International Journal for Modern Trends in Science and Technology
Volume 10, Issue 02, pages 143-150.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue02.html
DOI: https://doi.org/10.46501/IJMTST1002020

Vulnerability Scanner Build a Tool That Scans a System forPotential Vulnerability

P.Premchand, Galla.Tinkuvasavya, Muppavarapu.Thilak Raghavendra, Gangineni.Gopi, Narla.Bhaskar

Department of Computer Science and Engineering – Cyber Security, Chalapthi Institute of Technology,Guntur, Andhra Pradesh, India.

To Cite this Article
P.Premchand, Galla.Tinkuvasavya, Muppavarapu.Thilak Raghavendra, Gangineni.Gopi, Narla.Bhaskar, Vulnerability Scanner Build a Tool That Scans a System forPotential Vulnerability, International Journal for Modern Trends in Science and Technology, 2024, 10(02), pages. 143-150. https://doi.org/10.46501/IJMTST1002020

Article Info
Received: 24 January 2024; Accepted: 19 February 2024; Published: 20 February 2024.

ABSTRACT

In the ever-evolving landscape of information technology, ensuring the security and resilience of digital assets is paramount. Vulnerability scanners play a crucial role in this endeavour by systematically and comprehensively examining computer systems, networks, and applications to identify potential weaknesses and security gaps. This abstract introduces a state-of-the-art vulnerability scanner, a robust tool designed for proactive cybersecurity measures. The vulnerability scanner employs a multifaceted approach, combining automated scanning techniques with human intelligence to detect known vulnerabilities, misconfigurations, and potential entry points for unauthorized access. Utilizing a comprehensive vulnerability database, the scanner keeps pace with emerging threats and continuously updates its knowledge base.Key functionalities include network reconnaissance, system fingerprinting, and in-depth analysis of application code and configurations. The scanner's results are presented in a clear and actionable format, providing security professionals with prioritized recommendations to address identified vulnerabilities effectively. Furthermore, the tool facilitates compliance with industry standards and regulatory requirements, ensuring a resilient security posture. Thisabstractsfewer thanscore the significance of proactive vulnerability management in the face of an evolving threat landscape. The vulnerability scanner presented here serves as a vital component in the arsenal of cybersecurity measures, empowering organizations to fortify their digital infrastructure and safeguard sensitive information from potential cyber threats.

Keywords: Socket.IO, Broadcasting Messages, CORS, and Vulnerability Database Integration

1. INTRODUCTION

The Socket.IO Chat Application is a real-time messaging web application built using Flask, Socket.IO, and CORS. It allows users to communicate with each other in real-time through a simple chat interface. Real-Time Communication: Users can send and receive messages in real-time without the need to refresh the page.The chat interface is designed to be intuitive and user-friendly, with a text input field for typing messages and a button to send them.Messages sent by one user are broadcasted to all connected clients, allowing for group communication.Flask: Flask is a lightweight web

framework for Python used to build web applications.Socket.IO is a JavaScript library that enables real-time, bidirectional, and event-based communication between web clients and servers. It provides WebSocket support as well as fallbacks for environments where WebSocket is not available.CORS is a mechanism that allows web servers to specify which origins are permitted to access their resources. In this project, CORS is enabled to allow cross-origin requests from the client-side JavaScript code to the Flask server.

Python Server (Flask): The Flask server handles HTTP requests and WebSocket connections. It serves the static HTML file and handles Socket.IO events.The client-side JavaScript code establishes a WebSocket connection with the server using Socket.IO. It listens for incoming messages and sends messages typed by the user to the server.Starting the Server: The Flask server can be started by running the app.py script. This starts the server on localhost port 5001.Users can access the chat interface by navigating to http://localhost:5001 in a web browser.

Users can type messages in the input field and click the "Send" button to send them. The messages will be displayed in the chat interface in real-time.User Authentication: Implement user authentication to allow users to log in and have unique identities in the chat.Store chat messages in a database to preserve message history across server restarts.Improve the user interface and experience by adding features such as message timestamps, user avatars, and message styling.

