JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CREDIT CARD FRAUD DETECTION USING RANDOM FOREST ALGORITHM

[1]K. Nageswarao, [2] P.N.V Vamsi Lala
[3]Jattiboyina Hemalatha, [4]Kanaparthi Anoohya, [5]Narne Vyshnavi,
[6]Pulivarthi Srividya, [7]Singamsetty Srilatha
[1,2]Assisstant Professor, Department of IT, Vignan's Nirula Institute of Technology and Science, Guntur.
[3,4,5,6,7] B.Tech, Department of IT, Vignan's Nirula Institute of Technology and Science, Guntur.

Abstract

The today's world is driven by innovation, science and inventive measures making numerous ordinary errands much less complex for the people. One such occurrence where innovation comes convenient is utilization of installment cards and online exchanges. Installment cards give a straightforward and helpful strategy for making buys. Be that as it may, owing to the increment within the utilization of installment cards, particularly in online buys, extortion cases are on the rise. Within the later times, the e-payments have driven to an increment in monetary extortion cases such as credit card fakes. Subsequently, numerous companies have begun utilizing machine learning calculations to create models that are utilized for credit card extortion discovery. A few procedures utilized are Back Vector Machine, Calculated Relapse, Irregular Timberland and their blends. In this comparative think about, the proposed credit card extortion discovery is performed on a dataset of different card holders. The results emphatically point towards the viability of utilizing amassed highlights for undertaking real-world installment card extortion location issues. Catchphrases: Machine learning; Extortion discovery; Prescient modeling; Calculated Relapse

1.INTRODUCTION

In later a long time, different budgetary exchanges are been making advantage of the utilize of credit cards with the quick development of online exchanges and ecommerce have altogether expanded. [1] Whereas this move towards a cashless economy offers consolation and ampleness, it has moreover given rise to a belittling issue: [2] credit card extortion. False exercises related to credit cards not as it were cause significant budgetary misfortunes to both shoppers and money related teach but to disrupt the believe, utilization and secureness of electronic installment frameworks.

Conventional strategies of extortion discovery, [3] regularly essentially depend on manual surveys and rule-based frameworks, are getting to be progressively lacking and wrong in managing with the complicated and advancing strategies practiced by fraudsters. [4] These customary approaches regularly endure from tall false-positive rates and deferred discovery, which can result in tremendous monetary misfortunes to the companies in the event that went uncorrected and a bother to true blue clients. [5] The ubiquity of credit card utilize and the

advancement of false plans require the improvement of strong instruments for recognizing and anticipating extortion.

Once fraudsters steal card information, they are able to utilize the playing cards themselves or advance the cardboard information to distinctive human creatures, as is the case in India,[6] wherein the cardboard data of circular 70 million human creatures are being advertised at the darkish web. One of the greatest serious credit score card extortion occurrences in most recent memory that happened withinside the [7] UK finished in GBP 17 million common in financial misfortunes.

[8] Machine learning methods can analyze expansive volumes of exchange information to distinguish designs and peculiarities demonstrative of false behavior. By leveraging the control of ML, [9] it is conceivable to create more proficient, versatile and exact extortion location frameworks that can essentially diminish the dangers related with credit card extortion. ML and diverse related forms are regularly utilized, for case, [10-13] ANN (Counterfeit Neural Organize), the method of run the show acceptance framework, Calculated Relapse (LR), Choice Trees (DT), and the Bolster Vector Machine etc.

This paper investigates different machine learning calculations and their adequacy in recognizing credit card extortion. [14-16] We are going look at directed learning procedures such as calculated relapse, choice trees, arbitrary woodlands, and bolster vector machines, as well as unsupervised learning approaches like clustering and inconsistency location. For the rest of this paper, we to begin with show a writing study on fund applications of factual and machine learning calculations. [17] Also, we are going talk about the challenges related with actualizing these calculations, counting issues related to information awkwardness, include selection, and show interpretability.

The essential objective of this inquire about is to supply a comprehensive outline of the current state of [18-20] credit card extortion location utilizing machine learning, highlighting the qualities and restrictions of distinctive approaches. By doing so, we aim to contribute to the progressing endeavors in upgrading the security and unwavering quality of budgetary exchanges within the computerized age.

