IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

Machine Learning-Powered Protection Against Phishing Crimes

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 are a serious cybersecurity risk that uses phony emails, websites, or messages to target users and organizations in an attempt to steal confidential data. By examining data patterns and spotting questionable activity, machine learning (ML) offers creative ways to identify and stop these attacks. This study examines several machine learning (ML) techniques for phishing detection, including Principal Component Analysis (PCA), Random Forest (RF), and Decision Trees (DT). According to studies, RF models are very effective and can attain up to 97% accuracy. But there are still issues with feature extraction, data imbalance, and changing phishing strategies. Phishing detection capabilities can be further improved by incorporating real-time detection systems, hybrid approaches, and sophisticated deep learning models. Additionally, to increase detection accuracy and reduce detection errors, cybersecurity researchers and organizations must collaborate and update datasets continuously.*

Keywords: *Phishing attack, machine learning, Random Forest, decision tree, Principal Component Analysis, Cyber-security, deep learning*

I. INTRODUCTION

Cyber-security threats have become a growing concern in the digital era, with phishing being one of the most prevalent and damaging attack methods. Phishing involves cybercriminals impersonating legitimate organizations to deceive users into revealing sensitive information, such as login credentials, banking details, and personal data. These attacks exploit human psychology and trust, making them highly effective and difficult to detect.

With the rapid expansion of online platforms, phishing tactics have evolved significantly. Attackers now leverage social media, fraudulent websites, and sophisticated email campaigns to trick individuals and businesses. Spearphishing and whaling attacks, which target specific high-profile individuals, have also gained traction, posing a significant threat to organizations' security. Given the dynamic nature of phishing attacks, traditional defence mechanisms such as rule-based systems, blacklists, and manual monitoring have proven inadequate. These methods struggle to keep up with new attack variations, leading to increased vulnerability.

Machine Learning (ML) has emerged as a powerful solution for detecting phishing attempts by analysing complex patterns and anomalies in large datasets. Unlike traditional methods, ML models can dynamically adapt to new attack strategies and detect phishing websites or emails with high accuracy. Algorithms such as Random Forest (RF), Decision Trees (DT), and Principal Component Analysis (PCA) have demonstrated remarkable effectiveness, often achieving detection rates exceeding 95%. ML-powered phishing detection systems can operate in real-time, reducing response time and minimizing the impact of attacks.

II. LITERATURE SURVEY

Paper [1] proposed a deep embedded neural network expert system (DeNNeS) combining deep learning with rule-based logic for cyberattack detection. The Smishing Detector in [2] analyzed SMS and URLs, while [3] introduced a hybrid

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

clustering-classification method using PCA and K-means for phishing spam detection on Twitter. User awareness as a defense was studied in [4], and [5] applied machine learning to detect illicit accounts on the Ethereum blockchain.

Paper [6] proposed robust feature extraction for phishing URL detection using machine learning. Blockchain-based smart contracts were used to replace email protocols in [7], and [8] addressed children's phishing threats using content filtering with ML. Hard disk encryption for phishing protection was discussed in [9], while improved performance through URL feature selection was explored in [10].

Paper [11] proposed the Random Forest algorithm as most effective among traditional models. A deep learning-based detection system was developed in [12], followed by a multi-filter ML approach in [13]. URL consistency was emphasized in [14], and [15] analyzed the link between personality traits and phishing susceptibility.

Paper [16] proposed privacy-preserving mechanisms for phishing detection on big data. A distributed deep learning model for phishing on IoT was built in [17], while [18] used sine-cosine algorithms with ANNs. A knowledge-based system for IoT phishing detection appeared in [19], and logo detection via HOG features was applied in [20].

Paper [21] proposed SDN-based deep learning detection for phishing. A Botnet detection approach with ML and phishing overlap was discussed in [22]. A hybrid belief-rule and ML model was introduced in [23], and belief-rule systems were extended for phishing in [24]. Data warehousing for phishing detection was considered in [25], though limited in real-time scenarios.

Paper [26] proposed reusing ML techniques from vehicle tracking for phishing detection. Expert system logic was adapted by changing input features in [27]. Spatio-temporal crime analysis in [28] was recommended for phishing hotspot detection, and anomaly detection was used in [29] with high false positives. Hybrid ML models integrating heuristic features were developed in [30].

