Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

NetSentinel applications for website security

Atharv Ashish Talathi[1*], Darshit Deepak Mehta[1], Vaidehi Thombare[1], Janhavi Dhariya[1], Sahil Uday Daware[1]

Computer Engineering, Science & Technology, Vishwakarma University, Pune, India-411048

**Corresponding Author: athu812talathi@gmail.com*

DOI: https://doi.org/10.70295/SMDJ.2411013

Article history: Received: 10/09/2024, Revised:19/09/2024, Accepted: 27/09/2024, Published Online:30/09/2024

Abstract:

NetSentinel is an extensive web security platform designed to scan, detect and protect websites from potential vulnerabilities and cyber-threats. NetSentinel offers a proactive approach to strengthen and safeguard the website's security, in an era where data breaches and cyber-attacks are common. The platform analyzes critical security features like SSL security validity, DNSSEC implementation, threat detection, security headers, firewall, and open ports. The main feature of the platform is the scoring mechanism, which assesses the website's overall security to ensure it is protected from potential threats. The scoring method assigns different weights to the various security features according to their importance in the calculation. This scoring system helps users focus on the most important vulnerabilities and gives clear, practical advice on how to mitigate risks. Along with the main scoring feature the platform also includes 24 other critical security features which are Server location, Whois, DNS Data, DNS Records, Archives, Carbon Footprint, TLS Cipher Suites, TLS Security Configuration, TLS Handshake Simulation, Status, Traceroute, Blocklists, Pages, Social Tags, Headers, HSTS Check, Domain Rank, Tranco Rank, Linked Pages, Mail Services, Redirects, Security Txt, Robots Txt. NetSentinel breaks down complex information into a simple, easy to understand security score, which makes security assessment easier. It also offers clear explanations of the issues and provides step-by-step recommendations on how to fix them, helping users improve their overall security without needing advanced technical knowledge to be possessed. Using this platform, organizations can enhance their site's ability to withstand cyber threats, ensuring data integrity and secure communication. NetSentinel helps users take control of their web security by balancing technical accuracy with easy-to-use interfaces, making it simple for everyone to stay proactive about their safety online.

Keywords:

Web security, vulnerability detection, SSL certificate, DNSSEC, security scoring system.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

Introduction:

In today's technologically advanced world, the security of websites is a necessity, as they are the key access points for the sensitive data and communication between the users and the organization. Cyber threats, such as data breaches, malware, and phishing attacks are happening more often and becoming more advanced, making them harder to detect and stop. Therefore, it is necessary for website owners and administrators to regularly analyze and bolster their security structure. NetSentinel is a powerful web security platform that tackles these challenges, by offering set of tools to scan, detect, and protect websites from various vulnerabilities. NetSentinel performs an in-depth analysis of key security components, such as SSL certificates, DNSSEC, firewall, and open ports, while also checking for active threats and security headers.

Key security components analyzed by NetSentinel include, but are not limited to:

- SSL Certificates: Ensure that data sent between the website and users is encrypted and secure.
- DNS Security (DNSSEC): Protects your website's DNS records from being tampered with by attackers.
- Firewall Configurations: Controls what traffic can access your website, blocking unauthorized users.
- Open Ports: Checks if any open network ports could let hackers into your system. Security Headers: Adds extra protection to prevent attacks like stealing data or hijacking a user's session.
- TLS Cipher Suites: This makes sure your site uses strong, up-to-date encryption to protect sensitive information from hackers.
- Web Application Firewall (WAF) Rules: The firewall acts like a gatekeeper, monitoring all incoming traffic and blocking anything harmful.
- Threat Detection: It watches for known bad websites or phishing attempts that could put your site or users at risk.

NetSentinel stands out because it uses a unique scoring system that rates each website's security based on the number and seriousness of the issues it finds. This makes it easy to see how secure your website really is. The system checks for factors such as the strength of encryption, network exposure, presence of outdated components, and the likelihood of exploitation by attackers. Each vulnerability is weighted based on its impact, helping website owners to focus on addressing the most critical issues first [1-14].