2. LITERATURE REVIEW

The development of real-time messaging applications using web technologies has gained significant attention in recent years due to the increasing demand for instant communication solutions. Several studies and projects have explored various frameworks and libraries to implement real-time features in web applications. Here is a literature survey discussing relevant research and resources related to the Socket.IO Chat Application. A literature survey for your vulnerability scanner project involves reviewing existing research, publications, and resources related to vulnerability scanning, cybersecurity, and related topics.

Dhanjani, N., Rios, B., & Hardin, B. (2009).Hacking: The Next Generation. O'Reilly Media, Inc.This book provides insights into common vulnerabilities and exploitation techniques, offering valuable knowledge for developing effective vulnerability scanning algorithms.

Beale, J., & Weiss, J. (2010).Protecting Industrial Control Systems from Electronic Threats.Momentum Press.Focuses on vulnerabilities and security measures specific to industrial control systems, which can inform the development of targeted scanning techniques for critical infrastructure.

Gordon, S., et al. (2002).Building Secure Software: How to Avoid Security Problems the Right Way.Pearson Education.Offers principles and practices for building secure software, including vulnerability mitigation strategies that can be incorporated into the design and development of the vulnerability scanner.

Northcutt, S., et al. (2004). Network Security Assessment: Know Your Network. O'Reilly Media, Inc.Provides guidance on conducting network security assessments, including vulnerability scanning techniques and best practices for identifying and mitigating security risks.

National Institute of Standards and Technology (NIST). (2008). NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment.Offers guidelines and best practices for information security testing and assessment, including vulnerability scanning methodologies and standards.

Microsoft.(Website).Microsoft Security Vulnerability Research &Defense.Provides insights into Microsoft's approach to vulnerability research and defense, including security advisories, best practices, and tools for vulnerability scanning and mitigation.

Open Web Application Security Project (OWASP). (Website).OWASP Top Ten.Offers insights into common web application vulnerabilities and mitigation strategies, which can inform the development of web-focused vulnerability scanning capabilities.

CERT Coordination Center.(Website).CERT Vulnerability Analysis.Provides vulnerability analysis resources and advisories, offering insights into emerging threats and vulnerabilities that can be addressed through vulnerability scanning.Common Vulnerabilities and Exposures (CVE).(Website).CVE Database.A comprehensive database of publicly known information

security vulnerabilities and exposures, providing valuable data for vulnerability scanning and assessment.

National Vulnerability Database (NVD). (Website).NVD - National Vulnerability Database.A repository of standards-based vulnerability management data, including vulnerability descriptions and severity assessments, which can be leveraged to enhance the accuracy and effectiveness of vulnerability scanning [8].

3. SYSTEM MODELLING:

As of now, there are several existing vulnerability scanning systems available in the market, each with its own set of features, capabilities, and target audiences. Here are a few examples of existing vulnerability scanning systems:
Nessus:Developed by Tenable, Nessus is one of the most widely used vulnerability scanning tools in theindustry.It offers comprehensive vulnerability assessment capabilities, including network scanning, host discovery, and web application scanning.Nessus provides detailed reports with prioritized remediation steps and integrates with other security tools for automated workflows [8].

OpenVAS (Open Vulnerability Assessment System):OpenVAS is an open-source vulnerability scanning tool that offers similar capabilities to commercial solutions like Nessus.It provides network scanning, vulnerability detection, and reporting functionalities, with a focus on affordability and flexibility.

Qualys Vulnerability Management:Qualys offers a cloud-based vulnerability management platform that provides continuous monitoring, assessment, and remediation of security vulnerabilities.It offers comprehensive vulnerability scanning capabilities across IT infrastructure, including endpoints, servers, network devices, and cloud environments.Qualys Vulnerability Management integrates with other security solutions and provides centralized reporting and analytics for informed decision-making.