Paper [31] proposed ensemble learning models for imbalanced phishing data. Reinforcement learning was used in [32] to adapt phishing detection to evolving threats. Semantic phishing detection with NLP was implemented in [33], and lightweight ML models for mobile phishing detection were developed in [34]. Graph-based detection methods were discussed in [35].

Paper [36] proposed a retraining strategy to keep phishing models current. Adversarial training for robust phishing defense was introduced in [37], while a multimodal detection strategy was presented in [38]. Federated learning in [39] supported privacy-preserving training. Transfer learning from sentiment analysis was used in [40].

Paper [41] proposed visual similarity detection for brand-mimicking phishing sites. Language-independent detection across regions was implemented in [42], and clone site detection through image recognition appeared in [43]. Behavioral signals like urgency and authority to detect phishing threats were explored in [44].

III. METHODOLOGY

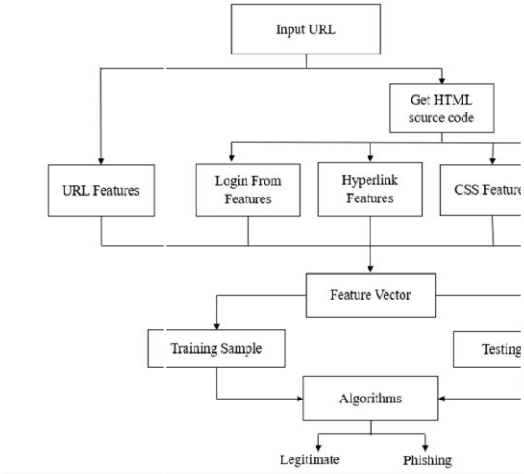


Fig.1

DOI: 10.48175/IJARSCT-27946

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

The above figure illustrates a methodical approach to machine learning-based phishing attack detection. Here's a detailed explanation:

Input URL:

The URL of the website that needs to be examined for possible phishing is supplied by the user.

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.).

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

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

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

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

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

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

IV. ARCHITECTURE

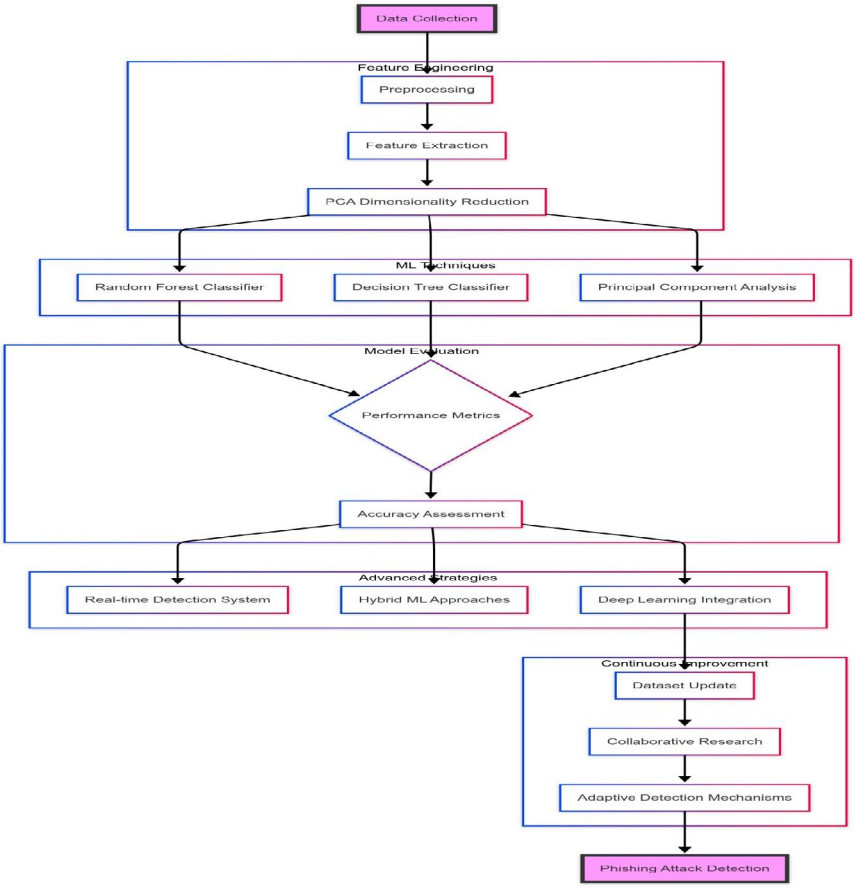


Fig.2

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

This diagram represents a Phishing Attack Detection System using Machine Learning. It outlines the entire pipeline from data collection to detection, including feature engineering, machine learning techniques, evaluation, and continuous improvement. Here's a brief breakdown:

Data Collection – Raw data is gathered from various sources.

Feature Engineering – Includes pre-processing and feature extraction.

Dimensionality Reduction (PCA) – Principal Component Analysis (PCA) is used to reduce the complexity of data.

Machine Learning Techniques – Different classifiers like Random Forest, Decision Tree, and PCA-based methods are applied.

Model Evaluation – Performance metrics are assessed for accuracy.

Accuracy Assessment – Determines the effectiveness of the model.

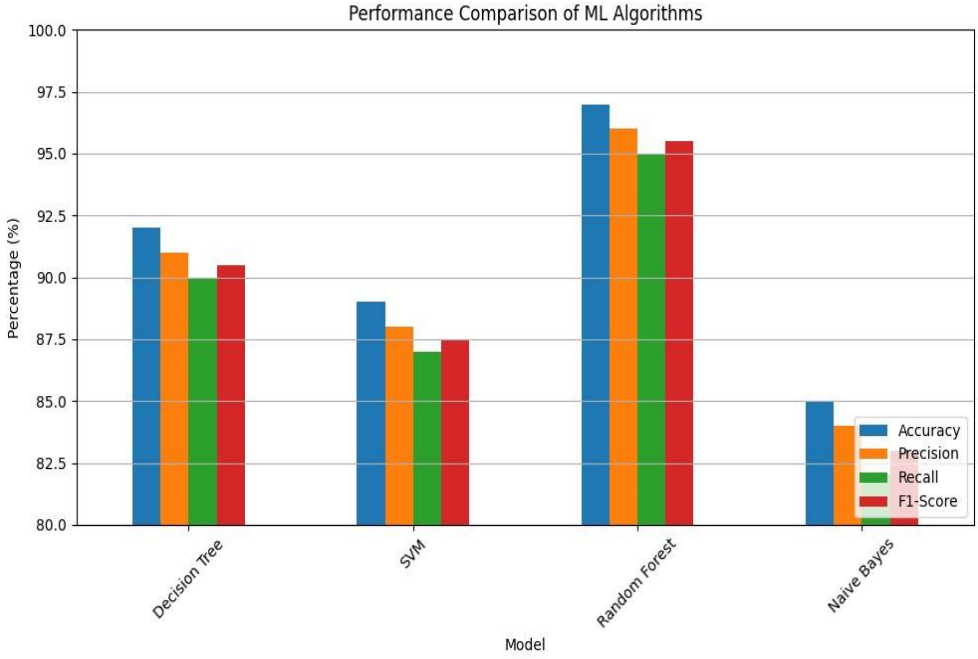
Advanced Strategies – Includes Real-time Detection, Hybrid ML approaches, and Deep Learning Integration.

Continuous Improvement – Regular dataset updates, collaborative research, and adaptive detection mechanisms.

Final Outcome – A robust Phishing Attack Detection System.

V. RESULT AND ANALYSIS

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:



Graph 1: Analysis of Algorithms

Table analysis based on the bar graph titled **"Performance Comparison of ML Algorithms"** (values are approximate from the image):

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	92	91	90	90.5
SVM	89	88	87	87.5

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

Random Forest	97	96	95	95.5
Naive Bayes	85	84	82	83

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 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

