International Journal for Modern Trends in Science and Technology
Volume 10, Issue 02, pages 110-116.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue02.html
DOI: https://doi.org/10.46501/IJMTST1002015

A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System

Dr.D.Kalyankumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh, Siddi Pavan Kumar

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

To Cite this Article
Dr.D.Kalyan Kumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh and Siddi Pavan Kumar, A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System, International Journal for Modern Trends in Science and Technology, 2024, 10(02), pages. 110-116. https://doi.org/10.46501/IJMTST1002015

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

ABSTRACT

In the rapidly evolving landscape of cyber security, the prevalence and sophistication of cyber threats demand robust and intelligent defense mechanisms. This project introduces an advanced Intrusion Detection System (IDS) designed to proactively identify and respond to malicious activities within computer networks. The system employs a multi-layered architecture, leveraging cutting-edge technologies to enhance the detection and mitigation of diverse cyber threats.The proposed IDS consists of strategically deployed sensors and agents across the network, collecting and analyzing data from various sources, including network traffic, system logs, and user behaviors. A sophisticated detection engine utilizes a combination of rule-based signatures and anomaly detection algorithms, providing a comprehensive approach to identifying known and unknown threats. The system's pre-processing mechanisms ensure efficient handling of large volumes of data, while normalization techniques maintain consistency in the representation of diverse data types. The proposed IDS integrate seamlessly with existing security infrastructure, fostering a holistic cyber security ecosystem. The project aims to contribute to the ongoing efforts in enhancing the overall security posture of organizations and safeguarding sensitive information from an ever-growing array of cyber threats. Through its intelligent design and adaptability, the Intelligent Intrusion Detection System represents a significant step forward in the realm of proactive cyber security measures.

Keywords: Intrusion Detection System (IDS), Network-Based IDS (NIDS), Detection EngineandNext-Generation IDS (NG-IDS).

1. INTRODUCTION

Cyber security is a paramount concern in the digital age, where organizations and individuals face an ever-expanding array of sophisticated threats. One crucial component of a robust cyber security strategy is an Intrusion Detection System (IDS). An IDS acts as a vigilant guardian, continuously monitoring network traffic and system activities to identify and respond to potential security incidents or malicious activities.

An Intrusion Detection System (IDS) is a crucial component of cyber security that helps protect computer systems and networks from unauthorized access, malicious activities, and security threats. Its primary function is to monitor network or system activities, analyze them for signs of potential security incidents, and provide timely alerts or responses to mitigate risks[1].

1. **Purpose:**Detection of Anomalies: IDS monitors network or system activities and identifies abnormal patterns or behaviors that may indicate a security breach.Signature-Based Detection: It compares observed activities against a database of known attack signatures to identify known threats.

2. **Types of Intrusion Detection Systems:**Network-Based IDS (NIDS): Monitors network traffic and analyzes packets to detect suspicious patterns or behaviors.Host-Based IDS (HIDS): Operates on individual devices, monitoring activities like file changes, logins, and system calls. Anomaly-Based IDS: Focuses on detecting deviations from normal behavior, often using statistical models or machine learning algorithms.

3. **Components:**Sensors: Collect data from the network or system for analysis. Analyzers: Examine the collected data to identify patterns or anomalies.User Interface/Console: Presents information to security administrators and **allows** them to manage and respond to alerts.Alerting System: Generates alerts when suspicious activities are detected.

4. **Deployment Locations:** Perimeter IDS: Monitors network traffic at the boundary between internal and external networks. Internal IDS: Focuses on monitoring activities within the internal network. Host-Based IDS: Installed on individual devices to monitor local activities**.**

5. **Challenges and Considerations:**False Positives/Negatives: Balancing the sensitivity to detect real threats while minimizing false alarms. Scalability: Adapting to the scale and complexity of modern networks.Encryption: Dealing with encrypted traffic and the challenges it poses to inspection.

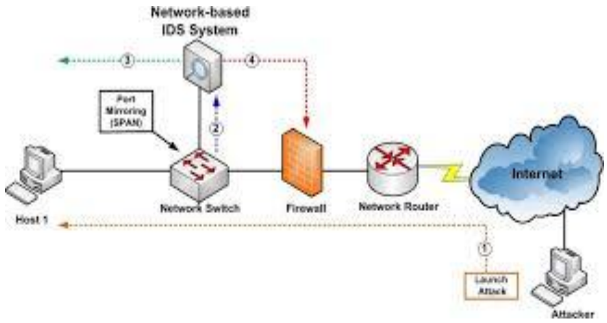

Fig 1: Intrusion Detection System (IDS)

6. **Response Mechanisms:** Passive Response: Generating alerts for human intervention.Active Response: Automatically taking actions to block or contain a threat**.**

7. **Integration with Other Security Measures:** IDS is often part of a larger security strategy that includes firewalls, antivirus software, and other security measures.

