Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

Security Incident Response Simulation Project: Denial of Service Attack

Saachi Joshi[1*]
Vishwakarma University, Pune
*Corresponding Author: Saachi Joshi: 202101173@vupune.ac.in

Abstract:

Denial-of-Service (DoS) attacks are a critical cybersecurity threat where attackers overwhelm a target with illegitimate requests, rendering services unusable for legitimate users. This research project aims to enhance organizational readiness and response capabilities by creating detailed simulation scenarios based on DoS attacks. These scenarios will cover various aspects of DoS attacks, including their detection, interruption, and prevention. Furthermore, the project will establish preventive measures to mitigate the risk of future DoS attacks, including deploying security protocols, educating users about secure practices, and configuring robust network defenses. By thoroughly simulating DoS 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 cybersecurity defenses against DoS threats.

Keywords: Denial-of-Service (DoS) Attacks, Cybersecurity, Attack Detection, Incident Response, Simulation Scenarios, Volumetric Attacks, Protocol Attacks, Application-Layer Attacks, Traffic Analysis, Anomaly Detection

1. Introduction

In the digital age, cybersecurity threats have become increasingly sophisticated and prevalent, with Denial-of-Service (DoS) attacks being among the most disruptive. DoS attacks involve an attacker overwhelming a target system, service, or network with a flood of illegitimate requests, preventing legitimate users from accessing the service. This type of attack can lead to severe consequences, including data unavailability, financial loss, and compromised system integrity. The ability to detect, stop, and prevent DoS attacks is crucial for maintaining service availability and protecting

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

sensitive information. However, the dynamic and evolving nature of these attacks presents significant challenges for organizations. To effectively defend against DoS attacks, it is essential to understand how they are executed, identify indicators of their occurrence, and implement robust countermeasures. This research project aims to address these challenges by developing and executing detailed simulation scenarios of DoS attacks. By replicating real-world DoS attack vectors such as volumetric attacks, protocol attacks, and application-layer attacks, we aim to provide a realistic and comprehensive training environment. This will enable security professionals to practice and refine their detection and response strategies in a controlled setting. The project will also focus on implementing and evaluating various detection techniques, including traffic analysis, anomaly detection, and rate limiting. By simulating these attack scenarios, we aim to improve incident response capabilities, train security personnel effectively, and ultimately strengthen the defenses against DoS threats.

