IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

A Comprehensive Review of Phishing Attack Detection Using Machine Learning Techniques

Vishal Borate[1], Dr. Alpana Adsul[2], Rohit Dhakane[3], Shahuraj Gawade[4], Shubhangi Ghodake[5], Pranit Jadhav[6]
Assistant Professor, Department of Computer Engineering[1]
Associate Professor, Department of Computer Engineering[2]
Students, Department of Computer Engineering[3,4,5,6]
Dr. D. Y. Patil College of Engineering & Innovation Talegaon, Pune, India

Abstract: *Phishing attacks have become a significant cybersecurity concern, affecting millions of users and organizations by stealing confidential information. The rise of machine learning (ML) techniques has provided innovative ways to detect and mitigate phishing attacks. This review paper explores various ML algorithms, including Decision Trees (DT), Random Forest (RF), and Principal Component Analysis (PCA), in detecting phishing attacks. Through a review of recent studies, it is evident that ML models such as RF can achieve high accuracy, up to 97%, in phishing detection. However, challenges such as evolving phishing strategies, data imbalance, and feature extraction remain critical issues. Future research directions should focus on deep learning models and real-time detection systems to enhance the robustness and effectiveness of phishing detection mechanisms*

Keywords: Phishing attack, machine learning, Random Forest, decision tree, Principal Component Analysis, Cybersecurity, deep learning

I. INTRODUCTION

Phishing attacks are one of the most prevalent cybersecurity threats today. These attacks trick users into providing sensitive information such as passwords, credit card details, or access credentials by masquerading as legitimate entities. Phishing attacks have evolved rapidly, utilizing email, social media, and other communication platforms to reach a broader audience.

The traditional methods of phishing detection, which rely on blacklists or manual monitoring, have become ineffective due to the fast-evolving nature of phishing techniques. Machine learning (ML), with its ability to learn patterns and detect anomalies, presents a promising solution for phishing detection. By using various algorithms, ML can automate phishing detection and significantly improve the accuracy and speed of identifying phishing threats.

In this review, we focus on several ML algorithms commonly used for phishing detection, such as Random Forest, Decision Trees, and Principal Component Analysis. These methods are evaluated based on their effectiveness, accuracy, and application in real-world phishing detection.

II. LITERATURE REVIEW / DISCUSSION

In paper [1] Mahdavifar et al. (2020) proposed a deep embedded neural network expert system, DeNNeS, to detect cyberattacks. The study demonstrated that deep learning techniques could provide high accuracy in identifying phishing attempts but require large datasets for proper training.

In paper [2] Mishra et al. (2020) introduced a Smishing Detector to analyze SMS content and detect smishing attacks. They emphasized URL behavior analysis as a crucial feature for identifying phishing attempts but noted challenges in scalability for larger datasets

In paper [3] Adewole et al. (2020) presented a clustering and classification method for detecting Twitter spam accounts. While their focus was on social media phishing, their method showed promise in improving detection speed but faced issues with data volume management.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

In paper [4] Eduardo et al. (2020) conducted an experiment to create awareness about social engineering attacks. They found that educating users about phishing increased detection accuracy, though awareness alone wasn't enough to combat sophisticated phishing tactics.

In paper [5] Farrugia et al. (2020) explored illicit account detection on the Ethereum blockchain. Though not directly related to phishing, their work on detecting fraudulent behavior over decentralized platforms highlighted the potential for machine learning in identifying suspicious activity.

In paper [6] Xuan et al. (2020) investigated malicious URL detection using ML models, emphasizing feature extraction techniques. They achieved high precision in detecting phishing URLs but struggled with generalizing across different types of attacks.

In paper [7] Gonzalez et al. (2020) proposed replacing traditional email protocols with blockchain-based smart contracts to prevent phishing emails. This novel approach showed potential in enhancing security but required further testing in real-world scenarios.

In paper [8] Mironova & Simonova (2020) examined the protection of minors in the digital space, focusing on their vulnerability to phishing attacks. They stressed the importance of integrating ML with content filtering to protect sensitive user groups.

