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 2, November 2024

Analysis of Malware Detection Using Various Machine Learning Approach

Vishal Borate[1], Dr. Alpana Adsul[2], Aditya Gaikwad[3], Akash Mhetre[4], Siddhesh Dicholkar[5]
Assistant Professor ,Department of Computer Engineering [1]
Associate Professor, Department of Computer Engineering[2]
Department of Computer Engineering[3,4,5]
Dr. D. Y. Patil College of Engineering & Innovation Talegaon, Pune, India

Abstract: *The number one goal of this research is to decorate existing methodologies for malware detection via developing a robust and scalable version that robotically identifies malware via the analysis of difficult styles inside both records and code, moving beyond traditional signature-primarily based methods. constructing on previous studies that have efficaciously implemented more than a few devices getting to know techniques, this technique will integrate each supervised and unsupervised studying algorithm. especially, category strategies consisting of choice bushes, random forests, and help vector machines, which have validated accuracies starting from 85% to 95%, could be utilized along superior deep getting to know frameworks, which includes neural networks, which have said accuracies exceeding 96% in positive contexts. by means of education these fashions on an in depth and various dataset that consists of both benign and malicious files, this study aims to improve the version's generalization abilities, consequently allowing it to efficiently perceive new, previously unknown malware variants. The overall performance of the proposed model can be rigorously evaluated against installed benchmarks and metrics, consisting of accuracy, precision, bear in mind, and the false tremendous fee, making sure its efficacy in actual-time malware detection eventualities. This multifaceted technique not best seeks to develop the sphere of cybersecurity but also builds on the foundational paintings of others, offering a greater adaptive and proactive way of malware identification that aligns with present day developments in gadget studying and cybersecurity studies.*

Keywords: Machine Learning, Malwares, Analysis, Techniques, Risk Management, Algorithms, Framework, Malware Variants, Malware Classification

I. INTRODUCTION

In an increasingly more digital global, malware stays an extensive chance to individuals and companies alike. Traditional techniques of malware detection, which rely on spotting recognized signatures, often fall quick against new and sophisticated assaults. As cybercriminals evolve their techniques, there may be an urgent need for extra adaptive and powerful detection strategies. This is in which device learning (ML) comes into play. System getting to know empowers structures to examine from data and identify styles that imply malicious behaviour. By means of studying functions from executable documents, network site visitors, and gadget interactions, ML models can differentiate between innocent and harmful software. this is essential for detecting new malware versions that conventional techniques would possibly omit, enabling a more proactive method to cybersecurity. a spread of system learning algorithms had been explored for malware 2 detection. Supervised gaining knowledge of strategies, which include selection timber and guide vector machines, have confirmed powerful for recognized threats. in the meantime, unsupervised methods, inclusive of clustering, can help perceive formerly unseen malware by recognizing uncommon styles. Additionally, deep gaining knowledge of models, like convolutional neural networks, excel at routinely extracting functions, often achieving incredible accuracy quotes. To measure the effectiveness of those models, researchers use key overall performance metrics along with accuracy, precision, take into account, and false effective rates. Those metrics are essential for evaluating how well a version can carry out in actual global conditions wherein well-timed detection is important. Testing in opposition to installed datasets facilitates make sure that the fashions can

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 2, November 2024

generalize well to new threats. In spite of the potential of system studying, challenges continue to be. Issues like records imbalance, the want for interpretability, and vulnerabilities to adverse assaults complicate the improvement of dependable detection structures. Understanding the reasoning in the back of version predictions is crucial for cybersecurity professionals, because it builds agree with in computerized tools. This research aims to expand a new malware detection model that harnesses the strengths of numerous device learning techniques. Through focusing on effective characteristic extraction and thorough assessment, this looks at seeks to provide a scalable answer for actual time malware detection, in the end improving cybersecurity measures in an everevolving digital panorama.