Nexpose:Developed by Rapid7, Nexpose is an enterprise-grade vulnerability management solution that offers advanced scanning capabilities and analytics.It provides real-time visibility into security risks across IT assets, with features such as asset discovery, vulnerability prioritization, and threat intelligence integration.Nexpose offers customizable dashboards and reporting options to facilitate collaboration and decision-making within organizations [9].

Acunetix:Acunetix is a web vulnerability scanner that focuses on identifying and mitigating security vulnerabilities in web applications and APIs.It offers features such as black-box scanning, white-box scanning, and interactive scanning to detect a wide range of vulnerabilities, including SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.Acunetix provides detailed reports with remediation recommendations and integrates with issue tracking systems for streamlined vulnerability management [8].

Burp Suite:Burp Suite is a popular toolkit for web application security testing developed by PortSwigger.It offers a wide range of tools for manual and automated testing of web applications, including scanning for vulnerabilities such as SQL injection, cross-site scripting (XSS), and broken authentication.Burp Suite is widely used by security professionals and penetration testers for identifying and exploiting vulnerabilities in web applications.

3.1Proposed system:

The proposed vulnerability scanner is a comprehensive security tool designed to proactively identify and mitigate potential vulnerabilities within computer systems. It offers a range of features and functionalities to enable users to conduct thorough vulnerability assessments, prioritize remediation efforts, and enhance the overall security posture of their systems.

Multi-Platform Support: The vulnerability scanner supports scanning of various platforms, including desktop computers, servers, and network devices, running popular operating systems such as Windows, Linux, and macOS.Comprehensive Scanning Techniques: Utilizes a variety of scanning techniques, including port scanning, service enumeration, configuration analysis, and vulnerability checks, to identify potential security weaknesses within target systems.Vulnerability Database Integration: Interfaces with a centralized vulnerability database to retrieve information about known vulnerabilities, including

descriptions, severity levels, and remediation steps, to aid in the scanning process.

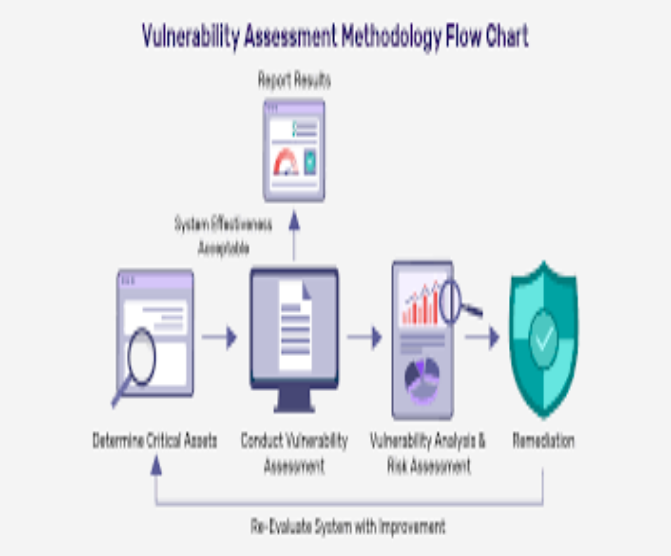

Fig 1:Vulnerability Assessment Types

Customizable Scanning Parameters: Allows users to customize scanning parameters and options based on their specific requirements and preferences, including scan targets, scanning frequency, and reporting preferences.Real-Time Reporting and Alerts: Generates real-time reports detailing identified vulnerabilities, their severity levels, and recommended remediation steps, enabling users to take immediate action to address critical security issues. Additionally, provides alerting mechanisms to notify users of critical vulnerabilities requiring immediate attention.User-Friendly Interface: Features an intuitive user interface with clear navigation and informative feedback to facilitate ease of use for users of varying technical backgrounds [8].

Integration with External Systems: Integrates with external systems such as SIEM (Security Information and Event Management) platforms, ticketing systems, and threat intelligence feeds to enhance threat detection capabilities and streamline incident response processes.

3.2. Architecture:

Scanning Engine: Conducts vulnerability scans on target systems using predefined scanning techniques and algorithms.

User Interface: Provides an interface for users to interact with the vulnerability scanner, configure scanning parameters, initiate scans, and view scan results.

