Impact and limitations of artificial intelligence in cyber security awareness

Dr.C.SENTHIL SELVI* ,Ramesh NSVSC Sripada, Gunawan Widjaja, RADHA.T, Auadhati Datta

Assistant Professor,Department of Computer Applications,B S Abdur Rahman Crescent Institute of Science and Technology,Vandalur,Chennai. selvichandramohan2019@gmail.com
Department of CSE, Aditya College of Engineering & Technology, Surampalem, ramesh.snsvsc@acet.ac.in
Universitas Pancasila ,widjaja_gunawan@yahoo.com
Assistant Professor, Department of Commerce, St Claret College, Bangalore, radhasaran26@gmail.com
Assistant Professor, Department of Management Studies, Vignan's Institute of Information Technology, Duvvada, auadhati.sriditi@gmail.com

Abstract:

The rapid advancement of technology has ushered in the era of artificial intelligence (AI), which has brought transformative changes to various fields, including cybersecurity. This paper delves into the intricate interplay between AI and cybersecurity awareness, exploring both the significant impacts and the inherent limitations of leveraging AI for bolstering cybersecurity awareness efforts. Through an in-depth analysis of recent developments, case studies, and expert opinions, this research paper aims to provide a comprehensive understanding of the role of AI in shaping the landscape of cybersecurity awareness.

Keywords : Cyber security Awareness ,Small and Medium Enterprises (SMEs) , Internet of Things (IoT), Cybersecurity Education ,SME Security Practices ,Cyber Threats, IoT Data Security, IoT Security Management, IoT Data Security, Cyber security Policy

DOI: 10.48047/ecb/2023.12.8.717

Introduction:

The field of cybersecurity is at a crossroads in an era characterized by the relentless surge of digital transformation, juggling both rising risks and unheard-of opportunities. Artificial intelligence (AI), a technical marvel that has transcended conventional boundaries and permeated sectors with its promise of automation, insight, and augmentation, is at the center of this paradigm change. The combination of AI with cybersecurity awareness marks a crucial advancement in how businesses protect themselves from the onslaught of cyberthreats. Threat detection could be revolutionized by this synergy, which also has the power to enhance response capabilities and improve user training. But while AI plays a bigger and bigger part in cybersecurity awareness, it also presents complex dynamics of impact and restrictions that demand careful investigation. [1];Cyberattacks are becoming more sophisticated at an increasing rate, which calls for protection methods to keep pace. AI is positioned to play a key role in this proactive defensive approach thanks to its capacity to process enormous volumes of data and recognize complex patterns. AI-driven solutions herald a paradigm shift from conventional rule-based systems to intelligent, learning-oriented models, promising real-time monitoring, early danger identification, and adaptive response mechanisms.[2]; Additionally, AI's personalized user education strategy has enormous promise for

developing a workforce that is security-conscious by adapting training materials to specific learning demands and knowledge gaps. These effects demonstrate how AI has the potential to increase cybersecurity awareness and serve as a vital defense against a constantly changing digital threat scenario.

But there are difficulties in this mutually beneficial link between AI and cybersecurity awareness. A collection of limits that the revolutionary power of AI encounters necessitate careful examination. Artificial intelligence-driven threat detection techniques have a tendency to produce false positives and negatives, which might result in alert fatigue or hidden vulnerabilities. Additionally, the vulnerability of AI systems to adversarial attacks reveals a perilous weakness where the very tools used for defense could be used against the defenders. Data bias raises questions about justice and ethics, especially when AI judgments unintentionally reinforce biased outcomes. As businesses manage these complex interactions, it's critical to balance AI's promise with its constraints in order to maximize its benefits while minimizing its drawbacks.

Fig 1:Cyber Security

Literature Review:

Nisha Rawindaran , Ambikesh Jayal, Edmond Prakash (2022) et.al ” Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime” This research paper explains the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales. It explores the use of intelligent software to combat cybercrime and its effectiveness in promoting cybersecurity awareness among SMEs. The authors emphasize the importance of SMEs being aware of cyber threats and prepared to handle them, as well as the need for further research on cyber security risk management in SMEs.

