Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

Ethical Hacking and Penetration Testing

Anay Rajesh Somani[1]
[1,2]Computer Engineering, Vishwakarma University, Pune,411048, Maharashtra, India.
*Corresponding Author: anaysomani03@gmail.com

DOI: https://doi.org/10.70295/SMDJ.2412002

Article history: Received: 10/11/2024, Revised:19/11/2024, Accepted: 27/11/2024, Published Online:30/11/2024

Abstract:

This research delves into ethical hacking and penetration testing, spotlighting their methodologies, tools, and real-world applications. We explore concepts such as vulnerability assessment, malware analysis, and evasion strategies for IDS and firewalls, emphasizing how they enhance system security and preempt malicious attacks.

Keywords:

Ethical Hacking, Penetration Testing, Cybersecurity, Malware, Vulnerability Assessment, IDS Evasion, Secure Networks.

1. Introduction:

In the digital age, ethical hacking has emerged as a cornerstone of modern cybersecurity. With organizations increasingly relying on technology, they also face growing threats from malicious actors. Ethical hackers, often referred to as “white hat hackers,” work within legal and organizational boundaries to identify vulnerabilities in systems, networks, and applications. The ethical hacking process follows a structured methodology. It begins with reconnaissance, where hackers gather information about the target system. This is followed by vulnerability scanning, exploiting identified issues, and generating detailed reports to inform remediation efforts. These steps mirror the attack phases of malicious hackers but are employed to strengthen defenses rather than breach them. Ethical hacking is crucial not only for thwarting attacks but also for compliance with global security standards like ISO 27001 and GDPR. By simulating attacks, organizations can gain insight into their preparedness and resilience. This paper explores tools, techniques, and methodologies that ethical hackers use to safeguard digital ecosystems.

2. Vulnerability Assessment and Penetration Testing (VAPT)

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

Vulnerability Assessment and Penetration Testing (VAPT) is a structured approach to evaluating the security of IT systems. Think of it as conducting a thorough health check-up for your digital infrastructure. It involves two interdependent processes: vulnerability assessment and penetration testing. Vulnerability assessment focuses on identifying potential security flaws in systems, networks, and applications without exploiting them, aiming to provide a detailed inventory of weaknesses. Penetration testing goes a step further by actively exploiting the identified vulnerabilities to evaluate their potential impact. This mimics real-world attack scenarios to uncover how damaging an exploited vulnerability could be.

A. Lifecycle of a Vulnerability Assessment

The vulnerability assessment process is systematic and involves several stages. The first step is asset identification, where all systems, applications, networks, and devices within the IT environment are mapped. This inventory helps define the scope of the assessment and ensures that all critical assets are covered. Tools like network scanners, inventory management systems, or even manual audits may be used during this phase.

The next phase is vulnerability discovery, where systems are scanned using automated tools such as Nessus, OpenVAS, or similar technologies. These tools scan for known vulnerabilities like outdated software, misconfigurations, or unpatched systems. Some also include heuristic analysis to identify unknown or emerging vulnerabilities.

After vulnerabilities are detected, a risk analysis is conducted to prioritize them based on factors such as severity, exploitability, and potential impact. For example, a high-severity vulnerability like an open port allowing unauthenticated remote access would be addressed before a minor misconfiguration. Many organizations use scoring systems like the Common Vulnerability Scoring System (CVSS) to quantify risk.

Finally, the mitigation and reporting phase involves recommending fixes, which might include applying patches, changing configurations, or strengthening system settings. A comprehensive report is generated detailing the findings, risk levels, and remediation steps, helping stakeholders understand the security posture and take informed actions.

B. Penetration Testing: Real-World Exploitation

Penetration testing, or "pen testing," is a proactive approach to simulate real-world attacks. By exploiting the vulnerabilities identified during the assessment phase, penetration testers can demonstrate the severity of potential breaches. For example, a penetration tester may discover a SQL injection vulnerability in a web application. By leveraging this flaw, they could extract sensitive data such as customer information or administrative credentials, illustrating the real-

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

world consequences of unaddressed vulnerabilities.

