Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

Security Incident Response Simulation Project Privilege Escalation Attack

Mayur Ghawate[1*]
Vishwakarma University, Pune
*Corresponding Author: Mayur Ghawate: mayurghawate17@gmail.com

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

Abstract:

Privilege escalation attack is a major security threat where an attacker tries to exploits vulnerabilities in the system to gain unauthorized access to higher-level like root or admin access, potentially leading to sensitive data breaches. This research-based project aims to show detailed simulation scenarios based on privilege escalation attacks. Various aspects of privilege escalation like detection and prevention will be simulated in this project.

Further, this project will also establish preventive steps to stop the future privilege escalation attacks. This includes security protocols, policies that define permission and access limitations, educating about secure practices, employee training programs and implementing robust system for defences. This simulation project aims to provide organizations with practical insights and blueprints to enhance their security measures and incident response strategies, train their teams to identify and respond to threats more effectively, and strengthen their overall security defences.

Keywords:

Privilege escalation, Unauthorized access, Access control, Elevated privileges, Security breaches, Horizontal escalation

1. Introduction

Cybersecurity threats have become increasingly became complex and widespread in today's digital era, with privilege escalation attacks ranking among the most dangerous. Privilege escalation occurs when attackers exploit system weakness to gain unauthorized access to elevated or higher privileges. Such attacks can result in serious consequences, including data breaches, financial damage, reputation damage and compromised system integrity. Detecting, avoiding and preventing the attack of privilege is must for maintaining system security and safeguarding critical information. However, the constantly emerging new technology and evolution of new cyber threats, it poses significant challenges for organizations.

To effectively prevent privilege escalation, it is important to understand their execution techniques, recognize warning signs, and implement strong defensive measures. This research project attempts to address these issues by showcasing detailed simulation scenarios

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

of privilege escalation attacks. By mimicking real-world attack such as exploiting system weakness, configuration mistakes, and poor access controls, we aim to create a realistic training environment. This will help security professionals to practice and enhance their detection and response strategies in a controlled setting.

The project will also develop and evaluate a variety of detection techniques, including as access monitoring, intrusion detection systems (IDS), and behaviour analysis. By simulating these attack scenarios, we hope to improve incident response capabilities, properly train security staff, and ultimately build defences against privilege escalation threats.