In this article "The Impact and Limitations of Artificial Intelligence in Cyber Security: A Literature Review" from 2022, Meraj Farheen Ansari describes how artificial intelligence (AI) might improve cyber security procedures. The writers present information on how AI can be used to enhance security measures and examine the benefits and drawbacks of AI in cyber security. The limitations and difficulties of deploying AI in cyber security are also highlighted by the author, including the possibility of AI

manipulation by adversaries. The impact of AI on cyber security is discussed in this research article, along with the possibilities for further study in this field.

Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, (2023)" et .al" Artificial intelligence for cyber security: A overview of the literature and recommendations for future research. In this research paper , the author told a complete evaluation of the research and analysis on the use of artificial intelligence (AI) in cyber security. The essay includes an introduction and conception of cyber security and AI themes as well as an explanation of the classification paradigms used in the literature on AI for cyber security. Along with describing the research technique used to conduct the literature review, the study also describes the data extraction process utilized to feed the descriptive analysis and cutting-edge research presented in the review. The author concludes with a descriptive analysis of the synthesis literature review, highlighting a number of research gaps that can be addressed by new studies and outlining potential future research avenues to address unresolved issues for the successful application of AI for cyber security.

Fig 2 : Cyber Attacks

Proposed Work:

Machine learning algorithms play a key role in the identification of malware by extracting patterns and traits from large datasets comprising samples of both benign and dangerous software. These techniques use qualities, behaviors, and patterns in the code of files to train models that can correctly categorize unfamiliar files as safe or harmful. Machine learning models generalize from training data to successfully identify new and evolving malware variants using techniques like decision trees, support vector machines, and neural networks, bolstering cyber security efforts by automating the process of quickly identifying and reacting to potentially harmful software threats.

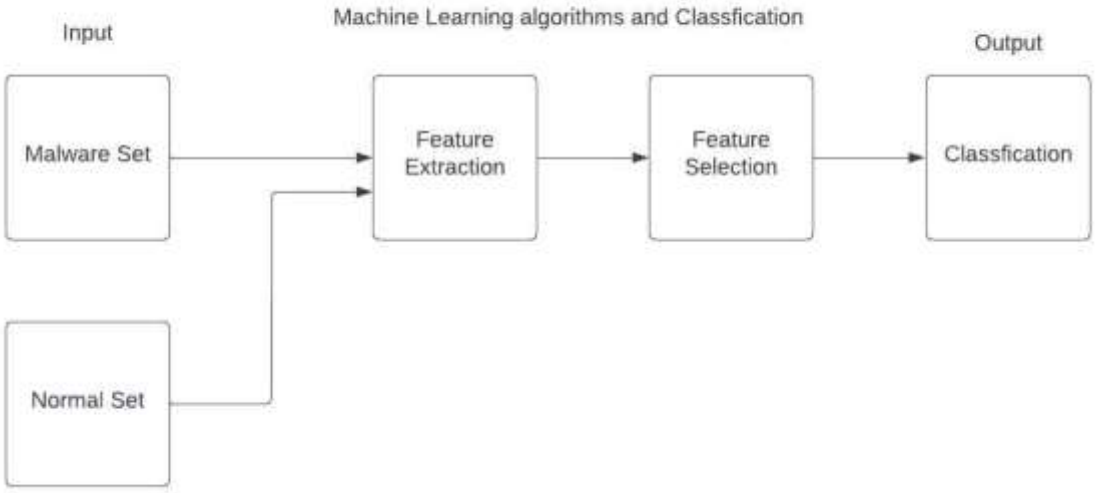


Fig 3:Machine Learning Algorithm for Malware detection

Data Collection:

Building powerful machine learning models is a fundamental step in many applications, including virus detection. Data collection for malware detection entails compiling a broad range of samples, both malicious (positive) and benign (negative) files. Machine learning algorithms are trained, evaluated, and fine-tuned using this dataset to discriminate between safe software and hazardous malware.