We presented a protective mechanism that evaluated three ML algorithm approaches to malware detection and chose the most appropriate one. The results show that compared with other classifiers, XGBoost (99%) and SVM (96.41%) performed well in terms of detection accuracy. XGBoost and SVM algorithms' performances detecting malware on a small FPR (XGBoost = 2.01%, and SVM = 4.63%,) in a given dataset were compared. In this experiment, we evaluated and quantified the detection accuracy of a machine learning (ML) classifier that used static analysis to extract features based on PE data by comparing it to two other ML classifiers. As a result of our efforts, machine learning algorithms can now identify dangerous versus benign data. The XGBoost machine learning method had the highest accuracy (99%) of any classifier we evaluated. In addition to potentially providing the highest detection accuracy and accurately characterizing malware, static analysis based on PE information and carefully selected data showed promise in experimental findings. That we do not have to execute anything to determine if data are malicious is a significant benefit, we presented a protective mechanism that evaluated three ML algorithm approaches to malware detection and chose the most appropriate one. The results show that compared with other classifiers, XGBoost (99%), and SVM (96.41%) performed well in terms of detection accuracy. XGBoost and SVM algorithms' performances detecting malware on a small FPR (XGBoost = 2.01%, and SVM = 4.63%,) in a given dataset were compared. In this experiment, we evaluated and quantified the detection accuracy of a machine learning (ML) classifier that used static analysis to extract features based on PE data by comparing it to two other ML classifiers. As a result of our efforts, machine learning algorithms can now identify dangerous versus benign data. The XGBoost machine learning method had the highest accuracy (99%) of any classifier we evaluated. In addition to potentially providing the highest detection accuracy and accurately characterizing malware, static analysis based on PE information and carefully selected data showed promise in experimental findings. That we do not have to execute anything to determine if data are malicious, is a significant benefit.

VI. 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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 6, June 2025 Impact Factor: 7.67

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.

Phishing continues to be a critical threat in the cybersecurity landscape, exploiting human behavior and technical vulnerabilities to steal sensitive data. Machine learning has proven to be a powerful countermeasure, with models such as Random Forest, Decision Tree, and XGBoost demonstrating high accuracy in detecting phishing attacks. However, the constantly evolving nature of phishing techniques necessitates adaptive and intelligent defense systems that go beyond static rule-based detection.

REFERENCES

[1]. Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav, Arya Zunjarrao, "A Role of Machine Learning Algorithms for Lung Disease Prediction and Analysis," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 3, pp. 425-434, October 2024, DOI: 10.48175/IJARSCT-19962.

[2]. V. K. Borate and S. Giri, "XML Duplicate Detection with Improved network pruning algorithm," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-5, doi: 10.1109/PERVASIVE.2015.7087007.

[3]. Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "Analysis of Malware Detection Using Various Machine Learning Approach," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 314-321, November 2024, DOI: 10.48175/IJARSCT-22159.

[4]. Borate, Mr Vishal, Alpana Adsul, Mr Rohit Dhakane, Mr Shahuraj Gawade, Ms Shubhangi Ghodake, and Mr Pranit Jadhav. "A Comprehensive Review of Phishing Attack Detection Using Machine Learning Techniques," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 435-441, October 2024 DOI: 10.48175/IJARSCT-19963.

[5]. Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar, Vishakha T. Mandage and Prof. Vishal K BBorate, FIRE ALARM AND RESCUE SYSTEM USING IOT AND ANDROID", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 2, Page No pp.815-821, May 2024.

[6]. Prof. Vishal Borate, Prof. Aaradana Pawale, Ashwini Kotagonde,Sandip Godase and Rutuja Gangavne, "Design of low-cost Wireless Noise Monitoring Sensor Unit based on IOT Concept", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.10, Issue 12, page no.a153-a158, December-2023.

[7]. Dnyanesh S. Gaikwad, Vishal Borate, "A REVIEW OF DIFFERENT CROP HEALTH MONITORING AND DISEASE DETECTION TECHNIQUES IN AGRICULTURE", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.10, Issue 4, Page No pp.114-117, November 2023.

[8]. Prof. Vishal Borate, Vaishnavi Kulkarni and Siddhi Vidhate, "A Novel Approach for Filtration of Spam using NLP", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.10, Issue 4, Page No pp.147-151, November 2023.

[9]. Prof. Vishal Borate, Kajal Ghadage and Aditi Pawar, "Survey of Spam Comments Identification using NLP Techniques", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.10, Issue 4, Page No pp.136-140, November 2023.