8. **Evolution:**Next-Generation IDS (NG-IDS): Incorporates advanced technologies such as machine learning and behavioral analysis for improved threat detection**.**

2. LITERATURE REVIEW

The Chief Information Warfare Officer for the entire United States teaches you how to protect your corporate network. This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. The authors are literally the most recognized names in this specialized field, with unparalleled experience in defending our country's government and military computer networks. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters [3].

Intrusion detection systems (IDS) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. Intrusion detection complements the protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that the users can understand the security threats and risks and thus be better prepared for future attacks.

Intrusion detection techniques are traditionally categorized into two classes: anomaly detection and misuse detection. Anomaly detection is based on the normal behavior of a subject any action that significantly deviates from the normal behavior is considered intrusive. Misuse detection catches intrusions in terms of characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of known attack or vulnerability is considered intrusive [2].

Alternatively, IDS may be classified into host-based IDSs, distributed IDSs, and network based IDSs according to the source of the audit information used by each IDS. Host-based IDSs get audit data from host audit trails and usually aim at detecting attacks against a single host; distributed IDSs gather audit data from multiple hosts and possibly the network and connects the hosts, aiming at detecting attacks involving multiple hosts; network-based IDSs use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services[6].

Intrusion Detection in Distributed Systems: An Abstraction-Based Approach presents research contributions in three areas with respect to intrusion detection in distributed systems. The first contribution is an abstraction-based approach to addressing heterogeneity and autonomy of distributed environments. The second contribution is a formal framework for modeling requests among cooperative IDSs and its application to Common Intrusion Detection Framework (CIDF). The third contribution is a novel approach to coordinating different IDSs for distributed event correlation [7].

3. SYSTEM MODELLING: Developing an Intrusion Detection System (IDS) involves several steps and considerations. Here's a general outline of the process:
Define Requirements: Understand the objectives and requirements of the IDS. Determine what types of threats it should detect, the network or system environment it will monitor, and the level of accuracy and performance expected.Data Collection: Gather relevant data for analysis. This may include network traffic data, system logs, and information about normal system behavior[10].Feature Selection: Identify features or attributes of the data that are relevant for intrusion detection. This may involve statistical analysis, domain knowledge, or machine learning techniques.Model Selection: Choose the appropriate detection model or algorithm. This could be rule-based, anomaly-based, signature-based, or machine learning-based [11].
Training: If using machine learning, train the model using labeled data. Labeled data consists of examples of both normal and anomalous behavior.Testing and Evaluation: Evaluate the performance of the IDS using separate test data. Metrics such as accuracy, precision, recall, and false positive rate are commonly used for evaluation. Deployment: Integrate the IDS into the target environment. This may involve configuring network sensors, setting up monitoring tools, and establishing alerting mechanisms[9].Tuning and Optimization: Continuously monitor the performance of the IDS and fine-tune its parameters as needed. This may involve adjusting thresholds, updating signatures, or retraining machine learning models.

Alert Handling: Define procedures for handling alerts generated by the IDS. This could include escalation paths, incident response protocols, and mechanisms for remediation [14].Maintenance and Updates: Regularly update the IDS to address new threats and vulnerabilities. This may involve updating signatures, retraining machine learning models, or installing patches and updates[13].Monitoring and Reporting: Monitor the effectiveness of the IDS over time and generate reports to stakeholders. This helps ensure that the IDS remains aligned with the organization's security objectives.

Throughout the development process, it's important to consider factors such as scalability, performance, and resource constraints[15]. Additionally, compliance requirements and privacy considerations should be taken into account when designing and deploying IDS.

4. PROPOSED METHOD OFINTRUSION DETECTION SYSTEM (IDS):

Cyber security threats are evolving rapidly, necessitating the development of a robust and proactive defense mechanism. The proposed Next-Generation Intrusion Detection and Prevention System (NG-IDPS) aims to address the limitations of traditional systems and provide an adaptive, intelligent, and comprehensive solution.

Objectives: Enhance threat detection accuracy and reduce false positives through advanced analytics. Provide real-time and adaptive response capabilities to emerging cyber threats. Securely inspect encrypted traffic without compromising privacy. Ensure scalability and compatibility with modern, dynamic network environments. Facilitate seamless integration with existing security infrastructure.