Furthermore, NetSentinel not only identifies vulnerabilities but also provides recommendations according to the website's structure. Users will receive a list of preventative measures to ensure effective mitigation of risks. The platform is designed in such a way that is user-friendly for experienced security experts as well as for people without any prior technical knowledge. It's simple, easy-to-use interface makes web security easier for everyone [14-20].

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

With regular monitoring, NetSentinel sends automatic security reports to keep you updated on new threats and weaknesses. These reports show the current security status, ensuring the necessary preventative steps are taken before attackers exploit the potential vulnerabilities.

Through its holistic approach to web security, NetSentinel helps users protect their websites from various types of cyberattacks. It also keeps sensitive information safe, preserves uptime, and builds trust with visitors. Whether it's a small business site or a big corporate platform, NetSentinel provides tools and information necessary to maintain a robust security system and to stay secure in a world with growing cyber threats [20-25].

Material and Methods:

a. Data Collection:

Data Collection is an important part of how NetSentinel works, it makes sure that its security analysis is based on correct and updated information. The following methods are used for data gathering:

- API Integrations:
  - SSL Certificate Authorities: NetSentinel checks with SSL providers to confirm if your certificates are valid, when they expire, and which domains they cover.
  - DNSSEC Validators: It works with DNSSEC tools to make sure your domain names are properly secured and authenticated.
  - Threat Intelligence Platforms: NetSentinel uses APIs from URLhaus and Phishtank, they provide information about any threats, which helps to detect any malicious activity has been performed on the domain evaluated.
- Webscraping techniques:
  - Web scraping scripts are used to extract information from webpages that give appropriate security configurations and threat reports, since some APIs may not provide relevant information.
  - Python libraries like Beautiful Soup and Requests libraries are used for real time data collection and web scraping.
- Data processing: Data is processed to get accurate results. Data cleansing and validation steps are implemented to resolve any errors that might occur during the data collection phase.

b. Implementation:

The implementation of NetSentinel has been methodically structured to ensure robust security analysis and user-friendly interactions. This section delves deeper into the technologies, architecture, and methods used to develop and maintain the platform.

- Backend Development:
  - Language and Framework: The backend is developed in Python, leveraging the Flask framework. Flask's simplicity and extensive

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

ecosystem make it ideal for developing lightweight and scalable web applications. The choice of Python aligns with the platform's need for comprehensive data handling and integration with various security-focused libraries and APIs.

- Modular Structure: The backend is divided into distinct modules to ensure maintainability and scalability:
  - WHOIS Data Module: Utilizes Python's whois library to extract domain registration data, including registrant information and expiration details
  - DNS Record Analysis: Built using dns-python to check DNSSEC status and verify domain configurations.
  - SSL/TLS Verification: Custom scripts employing ssl and socket libraries to establish TLS handshakes, checking for certificate validity, issuer details, and cipher strength.
  - Port Scanning: A lightweight port scanner using the socket library to identify open and potentially vulnerable ports.
  - Threat Intelligence Integration: API calls platforms like PhishTank and URLhaus for identifying reported threats and malicious activity associated with the target domain.
  - Security Headers Evaluation: Uses requests and header analysis functions to verify the presence and proper configuration of headers such as Content-Security-Policy, X-XSS-Protection, and X-Frame-Options.

Table – 1 Sample Data

Website URL	SSL Certificate Validity	DNSSEC Status	Open Ports	Threats Detected
https://www.google.com	Valid	Disabled	80, 443	Phishing Detected
https://www.foxnews.com	Valid	Enabled	80, 443	None
https://www.cricbuzz.com	Valid	Enabled	80, 443	None

- Data Processing Pipeline: Data collected from different modules is aggregated and preprocessed to ensure accuracy and consistency. The pipeline includes:
  - Data Cleansing: Removing duplicate records and normalizing data formats using pandas for streamlined processing.
  - Validation and Error Handling: Implementing exception handling to manage issues such as unreachable domains or API rate limits.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

- Communication Management: Flask-CORS is configured to handle Cross-Origin Resource Sharing, enabling smooth interaction between the backend and frontend. This ensures secure and efficient data flow across different web clients.