Automated tools like Burp Suite, Metasploit, and OWASP ZAP are invaluable for penetration testing, offering capabilities such as identifying and exploiting common vulnerabilities, generating attack payloads to bypass security defenses, and testing application behavior under simulated attack scenarios. However, tools alone are not sufficient. Human expertise is critical to detect logical vulnerabilities, business logic flaws, and complex attack vectors that automation might overlook. For instance, a tester might identify improper authorization mechanisms or exploit chain vulnerabilities, where minor issues are combined to achieve a critical breach.

C. Integration of VAPT into Cybersecurity

VAPT provides organizations with a clear understanding of their security weaknesses and the impact of potential breaches. Conducting VAPT periodically or after significant system changes ensures systems remain resilient against evolving threats. The integration of automated tools with skilled ethical hackers offers a comprehensive approach to securing IT systems.

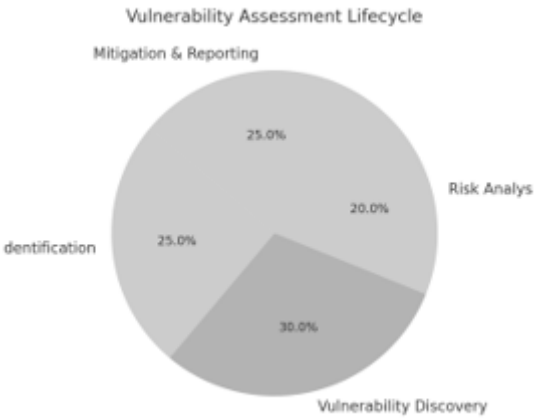

Figure 1. Vulnerability Assessment Lifecycle

3. Malware Threats and Social Engineering

Malware and social engineering represent two of the most persistent and versatile threats in cybersecurity. While malware targets vulnerabilities in systems and software, social engineering exploits human behavior. Understanding their mechanisms, impact, and countermeasures is critical to strengthening organizational defenses.

A. Malware Threats

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

Malware, short for malicious software, is designed to infiltrate, damage, or disrupt systems without the user's consent. It comes in various forms, each with specific attack vectors and goals.

1. *Trojans*

Trojans masquerade as legitimate software, deceiving users into installing them. Unlike viruses, they do not replicate but instead create backdoors for attackers to gain unauthorized access. For example, a Trojan disguised as a media player might install spyware to steal sensitive information such as login credentials.

2. *Viruses*

Viruses are self-replicating programs that attach themselves to legitimate files or programs. They spread across systems and networks, causing widespread damage. Common payloads include deleting files, stealing data, or corrupting operating systems. For example, the "ILOVEYOU" virus caused billions of dollars in damages by replicating through email attachments.

3. *Worms*

Unlike viruses, worms are standalone programs that do not require a host file to spread. They exploit vulnerabilities in network protocols to propagate rapidly across devices. For instance, the "Conficker" worm infected millions of devices by exploiting a Windows vulnerability.

4. *Ransomware*

Ransomware encrypts the victim's data, rendering it inaccessible until a ransom is paid. This type of malware has gained prominence in recent years, targeting healthcare, finance, and critical infrastructure sectors. Notable examples include the "WannaCry" ransomware attack, which disrupted global operations in 2017.

5. *Spyware and Adware*

Spyware secretly monitors user activity, capturing sensitive data such as passwords and financial information. Adware, while less harmful, displays intrusive ads and can serve as a gateway for other malware.

B.Malware Reverse Engineering

Reverse engineering involves dissecting malware to understand its behavior, capabilities, and potential impact. Tools such as IDA Pro and Ghidra are used by ethical hackers and security researchers to analyze malicious code. By identifying malware signatures and mechanisms, defenders can develop targeted countermeasures.

