Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

Security Incident Response Simulation Project: Man-in-the-Middle Attack

Sejal Kulkarni[1*]

Vishwakarma University, Pune

*Corresponding Author: Sejal Kulkarni: 202101165@vupune.ac.in

Article history: Received: 25/05/2024, Revised: 29/05/2024, Accepted: 30/05/2024, Published Online: 31/05/2024

Abstract:

Man-in-the-Middle (MitM) attacks are a critical cyber security threat where attackers intercept and manipulate communication between two parties without their knowledge. This research project aims to enhance organizational readiness and response capabilities by creating detailed simulation scenarios based on MitM attacks. These scenarios will cover various aspects of MitM attacks, including their detection, interruption, and prevention. Furthermore, the project will establish preventive measures to mitigate the risk of future MitM attacks. This includes deploying security protocols, educating users about secure practices, and configuring robust network defenses. By thoroughly simulating MitM 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 cyber security defenses against MitM threats.

Keywords:

Man-in-the-Middle (MitM) Attacks ,Cyber security, Attack Detection, Incident Response, Simulation Scenarios, ARP Spoofing, DNS Spoofing, HTTPS Hijacking, Network Monitoring

1. Introduction

In the digital age, cyber security threats have become increasingly sophisticated and prevalent, with Man-in-the-Middle (MitM) attacks being among the most dangerous. MitM attacks involve an attacker secretly intercepting and potentially altering the communication between two parties who believe they are directly communicating with each other. This type of attack can lead to severe consequences, including data theft, financial loss, and compromised system integrity. The ability to detect, stop, and prevent MitM attacks is crucial for maintaining secure

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

communications and protecting sensitive information[9-58]. However, the dynamic and evolving nature of these attacks presents significant challenges for organizations. To effectively defend against MitM 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 MitM attacks. By replicating real-world MitM attack vectors such as ARP spoofing, DNS spoofing, and HTTPS hijacking, 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 network monitoring, intrusion detection systems (IDS), and behavioral analysis.. By simulating these attack scenarios, we aim to improve incident response capabilities, train security personnel effectively, and ultimately strengthen the defenses againstMitM threats.

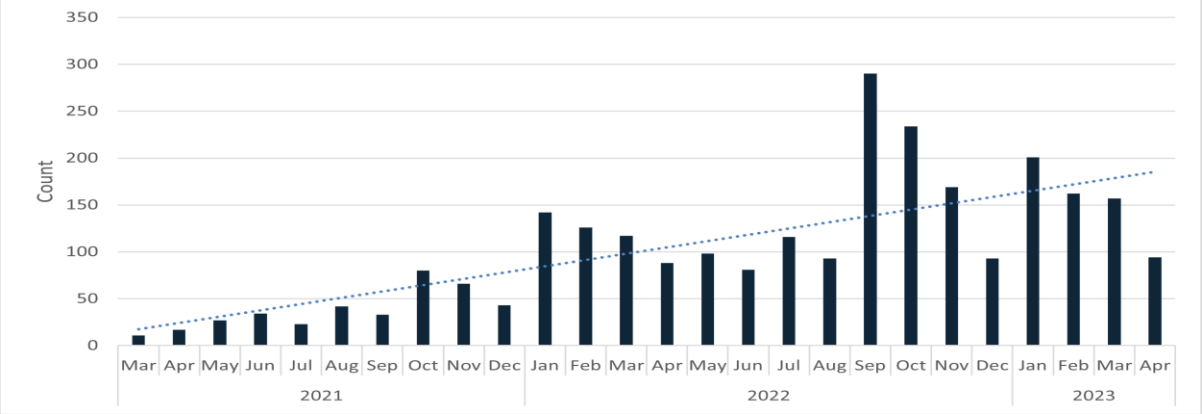

Figure 1: Number of MitM attacks in years

2. Motivation:

The increasing reliance on digital communication and online transactions has brought about a corresponding rise in cyber security threats. Among these, Man-in-the-Middle (MitM) attacks are particularly insidious due to their ability to intercept and manipulate communication without detection. 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 MitM 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 MitM attacks is more pressing than

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

ever.This project is motivated by the urgent need to bridge this gap in cyber security defenses. By developing comprehensive simulation scenarios of MitM 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 MitM attacks in a controlled setting will better prepare organizations to handle real-world incidents.Moreover, this project seeks to contribute to the broader cyber security community by sharing insights and strategies for combating MitM attacks. By understanding the nuances of these attacks and the effectiveness of various countermeasures, we can develop more robust defenses and improve overall cyber security resilience.