- Frontend Development:
  - Interface Design: The frontend is developed with a focus on user experience and accessibility:
    - Markup and Styling: Utilizes HTML5 and CSS3 for a clean and responsive layout. Lightweight CSS frameworks, such as Bootstrap, are optionally employed for consistent styling and responsive design elements.

Fig. 1: Homepage of Website

  - Dynamic User Interaction: JavaScript is the primary language for handling client-side interactivity:
    - AJAX Calls: Asynchronous JavaScript calls are used to communicate with backend endpoints, enabling real-time data retrieval and minimizing page reloads.
    - Visualization Tools: Libraries like Chart.js and D3.js are integrated for displaying visual representations of the security score, open ports, and other analysis data.

- Data Aggregation and Reporting:
  - Data Integration: Data is collected from multiple trusted sources:
    - API Responses: Data from SSL certificate authorities, DNSSEC validators, and threat intelligence providers.
    - Web Scraping: Custom scripts using Beautiful Soup and Requests libraries to extract additional security-related information.
  - Data Consolidation: The backend consolidates the data into a unified report:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

- Aggregation Logic: Combines structured data from APIs and unstructured data from web scraping.
- Data Transformation: Formats data into human-readable insights, with the pandas library performing transformations such as sorting, filtering, and merging datasets.

- Scoring System:
  - Weighted Scoring Model: A unique weighted scoring algorithm evaluates the security status of websites:
    - SSL Certificates: High weight due to their role in securing data transmission.
    - Threat Detection: Assigns a negative weight if threats are identified, reflecting the critical impact on overall security.
    - Other Features: DNSSEC, firewall settings, and security headers receive weights based on their contribution to overall security.
    - Calculation Method: The system aggregates scores by multiplying each component's evaluation result by its weight and summing the results to provide a comprehensive score.
  - Customizability and Transparency: The scoring system allows users to understand the rationale behind their scores through a detailed breakdown. Each security feature is documented with explanations and recommendations, ensuring transparency.
  - Recommendations Module: The platform provides tailored recommendations to improve security. These suggestions are derived from best practices, helping users address detected issues such as expired SSL certificates or misconfigured headers.

Fig. 2: Score Section

- Deployment and Maintenance:
  - Hosting and Scalability:
    - Hosting: The application is hosted on Amazon EC2 instances, chosen for their scalability and reliability.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

- Load Balancing: A load balancer is configured to distribute incoming traffic evenly, ensuring minimal response time and high availability.

- Domain and DNS Configuration:
  Domain Management: The application is hosted by netsentinel.in, with DNS records set for redundancy and performance optimization.
- Continuous Integration and Deployment (CI/CD):
  The project follows CI/CD practices using platforms like GitHub Actions or Jenkins, ensuring that new features and patches are deployed seamlessly.
- Monitoring and Updates:
  - Monitoring Tools: Integrated monitoring solutions, such as Prometheus and Grafana, provide insights into system health and performance.
  - Scheduled Updates: Regular updates keep the system aligned with the latest security trends and technologies.

- Testing and Quality Assurance:
  - Unit and Integration Testing:
    - Unit Tests: pytest framework is employed to test individual functions and ensure they work as intended.
    - Integration Tests: Comprehensive tests check the compatibility of different modules and the data flow between frontend and backend.
  - User Acceptance Testing (UAT): Feedback from beta testers is incorporated to improve user experience and identify any functional gaps.
  - Load Testing: Simulated load tests are conducted using tools like Apache JMeter to ensure the system can handle multiple concurrent users.
- Future Enhancements:
  - Advanced Threat Detection: Plans to integrate machine learning algorithms to predict potential threats based on historical data trends.
  - Real-Time Alerts: Adding a notification system to alert users immediately when a significant vulnerability or threat is detected.
  - Expanded API Integrations: Incorporating additional security APIs and data sources to enhance the platform's analysis capabilities.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