2. Literature survey:

An intelligent payment card fraud detection system.Credit cards give a simple and clear way to shop. In any case, as more individuals utilize credit cards, especially for online shopping, cases of extortion are expanding. [21-23] This surge in extortion postures a monetary danger and makes question, influencing businesses, which lose billions yearly due to extortion. However, getting exchange records that can offer assistance make precise prescient models for spotting extortion is challenging, primarily due to protection concerns with respect to client information. [24] In this consider, we utilize a assortment of 13 measurable and machine learning models to identify credit card extortion, utilizing both freely open and real exchange information. [25] -The discoveries affirm the utility of combining highlights for tackling real life issues related to credit card extortion discovery.

A machine learning based credit card fraud detection using the GA algorithm for feature selection.The later advancements in online shopping and e-payment frameworks have driven to a rise in occurrences of budgetary tricks, counting credit card burglary. Subsequently, it's fundamental to present frameworks able of distinguishing credit 2 card burglary. [26] Understanding the characteristics of credit card burglary is pivotal when applying machine learning to identify such extortion cases, and these characteristics must be carefully chosen. This consider presents a machine learning approach for distinguishing credit card burglary through a hereditary calculation (GA) to choose significant highlights. After the suitable highlights are chosen, the created approach utilizes a few machines learning models, counting [27] Choice Trees (DT), Irregular Woodlands (RF), Calculated Relapse (LR), Manufactured Neural Systems (ANN), and Gullible Bayes (NB) classifiers. The dataset utilized to test this approach is of [28-37] different European clients. The discoveries show that this strategy surpasses past arrangements in execution.

Enhanced Credit Card Fraud Detection Model Using Machine Learning.The covid-19 [38-46] widespread has made it harder for individuals to create everyday buys, driving to more online shopping and a more prominent reliance on credit cards. [47-50] Be that as it may, credit card extortion has ended up a risk online. This paper inquires about 66 machine learning models to discover the finest and ideal way to halt most credit card extortion. [51] It employments a genuine credit card extortion dataset of different users and tests nine models to discover the beat three. And after, that 19 distinctive models are used to test them once more. After a month of testing, [52] the AllKNNCatBoost demonstrate is chosen as the most excellent since it performs superior than other models in avoiding extortion. The paper too compares comparative models and appears that it's the most excellent since it includes a tall precision in identifying extortion.

Exploratory analysis of credit card fraud detection using machine learning techniques.In today's computerized age, it has gotten to be exceptionally [53] straightforward and less demanding for people to do their assignments since of the tech, but this too leads to a rise in unlawful exercises that harm the economy, such as credit card extortion. The models included here are Back Vector Machine, Slope Boost, Irregular Woodland, and their combinations, are utilized to analyze the information and distinguish false exercises. In any case, these confront impediments like lesson lopsidedness and how to illuminate it. The viability of these model contrast depending on the information. [54] The think about uncovers that in spite of calculated relapse being more accurate, K-Nearest Neighbors (KNN) may be a better choice for recognizing credit card extortion due to its capacity to memorize from information.

3. Proposed Methadology

As the machine learning has been broadly utilized in all divisions of E-commerce, it moreover plays a vital part in credit card extortion by sparing the time taken to distinguish the extortion and dispense with them. In this paper, we have utilized four ML calculations: Calculated Relapse, Arbitrary Woodland Classifier, Naive Bayes and Back Vector Machine. Out of which, the exactness for Irregular Woodland Classifier has been more noteworthy. Consequently, we have utilized Irregular Woodland Classifier to undertake and fathom the credit card extortion. We propose a viable arrangement for credit card extortion discovery utilizing the Irregular Timberland classifier calculation. The point is to precisely distinguish false exchanges from genuine ones, in this manner lessening budgetary misfortunes and progressing security measures for credit card clients and monetary educate.

Algorithm Choice

The Irregular Timberland classifier was chosen due to its strength, precision, and capacity to handle expansive datasets with various highlights. As an outfit learning strategy, it builds different choice trees amid preparing and blends them to create more dependable and exact forecasts. This strategy mitigates overfitting, which may be a common issue in single choice trees, and improves the generally execution of the show.

Data Preprocessing

To guarantee the model's viability, broad information preprocessing steps were embraced:

Data Cleaning: Expulsion of copy exchanges and dealing with of lost values to guarantee information astuteness.

