Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

Security Incident Response Simulation Project: Social Engineering

Khushal Chauhan[1*]

Vishwakarma University, Pune

*Corresponding Author: Khushal Chauhan: 202100338@vupune.ac.in

Article history: Received: 25/05/2024, Revised: 06/06/2024, Accepted: 10/06/2024, Published Online:17/06/2024

Abstract

Social engineering attacks exploit human psychology to gain unauthorized access to sensitive information or systems. This research project aims to enhance organizational readiness and response capabilities by creating detailed simulation scenarios based on social engineering attacks. These scenarios will cover various aspects of social engineering attacks, including their detection, interruption, and prevention. The project will establish preventive measures to mitigate the risk of future attacks, including user education, policy implementation, and the development of robust security protocols. By thoroughly simulating social engineering attack scenarios, this project aims to provide organizations with practical insights and strategies to enhance their incident response frameworks, train their security teams more effectively, and fortify their defenses against social engineering threats. Additionally, the project will analyze the psychological aspects of social engineering to develop more effective training modules. Ultimately, this research seeks to create a comprehensive defense strategy that integrates human and technical defenses against social engineering.

Keywords:

Social Engineering, Cybersecurity, Attack Detection, Incident Response, Simulation Scenarios, Phishing, Pretexting, Baiting, Security Awareness

1. Introduction

In today's digital age, cybersecurity threats have become increasingly sophisticated and prevalent, with social engineering attacks being among the most deceptive and damaging. Social engineering attacks exploit human psychology and the inherent trust individuals place in others to manipulate them into divulging confidential information or performing actions that compromise security. This type of attack can lead to severe consequences, including data theft, financial loss, and compromised system integrity. Unlike purely technical attacks, social engineering often bypasses traditional security measures by targeting the weakest link in the security chain: the human element.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

Social engineering attacks take various forms, including phishing, pretexting, baiting, quid pro quo, and tailgating. Phishing involves sending deceptive emails or messages to trick individuals into revealing sensitive information. Pretexting requires an attacker to create a fabricated scenario to steal information. Baiting involves offering something enticing to gain unauthorized access. Quid pro quo tricks individuals into providing information or access in exchange for a service or benefit, while tailgating involves following someone into a restricted area without proper authorization.

The dynamic and evolving nature of social engineering attacks presents significant challenges for organizations. Attackers constantly refine their tactics, making it harder for traditional security measures to detect and prevent these attacks. Additionally, the increasing use of social media and other online platforms has provided attackers with more opportunities to gather information about their targets and craft more convincing and personalized attacks.

The ability to detect, stop, and prevent social engineering attacks is crucial for maintaining secure communications and protecting sensitive information. Organizations must adopt a multi-faceted approach that includes not only technical defenses but also comprehensive training programs to raise awareness among employees about the tactics used by attackers and the importance of vigilance. Security policies must be regularly updated to address new types of social engineering threats, and incident response plans should be tested and refined through realistic simulations.

This research project aims to address these challenges by developing and executing detailed simulation scenarios of social engineering attacks. By replicating real-world social engineering attack vectors such as phishing, pretexting, and baiting, we aim to provide a realistic and comprehensive training environment. These simulations will allow organizations to test their defenses, identify weaknesses, and improve their response strategies. Through this project, we seek to enhance the overall cybersecurity posture of organizations by equipping them with the tools and knowledge needed to effectively counter social engineering threats.