[10]. Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar and Prof. Vishal K Borate, "Fire Evacuation System Using IOT & AI", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 23481269, P- ISSN 2349-5138, Volume.10, Issue 4, Page No pp.176-180, November 2023.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 6, June 2025 Impact Factor: 7.67

[11]. Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.51-56, May-June-2021.
[12]. Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.201-206, May-June-2021.
[13]. Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor, Mr Vishal Kisan Borate and Mr Prashant Laxmanrao Mandale, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.212-215, May-June-2021.
[14]. Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter"" International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395-602X, Volume 5, Issue 8, pp.80-84, December-2020.
[15]. Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395-602X, Volume 5, Issue 8, pp.210-215, December-2020.
[16]. Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor and Mr Vishal Kisan Borate, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395-602X, Volume 5, Issue 8, pp.221-226, December-2020.
[17]. Chame Akash Babasaheb, Mene Ankit Madhav, Shinde Hrushikesh Ramdas, Wadagave Swapnil Sunil, Prof. Vishal Kisan Borate, " IoT Based Women Safety Device using Android, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.153-158, March-April-2020.
[18]. Harshala R. Yevlekar, Pratik B. Deore, Priyanka S. Patil, Rutuja R. Khandebharad, Prof. Vishal Kisan Borate, " Smart and Integrated Crop Disease Identification System, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.189-193, March-April-2020.
[19]. Yash Patil, Mihir Paun, Deep Paun, Karunesh Singh, Vishal Kisan Borate, " Virtual Painting with Opencv Using Python, International Journal of Scientific Research in Science and Technology(IJSRST), Online ISSN : 2395602X, Print ISSN : 2395-6011, Volume 5, Issue 8, pp.189-194, November-December-2020.
[20]. Mayur Mahadev Sawant, Yogesh Nagargoje, Darshan Bora, Shrinivas Shelke and Vishal Borate, Keystroke Dynamics: Review Paper International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 10, October 2013.
[21]. Modi, S., Sale, D., Borate, V., Mali, Y.K. (2025). Enhancing Learning Outcomes Through the Use of Conducive Learning Spaces. In: Majumder, M., Zaman, J.K.M.S.U., Ghosh, M., Chakraborty, S. (eds) Computational Technologies and Electronics. ICCTE 2023. Communications in Computer and Information Science, vol 2376. Springer, Cham. https://doi.org/10.1007/978-3-031-81935-3_4.
[22]. 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.
[23]. Nadaf, N., Waghodekar, P., Magdum, A., Gupta, P., Borate, V.K., Mali, Y.K. (2025). Architecture for CostEffective Deployment of Models to Transfer Style Across Images. In: Shukla, P.K., Bhatt, A., Mittal, H., Engelbrecht, A. (eds) Computer Vision and Robotics. CVR 2024. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-97-8868-2_44.
[24]. Modi, S., Mali, Y., Sharma, L., Khairnar, P., Gaikwad, D.S., Borate, V. (2024). A Protection Approach for Coal Miners Safety Helmet Using IoT. In: Jain, S., Mihindukulasooriya, N., Janev, V., Shimizu, C.M. (eds) Semantic Intelligence. ISIC 2023. Lecture Notes in Electrical Engineering, vol 1258. Springer, Singapore. https://doi.org/10.1007/978-981-97-7356-5_30

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

[25]. Waghodekar, P. et al. (2025). Security Protecting Confirmation of IoMT in Distributed Cloud Computing. In: Shukla, P.K., Bhatt, A., Mittal, H., Engelbrecht, A. (eds) Computer Vision and Robotics. CVR 2024. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-97-8868-2_3

[26]. Rojas, Macedo, and Yolaina Malí. "Programa de sensibilización sobre norma técnica de salud N° 096 MINSA/DIGESA V. 01 para la mejora del manejo de residuos sólidos hospitalarios en el Centro de Salud Palmira, Independencia-Huaraz, 2017." (2017).

