algorithm [18].

For the insurance industry, an innovative Blockchain-based strategy is proposed to achieve the major goal of fraud detection and prevention. Furthermore, the Blockchain technique has the added benefits of cost savings, improved back-end efficiency, better assessment of risks, handling big data in addition to event triggered smart contracts. The remarkable learning ability of hybrid ERFSVM machine learning technique is capable of heightening the efficiency and smartness of the Blockchain approach.

2. Proposed System Description

The management of financial risks is the main focus of the insurance sector, since it involves a significant amount of daily financial transactions. As a result, the sector is constantly exposed to a high risk of invasions, fraudulent transactions and attacks. The insurance sector is also complicated in nature, with composite contracts involving numerous stakeholders that call for a lot of processing power. Therefore, with the aim of overcoming the challenges faced by the insurance sector a novel Blockchain based technique is developed by combining the learning capability of hybrid ERFSVM technique as seen in Fig. 2. The proposed hybrid machine learning technique obtained by the combination of RF and SVM, improves the efficiency and smartness of the Blockchain.

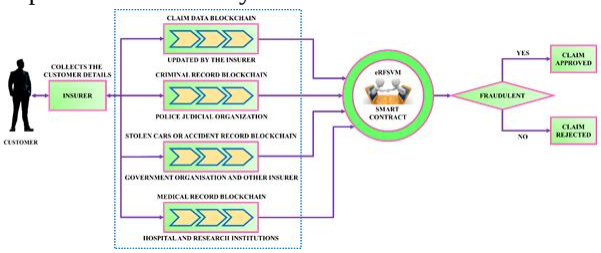

Fig. 2. Structure of the proposed blockchain based insurance fraud detection

If a customer claims for insurance, the details are initially gathered by the insurer and then the authenticity of the claim is validated using the blockchain technique. The claim data blockchain is updated by the insurer, while the criminal record blockchain is updated by the police and judiciary. The records about events such as accidents and theft are updated and maintained by the government organisation and other insurers. The health care records are obtained from hospitals and research institutions. The hybrid machine learning technique of ERFSVM is effective in determining whether the issued claim is genuine or fraudulent on the basis of analysing the information in various blockchains.

2.1. Blockchain technology

Blockchain is a shared, unchangeable digital ledger technology used to store the history of insurance. As the name indicates, a chain of blocks that reveals details, and every block joined together to form a chain by hashes of block that came before and after. The key component of Blockchain system include nodes, which keeps a local backup of the chain and is linked by end-to-end connection. Each block has a header, timestamp, ID for the preceding and following blocks and list of transaction. Generally, Blockchain (BC) is a decentralized technology that open up entirely new advanced technologies and economic models. Its decentralised nature aids in avoiding single point failure and heightening the security of the system. Data traction in conventional centralized method and decentralized Blockchain method is represented in Fig. 3. Moreover, the records stored in Blockchain are permanent and invariable in nature, thus guaranteeing the completeness and accuracy of the transaction history. Besides, it often integrates prior advancements like distributed consensus method, cryptographic hash, and digital signature.

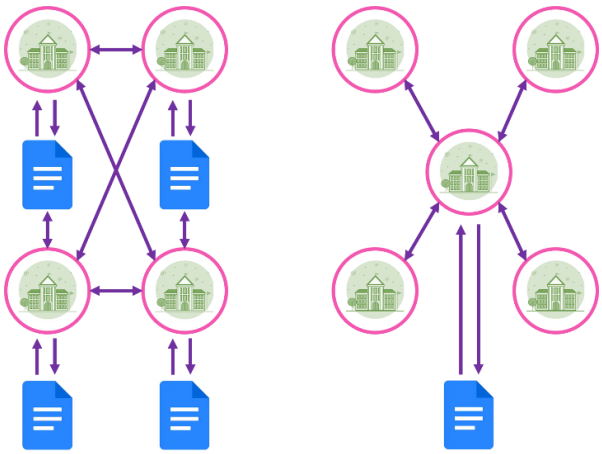

Fig. 3. Data transaction in conventional centralised method and decentralised blockchain method