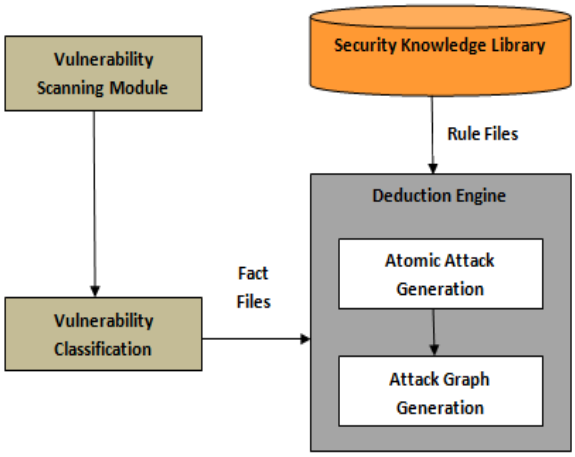

Fig 2: Vulnerability Scanner Architecture

Vulnerability Database: Stores information about known vulnerabilities and provides an interface for accessing this information during scans.

Reporting Module: Generates comprehensive reports based on scan results, including identified vulnerabilities, severity levels, and recommended remediation steps [9].

Integration Points: Interfaces with external systems such as SIEM platforms, ticketing systems, and threat intelligence feeds for enhanced functionality and interoperability [8].

3.3. Benefits: Proactive Vulnerability Management: Enables organizations and individuals to proactively identify and mitigate potential security vulnerabilities within their systems, reducing the risk of security breaches and data loss.Comprehensive Security Assessments: Offers comprehensive scanning capabilities across various platforms and environments

Streamlined Incident Response: Facilitates streamlined incident response processes through real-time reporting, alerts, and integration with external systems, enabling organizations to rapidly address security threats and vulnerabilities.Usability and Accessibility: Features an intuitive user interface and customizable reporting options to enhance usability and accessibility for users of all skill levels [7].

4. Future Enhancements:

Advanced Scanning Techniques: Explore the integration of advanced scanning techniques such as heuristic analysis, machine learning, and artificial intelligence to enhance vulnerability detection capabilities [4].

Support for Emerging Technologies: Extend support for emerging technologies such as cloud infrastructure, containerization, and IoT devices to address evolving security challenges.

Automated Remediation: Implement automated remediation capabilities to enable the automatic application of security patches and configuration changes.

Enhanced Collaboration and Threat Sharing: Integrate collaborative threat sharing capabilities to facilitate information exchange and collaboration among security professionals and organizations.

5. SYSTEM DEVELOPMENT

The system development for the Socket.IO Chat Application involves several key steps to create a real-time messaging platform. Initially, requirements are gathered to understand the stakeholders' needs and expectations. With this information, the system architecture is designed, considering both server-side (Flask, Socket.IO) and client-side (HTML, python) components, as well as the communication protocol (Web Socket) and data storage requirements. Once the environment is set up, development begins with the creation of the Flask server to handle HTTP requests and Web Socket connections using Socket.IO, alongside the client-side interface development. Integration and testing follow to ensure proper functionality, security measures are implemented to protect against common web vulnerabilities, and the application is deployed to a production environment. Ongoing maintenance, user authentication and authorization implementation, scaling, optimization, documentation, and continuous improvement complete the system development process, ensuring a robust, secure, and scalable real-time messaging platform.Identify the stakeholders and gather requirements for the chat application. Determine the features, functionality, and performance expectations.

1.ArchitectureDesign:Design the system architecture, including server-side components (Flask, Socket.IO) and client-side components (HTML, JavaScript). Decide on the communication protocol (WebSocket) and data storage requirements.

2. Environment Setup: Set up the development environment with Flask, Socket.IO, and any necessary dependencies. Configure CORS settings for cross-origin resource sharing.

3. Server-Side Development:Develop the Flask server to handle HTTP requests, serve static files (HTML, python), and establish WebSocket connections using Socket.IO. Implement event handlers for message broadcasting.