[27]. Sale, D., Khare, N., Kadam, S., Mali, Y.K., Borate, V., Gaur, A. (2025). A Secure Pin Entry Mechanism for Online Banking by Defending Shoulder-Surfing Attacks. In: Kumar, S., Mary Anita, E.A., Kim, J.H., Nagar, A. (eds) Fifth Congress on Intelligent Systems. CIS 2024. Lecture Notes in Networks and Systems, vol 1278. Springer, Singapore. https://doi.org/10.1007/978-981-96-2703-5_4

[28]. Rathod, V.U., Nandgoankar, V., Dhawas, N., Mali, Y.K., Chaudhari, H., Patil, D. (2025). Smart Traffic Light Management System Using IoT and Deep Learning. In: Singh, S., Arya, K.V., Rodriguez, C.R., Mulani, A.O. (eds) Emerging Trends in Artificial Intelligence, Data Science and Signal Processing. AIDSP 2023. Communications in Computer and Information Science, vol 2439. Springer, Cham. https://doi.org/10.1007/978-3-031-88759-8_9. [29]. Kale, Hrushikesh, Kartik Aswar, and Dr Yogesh Mali Kisan Yadav. "Attendance Marking using Face Detection." International Journal of Advanced Research in Science, Communication and Technology: 417-424. [30]. Inamdar, Faizan, Dev Ojha, C. J. Ojha, and D. Y. Mali. "Job Title Predictor System." International Journal of Advanced Research in Science, Communication and Technology (2024): 457-463.

[31]. Jagdale, Sudarshan, Piyush Takale, Pranav Lonari, Shraddha Khandre, and Yogesh Mali. "Crime Awareness and Registration System." International Journal of Scientific Research in Science and Technology 5, no. 8 (2020). [32]. Suoyi, Han, Yang Mali, Chen Yuandong, Yu Jingjing, Zhao Tuanjie, Gai Junyi, and Yu Deyue. "Construction of mutant library for soybean'Nannong 94-16'and analysis of some characters." Acta Agriculturae Nucleatae Sinica 22 (2008).

[33]. Van Wyk, Eric, and Yogesh Mali. "Adding dimension analysis to java as a composable language extension." In International Summer School on Generative and Transformational Techniques in Software Engineering, pp. 442456. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[34]. Mali, Yogesh, Vijay U. Rathod, Ravindra S. Tambe, Radha Shirbhate, Deepika Ajalkar, and Priti Sathawane. "Group-Based Framework for Large Files Downloading." In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-4. IEEE, 2023.

[35]. Modi, Shabina, Deepali Sale, Vishal Borate, and Yogesh Kisan Mali. "Enhancing learning outcomes through the use of conducive learning spaces." In International Conference on Computational Technologies and Electronics, pp. 45-53. Cham: Springer Nature Switzerland, 2023.

[36]. Mali, Yash, Himani Malani, Nishad Mahore, and Rushikesh Mali. "Hand Gesture Controlled Mouse." International Research Journal of Engineering and Technology (2022).

[37]. Gai Mali, Yustinus Calvin. "The exploration of Indonesian students' attributions in EFL reading and writing classes." Bahasa dan Seni: Jurnal Bahasa, Sastra, Seni, dan Pengajarannya 50, no. 1 (2022): 1.

[38]. Mali, Y. "Effort attributions in Indonesian EFL classrooms." Jurnal Ilmu Pendidikan 22, no. 1 (2016): 80-93.

[39]. Malî, Yôsef, ed. Narrative patterns in scientific disciplines. Cambridge University Press, 1994.

[40]. Das et al., "Antibiotic susceptibility profiling of Pseudomonas aeruginosa in nosocomial infection," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-5, doi: 10.1109/ICCCNT61001.2024.10723982.

[41]. Dhokale, Bhalchandra D., and Ramesh Y. Mali. "A Robust Image Watermarking Scheme Invariant to Rotation, Scaling and Translation Attack using DFT." International Journal of Engineering and Advanced Technology 3, no. 5 (2014): 269.

[42]. Yogesh Mali, NilaySawant, "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/IJARSCT8064

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

[43]. Mali, Yash, Anuja Tambade, Mrunmayi Magdum, and B. G. Patil. "Artificial Neural Network Based Automatic Number Plate Recognition System." International Journal on Recent and Innovation Trends in Computing and Communication 4, no. 5 (2016): 128-131.
[44]. Mali, Y., and E. Deore. "Design and Analysis with Weight Optimization of Two Wheeler Gear Set." International Advanced Research journal in Science, Engineering and Technology 4, no. 7 (2017)