Dynamic Threat Intelligence Integration: Integrate with threat intelligence feeds for real-time updates on the latest attack vectors, enabling the system to proactively defend against emerging threats. Leverage machine-readable threat intelligence formats for efficient data exchange.

Behavioral Analysis Engine: Develop a behavioral analysis engine to establish baseline behavior for users, applications, and devices. Detect anomalous activities by comparing real-time behavior with learned patterns.

Adaptive Rule Engine: Implement an adaptive rule engine that dynamically adjusts detection rules based on network changes and threat landscape evolution. Enable easy customization and rule creation for specific organizational needs.

Encrypted Traffic Inspection: Utilize advanced encryption protocols for secure traffic inspection without compromising user privacy.Employ techniques like secure key management and cryptographic controls to ensure the integrity of the inspection process.

Cloud-Native Architecture: Design the NG-IDPS as a cloud-native solution for scalability and flexibility. Utilize micro services architecture to allow seamless deployment, scaling, and maintenance.

Automated Response Mechanism: Integrate automated response mechanisms to execute predefined actions in response to detected threats.Enable security orchestration for coordinated incident response across the network.

User Interface and Reporting: Develop an intuitive and interactive user interface for security analysts. Provide detailed dashboards, real-time visualizations, and customizable reporting tools.

Security and Compliance: Implement robust encryption and secure communication protocols to protect sensitive data.Ensure compliance with data protection regulations and cyber security standards.

5. NEXT-GENERATION INTRUSION DETECTION AND PREVENTION SYSTEM (NG-IDPS):

Developing an Intrusion Detection System (IDS) involves several steps and considerations. Here's a general outline of the process:Define Requirements: Understand the objectives and requirements of the IDS. Determine what types of threats it should detect, the network or system environment it will monitor, and the level of accuracy and performance expected.Data Collection: Gather relevant data for analysis. This may include network traffic data, system logs, and information about normal system behavior [13].Feature Selection: Identify features or attributes of the data that are relevant for intrus [11]. This may involve statistical analysis, domain knowledge, or machine learning techniques.Model Selection: Choose the appropriate detection model or algorithm. This could be rule-based, anomaly-based, signature-based, or machine learning-based.Training: If using machine learning, train the model using labeled data. Labeled data consists of examples of both normal and anomalous behavior[8].Testing and Evaluation: Evaluate the performance of the IDS using separate test data. Metrics such as accuracy, precision, recall, and false positive rate are commonly used for evaluation[15].

Deployment: Integrate the IDS into the target environment. This may involve configuring network sensors, setting up monitoring tools, and establishing alerting mechanisms.Tuning and Optimization: Continuously monitor the performance of the IDS and fine-tune its parameters as needed[17]. This may involve adjusting thresholds, updating signatures, or retraining machine learning models.Alerthandling: Define procedures for handling alerts generated by the IDS. This could include escalation paths, incident response protocols, and mechanisms for remediation.Maintenance and Updates: Regularly update the IDS to address new threats and vulnerabilities. This may involve updating signatures, retraining machine learning models, or installing patches and updates.Monitoring and Reporting: Monitor the effectiveness of the IDS over time and generate reports to stakeholders[13]. This helps ensure that the IDS remains aligned with the organization's security objectives.

Throughout the development process, it's important to consider factors such as scalability, performance, and resource constraints. Additionally, compliance requirements and privacy considerations should be taken into account when designing and deploying IDS[18].

6. TRAINING PHASE PROPOSED NEXT-GENERATION INTRUSION DETECTION AND PREVENTION SYSTEM (NG-IDPS):

The architecture of an Intrusion Detection System (IDS) can vary depending on factors such as the type of threats being monitored, the scale of the network, and the desired level of security. However, here's a general overview of a typical IDS architecture:

1. Sensors: Sensors are deployed at various points within the network to collect data. These sensors passively monitor network traffic, system logs, or other sources of information. There are different types of sensors, including network-based sensors (e.g., sniffers, network taps) and host-based sensors (e.g., agents installed on individual systems).

2. Pre-Processing Layer: Raw data collected by sensors is pre-processed to extract relevant features and reduce noise. This may involve tasks such as protocol decoding, data normalization, and feature extraction. Pre-processing helps prepare the data for analysis by the detection engine [5].

3. Detection Engine: The detection engine analyzes the pre-processed data to identify potential security threats. There are several approaches to intrusion detection, including:Signature-based detection, Anomaly-based detection, Hybrid approaches Combine both signature-based and anomaly-based techniques for improved accuracy [10].