C. Social Engineering Threats

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

Social engineering bypasses technical safeguards by exploiting human psychology. Attackers manipulate individuals into divulging sensitive information or performing actions that compromise security.

1. *Phishing*

Phishing is one of the most common social engineering techniques. Attackers send fraudulent emails or messages that mimic legitimate entities, such as banks or employers, to trick victims into clicking malicious links or sharing credentials. Advanced variants, such as spear phishing, target specific individuals or organizations.

2. *Pretexting*

In pretexting, attackers fabricate a scenario to gain trust and extract information. For instance, an attacker might impersonate a system administrator to obtain login credentials.

3. *Baiting*

Baiting involves enticing victims with a "bait," such as a free USB drive or a download link, which contains malware. Once the victim interacts with the bait, the attacker gains access to the system.

4. *Impersonation on Social Media*

Social engineering has expanded to platforms like LinkedIn and Facebook. Attackers create fake profiles to connect with targets, building trust over time before executing an attack.

5. *Quid Pro Quo Attacks*

Quid pro quo attacks promise a service or benefit in exchange for information. For example, attackers may pose as IT support offering "help" in exchange for login details.

D. Countermeasures for Malware and Social Engineering [-10]

Effective defenses require a combination of technology and human awareness.

1. *Technical Measures*: Organizations should deploy antivirus software, firewalls, and intrusion detection systems (IDS) to detect and block malware. Regular updates to software and operating systems are essential to patch vulnerabilities.

2. *User Awareness and Training Employees* are the first line of defense against social engineering. Conducting regular security awareness programs helps users recognize phishing attempts and other manipulative tactics.

3. *Multi-Factor Authentication (MFA)*

MFA adds an additional layer of security, requiring users to verify their identity through multiple factors, such as passwords, biometrics, or one-time codes.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

4. *Secure Configurations:* Limiting user privileges and disabling unnecessary services reduces the attack surface. Enforcing strong password policies also mitigates risks.
5. *Incident Response Plans:* Organizations should develop and test incident response plans to handle malware infections or social engineering breaches promptly.

4. Evading IDS, Firewalls, and Honeypots

Intrusion Detection Systems (IDS), firewalls, and honeypots are foundational components of modern network security. They are designed to detect, prevent, and monitor unauthorized or malicious activities within a network. However, attackers often employ sophisticated evasion techniques to bypass these defenses, compromising the security of systems without being detected [10-20].

A. Evading Intrusion Detection Systems (IDS)

IDS are tools that monitor network traffic for signs of suspicious or malicious activity. They can be signature-based, detecting known attack patterns, or anomaly-based, identifying deviations from normal behavior. Despite their effectiveness, IDS are not impervious to evasion techniques.

One common method of evading an IDS is fragmentation, where attackers split malicious payloads into smaller packets. These fragments appear harmless individually but reassemble into a malicious payload on the target system. For instance, an attacker might divide a malware file into multiple packets to avoid triggering an IDS signature.

Another method is obfuscation, which involves disguising the content of malicious payloads. This can include encoding the payload in formats such as Base64 or encrypting it before transmission. By doing so, the attacker bypasses signature-based detection, as the payload no longer matches known patterns.

Protocol anomalies can also be leveraged to bypass IDS systems. Attackers deliberately craft packets that violate protocol standards, which some IDS tools may ignore or misinterpret, allowing the malicious payload to slip through undetected.

To counter these techniques, organizations deploy advanced IDS systems that incorporate behavioral analysis and machine learning to detect unusual patterns that traditional signature-based systems might miss.

B. Evading Firewalls

Firewalls are network security devices that control traffic flow based on predefined rules. While

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

they are effective at blocking unauthorized access, attackers have developed techniques to bypass them.

One such technique is IP spoofing, where attackers forge the source IP address of their packets to mimic trusted systems. This can trick firewalls into allowing unauthorized traffic. For example, an attacker might use the IP address of a trusted server to bypass restrictions.