Feature Designing: Creation of modern highlights from existing ones to capture more complex designs within the information.

Normalization: Standardization of highlights to guarantee that all factors contribute similarly to the model's execution.

Imbalanced Information: Taking care of: Since false exchanges are essentially less visit than true blue ones, procedures such as Destroyed (Engineered Minority Over-sampling Strategy) were utilized to adjust the dataset.

Model Training and Evaluation

The dataset was part into preparing and testing sets to assess the model's execution. The Arbitrary Woodland classifier was prepared on the preparing set employing a extend of hyperparameters, optimized through methods such as Network Look and Cross-Validation to distinguish the leading demonstrate setup.

Key execution measurements were utilized to assess the show, counting:
Accuracy: The extent of accurately recognized exchanges.
Precision: The proportion of genuine positive fraud cases to the full cases anticipated as extortion.
Recall (Affectability): The proportion of genuine positive extortion cases to the full real extortion cases.
F1 Score: It is the consonant cruel of exactness and review, that gives a adjust between the two. The proposed Random Forest classifier demonstrated high accuracy and robustness in detecting fraudulent transactions.

Implementation

For down to earth usage, the show can be coordinates into the exchange handling frameworks of money related educate. This integration would include real-time examination of exchanges, hailing suspicious exercises, and activating encourage examination or mechanized intercessions to avoid extortion.

ADVANTAGES

Credit card extortion discovery utilizing machine learning (ML) calculations offers a few focal points:
Exactness and Effectiveness: ML calculations can analyze endless sums of exchange information rapidly and precisely, identifying false designs more viably than conventional rule-based frameworks.
Real-time Discovery: ML models can prepare exchanges in genuine time, permitting for quick recognizable proof and reaction to possibly false
Flexibility: ML models can ceaselessly learn and adjust to unused extortion designs as they advance, making strides their discovery capabilities over time.
Versatility: ML calculations can handle large-scale information productively, making them appropriate for organizations with tall exchange volumes.
Upgraded Client Involvement: By precisely recognizing extortion without superfluously blocking true blue exchanges, ML-based frameworks make strides the by and large client involvement.

SYSTEM ARCHITECTURE

System design portrays the equipment components that are utilized and the parts of them:

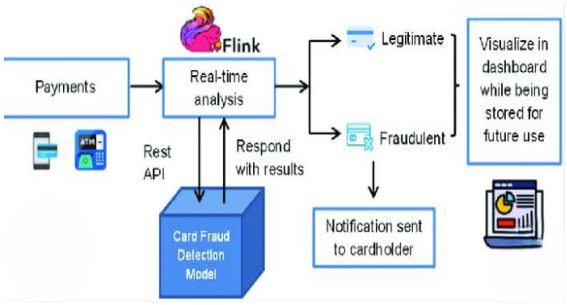

Fig 1: System Architecture

DATASET

We are able to collect the dataset from the Kaggle.com location and utilize it as the base information for investigate.

Table 1: Credit data

UML DIAGRAMS

CLASS DIAGRAM

The foundation of event-driven information investigation is the course diagram. Both wide down to earth confirmation of the application's devotion and fine-grained exhibit of the show interpretation into computer program code depend on its availability.

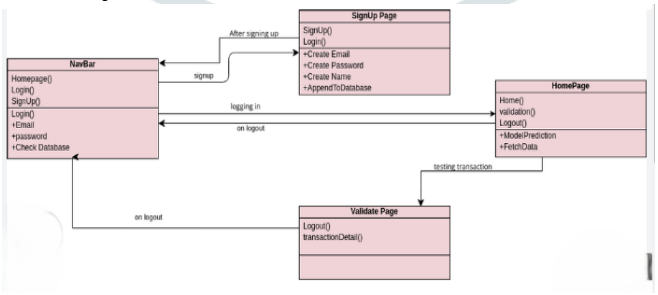

Fig 2 shows the class diagram of the project

USECASE DIAGRAM

A use case diagram within the Unified Modeling Language (UML) may be a kind of behavioral chart characterized by and made from a Use-case examination. Its premise is to show a graphical diagram of the

usefulness given by a framework in terms of on-screen characters, their objectives (represented as utilize cases), and any conditions between those utilize cases.