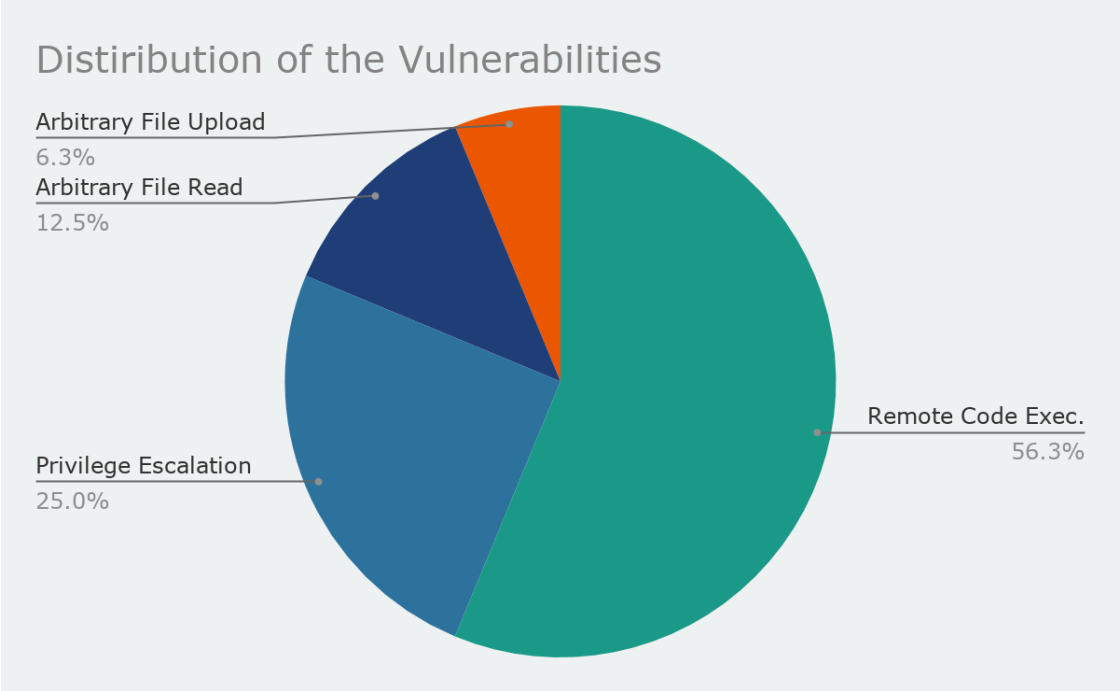


Fig.1: The breakdown of vulnerabilities by type of vulnerability

2. Motivation:

The rising reliance on digital communication and online transactions has resulted in an increase in issues related to cybersecurity. Privilege escalation attacks are especially harmful because they can exploit flaws to obtain unwanted access to higher-level system privileges. These attacks can have severe consequences such as illegal access to sensitive data, financial losses, and widespread system compromise. Despite the severe threat that comes with privilege escalation attacks, many businesses lack the ability to identify, eliminate, and prevent these sophisticated attacks. Traditional security solutions frequently fail against changing attack strategies, leaving networks and data vulnerable. The demand for advanced training and actual expertise dealing with privilege escalation assaults has become greater than ever.

The urgent necessity for filling this cybersecurity protection gap is the motivation behind our effort. Our goal is to build a realistic training environment where security professionals may hone their

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

skills by creating complete simulation scenarios of privilege escalation attacks. Organizations will be more equipped to manage problems in the real world if they can identify and address privilege escalation attacks in a controlled environment.

This initiative also aims to benefit the larger cybersecurity community by providing tactics and knowledge for preventing privilege escalation attacks. Through understanding of the specifics of these risks and evaluation of the success rate of different solutions, we may create stronger defences and enhance overall cybersecurity resilience.

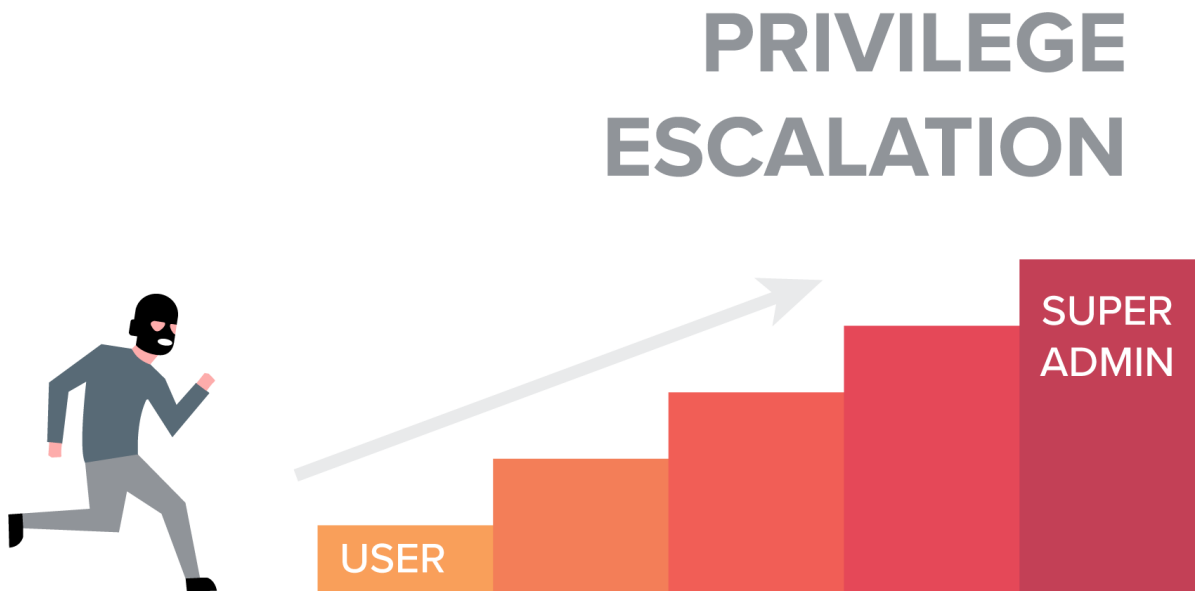


Fig.2: Privilege Escalation

3. Literature Review:

Although privilege escalation attacks have the potential to cause significant damage, the cybersecurity community has studied them in great detail. By taking advantage of flaws in programs and systems, these attacks allow attackers illegal access to higher-level privileges and even the ability to gain control over the entire system.