Another method involves tunneling protocols such as ICMP or DNS to encapsulate malicious traffic. Firewalls often allow these protocols for legitimate purposes, providing an attacker with a covert channel to communicate with the target system.

Port hopping is another evasion technique, where attackers dynamically change the ports they use for communication. Since firewalls often filter traffic based on port numbers, this approach allows attackers to avoid detection [20-30].

To mitigate these techniques, firewalls should be configured to block unused ports, implement deep packet inspection, and monitor for unusual traffic patterns.

C. Evading Honeypots

Honeypots are decoy systems designed to attract attackers, allowing administrators to observe their techniques and gather intelligence. Advanced attackers, however, can often identify honeypots and avoid interacting with them.

One way attackers evade honeypots is by fingerprinting the environment. Honeypots often lack the complexity or behavior of real systems, making them identifiable. For example, attackers may run reconnaissance to detect unrealistic system responses or services.

Attackers may also use time-based techniques, sending small packets over an extended period to observe the system's reaction. A honeypot might reveal itself by logging or responding to such minimal activity, unlike a typical production system.

Some attackers deploy low-interaction probes, where they send non-malicious requests to the system. If these requests result in unusual responses, the attacker may deduce that the system is a honeypot and avoid further interaction.

To counter these evasion strategies, honeypots can be designed with high interactivity, mimicking real systems more convincingly. Additionally, integrating honeypots with behavioral analysis tools can help administrators identify sophisticated evasion techniques.

D. Advanced Countermeasures

Organizations can employ the following strategies to bolster their defenses against IDS, firewall, and honeypot evasion techniques:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

- Use *multi-layered security* combining IDS, firewalls, and honeypots with continuous monitoring and threat intelligence.
- Implement adaptive systems powered by machine learning to identify evolving attack patterns.
- Regularly update signatures, protocols, and firewall rules to address newly discovered vulnerabilities.
- Deploy deception technologies that dynamically adjust honeypot behaviors to appear more authentic.

5. Hacking Web Servers and Wireless Networks

A. Web Server Vulnerabilities

Web servers play a central role in hosting applications and services, making them attractive targets for attackers. Their exposure to the internet, combined with the sensitive data they often store, creates numerous entry points for malicious actors. Below, we explore common web server vulnerabilities and their implications [30-50].

1. *SQL Injection (SQLi)* is a common attack where improperly sanitized user inputs are exploited to manipulate database queries. For instance, an attacker might input malicious SQL commands into a login field to gain unauthorized access. The consequences of SQL injection attacks can be severe, ranging from data breaches and unauthorized access to data modification and complete database compromise. To prevent such attacks, developers should use parameterized queries, input validation, and Object-Relational Mappers (ORMs) like SQLAlchemy. For example, an attacker could input *' OR '1'='1* into a login form to trick the server into bypassing authentication.
2. *Cross-Site Scripting (XSS)* involves injecting malicious scripts into web applications, which then execute on the client's browser. This can lead to session hijacking, credential theft, or unauthorized actions performed on behalf of the user. Stored XSS (script stored on the server) and reflected XSS (script reflected in HTTP responses) are two common forms of this vulnerability. Defending against XSS requires input sanitization, implementing a Content Security Policy (CSP), and escaping user-generated content. For instance, an injected script like *<script>alert('XSS')</script>* could compromise a comments section and execute malicious scripts on users' browsers.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