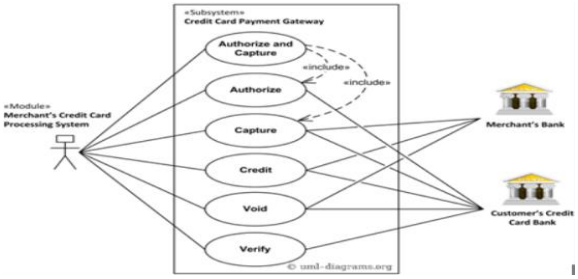

Fig 3 Shows the Use case Diagram

SEQUENCE DIAGRAM

A sequence diagram in bound together Modeling Dialect (UML) may be a kind of interaction graph that appears how forms work with one another and in what arrange. It may be a develop of a Message Arrangement Chart. Arrangement charts are some of the times called occasion graphs, occasion scenarios, and timing graphs.

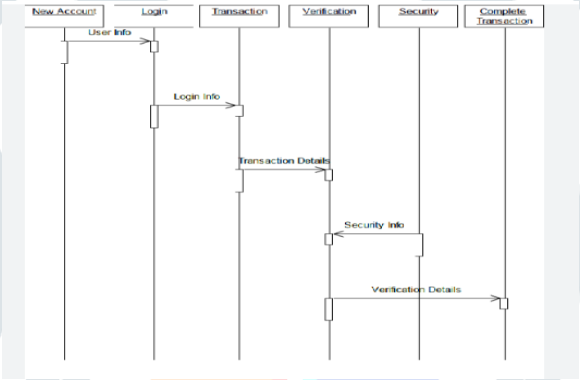

Fig 4 Shows the Sequence Diagram

4.Results and Discussion

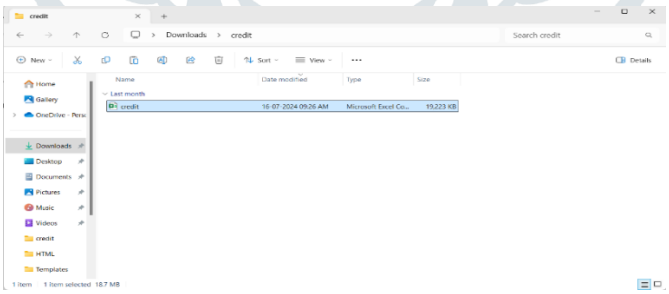

Fig 5 Uploading the Dataset File

In above screen selecting and uploading diabetes dataset and then click on ‘Open’ button to load dataset and to get below

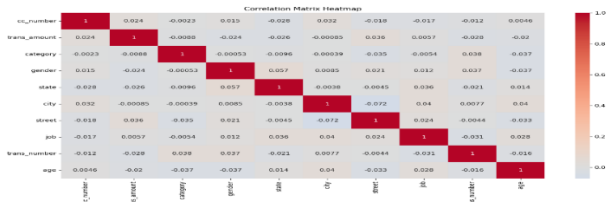

Fig 6 Preprocess the dataset

Within the above graph, at the top, we see names of columns and in boxes values with short images are not critical and positive column values are imperative and ML calculation will prepare only with positive values. Now we utilize the credit card dataset to test that trained model and to calculate prediction exactness. Now both prepare and test information is prepared and presently we will begin preparing all ML calculations on prepare and test information.

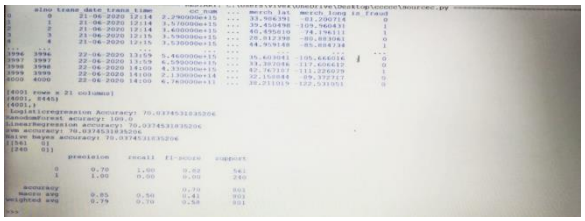

Fig 7 Run the Machine Learning Algorithms

In above screen we can see prediction accuracy of each algorithm and form all algorithms extension Extreme Machine Learning is giving good prediction accuracy and now all ML algorithms are ready with trained model and now we can see whether the credit card is fraud or not by using these algorithms.