Blockchain is a crucial digital framework that underpins programmes like bitcoin. The system improves the procedure for keeping track of transactions and assets in a cooperative network. Physical and virtual assets include things like titles, bonds, contracts, equities, money, deeds and almost every other sort of asserts may be safely stored and shared from peer to peer. Trust is enforced, and the confirmation is what makes this possible, which is performed by network consensus technique, cryptography, and smart code without the requirement of control mediators like banks and governments. Since data structures serve as the fundamental key component of current algorithms and nodes, in which nodes are meant to data store and data packets, in accordance with node communication methods. The transaction request is initially broadcast to the peer-to-peer network in Blockchain and then it is validated and verified. Then after the verification process is completed, it is subsequently included with other blocks in Blockchain as seen in Fig. 4.

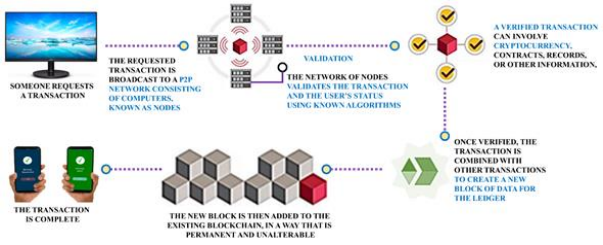

Fig. 4. Operation of a Blockchain

The features of block chain are listed below:

- **Security and Immutability:** Blockchain is an immutable technology that uses cryptographic operations to create a transparent and secure method of data processing and storage amongst Blockchain nodes. Transactions that are immutable are protected from unwanted changes made by fraudulent. Participants are capable of adding new transactions, but they are prohibited from deleting or amending prior ones, making it easier for every nodes to maintain record of all the past transactions.
- **Transparency:** All transactions are approved by their potential owners owing to the Blockchain rules of consensus, validation, and acceptance. Additionally, once a block is approved, smaller nodes transmit the block to every remaining nodes in the network due to the trustworthiness of involved participants.
- **Verifiability:** The transactions are handled by consensus mechanism and cryptography in such a way that both the outsiders and insiders are capable of verifying it. The participant approval of at least 51% is required for the transaction to be valid.
- **Authenticity:** The authenticity of the Blockchain is ensured with the application of smart contract. Additionally, every block in a Blockchain necessarily includes the digital signatures of the responder and creator in addition to the preceding and following hashed IDs.
- **Ownership and Accountability:** In case of Blockchain applications, the accountability and ownership control is ensured using originator endorsement, block connections and transaction immutability.

The benefits of block chain in insurance includes introduction of new insurance types, extends to the underserved, reduced costs, disintermediation, improved backend efficiency and smart contracts. Additionally, a secure decentralized transaction is assured with minimal counterparty risks and no overlapping issues.

2.2. Support Vector Machine (SVM)

Support Vector Machine is a supervised learning technique with corresponding machine learning algorithms which examine data for multi–variant classification and prediction. Similar to logistic regression, SVMs are a classification algorithmic rule. Despite of, the algorithms is most frequently used for classification issues. SVM model employs two distinct classifications. The fundamental model is linear, with greatest interval in feature space. It differs from the perceptron model due to longest time interval. A non-linear classifier can be obtain by using the SVM classifier with kernel tricks. The main approach of SVM technique is to optimize the interval, for solving convex quadratic programming and is also equal to issue of reducing the loss function. The training data set is given as,

$$\{x_k, y_k\} \in R^n \times \{-1,1\} \quad (1)$$

Where, the class labels and training samples are specified as y_k and x_k respectively. Based on function Φ, x is mapped in higher dimensional space and the decision function is given as,

$$f(x) = \langle w, \Phi(x) \rangle + b \quad (2)$$

The SVM classifier's optimization problem is given as,

$$min\frac{1}{2}||w||^2 + \sum_{i=1}^{m} C\xi_i \quad (3)$$

Subject to:

$$y_i f(x_i) \geq 1 - \xi_i \quad (4)$$

With variables α_i defined such that:

$$w = \sum_i^m \alpha_i y_i x_1 \quad (5)$$

The simplified problem is obtained by resolving the Lagrangian dual,

$$max_\alpha Q(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{m} \alpha_i\alpha_j y_i y_j \varphi(x_i)\varphi(x_j) \quad (6)$$