3. *Directory Traversal* allows attackers to access restricted directories and files by exploiting insecure web server configurations. A common example involves accessing files like *../../etc/passwd* on a vulnerable server, which can expose sensitive system files. Such access could lead to unauthorized data exposure and critical system compromise. To prevent directory traversal attacks, organizations should restrict directory access using permissions, validate input paths, and disable directory listing.
4. *Remote File Inclusion (RFI) and Local File Inclusion (LFI)* vulnerabilities occur when attackers exploit file upload functionalities to execute malicious scripts. For example, an attacker could upload a script that executes unauthorized commands on the server. These vulnerabilities can lead to server compromise and the execution of arbitrary code. Mitigation includes restricting file uploads to known-safe directories and validating file extensions rigorously.
5. *Denial of Service (DoS) and Distributed Denial of Service (DDoS)* attacks flood web servers with excessive requests to overwhelm resources and disrupt services. These attacks can result in service outages, customer dissatisfaction, and financial losses. Organizations can mitigate these risks through rate-limiting, web application firewalls (WAFs), and load balancers.
6. *Broken Authentication and Session Management* is another critical vulnerability where insecure authentication mechanisms or session handling practices expose users to impersonation attacks. This vulnerability can lead to identity theft and unauthorized account access. Organizations should implement secure session tokens, enforce strong password policies, and ensure the use of HTTPS to protect user authentication processes.

B. Tools for Web Vulnerability Identification

Web vulnerability identification relies on advanced tools that help ethical hackers uncover flaws before attackers exploit them. OWASP ZAP is a widely-used open-source tool for automated vulnerability scanning, while Burp Suite provides a comprehensive set of features for web application penetration testing. SQLmap automates SQL injection testing, and Nikto scans web servers for outdated software and misconfigurations. Each of these tools plays a vital role in identifying and mitigating web vulnerabilities.

6. Conclusion

Ethical hacking is not just about breaking systems; it's about thinking like an attacker to build stronger defenses. This paper explored the various techniques, tools, and methodologies that ethical hackers use to protect systems. As cyber threats evolve, ethical hacking must evolve

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

too, incorporating AI-driven tools and adaptive defense mechanisms. The importance of ethical hacking cannot be overstated. By proactively addressing vulnerabilities, organizations can safeguard their operations and build trust in a digital world.

References:

1. EC-Council, Certified Ethical Hacking Study Guide. (https://www.eccouncil.org)
2. IBM ICE, IT Network Security. (https://www.ibm.com)
3. Pearson, Network Security Essentials, Fifth Edition. (https://www.pearson.com)
4. Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems. (https://www.securityengineering.org)
5. NIST, Cybersecurity Framework. (https://www.nist.gov)
6. OWASP, Top 10 Security Risks for Web Applications. (https://owasp.org)
7. Schneier, B., Applied Cryptography. (https://www.schneier.com)
8. Dhumane, A. V., & Prasad, R. S. (2019). Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT. Wireless networks, 25, 399-413. https://doi.org/10.1007/s11276-017-1566-2
9. Dhumane, A., Prasad, R., & Prasad, J. (2016). Routing issues in internet of things: a survey. In Proceedings of the international multiconference of engineers and computer scientists (Vol. 1, pp. 16-18).
10. Ahammad, S. H., Kale, S. D., Upadhye, G. D., Pande, S. D., Babu, E. V., Dhumane, A. V., & Bahadur, M. D. K. J. (2022). Phishing URL detection using machine learning methods. Advances in Engineering Software, 173, 103288. https://doi.org/10.1016/j.advengsoft.2022.103288
11. Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2020). An optimal routing algorithm for internet of things enabling technologies. In Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 522-538). https://doi.org/10.4018/978-1-5225-9866-4.ch028
12. Dhumane, A. V., & Prasad, R. S. (2018). Fractional gravitational grey wolf optimization to multi-path data transmission in IoT. Wireless Personal Communications, 102(1), 411-436. https://doi.org/10.1007/s11277-018-5850-y
13. Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications, 19-20.
14. Dhumane, A. V., Markande, S. D., & Midhunchakkaravarthy, D. (2020). Multipath transmission in IoT using hybrid Salp swarm-differential evolution algorithm. J Netw Commun Syst, 3(1), 20-30. https://doi.org/10.46253/jnacs.v3i1.a3
15. Dhumane, A. V. (2020). Examining user experience of elearning systems using EKhool learners. Journal of Networking and Communication Systems, 3(4), 39-55. https://publisher.resbee.org/jnacs/archive/v3i4/a4/p4.pdf
16. Dhumane, A., Bagul, A., & Kulkarni, P. (2015). A review on routing protocol for low power and lossy networks in IoT. Int. J. Adv. Eng. Glob. Technol, 3(12), 1440-1444.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