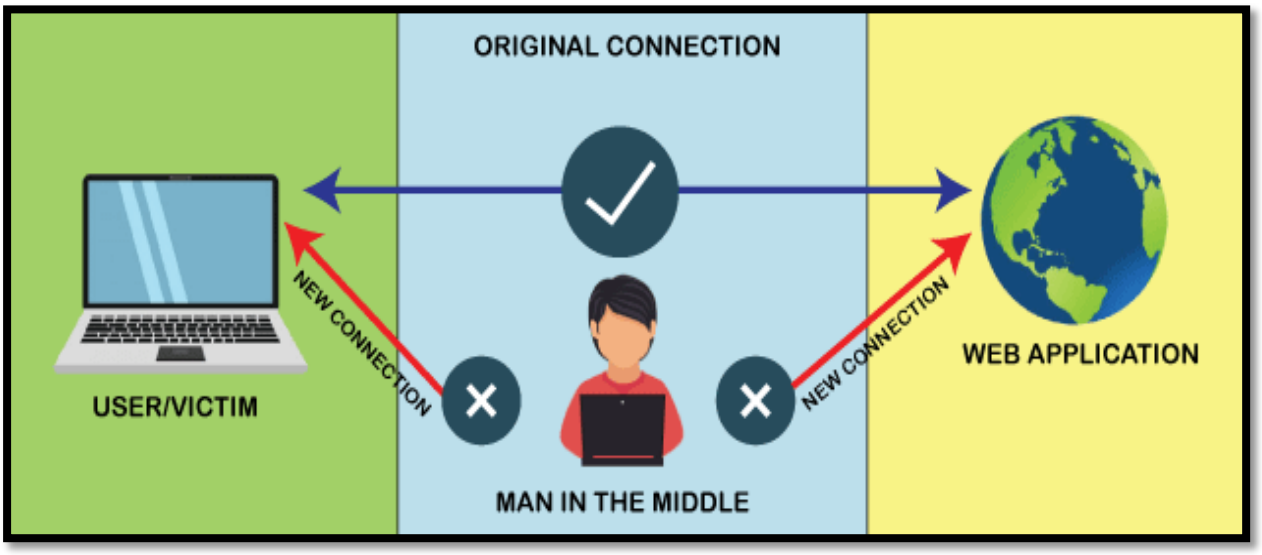

Fig.2:Man in the middle attack

3. Literature Review:

Man-in-the-Middle (MitM) attacks have been extensively studied within the cyber security community due to their potential to cause significant harm. These attacks exploit weaknesses in communication protocols, allowing attackers to intercept, modify, and potentially steal sensitive information transmitted between parties.

a. Historical Perspective: Historically, MitM attacks have evolved alongside advancements in network technologies. Early studies, such as those by Bellovin (1989), highlighted the vulnerabilities in early TCP/IP implementations that could be exploited for MitM attacks. As the internet grew, so did the sophistication of these attacks. For instance, ARP spoofing,

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

detailed in research by Shirey (2000), exploits the lack of authentication in the Address Resolution Protocol, allowing attackers to redirect network traffic.

b. Detection Techniques: Research on MitM attack detection has focused on various methods. Network monitoring tools, such as Wireshark, have been widely used to identify unusual traffic patterns indicative of MitM activity. Papers by Zhang et al. (2011) and Murthy et al. (2013) have proposed the use of Intrusion Detection Systems (IDS) that employ anomaly-based detection to identify deviations from normal network behavior. These systems can be enhanced with machine learning algorithms, as discussed by Buczak and Guven (2016), to improve their accuracy and adaptability.

c. Prevention and Countermeasures: Preventing MitM attacks involves securing communication channels and employing robust authentication mechanisms. SSL/TLS protocols have been fundamental in securing web communications, as highlighted in studies by Rescorla (2001) and Dierks and Rescorla (2008). Mutual authentication, where both parties verify each other's identity, is another critical measure, discussed in detail by Krawczyk et al. (2013). Furthermore, secure key management practices are essential to ensure that cryptographic keys are not compromised, as noted by Housley et al. (2002).

d. Simulation and Training; The value of simulation in cyber security 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.

4. Objectives:

The primary objectives of this research project are focused on enhancing organizations' ability to defend against Man-in-the-Middle (MitM) attacks:

1. Develop Realistic MitM Attack Scenarios: Create comprehensive simulation scenarios for various MitM attacks like ARP spoofing, DNS spoofing, and HTTPS hijacking, enabling practical training environments.
2. Identify and Implement Detection Techniques: Explore and implement effective detection methods, including network monitoring tools, intrusion detection systems

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

(IDS), and behavioural analysis techniques, to identify indicators of compromise associated with MitM attacks.