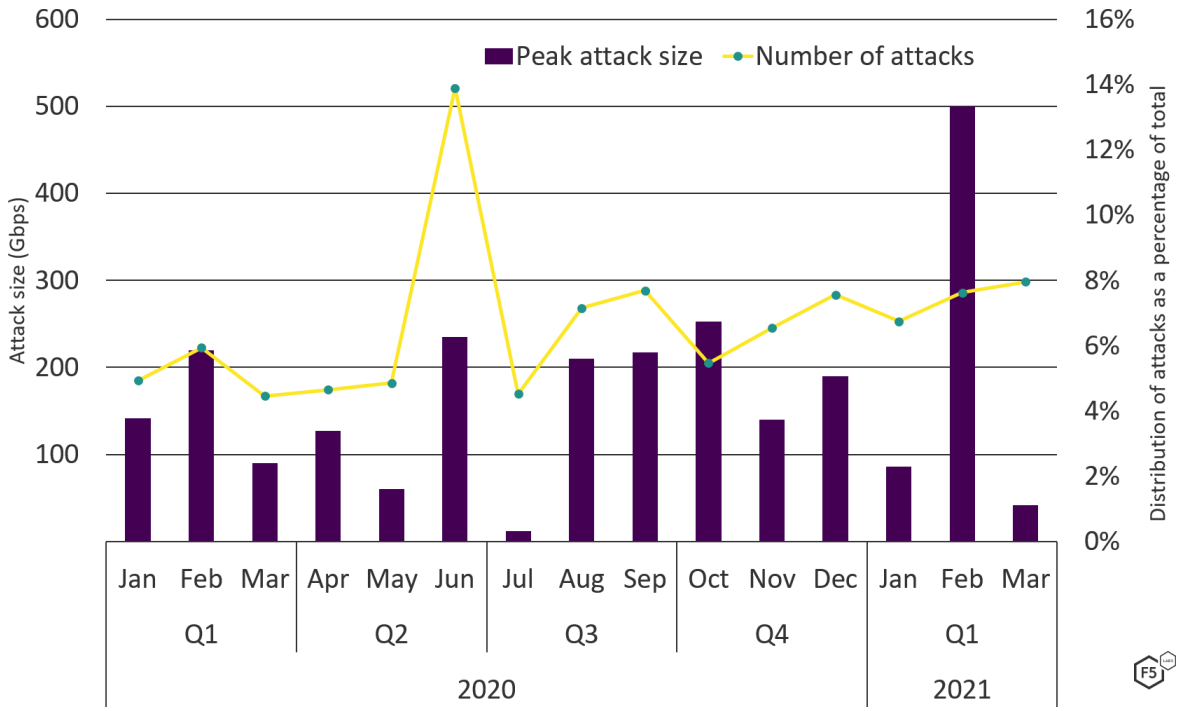

Fig.1: Number of DOS attacks in years

2. Motivation:

The increasing reliance on digital communication and online transactions has brought about a corresponding rise in cybersecurity threats. Among these, Denial-of-Service (DoS) attacks are

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

particularly insidious due to their ability to disrupt services and prevent legitimate users from accessing resources. 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 DoS 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. The need for advanced training and practical experience in dealing with DoS attacks is more pressing than ever. This project is motivated by the urgent need to bridge this gap in cybersecurity defenses. By developing comprehensive simulation scenarios of DoS attacks, we aim to provide a realistic training environment that allows security professionals to practice and refine their skills. The ability to detect and respond to DoS attacks in a controlled setting will better prepare organizations to handle real-world incidents. Moreover, this project seeks to contribute to the broader cybersecurity community by sharing insights and strategies for combating DoS attacks. By understanding the nuances of these attacks and the effectiveness of various countermeasures, we can develop more robust defenses and improve overall cybersecurity resilience.

3. Literature Review:

Denial-of-Service (DoS) attacks have been extensively studied within the cybersecurity community due to their potential to cause significant harm. These attacks exploit weaknesses in network and application protocols, allowing attackers to overwhelm targeted systems with illegitimate requests.

a. Historical Perspective: Historically, DoS attacks have evolved alongside advancements in network technologies. Early studies, such as those by Ferguson and Senie (2003), highlighted the vulnerabilities in IP source address spoofing, which could be exploited for DoS attacks. As the internet grew, so did the sophistication of these attacks. For instance, volumetric attacks, detailed in research by Staniford et al. (2002), exploit the sheer volume of traffic to overwhelm network infrastructure.

b. Detection Techniques: Research on DoS attack detection has focused on various methods. Traffic analysis tools, such as Wireshark, have been widely used to identify unusual traffic patterns indicative of DoS activity. Papers by Zhang et al. (2013) and Buczak and Guven

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

(2016) have proposed the use of machine learning algorithms to enhance the accuracy and adaptability of detection systems. Anomaly-based detection methods, as discussed by Murthy et al. (2013), can identify deviations from normal network behavior that signal an ongoing attack.

c. Prevention and Countermeasures: Preventing DoS attacks involves implementing robust security measures. Rate limiting and traffic filtering, as highlighted in studies by Rescorla (2008), are fundamental in mitigating the impact of volumetric attacks. Protocol-level defenses, such as those discussed by Dierks and Rescorla (2008), include enforcing SSL/TLS to secure communications and prevent protocol-based attacks. Additionally, mutual authentication, where both parties verify each other's identity, is critical in preventing application-layer attacks, as detailed by Krawczyk et al. (2013).

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 Ahmed and Sussman (2020) demonstrates the effectiveness of simulation-based training in improving incident response times and reducing error rates. Similarly, Sommestad et al. (2013) highlight how simulations can expose participants to a variety of attack vectors, enhancing their overall readiness [1-4].