Subject to:

$$\sum_{i=1}^{m} \alpha_i y_i = 0 \quad (7)$$

$$\alpha_i \geq 0 \quad (8)$$

2.3. Random Forest (RF) Algorithm

Panel of decision trees are used by the Random Forest (RF) algorithm. The RF algorithm achieves high quality classification by integrating numerous straightforward classifiers. On the basis of the replies aggregate of numerous trees the final classification outcome is generated. In comparison with a single decision tree, the RF algorithm reduces the issue of over fitting and enhances classification accuracy. In general the RF algorithms combines the strategy of random subspace approach, bootstrap aggregation and bagging.

In the RF technique, just like in bagging, classifiers are trained independently at various subsets of training set, which solve issues of creating identical trees on same dataset. Therefore, the class of any object will be equivalent to the class that received majority of votes from the trees, assuming that each tree has single vote. When implementing RF method, defining the parameter values is crucial. The following are the RF algorithm's essential parameters: the total number of trees in forest, the total number of factors to take into account while determining the optimum split, tree's maximum depth, and splitting criterion. Splitting criteria is performed using the Gini impurity:

$$Gini_t = 1 - \sum_{j=1}^{y} P^2\,(Y_h) \quad (9)$$

Where $P(Y_h)$ is a portion of objects in the subset belonging to the Y_hth class that are connected to the tree node$h = \overline{1,v}$, $P(Y_h) = \frac{l^{Yh}}{N}$; l^{Y_h} is the number of products in the subset belonging to the Y_hth class.

The splitting criterion based on binary classification is evaluated in congruence with equation (1) as follows:

$$Gini_t^{split} = \frac{N_1}{N} Gini_{t_1} + \frac{N_2}{N} Gini_{t_2} \rightarrow min \quad (10)$$

Where N - number of objects in tree node t, N_1 and N_2 objects belonging to node t_1 and t_2 resembling to the left and right descendants nodes of the binary tree respectively. In order to enhance the quality of SVM classification for more number of datasets, it is recommended to employ additional potent classifier based on RF algorithm as an auxiliary classifier. Hence, the hybrid ERFSVM algorithm has been implemented in this work.

2.4. Hybrid SVM-RF Algorithm

The introduced approach uses hybrid technique to address classification issues which simultaneously combines Random Forest, SVM and ERFSVM functionality. The classification system consists of several components, in which the sum of their predictions determines final classification. A bootstrap sample produced from the testing dataset is the input for each unit. Every unit is made up of smaller units whose outputs are determined by the kernel, feature extraction unit and the bootstrap sample. Utilizing the decision fusion process, the units' output is combined. The proposed method merely switches out the decision trees in a random forest for entire classifiers, so the random forest's architecture is intact (subunit). A vector is produced by a series of intermediate classification processes that make up the proposed Method SVM-Random Forest classification scheme. These output vectors are combined by the final decision fusion unit using a voting process. The following section provides a detailed description of classification architecture.

Classification Units: Each of the classification units is made up of a number of smaller units, all of which are identical in nature. A single Decision Fusion Subunit (DFS) and M subunit forms a complete unit.

Classification Subunit: Various classification subunits make different predictions about the test sample's class. Usually, the number of subunits is a parameter that is selected while developing an algorithm. In general, there are M subunit parameter present in the algorithm.