Historical Viewpoint: In the past, as operating systems and software applications have evolved, so too have privilege escalation risks. Early study, including that done in 1975 by Saltzer and Schroeder, highlighted the significance of the least privilege principle, which tries to restrict user access to only that which is needed for their role. The complicated nature of these attacks increased with the complexity of the software. For example, Aleph One's (1996) research reveals exploits that target buffer overflow vulnerabilities and illustrate how attackers can run arbitrary code with elevated privileges. The continuing threat posed by privilege escalation is highlighted by the ongoing discovery of new vulnerabilities, such as those listed in the Common Vulnerabilities and Exposures (CVE) database.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

Detection Strategies: Different approaches have been a topic of research on identifying privilege escalation attacks. Sysmon and other system monitoring tools are frequently used to detect unexpected behaviour that could be a sign of privilege escalation. To be able to detect deviations from typical system activity, behaviour-based detection systems, or host-based intrusion detection systems (HIDS), have been proposed in papers by Feng et al. (2014) and Abed et al. (2015). According to Buczak and Guven (2016), machine learning techniques can be used to increase these systems' accuracy and adaptability.

Prevention and Remedial Steps: Robust access control and authentication procedures must be implemented for safeguarding systems and applications in order to stop privilege escalation attacks. According to studies done by Ferraiolo and Kuhn (1992), implementing job-depending Access Control (RBAC) has proved essential to limiting user access depending on their job inside an organization. According to Howard and Lipner (2006), secure coding techniques are crucial for preventing vulnerabilities that could be used to escalate privileges. In addition, Szekeres et al. (2013) stress the need of using security-enhancing technologies like Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) as crucial steps towards decreasing the risk of exploitation.

Simulation and Awareness: Several studies have highlighted the importance of simulation in cybersecurity training. Security professionals can obtain hands-on experience in a controlled setting by simulating attack scenarios. According to research by Ahmed and Sussman (2020), incident reaction times can be shortened and mistake rates can be reduced with simulation-based training. In a similar vein, Sommestad et al. (2013) highlight how participants' overall readiness can be enhanced by exposure to a range of attack vectors by means of simulations.

4. Objectives:

This research project's main goals are to strengthen organizations' defences against attacks that escalate privileges:

Design Practical Scenarios for Privilege Escalation: To enable realistic training environments, create thorough simulation scenarios for many kinds of privilege escalation methods, such as taking advantage of software weaknesses incorrect setups, and insufficient access controls.

Identify and Utilise Detection tactics: To find warning signs of compromise related to privilege escalation attacks, investigate and implement detection techniques that work, such as behavioural analysis approaches, Host-based Intrusion Detection Systems (HIDS), and system monitoring tools.

Assess and Improve Response tactics: In an effort to stop privilege abuse, evaluate the effectiveness of the present response tactics for assaults that escalate privilege. Then, develop stronger countermeasures such Role-Based Access Control (RBAC), the least privilege principle, and secure coding practices.

Create Preventive Measures: Create and suggest countermeasures against future privilege escalation attacks, such as implementing strict access control policies, educating users on responsible conduct, and establishing up system defences.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

Boost the Organization's Readiness: By simulating privilege escalation attack scenarios, offer useful insights and approaches to improve an organization's incident response capabilities and strengthen its overall cybersecurity stance.
Add to the Awareness of Cybersecurity: Share the simulation project's results and observations with the wider cybersecurity community to encourage the creation of stronger defences against privilege escalation attacks.
Educate Security Staff: Provide practical experience in identifying, addressing, and avoiding privilege escalation attacks using realistic simulations to help in the training of security professionals.

The project hopes to greatly strengthen firm's defences against privilege escalation attacks by meeting these goals, which would promote a more secure and safe online environment.

5. Methodology:

A range of crucial phases are involved in the process for accomplishing the goals specified in the research project on privilege escalation attacks:
Conduct an extensive examination of the body of knowledge about privilege escalation attacks, detection methods, response plans, and preventive measures by studying through research articles, case studies, and other relevant materials. This aids in recognizing knowledge gaps and understanding the latest developments at the moment.

Development of Scenarios: Work with cybersecurity professionals to create thorough and accurate simulation scenarios for various kinds of privilege escalation attacks, such as those that take advantage of software flaws, improper setups, and weak access controls. These scenarios attempt to imitate actual attack vectors and offer a useful training environment.

Method of Detection Investigation: Look into and test out various detection strategies, such as behavioural analysis methodologies, host-based intrusion detection systems (HIDS), and system monitoring tools. Evaluate how well they recognize signs of compromise caused by attacks that escalate privileges.

Evaluation of Response Strategies: Evaluate the current response plans that organizations have put in place for dealing with privilege escalation attacks. Examine their advantages and disadvantages and create stronger defences against privilege abuse, such as secure coding strategies, the least privilege principle, and role-based access control (RBAC).

Implementation of Preventive Measures: Create and suggest defences against potential privilege escalation attacks in the future. This might include establishing in place strict access control guidelines, educating users about safe practices, and setting up system defences to reduce vulnerabilities.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

Simulated privilege escalation attack scenarios should be conducted in controlled environments for the purpose of testing detection methods, response plans, and preventive measures. Examine these precautions' efficiency in real-life scenarios and make any necessary modifications.