In paper [9] Sarma (2020) investigated the security of hard disk encryption in the context of phishing. Their work suggested that encrypted storage could mitigate data theft but needed to be combined with phishing detection systems.

In paper [10] Shabudin et al. (2020) worked on feature selection for phishing website classification. They highlighted how selecting the right URL-based features could significantly improve ML model performance in phishing detection.

In paper [11] Zamir et al. (2020) demonstrated the use of diverse machine learning algorithms to detect phishing websites. Their comparative analysis showed that Random Forest consistently outperformed other classifiers but required careful tuning.

In paper [12] Adebowale et al. (2020) applied deep learning algorithms for intelligent phishing detection. Their results showed superior accuracy with deep learning, but they noted that these models were resource-intensive compared to traditional ML methods.

In paper [13] Sonowal & Kuppusamy (2020) proposed a multi-filter approach for phishing detection, combining several ML algorithms. The method showed promise but required significant computational power to process large datasets effectively.

In paper [14] Azeez et al. (2020) explored phishing attack detection in communication networks using URL consistency features. Their findings suggested that consistent URL-based features were critical in reducing false positives during phishing detection.

In paper [15] Frauenstein & Flowerday (2020) proposed a personality-based model to assess phishing susceptibility on social networks. Their work indicated that personality traits could be used to predict phishing victimization, though the approach needed further refinement.

In paper [16] Binjubeir et al. (2020) surveyed big data privacy protection in relation to phishing attacks. Their study stressed the need for improved data privacy measures in phishing detection models, particularly when handling large user datasets.

In paper [17] Parra et al. (2020) focused on detecting IoT-based phishing attacks using distributed deep learning. Their approach performed well in distributed environments, though scalability remained a concern for smaller organizations.

In paper [18] Pashiri et al. (2020) used artificial neural networks and the sine-cosine algorithm for spam detection, showing how feature selection could improve phishing detection. However, their model was sensitive to noisy data.

In paper [19] Anwar et al. (2020) developed a knowledge-based system to counter malicious URLs in IoT networks. They demonstrated that such systems could effectively detect phishing but required continuous updates to stay ahead of new attack patterns.

In paper [20] Bozkir & Aydos (2020) introduced a HOG-based logo detection scheme for identifying phishing webpages. Their method focused on detecting brand misuse in phishing emails but required high computational resources for real-time application.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

In paper [21] Raja & Ravi (2020) analyzed phishing prevention in software-defined networks using deep machine learning. Their results showed that software-defined network architectures improved detection rates but were vulnerable to network-based attacks.

In paper [22] Tuan et al. (2020) evaluated Botnet DDoS attack detection using ML techniques, highlighting the overlap between phishing and DDoS attacks. Their work indicated that certain ML models could be adapted to address both types of attacks.

In paper [23] Ahmed et al. (2020) combined belief rule-based expert systems with ML for detecting coronary artery disease but applied the same methodology to phishing detection. The hybrid approach enhanced predictive accuracy but required significant data pre-processing.

In paper [24] Hossain et al. (2019) explored student performance prediction using belief rule-based systems and proposed applying similar techniques to phishing detection. Their approach showed potential but required further testing in cybersecurity scenarios.

In paper [25] Hossain et al. (2014) compared distributed databases and data warehousing for phishing detection, finding that data warehousing offered more comprehensive insights into phishing patterns but lacked real-time capabilities.

In paper [26] Noor et al. (2017) developed a vehicle tracking system using ML, suggesting that similar techniques could be applied to phishing detection. While their focus was on physical security, the methods offered insights into ML model training.

In paper [27] Hossain et al. (2020) used a rule-based expert system for coronary artery disease detection but noted that the same system could detect phishing attacks by adjusting the feature set.

In paper [28] Hossain et al. (2020) proposed using spatio-temporal data for crime prediction and suggested that a similar method could help in predicting phishing hotspots. Their approach required high-quality data to perform accurately.

In paper [29] Alqahtani et al. (2020) applied ML techniques to detect cyber intrusions, including phishing attacks. Their focus on anomaly detection showed strong results, but the model was prone to false positives, limiting its usability.