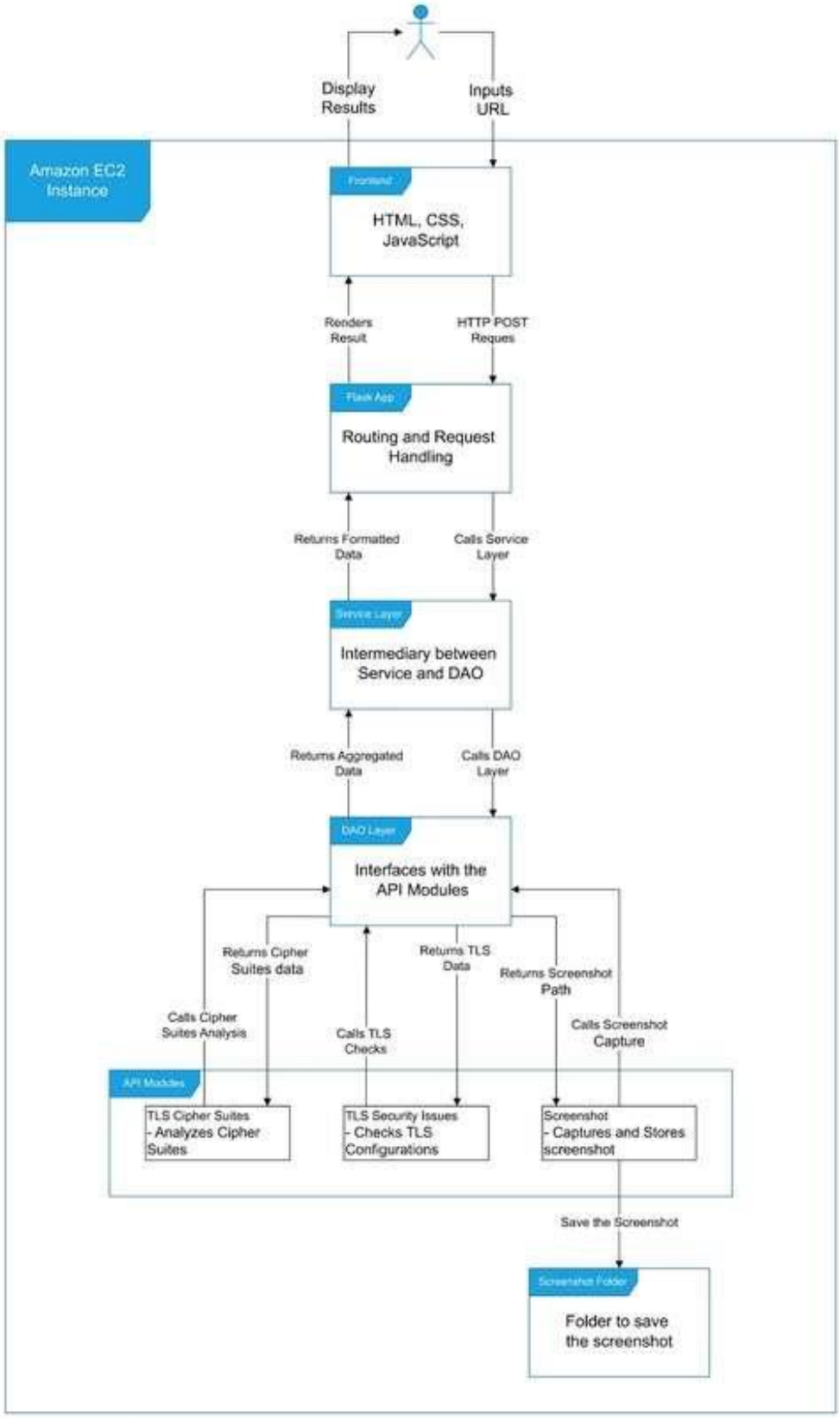

Fig. 3: System Architecture

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

c. System Workflow:

- User Input:
  - The user inputs the URL of the website they wish to analyse into the NetSentinel web interface.
- Request Handling (Frontend to Backend):
  - The user-submitted URL is sent from the frontend (via AJAX) to the backend server for processing.
  - The Flask framework handles the HTTP POST request and begins the data collection process.
- Data Collection Process:
  - SSL Certificate Check:
    The system communicates with SSL certificate authorities through their APIs to verify the website's SSL certificate status, validity, and expiration date.
  - DNSSEC Validation:
    The backend checks DNS records using DNSSEC validation APIs to ensure authenticity and security.
  - Threat Detection:
    APIs from threat intelligence sources like URLhaus and PhishTank are queried for any reports of malicious activity related to the domain.
  - Custom Web Scraping:
    Web scraping scripts using Beautiful Soup and Requests libraries gather security headers, open port details, and other configurations if not available via API.
- Data Processing:
  - Collected data undergoes cleansing to ensure consistency.
  - The backend applies custom algorithms to evaluate and score the different security components based on predefined weights.
- Scoring Mechanism:
  - The system calculates a security score using the weighted scoring model.
  - Each component (e.g., SSL certificates, DNSSEC, threat reports) is assigned a weight, and the overall score is the sum of these weighted scores.
- Result Generation:
  - The processed data and overall score are formatted into a detailed report.
  - Recommendations for security improvements are generated and included in the report.
- Report Display:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

- The detailed report is sent back to the frontend, where the user interface presents the results.
- Users can view the overall score, individual component evaluations, and tailored recommendations.

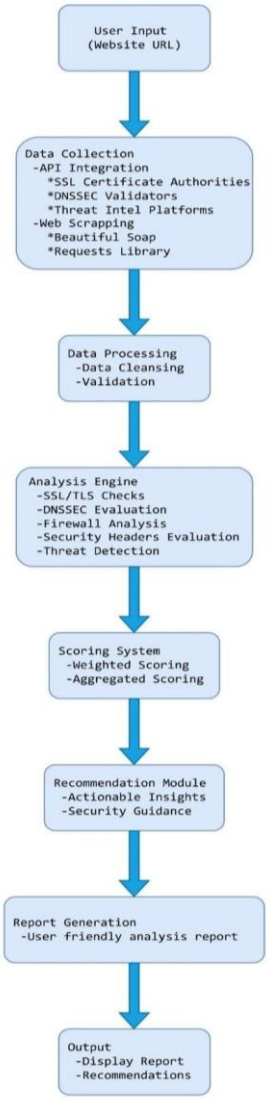

Fig. 4: Block Diagram

d. Deployment and Maintenance Hosting Infrastructure:

- Hosting Infrastructure:
  The platform is hosted on Amazon EC2, a cloud service that allows the system to handle many users at the same time and is easily scalable if needed. It is used to support Flask applications, for efficient request handling and uptime.
- Domain management:
  The website is accessible via the domain netsentinel.in, with DNS records configured for reliability and performance.
- Continuous Monitoring:

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

Regular monitoring of the platform is conducted to ensure that it remains up to date with the latest security standards and best practices.

Results and Discussion:

NetSentinel has helped us get a clearer picture of how secure websites really are by examining important security features. We discovered that many websites either don't have the right SSL certificates or are using outdated ones, which puts users' data at risk. While a lot of websites use SSL for protection, we found that fewer are using DNSSEC. DNSSEC is important because it helps prevent attacks that could trick users into visiting fake sites. This means that even with some security measures in place, many websites are still at risk from certain types of attacks. By partnering with external threat intelligence sources like URLhaus and Phishtank, we can easily spot active threats, dangerous websites, and compromised servers. This teamwork helps us protect users better and improve overall website security. Our scoring system gives us a way to measure how secure a website is. For instance, websites that have secure SSL certificates, active DNSSEC, valid security headers, and few threats score higher. On the other hand, websites with open ports, unconfigured firewalls, or known threats see their scores drop. This helps us identify where improvements are needed so we can make websites safer for everyone [25-45].