Feature Extraction:

A crucial preprocessing step in machine learning, feature extraction is especially important in situations like malware detection. Raw data, including files or network traffic, is converted into illuminating and numerical representations throughout this procedure. Features that can discriminate between dangerous and benign things are chosen for malware detection. These properties may include dynamic actions like API requests, system events, and code execution patterns, as well as file characteristics like size, type, and metadata. The goal of feature extraction is to reduce complex data to manageable properties that can be fed into machine learning algorithms. This is accomplished using methods like frequency analysis, code structure evaluation, and metadata extraction.

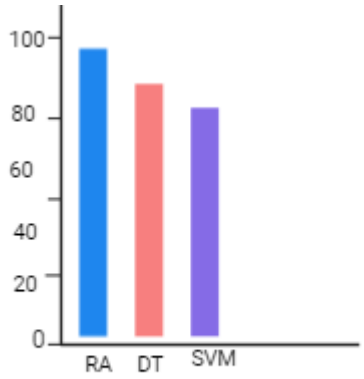
The basis for precise classification and detection is laid by this transformation, which improves the algorithms' capacity to identify patterns and behaviors that underpin the distinctions between malware and normal software. The power of feature extraction rests in its capacity to capture important information while omitting unimportant aspects, improving model efficiency and accuracy. Feature extraction fills the gap between raw data and algorithmic comprehension, enabling the development of models that can distinguish between the complex traits of malicious and benign files. Machine learning algorithms thrive on organized numerical data.

Feature Selection:

In order to increase model effectiveness, accuracy, and interpretability, important attributes are selected from a broader collection as part of the fundamental machine learning process known as feature selection. Especially important in activities like virus detection, feature selection speeds up learning by keeping only the most instructive features and removing redundant or ineffective ones. It prevents over fitting, improves computational effectiveness, and helps with model generalization by lowering dimensionality. Feature selection optimizes the trade-off between data complexity and predictive power using strategies including filter, wrapper, and embedding methods, ultimately resulting in the development of more efficient and streamlined machine learning models.

Classification:

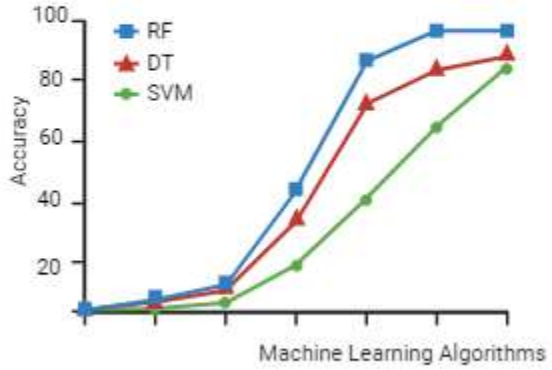
Differentiating between harmful (positive) and benign (negative) files is the main goal. In order to teach classification algorithms how to distinguish between two classes, labeled datasets with instances of both valid and malicious software are used. These algorithms can precisely identify whether a brand-new, unknown file is harmful or benign after being educated. An algorithm for categorizing data, for instance, might examine features taken from a file, like its binary content, code structure, system calls, and metadata. The basis for precise classification and detection is laid by this transformation, which improves the algorithms' capacity to identify patterns and behaviors that underpin the distinctions between malware and normal software. The power of feature extraction rests in its capacity to capture important information while omitting unimportant aspects, improving model efficiency and accuracy. Feature extraction fills the gap between raw data and algorithmic comprehension, enabling the development of models that can distinguish between the complex traits of malicious and benign files. Machine learning algorithms thrive on organized numerical data.



RF –Random Forest Algorithm

DT- Decision Tree Algorithm

SVM –Support Vector Machine Algorithm



Accuracy of various algorithms are performed and it show that Random forest algorithm and it showed that random forest algorithm give best result in malware detection.

Table 1: Experiment Results Algorithm

Algorithms	TP	F P	Accuracy
Random Forest Algorithms	0.96	0.04	98
Decision Tree Algorithms	0.93	0.07	93
Support Vector Machine Algorithms	0.86	0.14	86

We classify totally 2500 instance and correctly classified Instances as 98% that is 2470 instance using random forest algorithms .