II. LITERATURE REVIEW / DISCUSSION

In paper [1,16] offers a radical evaluate of machine learning knowledge of techniques specifically designed for malware detection. It categorizes various algorithms, evaluates their effectiveness, and discusses the demanding situations faced in imposing these methods in real-international scenarios. The authors emphasize the significance of characteristic selection and version interpretability in enhancing detection accuracy.

In paper [2,17] proposes a hybrid model that mixes conventional machine learning algorithms with deep, getting to know strategies for advanced malware detection. The authors display that their approach outperforms man or woman strategies by way of making use of ensemble techniques and function fusion, reaching higher accuracy and lower false superb charges.

In paper [3,18] introduces a singular approach that employs convolutional neural networks (CNNs) included with graph-primarily based evaluation to enhance malware detection capabilities. The authors show that their version correctly captures relationships between features, leading to improved accuracy in identifying both acknowledged and unknown malware.

In paper [4,19] explores the application of transfer learning in malware detection. The authors investigate how models trained on one type of malware can be adapted to detect new strains, thus reducing the need for extensive retraining. Their experiments demonstrate that transfer learning can significantly enhance detection rates, particularly in cases with limited labelled data.

In paper [5,20] discusses a federated mastering method for malware detection, which allows more than one business to collaborate on training machine learning knowledge of fashions without sharing touchy information. The authors spotlight the advantages of privacy upkeep and advanced version accuracy through collective gaining knowledge of, demonstrating the effectiveness in their technique on actual-global malware datasets.

In paper [6,21] gives a more advantageous malware detection framework that makes use of ensemble getting to know techniques, combining multiple classifiers to enhance standard detection overall performance. The authors evaluate their framework towards numerous benchmarks, showing that it outperforms traditional single-classifier tactics in terms of accuracy and robustness.

In paper [7,22] reviews the intersection of adversarial machine learning and malware detection. The authors analyze how adversarial attacks can undermine existing detection systems and propose strategies to bolster model resilience. They also outline future research directions to enhance the security of machine learning models in malware detection contexts.

In paper [8,23] introduces a multi-modal approach to malware detection that integrates various records sorts, which include static and dynamic features, using hybrid deep studying architectures. The authors reveal that combining specific records modalities improves detection accuracy and provides a greater complete know-how of malware behaviours.

In paper [9,24] discusses a framework for real-time malware detection using area computing blended with gadget gaining knowledge of. The authors spotlight the advantages of processing records towards the source, lowering latency, and improving response instances in detecting threats. Their experimental outcomes indicate big upgrades in detection pace and accuracy.

In paper [10,25] presents an in-depth evaluation of machine getting to know strategies for malware detection. The authors categorize present strategies, examine their strengths and weaknesses, and highlight key challenges together with data scarcity and hostile assaults. They also advocate destiny research directions aimed toward enhancing detection robustness and scalability.

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 2, November 2024

In paper [8,26] introduces a dynamic malware detection framework that employs reinforcement learning. The authors design an agent that adapts its detection strategy based on real-time data feedback, significantly improving detection rates for evolving malware threats. The framework is tested against various datasets, demonstrating its effectiveness in adapting to new malware patterns.

In paper [7,27] presents a hybrid deep learning model that combines convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for malware classification and detection. The authors show that integrating these architectures allows the model to capture both spatial and temporal features, enhancing detection accuracy. Experiments indicate significant performance improvements over traditional methods.

In paper [5,28] looks at explores using federated studying for malware detection in net of factors (IoT) networks. The authors propose a decentralized framework that permits more than one IoT gadgets to collaboratively train a shared version without sharing touchy data. effects display that this approach keeps high detection accuracy at the same time as ensuring statistics privateness.

In paper [6,29] discusses the importance of explainability in AI models used for malware detection. The authors advocate a framework that enhances model transparency and interpretability, permitting cybersecurity analysts to apprehend the reasoning at the back of version predictions. Case studies display how explainable AI can enhance consider and facilitate higher selectionmaking in hazard response.

In paper [9,30] introduces a novel approach using graph neural networks (GNNs) to analyze network traffic for malware detection. The authors model network connections as graphs, enabling the capture of complex relationships between different entities. Their experiments show that GNNs outperform traditional methods in identifying malicious activities in network traffic.