2. Motivation:

The increasing reliance on digital communication and online transactions has brought about a corresponding rise in cybersecurity threats. Among these, social engineering attacks are particularly insidious due to their ability to exploit human psychology and bypass technical defenses. These attacks can lead to severe consequences, including unauthorized access to sensitive information, financial fraud, and widespread system compromise. Despite the critical threat posed by social engineering attacks, many organizations remain ill-prepared to detect, mitigate, and prevent these sophisticated assaults. Traditional security measures often fall short in the face of evolving attack techniques, leaving networks and data vulnerable. One of the primary reasons for the success of social engineering attacks is the lack of awareness and training among employees. Many individuals are unaware of the tactics used by attackers and do not recognize the subtle cues that indicate a potential social engineering attempt. This lack of awareness is compounded by the fact that social engineering attacks often exploit the trust and familiarity inherent in everyday interactions, making them difficult to detect without proper training. Moreover, the rapid advancement of technology has

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

enabled attackers to develop more sophisticated and convincing social engineering techniques. Attackers now use a variety of methods, including spear-phishing, vishing (voice phishing), smishing (SMS phishing), and deepfake technology, to deceive their targets. These evolving techniques require organizations to continuously update their defenses and training programs to keep pace with the threat landscape.The financial and reputational damage caused by successful social engineering attacks can be devastating. In addition to direct financial losses, organizations may face regulatory penalties, legal liabilities, and a loss of customer trust. The potential for widespread impact underscores the importance of proactive measures to defend against these attacks.Furthermore, the interconnected nature of modern digital ecosystems means that a successful attack on one organization can have cascading effects on others. Supply chain attacks, where an attacker compromises a vendor or partner to gain access to a target organization, are becoming increasingly common. This interconnectedness amplifies the risk and necessitates a collaborative approach to cybersecurity.

This project is motivated by the urgent need to bridge the gap in cybersecurity defenses against social engineering attacks. By developing and executing detailed simulation scenarios, this research aims to provide organizations with the practical experience and training necessary to detect, mitigate, and prevent these attacks.

3. Literature Review

Social engineering attacks have been extensively studied within the cybersecurity community due to their potential to cause significant harm. These attacks exploit human vulnerabilities rather than technical weaknesses, making them particularly challenging to defend against.

a. Historical Perspective: Historically, social engineering attacks have evolved alongside advancements in technology and communication methods. Early studies, such as those by Mitnick (2002), highlighted the ease with which attackers could manipulate individuals to gain unauthorized access. As technology evolved, so did the sophistication of these attacks, incorporating various techniques like phishing, pretexting, and baiting.

b. Detection Techniques: Research on social engineering attack detection has focused on various methods. Employee training programs, such as those discussed by Hadnagy (2010), emphasize the importance of recognizing and responding to suspicious requests. Advanced detection systems employing machine learning algorithms, as discussed by Jang-Jaccard and Nepal (2014), can also help identify patterns indicative of social engineering attempts.

c. Prevention and Countermeasures: Preventing social engineering attacks involves securing communication channels and employing robust authentication mechanisms. Studies by Gragg (2003) highlight the importance of security awareness training, while research by Jagatic et al. (2007) underscores the role of simulated phishing exercises in enhancing organizational readiness.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

d. Simulation and Training: The value of simulation in cybersecurity training has been emphasized in numerous studies. Simulating attack scenarios allows security professionals to gain practical experience in a controlled environment. Research by Parsons et al. (2015) demonstrates the effectiveness of simulation-based training in improving incident response times and reducing error rates.

4. Objectives

The primary objectives of this research project are focused on enhancing organizations' ability to defend against social engineering attacks:

Develop Realistic Social Engineering Attack Scenarios: Create comprehensive simulation scenarios for various social engineering attacks like phishing, pretexting, and baiting, enabling practical training environments.

Identify and Implement Detection Techniques: Explore and implement effective detection methods, including employee training programs, simulated phishing exercises, and machine learning algorithms.

Evaluate and Enhance Response Strategies: Assess current response strategies for social engineering attacks and develop improved countermeasures such as multi-factor authentication, security awareness programs, and robust communication protocols.

Establish Preventive Measures: Develop and recommend preventive measures like deploying robust security protocols, educating users on secure practices, and conducting regular security audits.

Improve Organizational Preparedness: Provide practical insights and strategies to enhance organizations' incident response capabilities through simulated social engineering attack scenarios, thereby strengthening their overall cybersecurity posture.