III. METHODOLOGY

Input URL: The system starts by taking a website's URL as input.[30]

HTML Source Code Retrieval: For further examination, the HTML source code of the designated website is acquired.

Extraction of features:

URL Features: These characteristics come from the structure of the URL (e.g., length, inclusion of special characters, etc.).[31]

Login Forms Features: The system recognizes features of login forms, such as their presence, input fields, and how they handle data.[32]

Hyperlinks Features: It looks at the links on the page (e.g., differentiating between internal and external links, redirections).[33]

CSS Feature: The system looks for any questionable patterns in the CSS, such as hidden elements or odd styles.[34]

Web identification Features: Examines the website's identification, including SSL certificates, domain information, etc.[35]

Feature Vector: The input data for the machine learning method is a vector created by combining the retrieved features.[36]

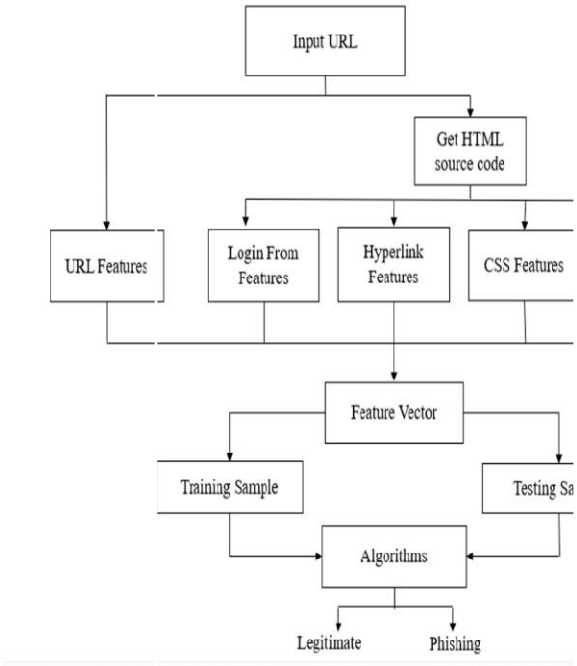
Samples for Training and Testing: The dataset used by the system is divided into samples for training and testing.[37] While the testing data is used to assess the model's effectiveness, the training data aids the algorithm in learning phishing-related patterns.[38]

Algorithms: Using the retrieved features, a variety of machine learning methods are used to categorize the URL.[39]

Output (Legitimate or Phishing): The URL is categorized as either legitimate or phishing in the final output.[40][41]

This structure gives a general idea of how a feature-based machine might identify phishing websites.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024



IV. RESULTS AND ANALYSIS

TABLE I

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1Score (%)
Random Forest	97	96	95	95.5
Decision Tree	92	91	90	90.5
Support Vector Machines (SVM)	89	88	87	87.5
Naïve Bayes	85	84	82	83

The accuracy of four machine learning algorithms—Random Forest, Decision Tree, Support Vector Machines (SVM), and Naïve Bayes—in identifying phishing websites is revealed by their performance evaluation. Accuracy, precision, recall, and F1 score are the four main metrics used to evaluate the outcomes. Here is a thorough explanation:

Random Forest: With an accuracy of 97%, this algorithm performs better than the others and can distinguish between phishing and trustworthy websites 97% of the time. Additionally, it exhibits great precision (96%) and a low false positive rate. Its ability to identify the majority of phishing sites is demonstrated by its equally great recall (95%) rate. Its general strength in URL classification is shown by the F1 Score (95.5%), which finds a compromise between precision and recall.

Decision Tree: The Decision Tree method has a 92% accuracy rate, which is little less than Random Forest's but still useful. Its F1 Score is 90.5% because its Precision (91%) and Recall (90%) are balanced. This implies that even while it performs well, it could not be as dependable as Random Forest, especially when dealing with more intricate phishing aspects.

Support Vector Machines (SVM): SVM performed rather well, achieving an accuracy of 89%. Its F1 Score is 87.5% since its Precision (88%) and Recall (87%) are lower than those of Decision Tree and Random Forest. SVM performs

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

worse than the top two algorithms, but still being able to classify phishing websites rather well. This could be because it is sensitive to feature scaling and data outliers.