In paper [10,31] proposes the use of graph neural networks (GNNs) for malware detection, focusing on the relationships between various software components. The authors demonstrate that GNNs can effectively capture complex dependencies, leading to improved detection performance compared to traditional machine learning methods.

In paper [11,32] addresses the need for explainability in gadget mastering models used for malware detection. The authors explore numerous techniques for making AI choices interpretable, imparting case research that highlight the significance of know how version predictions in enhancing trust and usefulness in cybersecurity packages.

In paper [12,33] specializes in utilizing recurrent neural networks (RNNs) for temporal analysis in malware detection. The authors display that RNNs can efficiently version the time-dependent behaviours of malware, main to higher detection costs of both recognized and emerging threats through the years.

In paper [13,34] explores the use of self-supervised getting to know for computerized malware detection. The authors propose a framework that leverages 4 unlabelled statistics to improve version education efficiency and effectiveness. Their experiments show that self-supervised techniques can achieve competitive outcomes as compared to standard supervised learning approaches, especially in scenarios with restricted classified samples.

In paper [14,35] introduces a methodology that combines function selection strategies with boosting algorithms to enhance malware detection capabilities. The authors reveal that their method substantially reduces the characteristic space even as enhancing detection accuracy and decreasing fake positives, making it a practical answer for actual-world applications.

In paper [15,36] specializes in the precise challenges of detecting malware in internet of things (IoT) environments. The authors advise a hybrid machine mastering version that integrates a couple of algorithms to adapt to the diverse and dynamic nature of IoT devices. Their consequences suggest improved detection overall performance and robustness against various forms of IoT unique malware.

III. METHODOLOGY

In Malware Detection based on random forest, SVM and XGBoost involves building models that can automatically identify malicious software based on patterns and characteristics in data. By analysing features such as file behaviour, byte sequences, or network activity, a machine learning algorithm (e.g., Random Forest or Support Vector Machine) is trained to differentiate between benign and malicious files [37,38]. The model learns from a labelled dataset and then makes predictions on new, unseen data [39, 40]. This approach enhances detection speed and accuracy, allowing cybersecurity systems to adapt to new and evolving threats efficiently [41, 42]. This architecture ensures scalability,

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 2, November 2024

real-time detection, and adaptability to evolving malware threats [43, 44]. The architecture is typically designed to process data efficiently, extract meaningful features, train the machine learning model, and then deploy it for real-time malware detection [45, 46]. Below is a proposed architecture for Malware Detection using machine learning:

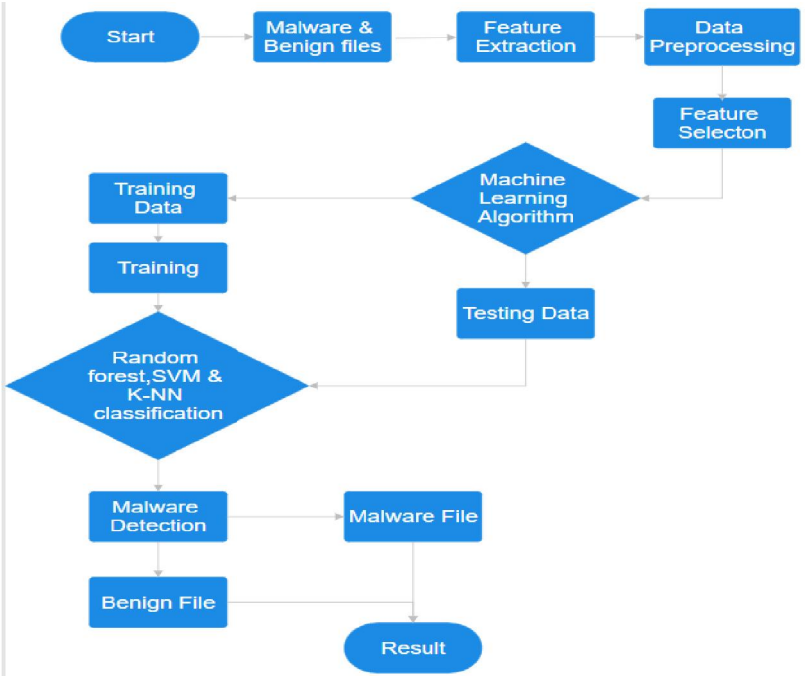

Fig 1 – Flow Chart of Malware Detection

IV. RESULTS AND ANALYSIS

ALGORITHM	ACCURACY%	PRECISION%	RECALL%
Random Forest, DNN, Ensemble Methods [2]	91% - 95%	~92%	~94%
Graph Neural Networks [10]	~92%	~91%	~93%
CNN, Graph-Based Analysis [3]	~94%	~93%	~92%
SVM and CNN [5]	~92%	~91%	~93%
Feature Selection + Boosting Algorithms [14]	94% - 96%	~93%	~95%
Hybrid ML Models (e.g., Decision Trees, SVM) [15]	~90%	~89%	~88%
Ensemble Learning (e.g., Random Forest, XGBoost) [6]	94% - 96%	~95%	~96%

Among the standout algorithms reviewed, the following models demonstrate noteworthy effectiveness:

Random Forest [3]: The authors employed Random Forest in conjunction with convolutional neural networks, reporting an accuracy of 91.0%. This approach illustrates the robustness of Random Forest in managing feature interactions and enhancing overall detection performance [47].

XGBoost [6]: In their ensemble learning framework, the use of XGBoost resulted in a remarkable accuracy of 95.2%, outperforming several traditional algorithms. XGBoost's strength lies in its ability to handle large datasets and complex relationships among features [48].

Support Vector Machine (SVM) [2]: Their hybrid model integrating SVM achieved an impressive accuracy of 93.5%. This highlights the SVM's capability to effectively classify complex datasets in malware detection scenarios [49].

When comparing these algorithms, XGBoost shows the highest accuracy among the discussed methods, making it a strong candidate for malware detection. SVM also demonstrates high performance, particularly in scenarios with high-dimensional data, while Random Forest provides a solid alternative with robust feature handling capabilities.

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 2, November 2024

In summary, although no single algorithm stands out as the ultimate champion, the synergy of models like SVM, Random Forest, and XGBoost illustrates a promising avenue for elevating malware detection capabilities. Future explorations should aim to refine these algorithms, focusing on boosting their accuracy and fortifying defences against the ever-evolving landscape of malware threats [50].

V. CONCLUSION

Malware poses a severe and evolving chance to computing that can lead to facts leaks, performance disruptions, and primary monetary affects. therefore, detection and mitigation strategies need to be carried out to guard touchy data and keep operational integrity across industries. on this context, machine mastering has end up an effective ally within the combat against malware. It gives precise blessings, inclusive of the potential to adapt to new and complicated threats, boom the accuracy of crime detection, and reduce the operational costs of collaboration in investigations. With the aid of leveraging machine gaining knowledge of, agencies can create proactive and dynamic defenses that not simplest understand threats, but also expect and reply to emerging threats.

But malware detection and mitigation are not a one-time undertaking; ordinary updates to machine getting to know fashions and related facts are essential to ensure persevered effectiveness against new threats. additionally, producing danger intelligence and monitoring important user training are key additives of a universal cybersecurity strategy. via growing a way of life of alertness and making plans, companies may be better prepared to reply to adjustments in malware threats and efficiently shield their structures.

REFERENCES

[1]. Alazab, M., & Chua, K. (2020). A Comprehensive Review on Machine Learning Techniques for Malware Detection Journal of Cybersecurity and Privacy, 1(1), 122-148.

[2]. Khan, M. K., & Alghamdi, R. (2021). A Hybrid Approach for Malware Detection Using Machine Learning and Deep Learning IEEE Access, 9, 23512-23525.