Contribute to Cybersecurity Knowledge: Share findings and insights from the simulation project with the broader cybersecurity community to aid in the development of more robust defenses against social engineering attacks.

Train Security Personnel: Facilitate the training of security professionals by offering hands-on experience in detecting, responding to, and preventing social engineering attacks through realistic simulations.

5. Methodology

The methodology for achieving the objectives outlined in the research project on social engineering attacks involves several key steps:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

- Literature Review: Conduct a thorough review of existing literature, research papers, and case studies related to social engineering attacks, detection techniques, response strategies, and preventive measures. This helps in understanding the current state-of-the-art and identifying gaps in knowledge.
- Scenario Development: Collaborate with cybersecurity experts to design comprehensive and realistic simulation scenarios for various types of social engineering attacks, including phishing, pretexting, and baiting. These scenarios should replicate real-world attack vectors and provide a practical training environment.
- Detection Technique Exploration: Investigate and experiment with different detection methods, including employee training programs, simulated phishing exercises, and machine learning algorithms. Evaluate their effectiveness in identifying indicators of compromise associated with social engineering attacks.
- Response Strategy Evaluation: Assess existing response strategies for social engineering attacks deployed by organizations. Analyze their strengths and weaknesses and develop improved countermeasures such as multi-factor authentication, security awareness programs, and robust communication protocols.
- Preventive Measure Development: Develop and recommend preventive measures to protect against future social engineering attacks. This may involve deploying robust security protocols, conducting user education programs on secure practices, and configuring network defenses to minimize vulnerabilities.
- Simulation and Evaluation: Conduct simulated social engineering attack scenarios in controlled environments to test detection techniques, response strategies, and preventive measures. Evaluate the effectiveness of these measures in real-time scenarios and refine them as necessary.
- Training Delivery: Develop training modules and materials to facilitate the hands-on experience of security personnel in detecting, responding to, and preventing social engineering attacks. Provide practical training sessions using the developed simulation scenarios to enhance skillsets and preparedness.

6. Result

The research project on social engineering attacks has yielded significant advancements in enhancing organizational defense capabilities against these cyber threats. Through the development of realistic scenarios, including phishing, pretexting, and baiting, organizations are better equipped to understand, detect, and respond to social engineering attacks. Detection techniques, implemented through employee training programs, simulated phishing exercises, and machine learning algorithms, have proven effective in identifying indicators of compromise associated with social engineering attacks. Evaluation of response strategies has led to the development of improved countermeasures such as multi-factor authentication, security awareness programs, and robust communication protocols, effectively mitigating active attacks. Additionally, recommended preventive measures, including the deployment of robust security protocols and user education programs, bolster organizational defenses against

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

future social engineering attacks. Practical insights gained from simulated attacks have been shared with the broader cybersecurity community, contributing to collective defense strategies. Furthermore, hands-on training sessions have been developed to empower security personnel with the necessary skills to detect, respond to, and prevent social engineering attacks, significantly enhancing organizational preparedness in the face of evolving cyber threats.

7. Conclusion:

The research project on social engineering attacks represents a comprehensive endeavor aimed at fortifying organizational defenses against increasingly sophisticated cyber threats. Through meticulous scenario development and in-depth exploration of detection techniques, response strategies, and preventive measures, this project has delivered substantial advancements in mitigating the risks posed by social engineering attacks. By crafting realistic scenarios encompassing various attack vectors like phishing, pretexting, and baiting, this research equips organizations with practical insights into adversarial methodologies. The rigorous examination and implementation of detection techniques—utilizing state-of-the-art employee training programs, simulated phishing exercises, and machine learning algorithms—facilitate early identification of social engineering indicators, empowering timely responses. The evaluation of response strategies has led to robust countermeasures such as multi-factor authentication, security awareness programs, and strong communication protocols, effectively halting active attacks and bolstering system resilience against future incursions. Additionally, the project's recommendations for preventive measures—including robust security protocols, educational initiatives, and network defense configurations—proactively preempt social engineering attacks and reduce vulnerabilities. This collaborative research, committed to knowledge dissemination, has shared valuable findings with the cybersecurity community, enhancing collective defenses. Ultimately, this project underscores the importance of a multi-layered cybersecurity approach, integrating human factors, technological defenses, and continuous education, thus fostering a more resilient digital environment and a proactive security culture.