3. Evaluate and Enhance Response Strategies: Assess current response strategies for MitM attacks and develop improved countermeasures such as SSL/TLS enforcement, mutual authentication, and secure key management 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 MitM attacks.
5. Improve Organizational Preparedness: Provide practical insights and strategies to enhance organizations' incident response capabilities through simulated MitM attack scenarios, thereby strengthening their overall cyber security posture.
6. Contribute to Cyber security Knowledge: Share findings and insights from the simulation project with the broader cyber security community to aid in the development of more robust defenses against MitM attacks.
7. Train Security Personnel: Facilitate the training of security professionals by offering hands-on experience in detecting, responding to, and preventing MitM attacks through realistic simulations.

By achieving these objectives, the project aims to significantly bolster organizations' defenses against MitM attacks, thereby fostering a safer and more secure digital environment.

4. Methodology:

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

1. Literature Review: Conduct a thorough review of existing literature, research papers, and case studies related to MitM 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 cyber security experts to design comprehensive and realistic simulation scenarios for various types of MitM attacks, including ARP spoofing, DNS spoofing, and HTTPS hijacking. 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: 1
Pages: 30-39

3. Detection Technique Exploration: Investigate and experiment with different detection methods, including network monitoring tools, intrusion detection systems (IDS), and behavioural analysis techniques. Evaluate their effectiveness in identifying indicators of compromise associated with MitM attacks.
4. Response Strategy Evaluation: Assess existing response strategies for MitM attacks deployed by organizations. Analyze their strengths and weaknesses and develop improved countermeasures such as SSL/TLS enforcement, mutual authentication, and secure key management to mitigate active attacks.
5. Preventive Measure Development: Develop and recommend preventive measures to protect against future MitM 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 MitM 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 MitM attacks. Provide practical training sessions using the developed simulation scenarios to enhance skillsets and preparedness.

5. Result:

The research project on Man-in-the-Middle (MitM) attacks has yielded significant advancements in enhancing organizational defense capabilities against these cyber threats. Through the development of realistic scenarios, including ARP spoofing, DNS spoofing, and HTTPS hijacking, organizations are better equipped to understand, detect, and respond to MitM attacks. Detection techniques, implemented using network monitoring tools, intrusion detection systems (IDS), and behavioral analysis methods, have proven effective in identifying indicators of compromise associated with MitM attacks. Evaluation of response strategies has led to the development of improved countermeasures such as SSL/TLS enforcement, mutual authentication, and secure key management, effectively mitigating active attacks. Additionally, recommended preventive measures, including the deployment of robust security protocols and user education programs, bolster organizational defenses against future MitM attacks. Practical insights gained from simulated attacks have been shared with the broader cyber security

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

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 MitM attacks, significantly enhancing organizational preparedness in the face of evolving cyber threats. We have been introducing characters that people relate to in real life with incidents happening and their corresponding events happening regarding man-in -the- middle attack with ARP spoofing. People playing will be given choices that will later decide in the end whether the attack is stopped or prevented. This enables us to educate people about future MitM attacks and how to detect them and prevent them from happening. What personal precautions should be taken to avoid this from happening is also listed in the project. Following are the snapshots of the output of the project:

Figure 3: Simulation of the environment.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