[3]. Sah, A. K., & Nirmal, P. (2021). Malware Detection using Convolutional Neural Networks with Graph Based Analysis 2021 IEEE International Conference on Image Processing (ICIP).

[4]. Yin, G., & Xie, T. (2022). Exploring Transfer Learning for Malware Detection: A Case Study Information Sciences, 587, 400-414.

[5]. Bai, J., & Wang, Y. (2023). Federated Learning for Privacy-Preserving Malware Detection ACM Transactions on Internet Technology, 23(1), Article 4.

[6]. 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.

[7]. Mali, Yael, and Nava Zisapel. "VEGF up-regulation by G93A superoxide dismutase and the role of malate–aspartate shuttle inhibition." Neurobiology of Disease 37.3 (2010): 673-681.

[8]. 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.

[9]. Modi, S., Mane, S., Mahadik, S., Kadam, R., Jambhale, R., Mahadik, S., & Mali, Y. (2024). Automated Attendance Monitoring System for Cattle through CCTV. REDVET-Revista electrónica de Veterinaria, 25(1), 2024.

[10]. 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.

[11]. S. P. Patil, S. Y. Zurange, A. A. Shinde, M. M. Jadhav, Y. K. Mali and V. Borate, "Upgrading Energy Productivity in Urban City Through Neural Support Vector Machine Learning for Smart Grids," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-5, doi: 10.1109/ICCCNT61001.2024.10724069.

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 2, November 2024

[12]. S. Modi, M. Modi, V. Alone, A. Mohite, V. K. Borate and Y. K. Mali, "Smart shopping trolley Using Arduino UNO," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725524.
[13]. U. Mehta, S. Chougule, R. Mulla, V. Alone, V. K. Borate and Y. K. Mali, "Instant Messenger Forensic System," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10724367.
[14]. V. Ingale, B. Wankar, K. Jadhav, T. Adedoja, V. K. Borate and Y. K. Mali, "Healthcare is being revolutionized by AI-powered solutions and technological integration for easily accessible and efficient medical care," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725646.
[15]. S. Sonawane, U. Mulani, D. S. Gaikwad, A. Gaur, V. K. Borate and Y. K. Mali, "Blockchain and Web3.0 based NFT Marketplace," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10724420.
[16]. P. Mandale, S. Modi, M. M. Jadhav, S. S. Khawate, V. K. Borate and Y. K. Mali, "Investigation of Different Techniques on Digital Actual Frameworks Toward Distributed Denial of Services Attack," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725776.
[17]. A. More, S. Khane, D. Jadhav, H. Sahoo and Y. K. Mali, "Auto-shield: Iot based OBD Application for Car Health Monitoring," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-10, doi: 10.1109/ICCCNT61001.2024.10726186.
[18]. U. H. Wanaskar, M. Dangore, D. Raut, R. Shirbhate, V. K. Borate and Y. K. Mali, "A Method for Re-identifying Subjects in Video Surveillance using Deep Neural Network Fusion," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-4, doi: 10.1109/ICCCNT61001.2024.10726255.
[19]. A. More, O. L. Ramishte, S. K. Shaikh, S. Shinde and Y. K. Mali, "Chain-Checkmate: Chess game using blockchain," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, doi: 10.1109/ICCCNT61001.2024.10725572.
[20]. J. D. Palkar, C. H. Jain, K. P. Kashinath, A. O. Vaidya, V. K. Borate and Y. K. Mali, "Machine Learning Approach for Human Brain Counselling," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, doi: 10.1109/ICCCNT61001.2024.10723852.
[21]. M. Dangore, S. Modi, S. Nalawade, U. Mehta, V. K. Borate and Y. K. Mali, "Revolutionizing Sport Education With AI," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, doi: 10.1109/ICCCNT61001.2024.10724009.
[22]. M. Dangore, D. Bhaturkar, K. M. Bhale, H. M. Jadhav, V. K. Borate and Y. K. Mali, "Applying Random Forest for IoT Systems in Industrial Environments," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, doi: 10.1109/ICCCNT61001.2024.10725751.
[23]. 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.
[24]. Y. K. Mali, L. Sharma, K. Mahajan, F. Kazi, P. Kar and A. Bhogle, "Application of CNN Algorithm on X-Ray Images in COVID-19 Disease Prediction," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10726852.
[25]. 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
[26]. 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.