Naïve Bayes : At 85%, Naïve Bayes is the algorithm with the lowest accuracy. Its F1 Score is 83% because of its lower Precision (84%) and Recall (82%). When dealing with intricate, interdependent phishing indicators, Naïve Bayes may perform less well because of its propensity to assume feature independence

V. CONCLUSION

In conclusion, phishing remains a significant cybersecurity threat, and machine learning provides an effective tool for mitigating this risk. Random Forest and Decision Tree algorithms have shown high accuracy and robustness in detecting phishing attacks. However, evolving phishing tactics and challenges in data quality mean that continued research is needed to improve these models. Future work should focus on integrating deep learning methods like Convolutional Neural Networks (CNNs) and applying real-time detection to stay ahead of phishing threats.

As phishing attacks evolve, models must also evolve, necessitating continuous learning systems and improved feature engineering. The integration of machine learning with real-time threat intelligence systems may offer enhanced detection capabilities, making it an area ripe for future research.

REFERENCES

[1] S. Mahdavifar and A. A. Ghorbani, "DeNNeS: deep embedded neural network expert system for detecting cyber attacks," (in English), Neural Computing & Applications, Article; Early Access p. 28.

[2] S. Mishra and D. Soni, "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis," (in English), Future Generation Computer Systems-the International Journal of Escience, Article vol. 108, pp. 803-815, Jul 2020.

[3] K. S. Adewole, T. Hang, W. Q. Wu, H. B. Songs, and A. K. Sangaiah, "Twitter spam account detection based on clustering and classification methods," (in English), Journal of Supercomputing, Article vol. 76, no. 7, pp. 4802-4837, Jul 2020.

[4] B. A. Eduardo, F. D. Walter, and S. G. Sandra, "An Experiment to Create Awareness in People concerning Social Engineering Attacks," (in Spanish), Ciencia Unemi, Article vol. 13, no. 32, pp. 27-40, Jan-Apr 2020.

[5] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," (in English), Expert Systems with Applications, Article vol. 150, p. 11, Jul 2020, Art. no. 113318.

[6] S. Modi, Y. K. Mali, V. Borate, A. Khadke, S. Mane and G. Patil, "Skin Impedance Technique to Detect Hand-Glove Rupture," 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, 2023, pp. 309-313, doi: 10.1109/OCIT59427.2023.10430992.

[7] Y. Mali, M. E. Pawar, A. More, S. Shinde, V. Borate and R. Shirbhate, "Improved Pin Entry Method to Prevent Shoulder Surfing Attacks," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306875

[8] A. Chaudhari et al., "Cyber Security Challenges in Social Meta-verse and Mitigation Techniques," 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon), Pune, India, 2024, pp. 1-7, doi: 10.1109/MITADTSoCiCon60330.2024.10575295.

[9] Y. K. Mali and A. Mohanpurkar, "Advanced pin entry method by resisting shoulder surfing attacks," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 37-42, doi: 10.1109/INFOP.2015.7489347 '.

[10] Y. K. Mali, S. A. Darekar, S. Sopal, M. Kale, V. Kshatriya and A. Palaskar, "Fault Detection of Underwater Cables by Using Robotic Operating System," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10474270.

[11] A. Chaudhari, S. Dargad, Y. K. Mali, P. S. Dhend, V. A. Hande and S. S. Bhilare, "A Technique for Maintaining Attribute-based Privacy Implementing Blockchain and Machine Learning," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-4, doi: 10.1109/ICCST59048.2023.10530511.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