Impact of AI in cyber security awareness :

Cyber security has entered a revolutionary phase as a result of the impact of artificial intelligence (AI), which has completely changed how threats are identified, handled, and countered. Rapid analysis of large datasets is made possible by AI's sophisticated capabilities, which also improve anomaly detection, early threat identification, and incident response. Organizations may proactively foresee weaknesses and changing attack vectors because to its superior predictive capabilities. AI-driven solutions are capable of automatically thwarting phishing attempts, learning user behaviors for accurate risk assessment, and offering individualized cyber security training. AI strengthens protection systems, but it also calls for caution, taking into account challenges like bias and adversarial attacks, highlighting the need for human skill in evaluating AI-generated insights for an all-encompassing and robust cyber security strategy.

How people and organizations approach recognizing and mitigating cyber dangers has fundamentally changed as a result of the impact of artificial intelligence (AI) in cyber security awareness. With the ability to deliver customized training programs based on individual behaviors and knowledge gaps, AI's capabilities have changed Cyber security education. Through real-time email content analysis, consumers are given the ability to spot phishing attempts and take appropriate action. Artificial intelligence-driven behavioral analysis improves the detection of suspicious activity and aids in the early identification of insider threats. The predictive insights provided by AI also foresee new hazards, enabling proactive security actions. However, the influence of AI also brings issues, such as the necessity to deal with data privacy and bias in algorithm training. By providing individualized, flexible, and forward-looking education, AI ultimately strengthens cyber security awareness by arming people and organizations with the tools they need to combat a constantly changing digital threat landscape.

Limitation of Artificial Intelligence in cyber security awareness:

Artificial intelligence (AI) has limitations when it comes to cyber security awareness. Due to AI's propensity for false positives and negatives, real dangers may be missed or overflowed with irrelevant notifications, which would undermine user trust and operational effectiveness. AI flaws can be used by adversarial assaults to control the very systems designed to increase security, potentially resulting in breaches. Furthermore, AI's effectiveness may be hampered by its reliance on previous data, which may perpetuate biases and leave it unable to adjust to new, creative attack strategies. As AI struggles to understand contextual nuances, it may misread user behaviors and their intentions, making human expertise still essential. Overall, even though AI has amazing potential, overcoming its current limitations will require careful balancing.

Conclusion:

As a result, threat detection, reaction time, and individualized user education have all improved thanks to the incorporation of AI in cyber security awareness. The processing power of AI has enabled the proactive detection of possible risks, and customized counsel encourages a culture of cyber alertness. However, there are difficulties present in this advancement. Biases, antagonistic weaknesses, and false positives can damage credibility and efficiency. To maximize AI's benefits and minimize its drawbacks, the correct balance must be struck between its strengths and human skills. This will provide a resilient cyber security posture that changes with the always shifting threat landscape.

Future Work:

Future research in the area of explainable AI models that offer visible insights into decision-making, reinforcing AI systems against adversarial attacks, and concentrating on privacy-preserving techniques are all important components of the field of AI in cybersecurity awareness. For proactive threat identification and individualized user education, the development of flexible training methods and the integration of AI with behavioral analysis are essential. In order to build a robust cybersecurity framework, seamless human-AI collaboration, integration with zero-trust architectures, and study of cross-domain applications will be crucial. Additionally, international cooperation, legal frameworks, and ethical concerns will be vital in directing the responsible and significant progress of AI in order to create a more secure digital environment.

References:

1. Rawindaran, Nisha, Ambikesh Jayal, and Edmond Prakash. 2022. "Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime"
2. Application of classification algorithms of Machine learning in cybersecurity, Procedia Computer Science.
3. Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, (2023)Artificial intelligence for cybersecurity: Literature review and future research directions
4. Rawindaran, Nisha & Jayal, Ambikesh & Prakash, Edmond. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. Computers. 11. 174. 10.3390/computers11120174.
5. Meraj Farheen Ansari1 , Bibhu Dash2 , Pawankumar Sharma3 , Nikhitha Yathiraju4(2022), The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review
6. https://wcd.nic.in/sites/default/files/Cyber%20Security%20Awareness%20_0.pdf
7. Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, (2023), Artificial intelligence for cybersecurity: Literature review and future research directions
8. Usukhbayar Baldangombo1 , Nyamjav Jambaljav1 , and Shi-Jinn Horng2 (2015).”A static malware detection system using data mining methods”
9. 10. D. Gavriluţ, M. Cimpoeşu, D. Anton and L. Ciortuz, "Malware detection using machine learning," 2009 International Multiconference on Computer Science and Information Technology, Mragowo, Poland, 2009, pp. 735-741, doi: 10.1109/IMCSIT.2009.5352759.
10. Dragos¸ Gavrilut , Mihai Cimpoes , Dan Anton, Liviu Ciortuz1 (2014) ,”Malware Detection Using Machine Learning.
11. Ansari, Meraj Farheen & Dash, Bibhu & Sharma, Pawankumar & Yathiraju, Nikhitha. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.
12. Johri, S., Rajagopal, B. R., Ahamad, S., Kannadasan, B., Dixit, C. K., & Singh, P. (2023). Cloud computing based renewable energy demand management system. PROCEEDING OF INTERNATIONAL CONFERENCE ON ENERGY, MANUFACTURE, ADVANCED MATERIAL AND MECHATRONICS 2021. https://doi.org/10.1063/5.0126132
13. RajBalaji, S., Raman, R., Pant, B., Rathour, N., Rajagopa, B. R., & Prasad, C. R. (2023, January 27). Design of deep learning models for the identifications of harmful attack activities in IIOT. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). https://doi.org/10.1109/aisc56616.2023.10085088
14. Malathi, M., Muniappan, A., Misra, P. K., Rajagopal, B. R., & Borah, P. (2023). A smart healthcare monitoring system for patients using IoT and cloud computing. PROCEEDING OF INTERNATIONAL CONFERENCE ON ENERGY, MANUFACTURE, ADVANCED MATERIAL AND MECHATRONICS 2021. https://doi.org/10.1063/5.0126275
15. Ahdal, A. A., Rakhra, M., Rajendran, R. R., Arslan, F., Khder, M. A., Patel, B., Rajagopal, B. R., & Jain, R. (2023, February 8). Monitoring Cardiovascular Problems in Heart Patients Using Machine Learning. Journal of Healthcare Engineering; Hindawi Publishing Corporation. https://doi.org/10.1155/2023/9738123