4. Client-Side Development: Develop the client-side interface using HTML, CSS, and JavaScript. Establish a WebSocket connection to the server using Socket.IO and handle message sending and receiving events.

5. Integration and Testing: Integrate the server-side and client-side components. Conduct unit testing, integration testing, and system test to ensure the application functions as expected. Test for real-time message delivery, cross-browser compatibility, and responsiveness.

6. Security Implementation: Implement security measures to protect against common web vulnerabilities, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). Configure CORS settings and enforce secure WebSocket connections.

7. Deployment: Deploy the application to a production environment. Choose a hosting platform (e.g., Heroku, AWS) and configure the deployment settings. Monitor the application for performance, scalability, and security issues.

8. User Authentication and Authorization: Implement user authentication and authorization mechanisms to control access to the chat application. Integrate with a user management system or implement custom authentication logic.

9. Maintenance and Support: Provide ongoing maintenance and support for the chat application. Monitor for bugs, performance issues, and security vulnerabilities. Regularly update dependencies and address user feedback.

10. Scaling and Optimization: Monitor application performance and scalability as user traffic increases. Implement scaling strategies, such as load balancing and horizontal scaling, to handle increased demand. Optimize code, database queries, and network communication for improved performance [8].

11. Documentation: Document the system architecture, deployment process, and development guidelines. Provide user documentation and support resources for end-users.

6. CONCLUSIONS

In conclusion, the development of the vulnerability scanner represents a significant milestone in enhancing cybersecurity measures for both organizations and individuals. The project aimed to address the critical need for proactive identification and mitigation of potential vulnerabilities within computer systems, thereby bolstering their resilience against malicious threats and attacks. Through meticulous planning, design, and implementation, the vulnerability scanner has emerged as a robust and indispensable tool for fortifying the security posture of target systems.

7. Future scope

While your vulnerability scanner project has achieved significant milestones in enhancing cybersecurity measures, there are several avenues for future development and expansion to further strengthen its capabilities and address emerging challenges in the cybersecurity landscape. The following are potential areas of future scope for your project:

Advanced Scanning Techniques: Explore the integration of advanced scanning techniques, such as heuristic analysis, machine learning, and artificial intelligence, to enhance the accuracy and efficiency of vulnerability detection. These techniques can help identify previously unknown vulnerabilities and adapt to evolving attack vectors.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] National Institute of Standards and Technology (NIST). "NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment." NIST, 2008. (Offers guidelines and best practices for information security testing and assessment, including vulnerability scanning.)

[2] Microsoft. "Microsoft Security Vulnerability ResearchDefense."[Website].Available:https://msrc-blog.microsoft.com/. (Provides insights into Microsoft's approach to vulnerability research and defense, including security advisories and best practices.)

[3] Kalyan Kumar Dasari & Dr, K.Venkatesh Sharma, "Mobile Agent Applications in Intrusion Detection System (IDS)"-JASC, Volume 4, Issue 5, October/2017, ISSN NO:1076-5131, Pages: 97-103.

[4] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System"-JASRAE, Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540, Pages: 566-573.

[5] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, "A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework"-JASRAE, Vol. XI, Issue No. 22, July-2016, ISSN 2230-7540, Pages: 209-214

[6] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[7] K. K. .Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J IntellSystApplEng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[8] Kalyan Kumar Dasari& M.Prabhakar "Professionally Resolve the Password Security knowledge in the Contexts of Technology"-IJCCIT, Vol. 3, Issue. 1, April' 2015;ISSN: 2345 – 9808 (2015).

[9] V.Mounika D. Kalyan Kumar "Background Subtraction by Using DE Color Algorithm" -IJATCSE, ISSN 2278-3091 Vol: 3, No: 1, Pages: 273-277(2014).

[10] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023- 15926-5

[11] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., &Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[12] K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. KhaderBasha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

[13] VenkateswaraRao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., &Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE [6]

[14] S Phani Praveen, RajeswariNakka, AnuradhaChokka, VenkataNagarajuThatha, SaiSrinivasVellela and UddagiriSirisha, "A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[15] Vellela, S. S., &Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[16] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., &Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[17] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583-021X), 2(1).