4. Alerting and Logging: When the detection engine identifies a potential security threat, it generates alerts to notify security personnel. Alerts may include information such as the type of threat detected, the severity level, and the affected system or network segment. Additionally, events and alerts are logged for auditing and forensic purposes [12].

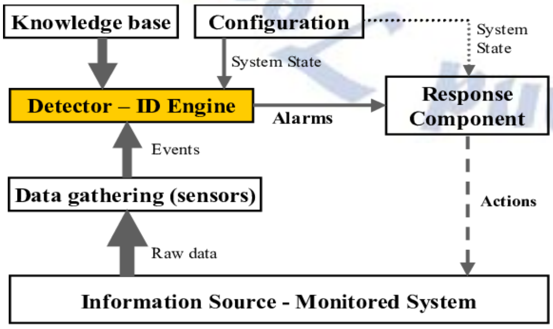

Fig: Architecture of IDS

5. Response Mechanisms: In some IDS architectures, automated response mechanisms may be integrated to mitigate detected threats in real-time. These mechanisms could include blocking malicious traffic, isolating compromised systems, or triggering incident response workflows. Care must be taken to avoid false positives and unintended consequences when implementing automated responses [5].

6. Management and Reporting: A management interface allows security administrators to configure and manage the IDS, view alerts and logs, and generate reports on security incidents and trends. The management interface may also provide features such as policy management, threat intelligence integration, and integration with other security tools and systems[8].

7. Integration with Security Operations Center (SOC): In larger organizations, the IDS may be integrated with a Security Operations Center (SOC) or other centralized security management infrastructure. This allows for centralized monitoring, analysis, and response to security incidents across the organization [11].

8. Scalability and Redundancy: The IDS architecture should be designed to scale with the size and complexity of the network environment. This may involve deploying multiple sensors, load balancing detection tasks, and ensuring redundancy and failover capabilities to maintain continuous monitoring and protection [12].

Overall, the architecture of an ID should be designed to provide comprehensive coverage, timely detection, and effective response to security threats while minimizing false positives and maintaining operational efficiency.

Testing and Evaluation: Conduct rigorous testing, including penetration testing and red teaming, to validate the system's effectiveness.Evaluate the system's performance against various attack scenarios and benchmark against industry standards.

7. CONCLUSIONS

In conclusion, the development and implementation of the intrusion detection system (IDS) represent a significant step forward in bolstering the security infrastructure of our organization. Throughout this project, rigorous research, design, and testing efforts have been undertaken to create a robust system capable of detecting and responding to a wide range of security threats. The successful deployment of the IDS has not only enhanced our organization's ability to identify and mitigate potential intrusions but has also instilled greater confidence in our overall security posture. By leveraging advanced detection algorithms and leveraging the expertise of our team, we have established a proactive defense mechanism against cyber threats. Moving forward, the insights gained from this project will serve as valuable assets, guiding future enhancements and ensuring that our IDS remain adaptive and resilient in the face of evolving security challenges.

Future scope: Explore integration with emerging technologies such as Artificial Intelligence for Threat Hunting (AITH) and threat deception techniques. - Continuously update and expand the threat intelligence capabilities to stay ahead of emerging threats. Investigate the feasibility of incorporating block chain technology for enhanced data integrity in log and event management.

Conflict of interest statement

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

REFERENCES

[1] Kantzavelou, I. and Katsikas, S. K. An attack detection system for secure computer systems - Outline of the solution. In Proceedings of the 13th International Information Security Conference, pages 123-135, May 1997.

[2] M. Sobirey, B. Richter, and H. Konig. The intrusion detection system AID. Architecture, and experiences in automated audit analysis. In Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security, pages 278-290, September 1996.

[3] AIMS was mentioned in GAO Executive Report - B-266140, Information Security - Computer Attacks at Department of Defense Pose Increasing Risks, May 1996.

[4] Moitra, A. Real-time Audit Log Viewer and Analyzer. In Proceedings of the 4th Workshop on Computer Security Incident Handling (Forum of Incident Response and Security Teams - FIRST), August 1992.

[5] Kalyan Kumar Dasari&amp; 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.

[6] 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.

[7] 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

[8] 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.

[9] 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.

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

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

[12] 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

[13] 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.

[14] 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.

[15] 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]

[16] 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

[17] 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.

[18] 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.

[19] 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).

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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).

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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).

[30] 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

[31] 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

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

[33] 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.

[34] 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,