The first phase involves the extraction of data from the concerned Block chains and choosing of ideal information using ERFSVM algorithm. In each subunit, these issues becomes a classification module. The ERFSVM is used to rank the information. The chosen data are selected as input for SVM classification. The subunits used by the Kernel function is selected empirically. Each classification component generates output vectors that are used for additional processing by decision fusion subunit. The final decision can be combined using three ways i.e. (1) by voting, (2) by vectors and (3) by weighted decision fusion. These methods promptly move towards the unit that fuses

final decisions, and all decisions will be merged at the end process.

Let the initial dataset be U which includes objects $z_i$and labels y_i classes that matches the objects,$i = \overline{1,s}$, the dataset G contains the objects that the SVM classification caused to appear in the Ω area and $V = U\backslash G$ is the dataset, comprising only the initial dataset U which is correctly classified objects.

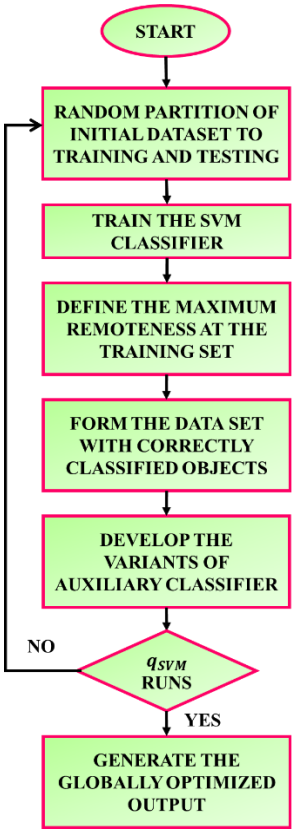

Fig. 5. Flowchart for the hybrid ERFSVM classifier

Implementing auxiliary classifier, it is possible to improve the quality of data classification using the following procedure:

- To randomly partition initial dataset U into corresponding training dataset U_{train} and testing datasetU_{test}.
- To evaluate SVM classifier at U_{train} training dataset using default classifier parameter values and to estimate various inductor qualities applied to the developed classifier in U_{train} andU_{test}.
- To determine the training dataset U_{train} with the maximum distance d^+ and d^- from the incorrectly classified objects of classes with labels "1^+" and "1^-" from the separating hyper plane. To create the Ω area that contains all the incorrectly classified items and is close to the hyper plane separating classes. In Ω area both symmetrical and asymmetrical areas are possible. The Ω area contains the symmetrical objects, separated from separating hyperplane by the distance that do not exceed$\beta = \max\{|d^-, d^+|\}$. The Ω area with its object along with their class labels form the dataset G.
- To create dataset $V = U\backslash G$ which only contains objects that were classified correctly along with their associated class labels.
- To perform q_{aux} runs and to create several auxiliary classifier variants based on the V dataset in order to clarify class affiliation of objects in study region. To utilize for each $\tau^{q_{aux}} - th\ (\tau^{q_{aux}} = \overline{1, q_{aux}})$ run the various auxiliary classification parameter values that are based on the unique number. In order to improve the values of classification quality indicators obtained using the SVM classifier for present splitting of initial dataset into the training U_{train} and test U_{test}datasets, the best variation of auxiliary classifier should be selected based onq_{aux}.
- Repeat steps 1 through 5 to get to the q_{svm} runs.
- To select on q_{svm} runs the uniform optimal outcome of auxiliary classifier and SVM classifier in congruence with the classification indicator quality is required to be maximized.

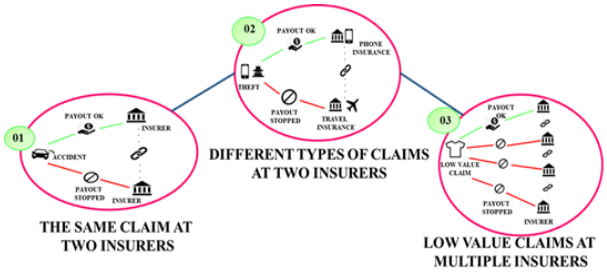

Fig. 6. Preventing various types of insurance frauds using the proposed Blockchain approach

The flowchart for the proposed hybrid eRFSVM is given in Fig. 5. Thus the proposed hybrid machine learning based blockchain technique is effective in preventing several types of insurance frauds as seen in Fig. 6.