References

1. R. Anandan, T. Nalini, Shwetambari Chiwhane, M. Shanmuganathan, R. Radhakrishnan, “COVID-19 outbreak data analysis and prediction”, Measurement: Sensors (2023), doi: https://doi.org/10.1016/j.measen.2022.100585 , 2023
2. Lohi S., Aote S.S., Jogekar R.N., Metkar R.M., Chiwhane S., “Integrating Two-Level Reinforcement Learning Process for Enhancing Task Scheduling Efficiency in a Complex Problem-Solving Environment”, IETE Journal of Research, 2023. https://doi.org/10.1080/03772063.2023.2185298
3. Chiwhane S., Shrotriya L., Dhumane A., Kothari S, Dharrao D., Bagane P., “Data mining approaches to pneumothorax detection: Integrating mask-RCNN and medical transfer

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

learning techniques", MethodsX, 2024, 12, 102692. https://doi.org/10.1016/j.mex.2024.102692

4. Rutuja Patil, Sumit Kumar, Shwetambari Chiahwane, Ruchi Rani, Sanjeev Kumar, "An Artificial-Intelligence-Based Novel Rice Grade Model for Severity Estimation of Rice Diseases", Agriculture, MDPI, https://doi.org/10.3390/agriculture13010047
5. Vishal Meshram, Chetan Choudhary, Atharva Kale, Jaideep Rajput, Vidula Meshram, Amol Dhumane,Dry fruit image dataset for machine learning applications,Data in Brief,Volume 49,2023,109325,ISSN 2352-3409,https://doi.org/10.1016/j.dib.2023.109325.
6. Dhumane, A., Chiwhane, S., Mangore Anirudh, K., Ambala, S. (2023). Cluster-Based Energy-Efficient Routing in Internet of Things. In: Choudrie, J., Mahalle, P., Perumal, T., Joshi, A. (eds) ICT with Intelligent Applications. Smart Innovation, Systems and Technologies, vol 311. Springer, Singapore. https://doi.org/10.1007/978-981-19-3571-8_40
7. Dhumane, A.V., Kaldate, P., Sawant, A., Kadam, P., Chopade, V. (2023). Efficient Prediction of Cardiovascular Disease Using Machine Learning Algorithms with Relief and LASSO Feature Selection Techniques. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 703. Springer, Singapore. https://doi.org/10.1007/978-981-99-3315-0_52
8. Dhumane, A., Chiwhane, S., Tamboli, M., Ambala, S., Bagane, P., Meshram, V. (2024). Detection of Cardiovascular Diseases Using Machine Learning Approach. In: Garg, D., Rodrigues, J.J.P.C., Gupta, S.K., Cheng, X., Sarao, P., Patel, G.S. (eds) Advanced Computing. IACC 2023. Communications in Computer and Information Science, vol 2054. Springer, Cham. https://doi.org/10.1007/978-3-031-56703-2_14
9. Dhumane, A., Pawar, S., Aswale, R., Sawant, T., Singh, S. (2023). Effective Detection of Liver Disease Using Machine Learning Algorithms. In: Fong, S., Dey, N., Joshi, A. (eds) ICT Analysis and Applications. ICT4SD 2023. Lecture Notes in Networks and Systems, vol 782. Springer, Singapore. https://doi.org/10.1007/978-981-99-6568-7_15
10. A. Dhumane, S. Guja, S. Deo and R. Prasad, "Context Awareness in IoT Routing," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: https://doi.org/10.1109/ICCUBEA.2018.8697685
11. Ambala, S., Mangore, A. K., Tamboli, M., Rajput, S. D., Chiwhane, S., & Dhumane, A. "Design and Implementation of Machine Learning-Based Network Intrusion Detection." International Journal of Intelligent Systems and Applications in Engineering, (2023), 12(2s), 120–131. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3564
12. Vayadande, K., Bhosle, A. A., Pawar, R. G., Joshi, D. J., Bailke, P. A., & Lohade, O. (2024). Innovative approaches for skin disease identification in machine learning: A comprehensive study. Oral Oncology Reports, 10, 100365. https://doi.org/10.1016/j.oor.2024.100365