17. Dhumane, A., Guja, S., Deo, S., & Prasad, R. (2018). Context awareness in IoT routing. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-5). IEEE. 10.1109/ICCUBEA.2018.8697685
18. Dhumane, A., Chiwhane, S., Mangore Anirudh, K., & Ambala, S. (2022). Cluster-based energy-efficient routing in Internet of Things. In ICT with Intelligent Applications: Proceedings of ICTIS 2022, Volume 1 (pp. 415-427). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3571-8_40
19. 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. 10.1109/ICCUBEA54992.2022.10010984
20. Mahir, A., Banavalikar, T., Budukh, M., Dhodapkar, S., & Dhumane, A. V. (2018). Soil monitoring system using Zigbee for smart agriculture. International Journal of Science Technology and Engineering, 4(7), 32-38. https://www.ijste.org/articles/IJSTEV4I7019.pdf
21. Bhute, A., Bhute, H., Pande, S., Dhumane, A., Chiwhane, S., & Wankhade, S. (2024). Acute Lymphoblastic Leukemia Detection and Classification Using an Ensemble of Classifiers and Pre-Trained Convolutional Neural Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(2024), 571-580. https://ijisae.org/index.php/IJISAE/article/view/3955
22. Prasad, J. R., Prasad, R. S., Dhumane, A., Ranjan, N., & Tamboli, M. (2024). Gradient bald vulture optimization enabled multi-objective Unet++ with DCNN for prostate cancer segmentation and detection. Biomedical Signal Processing and Control, 87, 105474. https://doi.org/10.1016/j.bspc.2023.105474
23. Meshram, V., Choudhary, C., Kale, A., Rajput, J., Meshram, V., & Dhumane, A. (2023). Dry fruit image dataset for machine learning applications. Data in Brief, 49, 109325. https://doi.org/10.1016/j.dib.2023.109325
24. 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 International Conference On Innovative Computing And Communication (pp. 677-693). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3315-0_52
25. Dhumane, A., & Midhunchakkaravarthy, D. (2020). Multi-objective whale optimization algorithm using fractional calculus for green routing in internet of things. Int. J. Adv. Sci. Technol, 29, 1905-1922. http://sersc.org/journals/index.php/IJAST/article/view/6209
26. Midhunchakkaravarthy, D., & Dhumane, A. (2020). Routing Protocols in Internet of Things: A Survey. 2273
27. Amol, D., & Rajesh, P. (2014). A review on active queue management techniques of congestion control. In 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (pp. 166-169). IEEE. https://doi.org/10.1109/ICESC.2014.34