3. Results and Discussion

The effectiveness of the proposed blockchain design in identifying problematic clients and their potential fraudulent claims is the major focus of this section. Then the performance accuracy of the hybrid machine learning technique of ERFSVM in identifying and classifying the variety of fraud types is also discussed in detail in this section. The datasets required for evaluating the performance of the designed blockchain based insurance fraud detection model is assessed from real world insurance agencies. The variety of insurance frauds found in different data samples is given in Tab. 1 and Fig. 7.

Table. 1. Various fraud types in the selected dataset

Insurance Fraud types	Data set samples				
	100	300	500	750	1000
Impersonation claims	0	4	12	25	36
Upcoded Claims	6	36	52	124	8
Unbundled Claims	2	20	12	56	2
Overbilling Claims	46	62	93	123	206
Uncovered Claims	6	58	67	111	408
Duplicate Claims	4	6	8	6	0
Total Suspected Claims	64	186	244	445	660

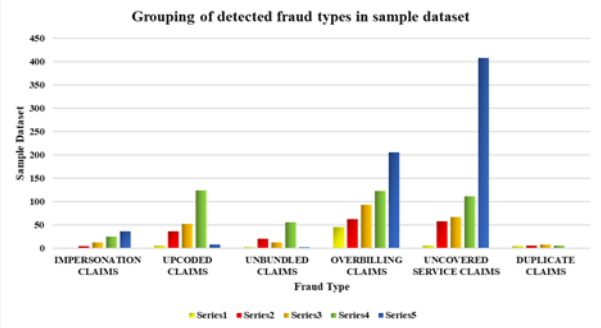

Fig. 7. The distribution of fraud types in corresponding data sets

Five different data set samples including 100 dataset, 300 dataset, 500 dataset, 750 dataset and 1000 dataset are selected for evaluating the working of the proposed fraud detection model. The types of insurance frauds considered includes Impersonation claims (fraudulent payment requested by an imposter), Upcoded or Inflated claims (Submitting inaccurate or exaggerated billings/information for receiving insurance), Unbundled claims (This fraudulent plan entails invoicing for several treatments that are typically carried out and reported under a single CPT code or it also refers to fake death claims), Overbilling claims (Charging more than the legally permissible limit on a bill or invoice), Uncovered service claims and Duplicate claims (any claims that have been paid across several claim numbers for the same beneficiary).

Table 2. Confusion matrix table

Predicted Observed	True	False
Positive	True Positive (TP)	False Positive (FP)
Negative	False Negative (FN)	True Negative (TN)

The performance evaluation of the hybrid ERFSVM is based on the following metrics of classification estimated using the confusion matrix given in Tab. 2,

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

$$Recall = \frac{TP}{TP+FN} \quad (12)$$

$$Precision = \frac{TP}{TP+FP} \quad (13)$$

$$F1-Score = 2\frac{Precison.Recall}{Precision+Recall} \quad (14)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (15)$$

$$Specificity = \frac{TN}{TN+FP} \quad (16)$$

Classifiers	Dataset Samples Accuracy (%)				
	1000	750	500	300	100
kNN	92.21	94.49	94.88	95.12	95.47
RF	93.25	95.57	95.74	96.04	96.46
SVM	94.43	94.87	95.13	95.63	95.84
eRFSVM	96.58	96.86	97.01	97.54	97.89