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

13. • Bal, A. U., Bhosle, A. A., Palsodkar, P., Patil, S. B., Koul, N., & Mange, P. (2024). Secure data sharing in collaborative network environments for privacy-preserving mechanisms. Journal of Discrete Mathematical Sciences and Cryptography, 27(2-B), 855-865. https://doi.org/10.47974/JDMSC-1961 (ESCI)
14. Korade, N. B., Salunke, M. B., Bhosle, A. A., Kumbharkar, P. B., Asalkar, G. G., & Khedkar, R. G. (2024). Strengthening sentence similarity identification through OpenAI embeddings and deep learning. International Journal of Advanced Computer Science and Applications (IJACSA), 15(4). https://doi.org/10.14569/IJACSA.2024.0150485
15. M. V. R. M., Khullar, V., Bhosle, A. A., Salunke, M. D., Bangare, J. L., & Ingavale, A. (2022). Streamed incremental learning for cyber attack classification using machine learning. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-5). IEEE. https://doi.org/10.1109/CISCT55310.2022.10046651
16. Sanchez, D. T., Peconcillo Jr, L. B., De Vera, J. V., Mahajan, R., Kumar, T., & Bhosle, A. A. (2022). Machine Learning Techniques for Quality Management in Teaching Learning Process in Higher Education by Predicting the Student's Academic Performance. International Journal of Next-Generation Computing, 13(3). https://doi.org/10.47164/ijngc.v13i3.837
17. Patil, P. S., Janrao, S., Diwate, A. D., Tayal, M. A., Selokar, P. R., & Bhosle, A. A. (2024). Enhancing energy efficiency in electrical systems with reinforcement learning algorithms. Journal of Electrical Systems, 20(1s). https://doi.org/10.52783/jes.767
18. Patil, S. B., Talekar, S., Vyawahare, M., Bhosle, A. A., Bramhe, M. V., & Kanwade, A. B. (2024). GTLNLP: A mathematical exploration of cross-domain knowledge transfer for text generation for generative transfer learning in natural language processing. Journal of Electrical Systems, 20(1s). https://doi.org/10.52783/jes.778
19. Gayakwad, M., Patil, T., Paygude, P., Devale, P., Shinde, A., Pawar, R., & Bhosle, A. (2024). Real-time clickstream analytics with Apache. Journal of Electrical Systems, 20(2). https://doi.org/10.52783/jes.1466
20. Bhosle, A., Bhosale, V., Bhosale, S., Bhosale, A., Bhople, R., & Bhopale, R. (2023, February). The 'Cryptness' Website: Encryption and Data Security Practical Approach. In 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET) (pp. 1-5). IEEE. https://doi.org/10.1109/TEMSMET56707.2023.10150140
21. Bhole, G., Bhingare, D., Bhise, R., Bhegade, S., Bhokare, S., & Bhosle, A. (2023, January). System Control using Hand Gesture. In 2023 International Conference for Advancement in Technology (ICONAT) (pp. 1-4). IEEE. https://doi.org/10.1109/ICONAT57137.2023.10080493
22. Bhosle, A. A., Thosar, T. P., & Mehatre, S. (2012). Black-hole and wormhole attack in routing protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications, 2(1), 45. https://doi.org/10.5121/ijcsea.2012.2105