16. Banu, S. R., Rajagopal, B. R., Venkatesan, K., & Rawat, P. (2023, May 10). Smart Financial Management System Based on Integrated Artificial Intelligence and Big Data analytics. ResearchGate. https://www.researchgate.net/publication/370652400_Smart_Financial_Management_System_Based_on_Integrated_Artificial_Intelligence_and_Big_Data_analytics
17. Rajagopal, B. R., Anjanadevi, B., Tahreem, M., Kumar, S., Debnath, M., &Tongkachok, K. (2022). Comparative Analysis of Blockchain Technology and Artificial Intelligence and its impact on Open Issues of Automation in Workplace. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 288-292. https://doi.org/10.1109/ICACITE53722.2022.9823792
18. Rajagopal, B. R.,Kannapiran, E., Gupta, A. D., Momin, M. & Chakravarthy, D. S. K. (2022).The future prospects and challenges of implementing big data in healthcare management using Structural equation model analysis. Bull. Env. Pharmacol. Life Sci., (Spl Issue [1] 2022), 1111-1119
19. Krishnam, N. P., Ashraf, M. S., Rajagopal, B. R., Vats, P., Chakravarthy, D. S. K., & Rafi, S. M. (2022). ANALYSIS OF CURRENT TRENDS, ADVANCES AND CHALLENGES OF MACHINE LEARNING (ML) AND KNOWLEDGE EXTRACTION: FROM ML TO EXPLAINABLE AI. Industry Qualifications The Institute of Administrative Management UK, 58(Special Issue May 2022), 54-62.
20. Gupta, A. D., Rafi, S. M., Rajagopal, B. R., Milton, T., &Hymlin, S. G. (2022). Comparative analysis of internet of things (IoT) in supporting the health care professionals towards smart health research using correlation analysis. Bull.Env.Pharmacol. Life Sci., (Spl Issue [1] 2022), 701-708.
21. Bhanushali, M. M., Sharma, A., Sharma, S., Gehlot, A., Rawal, P., & Kapila, D. (2023, May). A detailed and significant analysis of The Effects of Big-Data over The Revolution of Internet Marketing. In 2023 3rd International Conference on Advance Computing and Innovative Technologiesin Engineering (ICACITE) (pp. 1026-1031). IEEE, doi: 10.1109/ICACITE57410.2023.10182372.
22. Bhanushali, M. M., & Sharma, A. (2020). A Bibliometric Study on Purchase and Technology Transfer with Reference to Industrial Equipments. Journal of Computational and Theoretical Nanoscience, 17(9-10), 4698-4702, DOI: https://doi.org/10.1166/jctn.2020.9303.
23. Sharma, S. Poojitha, A. Saxena, M. M. Bhanushali and P. Rawal, "A Conceptual Analysis of Machine Learning Towards Digital Marketing Transformation," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 313-316, doi: 10.1109/IC3I56241.2022.10073416.
24. M. Thaseen, G. L, P. Tripathi, Y. Z. Elena, M. M. Bhanushali and J. Alanya-Beltran, "An Review on Internet of Things (IOT) in Creating Better World Through Reduction in Emission of Greenhouse Gases – Multiple Regression Analysis," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 312-316, doi: 10.1109/ICACITE53722.2022.9823835.
25. Sidana, T. Jindal, U. K. Pandey, J. Singh, S. T. Vasantham and M. M. Bhanushali, "Investigation of Block chain Technology Based on Digital Management System with Data Mining Technology for Green Marketing," 2022 2nd International Conference on Advance Computing and Innovative

Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1309-1313, doi: 10.1109/ICACITE53722.2022.9823696.

26. Veerasamy, K., Sanyal, S., Almahirah, M.S., Saxena, M., Manohar Bhanushali, M. (2022). An Investigative Analysis for IoT Based Supply Chain Coordination and Control Through Machine Learning. In: Balas, V.E., Sinha, G.R., Agarwal, B., Sharma, T.K., Dadheech, P., Mahrishi, M. (eds) Emerging Technologies in Computer Engineering: Cognitive Computing and Intelligent IoT. ICETCE 2022. Communications in Computer and Information Science, vol 1591. Springer, Cham. https://doi.org/10.1007/978-3-031-07012-9_13.
27. S. K, A. Sabarirajan, K. S. U, P. Narang, M. M. Bhanushali and A. K. Turai, "Human Resource Management based Economic analysis using Data Mining," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 872-876, doi: 10.1109/ICIEM54221.2022.9853202.
28. Sindhura, K., Sabarirajan, A., Narang, P., Bhanushali, M. M., & Turai, A. K. (2022, April). Human Resource Management based Economic analysis using Data Mining. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 872-876). IEEE.
29. Bhanushali, M. M., Bhattacharyya, R., Agarkar, S. C., & Moghe, S. COVID-19.
30. Bhanushali, M., &Periwal, D. Designing the Distributor Evaluation Criteria with reference to the Indian Consumer Durable Industry. Srujan, 33.
31. Bhanushali, M. M., & George, S. P. (2017). MARKET RESEARCH ON CONSUMER BUYING BEHAVIOUR FOR MICROWAVE OVENS IN THANE DISTRICT.
32. Gedamkar, R., & Bhanushali, M. M. A MULTI-PERSPECTIVE ANALYSIS OF INTERNATIONALIZATION STRATEGIES.
33. Durga, S., Perugu, P., Nidhi Sree, D., Podile, V., Bhanushali, M. M., & Revathi, R. Human Resource Data Analysis & prediction using Decision Tree Algorithm and Random Forest.
34. Sindhura, K., Sabarirajan, A., Narang, P., Bhanushali, M. M., & Turai, A. K. (2022, April). Human Resource Management based Economic analysis using Data Mining. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 872-876). IEEE.