[12] Y. K. Mali, S. Dargad, A. Dixit, N. Tiwari, S. Narkhede and A. Chaudhari, "The Utilization of Block-chain Innovation to Confirm KYC Records," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-5, doi: 10.1109/ICCST59048.2023.10530513.
[13] V. Borate, Y. Mali, V. Suryawanshi, S. Singh, V. Dhoke and A. Kulkarni, "IoT Based Self Alert Generating Coal Miner Safety Helmets," 2023 International Conference on Computational Intelligence, Networks and Security (ICCINS), Mylavaram, India, 2023, pp. 01-04, doi: 10.1109/ICCINS58907.2023.10450044.
[14] M. Dangore, A. S. R, A. Ghanashyam Chendke, R. Shirbhate, Y. K. Mali and V. Kisan Borate, "Multi-class Investigation of Acute Lymphoblastic Leukemia using Optimized Deep Convolutional Neural Network on Blood Smear Images," 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon), Pune, India, 2024, pp. 1-6, doi: 10.1109/MITADTSoCiCon60330.2024.10575245.
[15] N. P. Mankar, P. E. Sakunde, S. Zurange, A. Date, V. Borate and Y. K. Mali, "Comparative Evaluation of Machine Learning Models for Malicious URL Detection," 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon), Pune, India, 2024, pp. 1-7, doi: 10.1109/MITADTSoCiCon60330.2024.10575452.
[16] M. D. Karajgar et al., "Comparison of Machine Learning Models for Identifying Malicious URLs," 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS), Bangalore, India, 2024, pp. 1-5, doi: 10.1109/ICITEICS61368.2024.10625423.
[17] J. Pawar, A. A. Bhosle, P. Gupta, H. Mehta Shiyal, V. K. Borate and Y. K. Mali, "Analyzing Acute Lymphoblastic Leukemia Across Multiple Classes Using an Enhanced Deep Convolutional Neural Network on Blood Smear," 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/ICITEICS61368.2024.10624915.
[18] D. R. Naik, V. D. Ghonge, S. M. Thube, A. Khadke, Y. K. Mali and V. K. Borate, "Software-Defined-Storage Performance Testing Using Mininet," 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS), Bangalore, India, 2024, pp. 1-5, doi: 10.1109/ICITEICS61368.2024.10625153.
[19] A. O. Vaidya, M. Dangore, V. K. Borate, N. Raut, Y. K. Mali and A. Chaudhari, "Deep Fake Detection for Preventing Audio and Video Frauds Using Advanced Deep Learning Techniques," 2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Kothamangalam, Kerala, India, 2024, pp. 1-6, doi: 10.1109/RAICS61201.2024.10689785.
[20] Bhongade, A., Dargad, S., Dixit, A., Mali, Y.K., Kumari, B., Shende, A. (2024). Cyber Threats in Social Metaverse and Mitigation Techniques. In: Somani, A.K., Mundra, A., Gupta, R.K., Bhattacharya, S., Mazumdar, A.P. (eds) Smart Systems: Innovations in Computing. SSIC 2023. Smart Innovation, Systems and Technologies, vol 392. Springer, Singapore. https://doi.org/10.1007/978-981-97-3690-4_34.
[21] Sawardekar, S., Mulla, R., Sonawane, S., Shinde, A., Borate, V., Mali, Y.K. (2025). Application of Modern Tools in Web 3.0 and Blockchain to Innovate Healthcare System. In: Rawat, S., Kumar, A., Raman, A., Kumar, S., Pathak, P. (eds) Proceedings of Third International Conference on Computational Electronics for Wireless Communications. ICCWC 2023. Lecture Notes in Networks and Systems, vol 962. Springer, Singapore. https://doi.org/10.1007/978-981-97-1946-4_2
[22] Mali, Y., & Chapte, V. (2014). Grid based authentication system, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014 pg. 93-99, 2(10).
[23] Yogesh Mali, Nilay Sawant, "Smart Helmet for Coal Mining", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 3, Issue 1, February 2023, DOI: 10.48175/IJARSCT-8064
[24] Pranav Lonari, Sudarshan Jagdale, Shraddha Khandre, Piyush Takale, Prof Yogesh Mali, "Crime Awareness and Registration System ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.287-298, May-June-2021.
[25] Jyoti Pathak, Neha Sakore, Rakesh Kapare , Amey Kulkarni, Prof. Yogesh Mali, "Mobile Rescue Robot", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4, Issue 8, pp.10-12, September-October-2019.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