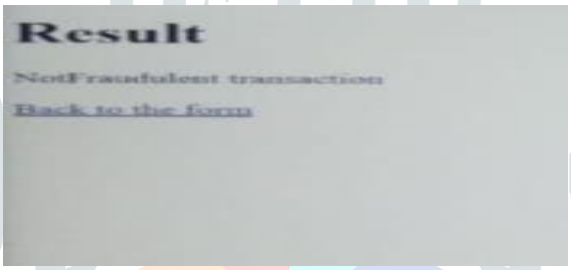

Fig 8 Accuracy of ML Algorithms

In above screen for each test lab record ML predict whether card is fraud or not. Now write a code to print the 'Accuracy Comparison Graph'. Now see the graph below.

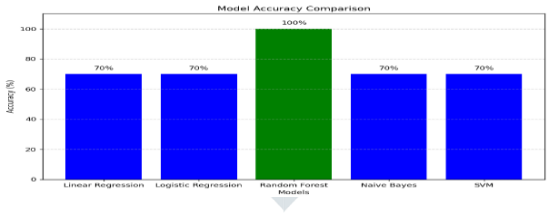

Fig 9 Accuracy Comparison Graph

In the above graph x-axis represents ML algorithms names and y-axis represents accuracy of all those algorithms and from above graph we can conclude that 'Random Forest' is giving the best accuracy, that is, 100%.

5.CONCLUSION

In this paper, we have executed machine learning and calculations for the discovery of credit card fraud. It may be a frequent event for clients to drop casualty to these fraudulent exercises, coming about in major monetary misfortunes. To address these special cases, we investigated a assortment of extortion discovery strategies, counting Measurable Examination, Machine Learning, and Profound Learning Strategies, pointed at identifying suspicious designs in exchange information. For classification errands, we made utilize of a differing run of machine learning models, from Linear Regression (LR) to Support Vector Machines (SVM), Logistic

Regression (LR), Naive Bayes (NB), Random Forest (RF), all of which demonstrated to be compelling apparatuses in recognizing and disposing of extortion. In our project, we utilized the Random Forest Classifier algorithm, in addition to other Python libraries such as Scikit-learn, Numpy, and Pandas, to develop a satisfactory solution.
Based on the accuracy accomplished by the calculation on the given dataset, this project has the potential of deciding whether a client is legitimate or false.

REFERENCES

1. Sahithi, G.L.; Roshmi, V.; Sameera, Y.V.; Pradeepini, G. Credit Card Fraud Detection using Ensemble Methods in Machine Learning. In Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 28–30 April 2022; pp. 1237–1241. [CrossRef]

2. Federal Trade Commission. CSN-Data-Book-2022. no. February 2023. Available onlin: https://www.ftc.gov/system/files/ftc_ gov/pdf/CSN-Data-Book-2022.pdf (accessed on 11 March 2023).

3. UK Finance. Annual Report and Financial Statements 2022. Available online: https://www.ukfinance.org.uk/annual-reports (accessed on 20 November 2023).

4. Vejendla, L. N., Bysani, B., Mundru, A., Setty, M., & Kunta, V. J. (2023). Score-based support vector machine for spam mail detection. Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies (ICOEI), 915–920. https://doi.org/10.1109/ICOEI56765.2023.10125718

5. Anusha, P., Ravikiran, A., Lakshman Narayana, V., & Maddumala, V. R. (2020). Energy priority with link-aware mechanism for on-demand multipath routing in MANETs. Journal of Electrical Engineering and Automation, 29(3), 8979–8991.

6. Narayana, V. L., & Bharathi, C. R. (2017). Identity-based cryptography for mobile ad hoc networks. International Journal of Engineering and Technology Innovation, 95(5), 1173–1181

7. Narayana, V. L., & Midhunchakkaravarthy, D. (2020). A time interval-based blockchain model for detection of malicious nodes in MANET using network block monitoring node. Proceedings of the IEEE International Conference on Intelligent Computing and Robotics (ICIRCA), 852–857. https://doi.org/10.1109/ICIRCA48905.2020.9183256

8. Bharathi Vejendla, C. R., Narayana, L., & Ramesh, L. V. (2020). Secure data communication using Internet of Things. Journal of Advanced Research in Dynamic and Control Systems, 9(4), 3516–3520.