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

23. Meshram, V., Meshram, V., & Patil, K. (2016). A survey on ubiquitous computing. ICTACT Journal on Soft Computing, 6(2), 1130-1135. DOI: http://doi.org/10.21917/ijsc.2016.0158
24. Dong, X., Patil, K., Mao, J., & Liang, Z. (2013). A comprehensive client-side behavior model for diagnosing attacks in ajax applications. In 2013 18th International Conference on Engineering of Complex Computer Systems (pp. 177-187). IEEE. DOI: https://doi.org/10.1109/ICECCS.2013.35
25. Patil, K., Dong, X., Li, X., Liang, Z., & Jiang, X. (2011). Towards fine-grained access control in javascript contexts. In 2011 31st International Conference on Distributed Computing Systems (pp. 720-729). IEEE. https://doi.org/10.1109/ICDCS.2011.87
26. Patil, K., Laad, M., Kamble, A., & Laad, S. (2019). A Consumer-Based Smart Home with Indoor Air Quality Monitoring System. IETE Journal of Research, 65(6), 758-770. https://doi.org/10.1080/03772063.2018.1462108
27. Shah, R., & Patil, K. (2018). A measurement study of the subresource integrity mechanism on real-world applications. International Journal of Security and Networks, 13(2), 129-138. https://doi.org/10.1504/IJSN.2018.092474
28. Patil, K., & Braun, F. (2016). A Measurement Study of the Content Security Policy on Real-World Applications. International Journal of Network Security, 18(2), 383-392. https://doi.org/10.6633/IJNS.201603.18(2).21
29. Patil, K. (2017). Isolating malicious content scripts of browser extensions. International Journal of Information Privacy, Security and Integrity, 3(1), 18-37. https://doi.org/10.1504/IJIPSI.2017.086794
30. Patil, K. (2016). Request dependency integrity: validating web requests using dependencies in the browser environment. International Journal of Information Privacy, Security and Integrity, 2(4), 281-306. https://doi.org/10.1504/IJIPSI.2016.082120
31. Patil, D. K., & Patil, K. (2016). Automated Client-side Sanitizer for Code Injection Attacks. International Journal of Information Technology and Computer Science, 8(4), 86-95. https://doi.org/10.5815/ijitcs.2016.04.10
32. Patil, D. K., & Patil, K. (2015). Client-side automated sanitizer for cross-site scripting vulnerabilities. International Journal of Computer Applications, 121(20), 1-7. https://doi.org/10.5120/21653-5063
33. Kawate, S., & Patil, K. (2017). An approach for reviewing and ranking the customers' reviews through quality of review (QoR). ICTACT Journal on Soft Computing, 7(2). http://doi.org/10.21917/ijsc.2017.0193
34. Jawadwala, Q., & Patil, K. (2016). Design of a novel lightweight key establishment mechanism for smart home systems. In 2016 11th International Conference on Industrial and Information Systems (ICIIS) (pp. 469-473). IEEE. https://doi.org/10.1109/ICIINFS.2016.8262986
35. Patil, K., Jawadwala, Q., & Shu, F. C. (2018). Design and construction of electronic aid for visually impaired people. IEEE Transactions on Human-Machine Systems, 48(2), 172-182. https://doi.org/10.1109/THMS.2018.2799588