[26] Devansh Dhote , Piyush Rai , Sunil Deshmukh, Adarsh Jaiswal, Prof. Yogesh Mali, "A Survey : Analysis and Estimation of Share Market Scenario ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4, Issue 8, pp.77-80, September-October-2019.
[27] Rajat Asreddy, Avinash Shingade, Niraj Vyavhare, Arjun Rokde, Yogesh Mali, "A Survey on Secured Data Transmission Using RSA Algorithm and Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4, Issue 8, pp.159-162, September-October-2019
[28] Shivani Chougule, Shubham Bhosale, Vrushali Borle, Vaishnavi Chaugule, Prof. Yogesh Mali, "Emotion Recognition Based Personal Entertainment Robot Using ML & IP", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X, Volume 5, Issue 8, pp.73-75, November-December-2020.
[29] Amit Lokre, Sangram Thorat, Pranali Patil, Chetan Gadekar, Yogesh Mali, " Fake Image and Document Detection using Machine Learning", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X, Volume 5, Issue 8, pp.104-109, November-December-2020.
[30] Ritesh Hajare, Rohit Hodage, Om Wangwad, Yogesh Mali, Faraz Bagwan, "Data Security in Cloud", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.240-245, May-June-2021
[31] Yogesh Mali and Tejal Upadhyay, "Fraud Detection in Online Content Mining Relies on the Random Forest Algorithm", SWB, vol. 1, no. 3, pp. 13–20, Jul. 2023, doi: 10.61925/SWB.2023.1302.
[32] Mali, Y. K., Rathod, V. U., Borate, V. K., Chaudhari, A., & Waykole, T. (2023, June). Enhanced Pin Entry Mechanism for ATM Machine by Defending Shoulder Surfing Attacks. In International Conference on Recent Developments in Cyber Security (pp. 515-529). Singapore: Springer Nature Singapore.
[33] Mali, Y. K., Rathod, V., Dargad, S., & Deshmukh, J. Y. (2024). Leveraging Web 3.0 to Develop Play-to-Earn Apps in Healthcare using Blockchain. In Computational Intelligence and Blockchain in Biomedical and Health Informatics (pp. 243-257). CRC Press.
[34] Deshmukh, J. Y., Rathod, V. U., Mali, Y. K., & Sable, R. (2024). and Classification. Data-Centric Artificial Intelligence for Multidisciplinary Applications, 114.
[35] Sawant, M. M., Nagargoje, Y., Bora, D., Shelke, S., & Borate, V. (2013). Keystroke Dynamics. International Journal of Advanced Research in Computer and Communication Engineering, 2(10), 4018-4020.
[36] Ingale, N., Jha, T. A., Dixit, R., & Borate, V. K. (2021). College enquiry Chatbot using rasa. College Enquiry ChatBot Using RASA.
[37] Patil, Yash, Mihir Paun, Deep Paun, Karunesh Singh, and Vishal Kisan Borate. "Virtual painting with OpenCV using Python." International Journal of Scientific Research in Science and Technology 5, no. 8 (2020): 189-194.
[38] Borate, V. K., & Giri, S. (2015, January). XML duplicate detection with improved network pruning algorithm. In 2015 International Conference on Pervasive Computing (ICPC) (pp. 1-5). IEEE.
[39] Shabina Modi, Sunita Mane, Sakshi Mahadik, Rutuja Kadam, Rutuja Jambhale, Sampada Mahadik, & Yogesh Mali. (2024). Automated Attendance Monitoring System for Cattle through CCTV. Revista Electronica De Veterinaria, 25(1), 1025 -1034. https://doi.org/10.69980/redvet.v25i1.724
[40] Sawardekar, S., Mulla, R., Sonawane, S., Shinde, A., Borate, V., & Mali, Y. K. (2023, December). Application of Modern Tools in Web 3.0 and Blockchain to Innovate Healthcare System. In International Conference on Computational Electronics for Wireless Communications (ICCWC) (pp. 1-12). Singapore: Springer Nature Singapore.
[41] A. More, S. R. Shinde, P. M. Patil, D. S. Kane, Y. K. Mali and V. K. Borate, "Advancements in Early Detection of Lung Cancer using YOLOv7," 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024, pp. 1739-1746, doi: 10.1109/ICOSEC61587.2024.10722534.