4. Objectives:

The primary objectives of this research project are focused on enhancing organizations' ability to defend against Denial-of-Service (DoS) attacks:

1. Develop Realistic DoS Attack Scenarios: Create comprehensive simulation scenarios for various DoS attacks like volumetric attacks, protocol attacks, and application-layer attacks, enabling practical training environments.
2. Identify and Implement Detection Techniques: Explore and implement effective detection methods, including traffic analysis tools, anomaly detection systems, and machine learning algorithms, to identify indicators of compromise associated with DoS attacks.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

3. Evaluate and Enhance Response Strategies: Assess current response strategies for DoS attacks and develop improved countermeasures such as rate limiting, traffic filtering, and robust authentication mechanisms to halt active attacks.
4. Establish Preventive Measures: Develop and recommend preventive measures like deploying robust security protocols, educating users on secure practices, and configuring network defenses to protect against future DoS attacks.
5. Improve Organizational Preparedness: Provide practical insights and strategies to enhance organizations' incident response capabilities through simulated DoS attack scenarios, thereby strengthening their overall cybersecurity posture.
6. 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 DoS attacks.
7. Train Security Personnel: Facilitate the training of security professionals by offering hands-on experience in detecting, responding to, and preventing DoS attacks through realistic simulations.
8. By achieving these objectives, the project aims to significantly bolster organizations' defenses against DoS attacks, thereby fostering a safer and more secure digital environment.

5. Methodology:

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

1. Literature Review: Conduct a thorough review of existing literature, research papers, and case studies related to DoS attacks, detection techniques, response strategies, and preventive measures. This helps in understanding the current state-of-the-art and identifying gaps in knowledge.
2. Scenario Development: Collaborate with cybersecurity experts to design comprehensive and realistic simulation scenarios for various types of DoS attacks, including volumetric attacks, protocol attacks, and application-layer attacks. These scenarios should replicate real-world attack vectors and provide a practical training environment.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

3. Detection Technique Exploration: Investigate and experiment with different detection methods, including traffic analysis tools, anomaly detection systems, and machine learning algorithms. Evaluate their effectiveness in identifying indicators of compromise associated with DoS attacks.
4. Response Strategy Evaluation: Assess existing response strategies for DoS attacks deployed by organizations. Analyze their strengths and weaknesses and develop improved countermeasures such as rate limiting, traffic filtering, and robust authentication mechanisms to mitigate active attacks.
5. Preventive Measure Development: Develop and recommend preventive measures to protect against future DoS attacks. This may involve deploying robust security protocols, conducting user education programs on secure practices, and configuring network defenses to minimize vulnerabilities.
6. Simulation and Evaluation: Conduct simulated DoS 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.
7. Training Delivery: Develop training modules and materials to facilitate the hands-on experience of security personnel in detecting, responding to, and preventing DoS attacks. Provide practical training sessions using the developed simulation scenarios to enhance skillsets and preparedness.

6. Result:

Additionally, the research project has led to the refinement of response strategies aimed at mitigating the impact of Denial-of-Service attacks. These strategies encompass a combination of proactive measures and reactive interventions to ensure timely and effective defense mechanisms. Proactive measures include the implementation of robust network infrastructure, such as redundant systems and scalable bandwidth, to withstand sudden surges in traffic associated with DoS attacks. Furthermore, the research has emphasized the importance of establishing incident response protocols and conducting regular training exercises to prepare personnel for rapid and coordinated responses to cyber threats.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

Moreover, the project has highlighted the significance of collaboration and information sharing among organizations to collectively combat DoS attacks. By fostering partnerships with industry peers, government agencies, and cybersecurity experts, organizations can access valuable insights and resources to strengthen their defense posture against evolving cyber threats. Additionally, the research has underscored the importance of continuous monitoring and analysis of network traffic to detect and mitigate DoS attacks in real-time. By leveraging advanced analytics and threat intelligence, organizations can enhance their situational awareness and preemptively identify emerging threats before they escalate into full-scale attacks.