Training Delivery: Provide training courses and resources to help security staff gain practical experience in identifying, addressing, and preventing privilege escalation attacks. Using the created simulation situations, conduct hands-on training sessions to improve awareness and skill sets.

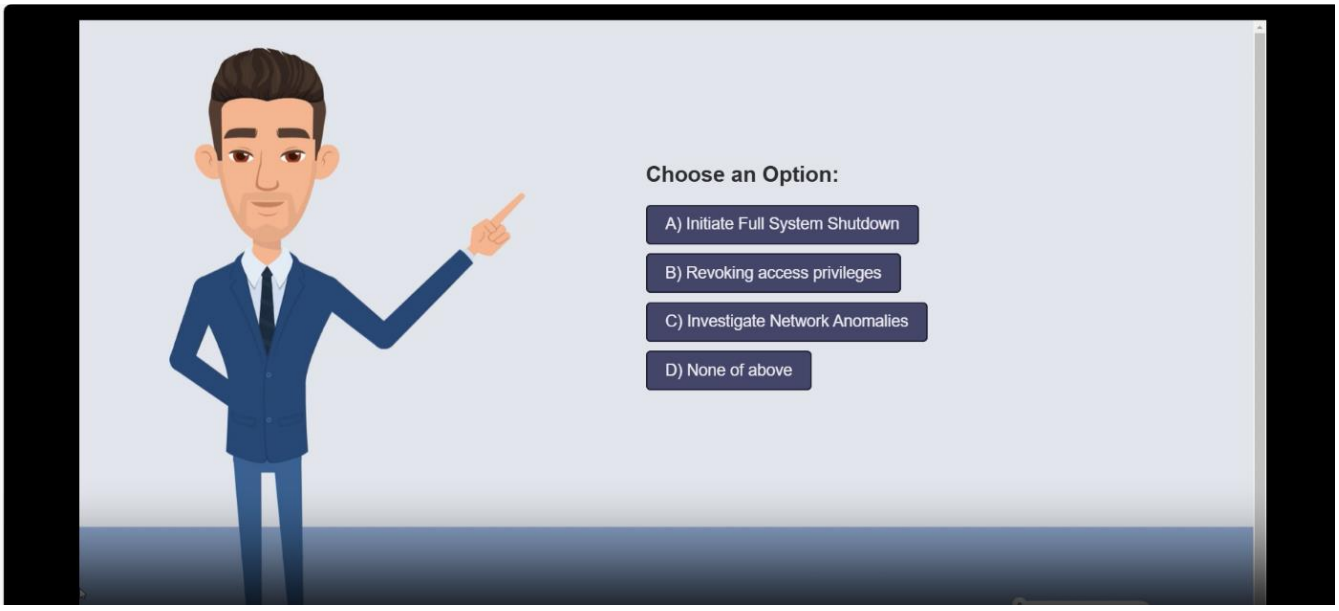
While keeping a structured approach towards achieving the goals of the research project, this modified methodology focuses on the particular context of privilege escalation attacks.

6. Result:

The privilege escalation attack research project significantly enhanced organizational defensive capabilities against these cyberthreats in a big way. Organizations can enhance their ability to detect, identify, and counterattack privilege escalation threats by creating realistic scenarios that showcase diverse tactics such software vulnerabilities, misconfigurations, and weak access controls.