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

28. Dhumane, A., Chiwhane, S., Tamboli, M., Ambala, S., Bagane, P., & Meshram, V. (2023). Detection of Cardiovascular Diseases Using Machine Learning Approach. In International Advanced Computing Conference (pp. 171-179). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56703-2_14
29. Ramani, A., Chhabra, D., Manik, V., Dayama, G., & Dhumane, A. (2022). Healthcare information exchange using blockchain technology. In International Conference on Communication and Intelligent Systems (pp. 91-102). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-2322-9_8
30. Chaturvedi, A., & Dhumane, A. V. (2021). Future of 5G Wireless System. Journal of Science & Technology (JST), 6(Special Issue 1), 47-52. https://doi.org/10.46243/jst.2021.v6.i04.pp47-52
31. Dhumane, A., Sakhare, N. N., Dehankar, P., Kumar, J. R. R., Patil, S. S., & Tatiya, M. (2024). Design of an Efficient Forensic Layer for IoT Network Traffic Analysis Engine Using Deep Packet Inspection via Recurrent Neural Networks. International Journal of Safety & Security Engineering, 14(3), 853-863. https://doi.org/10.18280/ijsse.140317
32. Chiwhane, S., Shrotriya, L., Dhumane, A., Kothari, S., Dharrao, D., & Bagane, P. (2024). Data mining approaches to pneumothorax detection: Integrating mask-RCNN and medical transfer learning techniques. MethodsX, 12, 102692. https://doi.org/10.1016/j.mex.2024.102692
33. Tamboli, M. S., Dhumane, A., Prasad, R., Prasad, J. R., & Ranjan, N. M. (2024). Stationary wavelet transform and SpinalNet trained light spectrum Tasmanian devil optimization enabled DR detection using fundus images. Multimedia Tools and Applications, 1-30. https://doi.org/10.1007/s11042-024-19048-4
34. Rao, A. T., Kumar, A., Choudhary, R., Kanjia, K., Dhumane, A., Zade, N., & Deokar, S. (2024). Smart IoT Devices: An Efficient and Elegant Revolution Using Smart Switches. In International Conference on Smart Computing and Communication (pp. 129-141). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-1313-4_12
35. Prasad, R., Prasad, J., Ranjan, N., Dhumane, A., & Tamboli, M. (2024). Fractional Pelican African Vulture Optimization-based classification of breast cancer using mammogram images. The Imaging Science Journal, 1-21. https://doi.org/10.1080/13682199.2023.2298111
36. Dhumane, A., Chiwhane, S., Thakur, S., Khatter, U., Gogna, M., & Bayas, A. (2023). Diabetes Prediction Using Ensemble Learning. In International Advanced Computing Conference (pp. 322-332). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56703-2_26
37. Dhumane, A., Chiwhane, S., Singh, A., Koul, A., Panchal, M., & Parida, P. (2023). ELECTRA: A Comprehensive Ecosystem for Electric Vehicles and Intelligent Transportation Using YOLO. In International Advanced Computing Conference (pp. 178-189). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56700-1_15
38. Dhumane, A., Tamboli, M., Ambala, S., Game, P., Meshram, V., & Patil, R. (2023). Machine Learning Approach for Predicting the Placement Status of Students. In 2023

ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

7th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-6). IEEE. https://doi.org/10.1109/ICCUBEA58933.2023.10392268

39. Dhumane, A., Pawar, S., Aswale, R., Sawant, T., & Singh, S. (2023). Effective Detection of Liver Disease Using Machine Learning Algorithms. In International Conference on ICT for Sustainable Development (pp. 161-171). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-6568-7_15
40. Shinde, M. A. R., Dumbre, M. P. G., Borkar, M. R. K., Patil, M. K. H., & Dhumane, A. V. (2021). Identifying Individual Specimens Among Species Using Computer Vision. International Journal of Innovations in Engineering Research and Technology, 8(06), 184-193. https://doi.org/10.17605/OSF.IO/GHWDY
41. Nalini, C. Kharabe.S (2017). A Comparative Study On Different Techniques Used For Finger–Vein Authentication. International Journal Of Pure And Applied Mathematics, 116(8), 327-333.
42. Birajdar, U., Gadhave, S., Chikodikar, S., Dadhich, S., & Chiwhane, S. (2020). Detection and classification of diabetic retinopathy using AlexNet architecture of convolutional neural networks. In Proceeding of International Conference on Computational Science and Applications: ICCSA 2019 (pp. 245-253). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-0790-8_25
43. Kothari, S., Chiwhane, S., Jain, S., & Baghel, M. (2022). Cancerous brain tumor detection using hybrid deep learning framework. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 26(3), 1651-1661. http://doi.org/10.11591/ijeecs.v26.i3.pp1651-1661
44. Kharabe, S., & Nalini, C. (2018). Using adaptive thresholding extraction—robust ROI localization based finger vein authentication. J. Adv. Res. Dyn. Control Syst, 10(7), 500-514.
45. Kharabe, S., & Nalini, C. (2018). Survey on finger-vein segmentation and authentication. Int J Eng Technol, 7(1-2), 9-14.
46. Chiwhane, S. A., Deepa, M., & Shweta, K. (2017). IOT Based Fuel Monitoring for Future Vehicles. International Journal of Advanced Research in Computer and Communication Engineering, 6, 295-297.
47. Anandan, R., Nalini, T., Chiwhane, S., Shanmuganathan, M., & Radhakrishnan, P. (2023). COVID-19 outbreak data analysis and prediction. Measurement: Sensors, 25, 100585. https://doi.org/10.1016/j.measen.2022.100585
48. Chaudhary, S., Shah, P., Paygude, P., Chiwhane, S., Mahajan, P., Chavan, P., & Kasar, M. (2024). Varying views of maxillary and mandibular aspects of teeth: A dataset. Data in Brief, 56, 110772. https://doi.org/10.1016/j.dib.2024.110772
49. Patil, J., & Chiwhane, S. (2023). AI-Powered Automated Methods for Predicting Liver Disease: A Recent Review. In International Conference on Advancements in Smart Computing and Information Security (pp. 161-172). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-58604-0_11