[18] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07), 2020.

[19] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[20] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[21] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers.In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409).IEEE.

[22] Vellela, S. S., BashaSk, K., &Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[23] Rao, M. V., Vellela, S. S., Sk, K. B., Venkateswara, R. B., &Roja, D. (2023). SYSTEMATIC REVIEW ON SOFTWARE APPLICATION UNDERDISTRIBUTED DENIAL OF SERVICE ATTACKS FOR GROUP WEBSITES. DogoRangsang Research Journal UGC Care Group I Journal, 13(3), 2347-7180.

[24] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., &Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[25] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.

[26] Sk, K. B., &Vellela, S. S. (2019). Diamond Search by Using Block Matching Algorithm. DIAMOND SEARCH BY USING BLOCK MATCHING ALGORITHM. International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[27] Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., &Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[28] Vellela, SaiSrinivas and Chaganti, Aswini and Gadde, Srimadhuri and Bachina, Padmapriya and Karre, Rohiwalter, A Novel Approach for Detecting Automated Spammers in Twitter (June 24, 2023). MuktShabd Journal Volume XI, Issue VI, JUNE/2022 ISSN NO : 2347-3150, pp. 49-53 , Available at SSRN: https://ssrn.com/abstract=4490635

[29] Vellela, SaiSrinivas and Pushpalatha, D and Sarathkumar, G and Kavitha, C.H. and Harshithkumar, D, ADVANCED INTELLIGENCE HEALTH INSURANCE COST PREDICTION USING RANDOM FOREST (March 1, 2023). ZKG International, Volume VIII Issue I MARCH 2023, Available at SSRN: https://ssrn.com/abstract=4473700

[30] Dalavai, L., Javvadi, S., Sk, K. B., Vellela, S. S., &Vullam, N. (2023). Computerised Image Processing and Pattern Recognition by Using Machine Algorithms.

[31] Vellela, S. S., BashaSk, K., &Javvadi, S. (2023). MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE. MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE", International Journal of Emerging Technologies and Innovative Research (www. jetir. org| UGC and issn Approved), ISSN, 2349-5162.

[32] Vellela, SaiSrinivas and Sk, KhaderBasha and B, Venkateswara Reddy, Cryonics on the Way to Raising the Dead Using Nanotechnology (June 18, 2023). INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS), Vol. 03, Issue 06, June 2023, pp : 253-257,

[33] Vellela, SaiSrinivas and D, Roja and B, Venkateswara Reddy and Sk, KhaderBasha and Rao, Dr M Venkateswara, A New Computer-Based Brain Fingerprinting Technology (June 18, 2023). International Journal Of Progressive Research In Engineering Management And Science, Vol. 03, Issue 06, June 2023, pp : 247-252 e-ISSN : 2583-1062.,

[34] Gajjala, Buchibabu and Mutyala, Venubabu and Vellela, SaiSrinivas and Pratap, V. Krishna, Efficient Key Generation for Multicast Groups Based on Secret Sharing (June 22, 2011). International Journal of Engineering Research and Applications,Vol. 1, Issue 4, pp.1702-1707, ISSN: 2248-9622 .

[35] Venkateswara Reddy, B., &KhaderBashaSk, R. D. Qos-Aware Video Streaming Based Admission Control And Scheduling For Video Transcoding In Cloud Computing. In International Conference on Automation, Computing and Renewable Systems (ICACRS 2022).

[36] Reddy, N. V. R. S., Chitteti, C., Yesupadam, S., Desanamukula, V. S., Vellela, S. S., &Bommagani, N. J. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmesd'Information, Vol. 28, No. 4.

[37] Vellela, S. S., &Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.

[38] Rao, D. M. V., Vellela, S. S., Sk, K. B., &Dalavai, L. (2023). Stematic Review on Software Application Under-distributed Denial of Service Attacks for Group Website. DogoRangsang Research Journal, UGC Care Group I Journal, 13.