The scoring model focuses on protection by giving advice for any improvement. For example, websites that don't have proper HTTP headers or have weak TLS configurations will be given proper recommendations to improve the security structure of the website. These findings support the fact that a multi-layered security approach is necessary to safeguard websites effectively.The discussion also proves that many websites often ignore basic security measures due to either lack of awareness or since it is expensive to implement it [45-51].

NetSentinel works as a comprehensive tool to address these issues and provides practical steps to mitigate vulnerabilities and improve the overall website security.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

Fig. 5: Results Page

Conclusion:

The NetSentinel platform helps meet the growing need for thorough website security checks by providing a detailed look at several key security features. Its scoring system assesses things like SSL certificates, DNSSEC, potential threats, security headers, TLS settings, open ports, and firewalls. This gives website owners a clear idea of how secure their site is. It not only shows where vulnerabilities are but also gives practical suggestions for improvement, making it a helpful tool for administrators who want to keep their sites safe from cyber threats. Our analysis found that while many websites use SSL for protection, they often ignore other important security measures like DNSSEC and proper security headers. This is a problem because it means they may not be fully secure. We also discovered that when threats are detected, a website's security score drops. This highlights the need for websites to be proactive in finding and addressing potential threats to improve their overall security. By providing detailed information and easy-to-understand recommendations, NetSentinel helps the users to improve their defense mechanism against any potential vulnerabilities. As we see the increasing cyber-attacks around the world it very necessary for websites to improve their overall security posture and be aware of the potential threats and Net sentinel's adaptive and multi-layered approach does the exact job. In conclusion, NetSentinel proves to be an effective and essential tool for maintaining website security in today's increasingly hostile online environment.

Acknowledgement:

First and foremost, we would want to express our gratitude to Atharva Ashish Talathi, the primary group leader and principal architect of NetSentinel. His devotion, vision, and leadership were crucial to the project's successful completion from the beginning.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

Second, we would like to thank Darshit Mehta, the second author and developer, for his significant contributions to the development of the website and the incorporation of the core features that create the structure of the platform.We are also grateful to Vaidehi Thombare and Janhavi Dhayria for their significant contributions to the documentation and study. The quality and depth of the work were greatly improved by Vaidehi's crucial contributions to the project's thorough investigation and accurate documentation. Along with Vaidehi's work, Janhavi made a significant contribution to the research and documentation, which helped the project go forward as a whole. Lastly, we want to thank Sahil Daware for his little but significant efforts, which were crucial to the project's successful conclusion.

References:

1. 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
2. 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).
3. 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
4. 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
5. 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
6. Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. *CSI Communications*, 19-20.
7. 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
8. 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
9. 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.
10. 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
11. Dhumane, A., Chiwhane, S., Mangore Anirudh, K., & Ambala, S. (2022). Cluster-based energy-efficient routing in Internet of Things. In *ICT with Intelligent*

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

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

12. 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
13. 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
14. 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
15. 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
16. 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
17. 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
18. 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
19. Midhunchakkaravarthy, D., & Dhumane, A. (2020). Routing Protocols in Internet of Things: A Survey. 2273
20. 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
21. 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
22. 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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

23. 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
24. 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
25. 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
26. 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
27. 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
28. 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
29. 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
30. 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
31. 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 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCUBEA58933.2023.10392268
32. 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
33. 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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

Vision. *International Journal of Innovations in Engineering Research and Technology*, *8*(06), 184-193. https://doi.org/10.17605/OSF.IO/GHWDY

34. 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.
35. 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
36. 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
37. 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.
38. Kharabe, S., & Nalini, C. (2018). Survey on finger-vein segmentation and authentication. *Int J Eng Technol*, *7*(1-2), 9-14.
39. 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.
40. 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
41. 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
42. 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
43. 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
44. 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
45. 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
46. 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

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 4
Pages: 1-17

47. 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
48. 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
49. 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
50. 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
51. 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