ISSN: 2583-925X
Volume: 2
Issue: 6
Pages: 1-14

50. Dawkhar, S., & Chiwhane, S. (2021). Privacy Violation Patterns in Non-Relational Databases. Journal of Science & Technology (JST), 6(Special Issue 1), 42-46. https://doi.org/10.46243/jst.2021.v6.i04.pp42-46
51. Sawant, S., Garg, R. D., Meshram, V., & Mistry, S. (2023). Sen-2 LULC: Land use land cover dataset for deep learning approaches. Data in Brief, 51, 109724. https://doi.org/10.1016/j.dib.2023.109724
52. Rasane, K., Bewoor, L., & Meshram, V. (2019). A comparative analysis of intrusion detection techniques: Machine learning approach. In Proceedings of International Conference on Communication and Information Processing (ICCIP). http://dx.doi.org/10.2139/ssrn.3418748
53. Jadhav, R., Suryawanshi, Y., Bedmutha, Y., Patil, K., & Chumchu, P. (2023). Mint leaves: dried, fresh, and spoiled dataset for condition analysis and machine learning applications. Data in Brief, 51, 109717. https://doi.org/10.1016/j.dib.2023.109717
54. Meshram, V., Suryawanshi, Y., Meshram, V., & Patil, K. (2023). Addressing misclassification in deep learning: a merged net approach. Software Impacts, 17, 100525. https://doi.org/10.1016/j.simpa.2023.100525
55. Kanorewala, B. Z., & Suryawanshi, Y. C. (2022). The Role of Alternate Nostril Breathing (Anuloma Viloma) technique in regulation of blood pressure. Asian Pacific Journal of Health Sciences, 9(2), 48-52. https://doi.org/10.21276/apjhs.2022.9.2.12
56. Suryawanshi, Y. C. (2021). Hydroponic cultivation approaches to enhance the contents of the secondary metabolites in plants. In Biotechnological approaches to enhance plant secondary metabolites (pp. 71-88). CRC Press. https://doi.org/10.1201/9781003034957
57. Visvanathan, G., Patil, K., Suryawanshi, Y., & Chumchu, P. (2023). Sensor based dataset to assess the impact of urban heat island effect mitigation and indoor thermal comfort via terrace gardens. Data in Brief, 49, 109431. https://doi.org/10.1016/j.dib.2023.109431
58. Suryawanshi, Y., Meshram, V., Patil, K., Testani, M., Chumchu, P., & Sharma, A. (2024). The image dataset of Indian coins: A machine learning approach for Indian currency. Data in Brief, 53, 110098. https://doi.org/10.1016/j.dib.2024.110098