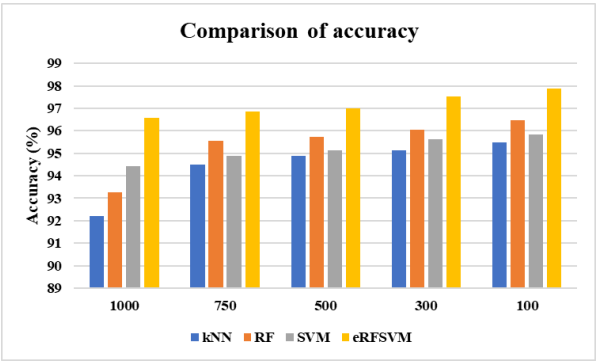

Fig. 8. Accuracy comparison of different classifiers

Classifiers	Dataset Samples Specificity (%)				
	1000	750	500	300	100
kNN	92.25	92.3	92.58	93.01	93.56
RF	92.94	93.14	93.46	93.85	94.09
SVM	93.58	93.96	94.36	94.92	95.63
eRFSVM	95.56	95.78	95.97	96.43	97.05

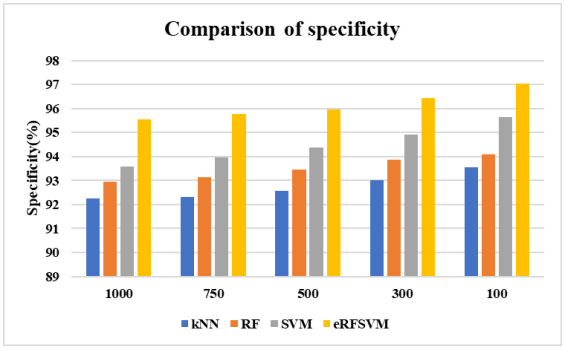

Fig. 9. Specificity comparison of different classifiers

Classifiers	Dataset Samples Precision				
	1000	300	500	750	1000
kNN	0.84	0.87	0.9	0.91	0.92
RF	0.85	0.88	0.89	0.91	0.93
SVM	0.87	0.89	0.92	0.93	0.95
eRFSVM	0.92	0.94	0.95	0.97	0.98

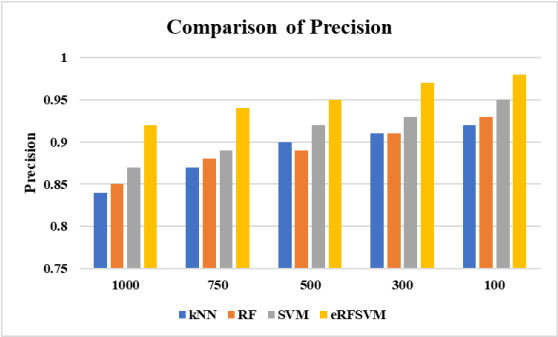

Fig. 10. Precision comparison of different classifiers

Classifiers	Dataset Samples Sensitivity (%)				
	1000	750	500	300	100
kNN	89.88	90.15	90.58	91.23	91.42
RF	91.76	92.04	92.54	92.99	93.47
SVM	93.54	94.85	95.72	96.12	96.37
eRFSVM	95.77	96.11	96.46	96.88	97.95

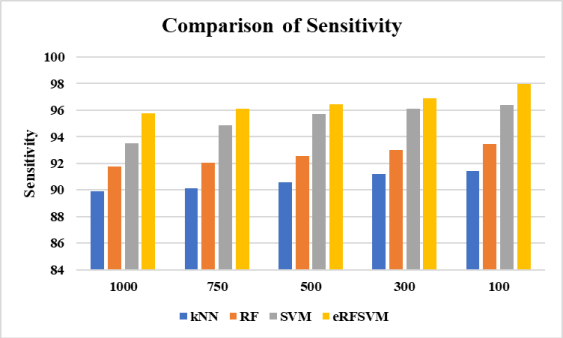

Fig. 11. Sensitivity comparison of different classifiers

Classifiers	Dataset Samples Recall				
	1000	750	500	300	100
kNN	0.83	0.84	0.87	0.88	0.89
RF	0.84	0.86	0.89	0.91	0.93
SVM	0.87	0.88	0.9	0.92	0.94
eRFSVM	0.9	0.91	0.93	0.96	0.98