9. Narayana, V. L., Sujatha, V., Sri, K. S., Pavani, V., Prasanna, T. V. N., & Ranganarayana, K. (2023). Computer tomography image-based interconnected antecedence clustering model using deep convolutional neural network for prediction of COVID-19. Traitement du Signal, 40(4), 1689–1696. https://doi.org/10.18280/ts.400437

10. Patibandla, R. S. M. L., Rao, B. T., & Narayana, V. L. (2022). Prediction of COVID-19 using machine learning techniques. In Handbook of Machine Learning for Computational Biology and Bioinformatics (pp. 219–231). https://doi.org/10.1016/B978-0-12-824145-5.00007-1

11. Pavani, V., Sri, K. S., Krishna, P. S., & Narayana, V. L. (2021). Multi-level authentication scheme for improving privacy and security of data in decentralized cloud server. Proceedings of the IEEE International Conference on Systems and Electronics Engineering (ICOSEC), 391–394. https://doi.org/10.1109/ICOSEC51865.2021.9591698

12. Arepalli, P. G., Jairam Naik, K., & Rout, J. K. (2024). Aquaculture water quality classification with sparse attention transformers: Leveraging water and environmental parameters. In ACM International Conference Proceeding Series (pp. 318-325). https://doi.org/10.1145/3651781.3651829

13. Kumar, S. A., Babu, E. S., Nagaraju, C., & Gopi, A. P. (2015). An empirical critique of on-demand routing protocols against rushing attack in MANET. International Journal of Electrical and Computer Engineering, 5(5), 1102-1110. https://doi.org/10.11591/ijece.v5i5.pp1102-1110
14. Arepalli, G., Erukula, S. B., Gopi, A. P., & Nagaraju, C. (2016). Secure multicast routing protocol in MANETs using efficient ECGDH algorithm. International Journal of Electrical and Computer Engineering, 6(4), 1857-1865. https://doi.org/10.11591/ijece.v6i4.9941
15. Arepalli, P. G., Akula, M., Kalli, R. S., Kolli, A., Popuri, V. P., & Chalichama, S. (2022). Water quality prediction for salmon fish using Gated Recurrent Unit (GRU) model. In 2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022. https://doi.org/10.1109/ICCSEA54677.2022.9936539
16. Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208
17. Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117
18. Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181
19. Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539
20. Vejendla, L. N., Naresh, A., & Arepalli, P. G. (2021). Traffic analysis using IoT for improving secured communication. In Innovations in the Industrial Internet of Things (IIoT) and Smart Factory (pp. 106-116). https://doi.org/10.4018/978-1-7998-3375-8.ch008
21. Kanumalli, S. S., Lavanya, K., Rajeswari, A., Samyuktha, P., & Tejaswi, M. (2023, February). A scalable network intrusion detection system using bi-lstm and cnn. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 1-6). IEEE.
22. Kanumalli, S. S., Mantena, S. J., Kandula, S., Doppalapudi, K., & Atluri, T. (2022, May). Automated Irrigation Management System using IoT. In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 476-482). IEEE.
23. Kanumalli, S. S., Swathi, S., Sukanya, K., Yamini, V., & Nagalakshmi, N. (2022). Classification of dna sequence using machine learning. In *Soft Computing for Security Applications:*
24. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.
25. Kosaraju, Chaitanya, et al. "Mirchi crop yield prediction based on soil and environmental characteristics using modified RNN." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023
26. Chaitanya, Kosaraju, et al. "Ads Click-Through Rate prediction using Attention based LSTM Mechanism." 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2024.
27. Sujatha, V., Prasanthi, Y., Pravallika, C.H., ... Ayesha Banu, S.K., Sahithi, M.,K(23)
28. " A Computer Vision Method for Detecting the Lanes and Finding the Direction of Traveling the Vehicle*Lecture Notes in Networks and Systems"*, 2023, 612, pp. 373–382
29. Sri, L. Akhila, K. Manvitha, G. Amulya, I. Sai Sanjuna, and V. Pavani. "FBI crime analysis and prediction using machine learning." *Journal of Engineering Sciences* 11, no. 4 (2020): 441-448.
30. P. V, L. S. K, P. Vyshnavi A, M. Ch and S. B. G, "Students Community Portal using Machine Learning," *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2023, pp. 1109-1113, doi: 10.1109/ICEARS56392.2023.10085516.