[39] Priya, S. S., Vellela, S. S., Reddy, V., Javvadi, S., Sk, K. B., &Roja, D. (2023, June). Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[40] Vullam, N., Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., &Priya, S. S. (2023, June). Prediction And Analysis Using A Hybrid Model For Stock Market. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[41] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[42] Sk, K. B., Vellela, S. S., Yakubreddy, K., &Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. KhaderBashaSk, Venkateswara Reddy B, SaiSrinivasVellela, KancharakuntYakub Reddy, M VenkateswaraRao, Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation, 10(3).

[43] Vellela, S. S., Sk, K. B., Dalavai, L., Javvadi, S., &Rao, D. M. V. (2023). Introducing the Nano Cars Into the Robotics for the Realistic Movements. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3, 235-240.

[44] Kumar, K. &Babu, B. &Rekha, Y.. (2015). Leverage your data efficiently: Following new trends of information and data security. International Journal of Applied Engineering Research. 10. 33415-33418.

[45] Vellela, S. S., Reddy, V. L., Roja, D., Rao, G. R., Sk, K. B., & Kumar, K. K. (2023, August). A Cloud-Based Smart IoT Platform for Personalized Healthcare Data Gathering and Monitoring System. In 2023 3rd Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-5). IEEE.

[46] Davuluri, S., Kilaru, S., Boppana, V., Rao, M. V., Rao, K. N., &Vellela, S. S. (2023, September). A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 2447-2453). IEEE.

[47] Vellela, S. S., Vuyyuru, L. R., MalleswaraRaoPurimetla, N., Dalavai, L., &Rao, M. V. (2023, September). A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1677-1681). IEEE.

[48] Vellela, S. S., Roja, D., Sowjanya, C., SK, K. B., Dalavai, L., & Kumar, K. K. (2023, September). Multi-Class Skin Diseases Classification with Color and Texture Features Using Convolution Neural Network. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1682-1687). IEEE.

[49] Vellela, S. S., Sk, K. B., & Reddy, V. An Intelligent Decision Support System for retrieval of patient's information.

[50] Rao, M. V., Sreeraman, Y., Mantena, S. V., Gundu, V., Roja, D., &Vatambeti, R. (2023). Brinjal Crop yield prediction using Shuffled shepherd optimization algorithm based ACNN-OBDLSTM model in Smart Agriculture. Journal of Integrated Science and Technology, 12(1), 710. Retrieved from https://pubs.thesciencein.org/journal/index.php/jist/article/view/a710

[51] Vellela, S. S., Narapasetty, S., Somepalli, M., Merikapudi, V., &Pathuri, S. (2022). Fake News Articles Classifying Using Natural Language Processing to Identify in-article Attribution as a Supervised Learning Estimator. MuktShabd Journal, 11.

[52] V. R. B, K. BashaSk, R. D, N. RaoPurimetla, S. S. Vellela and K. K. Kumar, "Detection of DDoS Attack in IoT Networks Using Sample elected RNN-ELM," 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G NAGARA, India, 2023, pp. 1-7, doi: 10.1109/ICRASET59632.2023.10420193.

[53] E. S. R. R. Kumar et al., "UAVC: Unmanned Aerial Vehicle Communication Using a Coot Optimization-Based Energy Efficient Routing Protocol," 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G NAGARA, India, 2023, pp. 1-5, doi: 10.1109/ICRASET59632.2023.10420027

[54] S Phani Praveen, SaiSrinivasVellela, Dr. R. Balamanigandan,Hrituparna Paul, , " SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication", Journal of Next Generation Technology (ISSN: 2583-021X), 4(1), pp.25-36 . Jan 2024.

[55] Mohd, A. A., Kummarikunta, S., Thumboor Naga, S. K., Buthukuri, V. R., Chintamaneni, P., &Vatambeti, R. (2023). Design of Mutual Authentication Method for Deep Learning Based Hybrid Cryptography to Secure data in Cloud Computing. International Journal of Safety & Security Engineering, 13(5).