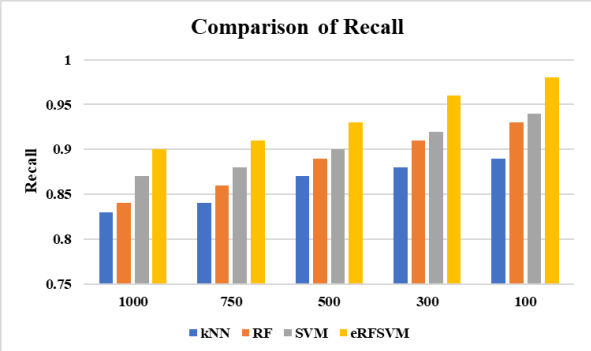

Fig. 12. Recall comparison of different classifiers

Classifiers	Dataset Samples F1-Score				
	1000	750	500	300	100
kNN	0.84	0.83	0.9	0.93	0.94
RF	0.87	0.91	0.92	0.94	0.95
SVM	0.85	0.87	0.89	0.94	0.95
eRFSVM	0.92	0.94	0.95	0.97	0.98

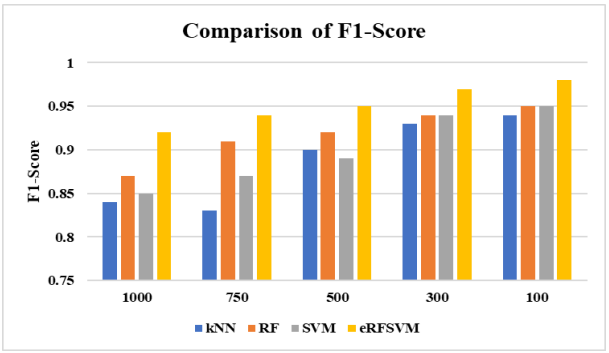

Fig. 13. F1-Score comparison of different classifiers

The Figs (8-13) represents the comparison of the proposed hybrid ERFSVM classifier with other existing converters in terms of accuracy, Specificity, Precision, Sensitivity, Recall and F1-Score in order to evaluate its effectualness in classifying the insurance frauds. From the obtained results, it is seen that the adopted hybrid ERFSVM displays exceptional performance in comparison to other existing classifiers with 97.176% accuracy, 96.158% specificity and 96.634% sensitivity.

4. Conclusion

The problem of claim leakage deprives insurance companies of a sizeable portion of their anticipated benefit. For insurance companies, fraudulent claims are a serious and expensive problem that might cost the industry billions of dollars per year in unwarranted expenses. So, an innovative blockchain technique is proposed for effective detection of fraudulent activities in insurance industry. The accuracy of the blockchain is further improved by hybrid ERFSVM classifier. The overall approach is evaluated in Python with dataset samples obtained from insurance agencies. The proposed insurance fraud detection technique shows remarkable performance in evaluating the authenticity of the customer claims. On the basis of analysing the dataset samples obtained from insurance industry, it is determined that the hybrid ERFSVM classifier operates with exceptional accuracy of 97.176%. Additionally, the value of specificity and sensitivity is 96.158% and 96.634% respectively.

5. References

[1]. Austin, Insurance Fraud Handbook, Association of Certified Fraud Examiners, TX, USA, Oct. 2018.

[2]. N. Dhieb, H. Ghazzai, H. Besbes and Y. Massoud, "A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement," in IEEE Access, Vol. 8, pp. 58546-58558, 2020.

[3]. I. Matloob, S. A. Khan and H. U. Rahman, "Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology," in IEEE Access, Vol. 8, pp. 143256-143273, 2020.

[4]. Chauhan, T., and S. Sonawane. "The Contemplation of Explainable Artificial Intelligence Techniques: Model Interpretation Using Explainable AI". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 65-71, doi:10.17762/ijritcc.v10i4.5538.