31. Sirisha, Aswadati, et al. "Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation." *International Journal of Safety and Security Engineering* 11.1 (2021): 51-58.

32. Krishna, KVSS Rama, et al. "Vehicle Number Plate Detection using Deep Learning." *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. IEEE, 2024.

33. Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using CNN and Firefly Optimization." *Traitement du Signal* 38.1 (2021).

34. Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "Watermarking system for telemedicine based on FABEMD." *Multimedia Tools and Applications* 81.30 (2022): 44383-44404.

35. Chaitanya, P. Silpa, KV Narasimha Reddy, and G. Madhavi. "Effective Search of Color-Spatial Image Using Semantic Indexing." *International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol* 2 (2012): 9-19.

36. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.

37. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.

38. Srikanth Kilaru ” A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm” 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),

39. DOI: 10.1109/IC3I59117.2023.10397886, ISBN Information:Electronic ISBN:979-8-3503-0448-0 Print on Demand(PoD) ISBN:979-8-3503-0449-7

40. Srikanth Kilaru “Analytical models for collaborative autonomous mobile robot solutions in fulfillment centers” in Applied Mathematical Modelling, Volume 91, March 2021, Pages 438-457, https://doi.org/10.1016/j.apm.2020.09.059

41. Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617

42. Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. *Journal of Supercomputing, 80*(2), 2718-2747. https://doi.org/10.1007/s11227-023-05580-x

43. Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. *Environmental Monitoring and Assessment, 195*(12), Article 1516. https://doi.org/10.1007/s10661-023-12126-4

44. Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In *Smart Innovation, Systems and Technologies* (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_30

45. Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In *Advances in Intelligent Systems and Computing* (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56

46. Mohiddin, S.K., Sharmila, S., & Sharma, V. (2024). Wireless technology for providing safety in VANETs. In *Wireless Communication Technologies: Roles, Responsibilities, and Impact of IoT, 6G, and Blockchain Practices* (pp. 19–35). https://doi.org/10.1201/9781003389231-2

47. Sharmila, S.K., Nikhila, M., Lakshmi Prasanna, J., Lavanya, M., & Bhavana, S. (2023). Unique web-based assessment with a secure environment. *Lecture Notes in Networks and Systems, 673*, 725–736. https://doi.org/10.1007/978-981-99-1745-7_53
48. Sharmila, S.K., Lakshmi, M.S., Chowdary, G.S., Mounika, P., & Srujana, C. (2023). Speech emotion recognition using Mel Frequency Cepstral Coefficients. In *Proceedings of the 5th International Conference on Smart Systems and Inventive Technology* (ICSSIT 2023, pp. 1599–1604).5https://doi.org/10.1109/ICSSIT55814.2023.10060950
49. Mohiddin, S.K., Sharmila, S., & Sharma, V. (2024). Integration of mobile edge computing in wireless technology. In *Wireless Communication Technologies: Roles, Responsibilities, and Impact of IoT, 6G, and Blockchain Practices* (pp. 1–18). https://doi.org/10.1201/9781003389231-1
50. Mohiddin, S.K., Yalavarthi, S.B., & Sharmila, S. (2017). A complete ontological survey of cloud forensic in the area of cloud computing. In *Advances in Intelligent Systems and Computing* (Vol. 547, pp. 38–47). https://doi.org/10.1007/978-981-10-3325-4_5
51. Gupta, P.; Varshney, A.; Khan, M.R.; Ahmed, R.; Shuaib, M.; Alam, S. Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. Procedia Comput. Sci. 2023, 218, 2575–2584. [CrossRef]
52. Mondal, I.A.; Haque, M.E.; Hassan, A.-M.; Shatabda, S. Handling imbalanced data for credit card fraud detection. In Proceedings of the 2021 24th International Conter and Information Technology (ICCIT), Dhaka, Bangladesh, 18–20 December 2021; pp. 1–6.
53. Ahmad, H.; Kasasbeh, B.; Aldabaybah, B.; Rawashdeh, E. Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). Int. J. Inf. Technol. 2023, 15, 325–333. [CrossRef] [PubMed]
54. Bagga, S.; Goyal, A.; Gupta, N.; Goyal, A. Credit card fraud detection using pipelining and ensemble learning. Procedia Comput. Sci. 2020, 173, 104–112. [CrossRef]