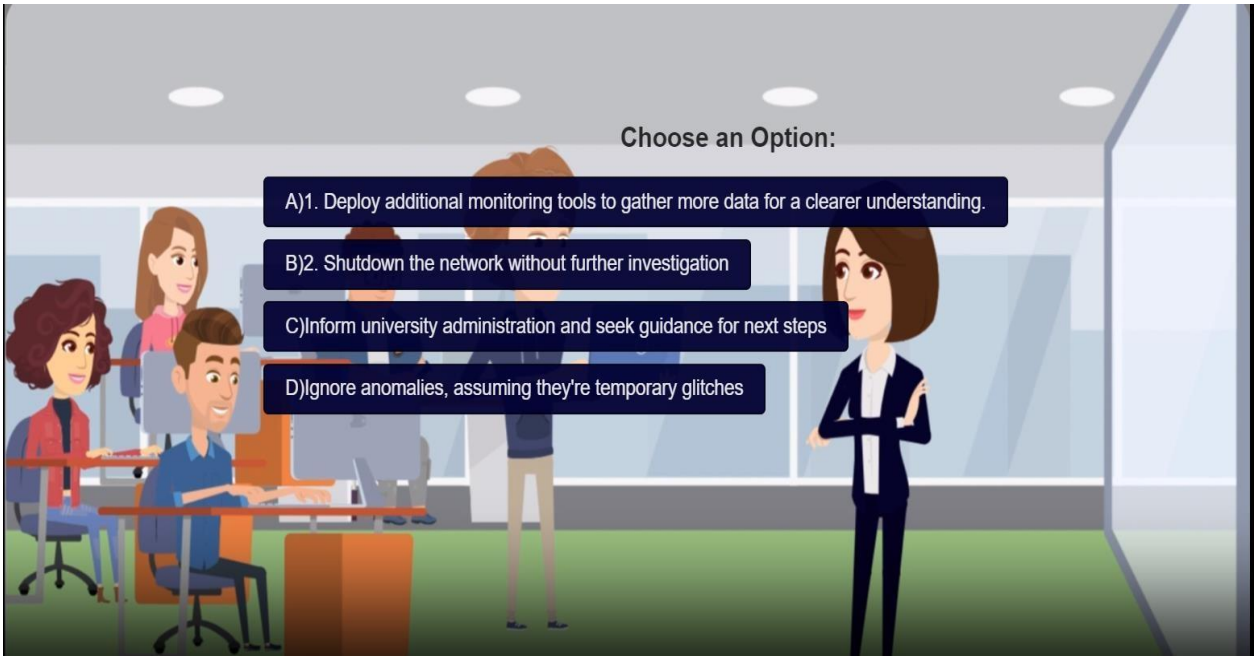

Figure 4: Choices given in the simulation.

6. Conclusion:

The research project on Man-in-the-Middle (MitM) attacks represents a comprehensive endeavour aimed at fortifying organizational defenses in the face of 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 MitM attacks.By crafting realistic scenarios encompassing various MitM attack vectors, including ARP spoofing, DNS spoofing, and HTTPS hijacking, this research equips organizations with practical insights into the methodologies employed by adversaries. Through the rigorous examination and implementation of detection techniques utilizing state-of-the-art network monitoring tools, intrusion detection systems (IDS), and behavioral analysis methods, the project has facilitated the early identification of MitM attack indicators, thus empowering organizations to mount timely responses. The evaluation and refinement of response strategies have culminated in the development of robust countermeasures such as SSL/TLS enforcement, mutual authentication, and secure key management. These measures not only serve to halt active attacks effectively but also to fortify the resilience of organizational systems against future MitM incursions. Furthermore, the project's recommendations for preventive measures, encompassing the

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

deployment of robust security protocols, educational initiatives to promote secure practices, and the meticulous configuration of network defenses, represent proactive steps towards preempting MitM attacks and reducing vulnerabilities. The collaborative nature of this research, coupled with its commitment to knowledge dissemination, has facilitated the sharing of findings and insights with the broader cyber security community. By contributing to collective defense strategies, this project fosters a collaborative ecosystem aimed at bolstering cyber security resilience on a global scale. Moreover, the development of hands-on training sessions ensures that security personnel are not only equipped with theoretical knowledge but also possess the practical skills necessary to detect, respond to, and mitigate MitM attacks effectively. This capacity-building aspect of the project represents a critical investment in enhancing organizational preparedness and response capabilities. In conclusion, the research project on MitM attacks stands as a testament to the 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 MitM attacks and advancing the overarching goal of cyber security resilience.

8. References:

1. Bellovin, S. M. (2004). "Security Problems in the TCP/IP Protocol Suite". ACM SIGCOMM Computer Communication Review, 34(1), 32-38.
2. Ferguson, P., & Senie, D. (2003). "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". RFC 2827.
3. Rescorla, E. (2008). "SSL and TLS: Designing and Building Secure Systems". Addison-Wesley Professional.
4. Rouse, M. (2018). "Man-in-the-Middle Attack (MitM)". TechTarget.
5. Staniford, S., Paxson, V., & Weaver, N. (2002). "How to Own the Internet in Your Spare Time". Proceedings of the 11th USENIX Security Symposium.
6. Tanenbaum, A. S., & Wetherall, D. J. (2011). "Computer Networks". Pearson Education.
7. Zarpelão, B. B., Miani, R. S., & Granville, L. Z. (2017). "Man-in-the-Middle Attacks in Software Defined Networks: Threats and Countermeasures". IEEE Communications Surveys & Tutorials, 19(2), 1261-1284.

ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

8. Zhang, Y., & Yadav, S. B. (2013). "A Survey on Recent Advances in MANET Intrusion Detection and Security". International Journal of Computer Applications, 69(19), 17-24.

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., and D. Midhunchakkaravarthy. "Multi-objective whale optimization algorithm using fractional calculus for green routing in internet of things." Int. J. Adv. Sci. Technol 29 (2020): 1905-1922.