[5]. C. Sun, Q. Li, H. Li, Y. Shi, S. Zhang and W. Guo, "Patient Cluster Divergence Based Healthcare Insurance Fraudster Detection," in IEEE Access, Vol. 7, pp. 14162-14170, 2019.

[6]. C. Sun, Z. Yan, Q. Li, Y. Zheng, X. Lu and L. Cui, "Abnormal Group-Based Joint Medical Fraud Detection," in IEEE Access, Vol. 7, pp. 13589-13596, 2019.

[7]. K. Nian, H. Zhang, A. Tayal, T. Coleman, Y. Li, "Auto insurance fraud detection using unsupervised spectral ranking for anomaly." The Journal of Finance and Data Science 2, no. 1: 58-75, 2016.

[8]. Agarwal, D. A. . (2022). Advancing Privacy and Security of Internet of Things to Find Integrated Solutions. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 05–08. https://doi.org/10.17762/ijfrcsce.v8i2.2067

[9]. S. Subudhi, S. Panigrahi, "Use of optimized Fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection." Journal of King Saud University-Computer and Information Sciences 32, no. 5: 568-575, 2020.

[10]. S. K. Majhi, S. Bhatachharya, R. Pradhan, S. Biswal, "Fuzzy clustering using salp swarm algorithm for automobile insurance fraud detection." Journal of Intelligent & Fuzzy Systems 36, no. 3: 2333-2344, 2019.

[11]. I. Fursov et al., "Sequence Embeddings Help Detect Insurance Fraud," in IEEE Access, Vol. 10, pp. 32060-32074, 2022.

[12]. A. Shetty, A.D. Shetty, R. Y. Pai, R. R. Rao, R. Bhandary, J. Shetty, S. Nayak, T. Keerthi Dinesh, K. J. Dsouza, "Block Chain Application in Insurance Services: A Systematic Review of the Evidence." SAGE Open 12, no. 1, 2022.

[13]. S Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review, 2008.

[14]. A. A. Amponsah, F. A. Adebayo, B. A. WEYORI, "Blockchain in Insurance: Exploratory Analysis of Prospects and Threats." International Journal of Advanced Computer Science and Applications 12, no. 1 2021.

[15]. F. Casino, T. K. Dasaklis, C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36: 55-81, 2019.

[16]. Joy, P., Thanka, R., & Edwin, B. (2022). Smart Self-Pollination for Future Agricultural-A Computational Structure for Micro Air Vehicles with Man-Made and Artificial Intelligence. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 170–174. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/1743

[17]. E. Kapsammer, B. Pröll, W. Retschitzegger, W. Schwinger, M. Weißenbek, J. Schönböck, "The Blockchain Muddle: A Bird's-Eye View on Blockchain Surveys." In Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services, pp. 370-374, 2018.

[18]. Y. Dong, K. Xie, Z. Bohan and L. Lin, "A Machine Learning Model for Product Fraud Detection Based On SVM," 2021 2nd International Conference on Education, Knowledge and Information Management (ICEKIM), pp. 385-388, 2021.

[19]. André Sanches Fonseca Sobrinho. (2020). An Embedded Systems Remote Course. Journal of Online Engineering Education, 11(2), 01–07. Retrieved from http://onlineengineeringeducation.com/index.php/joe/article/view/39

[20]. P. Naveen and B. Diwan, "Relative Analysis of ML Algorithm QDA, LR and SVM for Credit Card Fraud Detection Dataset," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 976-981, 2020.

[21]. P. Singh, V. Chauhan, S. Singh, P. Agarwal and S. Agrawal, "Model for Credit Card Fraud Detection using Machine Learning Algorithm," 2021 International Conference on Technological Advancements and Innovations (ICTAI), pp. 15-19, 2021.

[22]. M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika and E. Aswini, "Credit Card Fraud Detection Using Random Forest Algorithm," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 2019.