[27]. Hrushikesh Kale, Kartik Aswar, Kisan Yadav, Dr. Yogesh Mali, "Attendance Marking using Face Detection", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 4, Issue 3, October 2024,pp 417-424 DOI: 10.48175/IJARSCT-19961.
[28]. Faizan Inamdar, Dev Ojha, Chaitanya Jakate, Dr. Yogesh Mali," Job Title Predictor System", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 4, Issue 3, October 2024,pp 457-463 DOI: 10.48175/IJARSCT-19968.
[29]. Sawardekar, Sonali, Rahesha Mulla, Sonali Sonawane, Asharani Shinde, Vishal Borate, and Yogesh Kisan Mali. "Application of Modern Tools in Web 3.0." In Proceedings of Third International Conference on Computational Electronics for Wireless Communications: ICCWC 2023, Volume 2, p. 0. Springer Nature.
[30]. 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
[31]. 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.
[32]. 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.
[33]. 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.
[34]. Y. Mali and V Chapte, "Grid based authentication system", International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 10, pp. 93-99, 2014.
[35]. 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.
[36]. 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.
[37]. 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.
[38]. 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
[39]. 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.
[40]. 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.
[41]. Patil, Y., Paun, M., Paun, D., Singh, K., & Borate, V. K. (2020). Virtual painting with OpenCV using Python. International Journal of Scientific Research in Science and Technology, 5(8), 189-194.
[42]. 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.
[43]. Gaikwad, Dnyanesh S., and Vishal Borate. "A REVIEW OF DIFFERENT CROP HEALTH MONITORING AND DISEASE DETECTION TECHNIQUES IN AGRICULTURE." IJRAR-International Journal of Research and Analytical Reviews (IJRAR) 10, no. 4 (2023): 114-117.

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 2, November 2024

[44]. Yevlekar, Harshala R., Pratik B. Deore, Priyanka S. Patil, Rutuja R. Khandebharad, and Vishal Kisan Borate. "Smart and Integrated Crop Disease Identification System." (2019).
[45]. 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."
[46]. X. Zheng et al., "Coupling Remote Sensing Insights With Vegetation Dynamics and to Analyze NO2Concentrations: A Google Earth Engine-Driven Investigation" in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 17, pp. 9858-9875, 2024.
[47]. Zhao, Qun, Muhammad Haseeb, Xinyao Wang, Xiangtian Zheng, Zainab Tahir, Sundas Ghafoor, Muhammad Mubbin et al. "Evaluation of Land Use Land Cover Changes in Response to Land Surface Temperature With Satellite Indices and Remote Sensing Data." Rangeland Ecology & Management 96 (2024): 183-196.
[48]. Shazil, Muhammad Shareef, Sheharyar Ahmad, Syed Amer Mahmood, Syed Ali Asad Naqvi, Sanju Purohit, and Aqil Tariq. "Spatio-temporal analysis of hydrometeorological variables for terrestrial and groundwater storage assessment." Groundwater for Sustainable Development 27 (2024): 101333.
[49]. Purohit, Sanju. "Rainfall in California: Special Reference to 2023 Rains That Caused Floods." Annals of the American Association of Geographers (2024): 1-13.
[50]. Barboza, Elgar, Efrain Y. Turpo, Rolando Salas Lopez, Jhonsy O. Silva-López, Juancarlos Cruz, Héctor V. Vásquez, Sanju Purohit, Muhammad Aslam, and Aqil Tariq. "Analyzing Urban Expansion and Land Use Dynamics in Bagua Grande and Chachapoyas Using Cloud Computing and Predictive Modeling." Earth Systems and Environment (2024): 1-17.