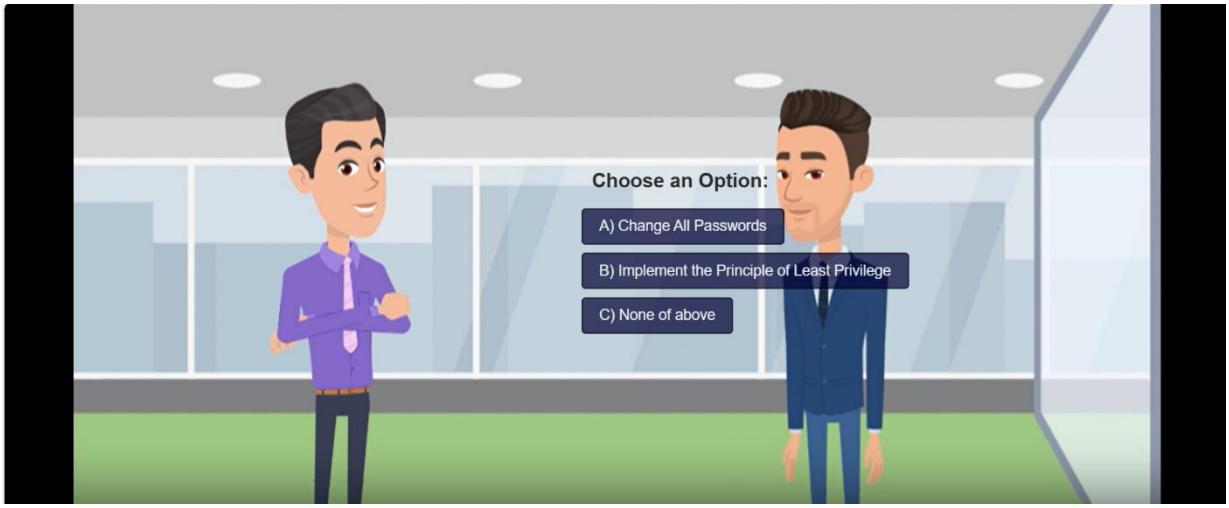
Behavioural analysis approaches, along with Host-based Intrusion Detection Systems (HIDS) and system monitoring tools, have been used to implement detection strategies that have been effective in identifying indicators of compromise connected with privilege escalation attacks. The assessment of response tactics has led to the creation of improved defences, such as secure coding methods the least privilege principle, and role-based access control (RBAC), which successfully eliminate ongoing attacks.

Security professionals are presented with a range of alternatives for responding to threats during simulated attack scenarios. Among these choices are:



Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

Option B) Revoke access privileges: "After detecting the potential compromise, one immediate action is to revoke access privileges for any user accounts or systems suspected to be compromised. Users will be asked to choose more actions after the simulation. Among these choices follows:
(Correct) Put the principle of least privilege into practice.
"We have to make sure that user access is restricted to what's necessary required for them to carry out their tasks. This idea, referred to as the Principle of Least Privilege, minimizes the possibility of privilege escalation and lowers the severity of possible security breaches."



While proactive, the following alternatives might not adequately handle the immediate risk of privilege escalation:
Option B: Tempting yet Misguided Change all Password
Although it's crucial to change your password, doing so might not stop an attacker from increasing their level of access. This choice is ineffective in stopping the attack."
Option C: Start a Full System Shutdown (Irrational yet Tempting)
"We must stop the breach right away. But even if you start a complete system shutdown, the attacker can still escalate their privileges. Additionally, this method is unable to stop the attack."
Below are few more snapshots from simulation:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

By means of interactive quizzes and situations such as these, participants are provided with realistic insights into efficient response tactics, thereby strengthening their ability to counter privilege escalation attacks in real-life contexts. Using simulated animations, viewers select the right or incorrect decision depending on the options that are shown. The subsequent simulation result illustrates whether the option they selected prevented the attack or allowed the attacker to get in, offering valuable insights. Simulation outcome demonstrates whether their chosen option successfully safeguarded against the attack or if the attacker gained access, providing valuable learning experiences.

7. Conclusion:

To sum up, the privilege escalation attack research study has shown how crucial it is to have proactive defensive plans and efficient incident response procedures in place in order to reduce the risks associated with modern cyberthreats. Participants have acquired useful insights into recognizing, responding to, and preventing privilege escalation threats through interactive dialogue regarding response options and realistic simulation scenarios. Through the project's emphasis on steps like withdrawing access privileges and applying the Principle of Least Privilege, security personnel are given essential resources to effectively fight growing cyber threats. In addition to strengthening theoretical knowledge, the simulation-based method develops flexible decision-making abilities that are critical for addressing real-world cybersecurity concerns.

To sum up, the privilege escalation attack research study has shown how crucial it is to have proactive defensive tactics and efficient incident response methods implemented in order to reduce the risks associated with modern cyberthreats. Participants have acquired useful insights into recognizing, responding to, and preventing privilege escalation threats through interactive dialogue regarding response options and realistic simulation scenarios. Through the project's emphasis on steps like withdrawing access privileges and applying the Principle of Least Privilege, security personnel are given essential resources to effectively battle growing cyber threats. In

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

addition to enhancing theoretical knowledge, the simulation-based method develops reactive decision-making abilities that are critical for tackling real-world cybersecurity concerns.

In addition, the project's simulation part offers cybersecurity experts an essential learning aid by letting them put their knowledge and abilities to the test in a risk-free, realistic setting. Users can improve their reaction approaches, boost their sense of security, and ultimately strengthen their organization's cybersecurity defences against privilege escalation threats by frequently interacting with the simulation.

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 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.,

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

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
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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

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
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

ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

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
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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 25-37

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
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