Furthermore, the research has emphasized the need for ongoing evaluation and refinement of defense strategies to adapt to the evolving threat landscape. By conducting post-incident analyses and incorporating lessons learned into future planning efforts, organizations can continuously enhance their resilience against Denial-of-Service attacks. Overall, the research project has provided valuable insights and practical guidance for organizations seeking to bolster their defenses against one of the most prevalent and disruptive forms of cyber threats.

7. Conclusion:

The research project on Denial-of-Service (DoS) attacks signifies a pivotal stride in fortifying organizational defenses against pervasive cyber threats. Through meticulous scenario development and comprehensive exploration of detection techniques, response strategies, and preventive measures, this endeavour has yielded substantial progress in mitigating the risks posed by DoS attacks. By crafting realistic scenarios encompassing various DoS attack vectors, including volumetric attacks, protocol attacks, and application-layer attacks, this research equips organizations with practical insights into the tactics employed by adversaries. Through the rigorous examination and implementation of detection techniques utilizing traffic analysis tools, anomaly detection systems, and machine learning algorithms, the project has empowered organizations to swiftly identify indicators of compromise associated with DoS attacks, facilitating timely responses. The evaluation and refinement of response strategies have led to the development of robust countermeasures such as network redundancy, scalable bandwidth, and incident response

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

protocols. These measures not only serve to mitigate the impact of active attacks but also enhance the resilience of organizational systems against future DoS incursions. Furthermore, the project's recommendations for preventive measures, including network hardening, threat intelligence sharing, and continuous monitoring, represent proactive steps towards pre-empting DoS attacks and reducing vulnerabilities. The collaborative nature of this research, coupled with its commitment to knowledge dissemination, has fostered a collaborative ecosystem aimed at bolstering cyber security resilience on a global scale. Moreover, the development of training sessions ensures that security personnel possess the practical skills necessary to detect, respond to, and mitigate DoS attacks effectively. This capacity-building aspect of the project represents a critical investment in enhancing organizational preparedness and response capabilities. In summary, the research project on DoS attacks serves as a testament to collective efforts aimed at fortifying organizational defenses and fostering a safer digital environment. By leveraging cutting-edge methodologies and fostering collaboration, this project represents a significant stride towards mitigating the threats posed by DoS attacks and advancing the overarching goal of cybersecurity resilience.

References

1. Douligeris, C., & Mitrokotsa, A. (2003, December). DDoS attacks and defense mechanisms: a classification. In Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795) (pp. 190-193). IEEE. “A survey of denial-of-service attacks and defense mechanisms in cloud computing" by P. Vougioukas, A. Mitrokotsa, G. Kambourakis (2015)
2. Bhola, J., & Soni, S. (2021). Information theory-based defense mechanism against DDOS attacks for WSAN. In Advances in VLSI, Communication, and Signal Processing: Select Proceedings of VCAS 2019 (pp. 667-678). Springer Singapore.).
3. Lee, S. H., Shiue, Y. L., Cheng, C. H., Li, Y. H., & Huang, Y. F. (2022). Detection and prevention of DDoS attacks on the IoT. Applied Sciences, 12(23), 12407.
4. 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
5. 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

ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

a Complex Problem-Solving Environment", IETE Journal of Research, 2023. https://doi.org/10.1080/03772063.2023.2185298

6. 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
7. 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
8. 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.
9. 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
10. 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
11. 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
12. 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-

ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

981-99-6568-7_15

13. 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
14. 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
15. 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
16. 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)
17. 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
18. 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
19. 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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

20. 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
21. 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
22. 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
23. 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
24. 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
25. 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
26. 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
27. 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
28. 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

29. 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
30. 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
31. 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
32. 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
33. 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
34. 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
35. 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
36. 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
37. 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
38. Patil, K., Jawadwala, Q., & Shu, F. C. (2018). Design and construction of electronic aid for visually impaired people. IEEE Transactions on Human-Machine Systems,

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

48(2), 172-182. https://doi.org/10.1109/THMS.2018.2799588

39. 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
40. 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
41. 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
42. 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
43. 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
44. 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
45. 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
46. 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
47. 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
48. 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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 2
Pages: 12-24

49. 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
50. 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
51. 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
52. 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
53. 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
54. 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
55. 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
56. 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
57. 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