12. 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

13. 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

14. 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: 10.1109/ICCUBEA.2018.8697685.

15. 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

16. Kurle, A. S., & Patil, K. R. (2015). Survey on privacy preserving mobile health monitoring system using cloud computing. International Journal of Electrical, Electronics and Computer Science Engineering, 3(4), 31-36.
17. Meshram, V., Meshram, V., & Patil, K. (2016). A survey on ubiquitous computing. ICTACT Journal on Soft Computing, 6(2), 1130-1135.
18. Omanwar, S. S., Patil, K., & Pathak, N. P. (2015). Flexible and fine-grained optimal network bandwidth utilization using client side policy. International Journal of Scientific and Engineering Research, 6(7), 692-698.
19. 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.
20. Patil, K. (2016). Preventing click event hijacking by user intention inference. ICTACT Journal on Communication Technology, 7(4), 1408-1416.
21. 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.
22. 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.
23. 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.
24. 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.
25. Patil, K. (2017). Isolating malicious content scripts of browser extensions. International Journal of Information Privacy, Security and Integrity, 3(1), 18-37.
26. Shah, R., & Patil, K. (2016). Evaluating effectiveness of mobile browser security warnings. ICTACT Journal on Communication Technology, 7(3), 1373-1378.
27. Patil, K. (2016). Request dependency integrity: validating web requests using dependencies in the browser environment. International Journal of Information

ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

Privacy, Security and Integrity, 2(4), 281-306.

28. 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.
29. Patil, D. K., & Patil, K. (2015). Client-side automated sanitizer for cross-site scripting vulnerabilities. International Journal of Computer Applications, 121(20), 1-7.
30. 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).
31. 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.
32. Patil, K., Vyas, T., Braun, F., Goodwin, M., & Liang, Z. (2013). Poster: UserCSP-user specified content security policies. In Proceedings of Symposium on Usable Privacy and Security (pp. 1-2).
33. 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.
34. 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.
35. 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.
36. 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.
37. Meshram, V., Patil, K., & Hanchate, D. (2020). Applications of machine learning in agriculture domain: A state-of-art survey. International Journal of Advanced Science and Technology, 29(5319), 5343.
38. 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.

ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

39. 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.
40. 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.
41. Meshram, V., & Patil, K. (2022). FruitNet: Indian fruits image dataset with quality for machine learning applications. Data in Brief, 40, 107686.
42. Meshram, V., Thanomliang, K., Ruangkan, S., Chumchu, P., & Patil, K. (2020). Fruitsgb: top Indian fruits with quality. IEEE Dataport.
43. Bhutad, S., & Patil, K. (2022). Dataset of Stagnant Water and Wet Surface Label Images for Detection. Data in Brief, 40, 107752.
44. 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.
45. Meshram, V., Patil, K., & Chumchu, P. (2022). Dataset of Indian and Thai banknotes with Annotations. Data in Brief, 108007.
46. Bhutad, S., & Patil, K. (2022). Dataset of Road Surface Images with Seasons for Machine Learning Applications. Data in Brief, 108023.
47. Pise, R., & Patil, K. (2022). Automatic Classification of Mosquito Genera Using Transfer Learning. Journal of Theoretical and Applied Information Technology, 100(6), 1929-1940.
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.
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.
50. Suryawanshi, Y., Patil, K., & Chumchu, P. (2022). VegNet: Dataset of vegetable quality images for machine learning applications. Data in Brief, 45, 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.
52. Meshram, V., Patil, K., Meshram, V., & Bhatlawande, S. (2022). SmartMedBox: A

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 30-39

Smart Medicine Box for Visually Impaired People Using IoT and Computer Vision Techniques. Revue d'Intelligence Artificielle, 36(5), 681-688.

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.
54. Chumchu, P., & Patil, K. (2023). Dataset of cannabis seeds for machine learning applications. Data in Brief, Elsevier, 108954.
55. Meshram, V., Patil, K., & Bhatlawande, S. (2022). IndianFoodNet: Dataset of Indian Food images for machine learning applications. Data in Brief, 107927.
56. Meshram, V., Patil, K., & Ruangkan, S. (2022). Border-net: fruit classification model based on combined hierarchical features from convolutional deep network for Indian fruits. Multimedia Tools and Applications, 81, 4627-4656.
57. Meshram, V., & Patil, K. (2023). Border-Net: fruit classification model based on combined hierarchical features from convolutional deep network for Indian fruits. Multimedia Tools and Applications, 82, 22801-22830.
58. Patil, K., & Pise, R. (2023). Automation of coconut plantation system using sensors and wireless technology for smart agriculture. IETE Journal of Research.