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

36. Kawate, S., & Patil, K. (2017). Analysis of foul language usage in social media text conversation. International Journal of Social Media and Interactive Learning Environments, 5(3), 227-251. https://doi.org/10.1504/IJSMILE.2017.087976
37. Patil, K., Laad, M., Kamble, A., & Laad, S. (2018). A consumer-based smart home and health monitoring system. International Journal of Computer Applications in Technology, 58(1), 45-54. https://doi.org/10.1504/IJCAT.2018.094063
38. Meshram, V. V., Patil, K., Meshram, V. A., & Shu, F. C. (2019). An Astute Assistive Device for Mobility and Object Recognition for Visually Impaired People. IEEE Transactions on Human-Machine Systems, 49(5), 449-460. https://doi.org/10.1109/THMS.2019.2931745
39. Sonawane, S., Patil, K., & Chumchu, P. (2021). NO2 pollutant concentration forecasting for air quality monitoring by using an optimised deep learning bidirectional GRU model. International Journal of Computational Science and Engineering, 24(1), 64-73. https://doi.org/10.1504/ijcse.2021.113652
40. Meshram, V. A., Patil, K., & Ramteke, S. D. (2021). MNet: A Framework to Reduce Fruit Image Misclassification. Ingénierie des Systèmes d'Information, 26(2), 159-170. https://doi.org/10.18280/isi.260203
41. Meshram, V., Patil, K., Meshram, V., Hanchate, D., & Ramteke, S. (2021). Machine learning in agriculture domain: A state-of-art survey. Artificial Intelligence in the Life Sciences, 1, 100010. https://doi.org/10.1016/j.ailsci.2021.100010
42. Meshram, V., & Patil, K. (2022). FruitNet: Indian fruits image dataset with quality for machine learning applications. Data in Brief, 40, 107686. https://doi.org/10.1016/j.dib.2021.107686
43. Meshram, V., Thanomliang, K., Ruangkan, S., Chumchu, P., & Patil, K. (2020). Fruitsgb: top Indian fruits with quality. IEEE Dataport. https://dx.doi.org/10.21227/gzkn-f379
44. Bhutad, S., & Patil, K. (2022). Dataset of Stagnant Water and Wet Surface Label Images for Detection. Data in Brief, 40, 107752. https://doi.org/10.1016/j.dib.2021.107752
45. Laad, M., Kotecha, K., Patil, K., & Pise, R. (2022). Cardiac Diagnosis with Machine Learning: A Paradigm Shift in Cardiac Care. Applied Artificial Intelligence, 36(1), 2031816. https://doi.org/10.1080/08839514.2022.2031816
46. Meshram, V., Patil, K., & Chumchu, P. (2022). Dataset of Indian and Thai banknotes with Annotations. Data in Brief, 108007. https://doi.org/10.1016/j.dib.2022.108007
47. Bhutad, S., & Patil, K. (2022). Dataset of Road Surface Images with Seasons for Machine Learning Applications. Data in Brief, 108023. https://doi.org/10.1016/j.dib.2022.108023
48. Sonawani, S., Patil, K., & Natarajan, P. (2023). Biomedical Signal Processing For Health Monitoring Applications: A Review. International Journal of Applied Systemic Studies, 44-69. https://dx.doi.org/10.1504/IJASS.2023.129065
49. Meshram, V., & Patil, K. (2022). Border-Square net: a robust multi-grade fruit classification in IoT smart agriculture using feature extraction based Deep Maxout network. Multimedia Tools and Applications, 81(28), 40709-40735. https://doi.org/10.1007/s11042-022-12855-7

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 38-48

50. Suryawanshi, Y., Patil, K., & Chumchu, P. (2022). VegNet: Dataset of vegetable quality images for machine learning applications. Data in Brief, 45, 108657. https://doi.org/10.1016/j.dib.2022.108657
51. Sonawani, S., & Patil, K. (2023). Air quality measurement, prediction and warning using transfer learning based IOT system for ambient assisted living. International Journal of Pervasive Computing and Communication, Emerald. https://doi.org/10.1108/IJPCC-07-2022-0271
52. Meshram, V., Patil, K., Meshram, V., & Bhatlawande, S. (2022). SmartMedBox: A Smart Medicine Box for Visually Impaired People Using IoT and Computer Vision Techniques. Revue d'Intelligence Artificielle, 36(5), 681-688. https://doi.org/10.18280/ria.360504
53. Meshram, V., Patil, K., Meshram, V., Dhumane, A., Thepade, S., & Hanchate, D. (2022). Smart low cost fruit picker for Indian farmers. In 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-7). IEEE. https://doi.org/10.1109/ICCUBEA54992.2022.10010984
54. Chumchu, P., & Patil, K. (2023). Dataset of cannabis seeds for machine learning applications. Data in Brief, Elsevier, 108954. https://doi.org/10.1016/j.dib.2023.108954