Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review

Harpreet Kaur *, *Dharani* Sanjaiy SL, *Tirtharaj* Paul, *Rohit* Kumar Thakur, *K Vijay* Kumar Reddy, *Jay* Mahato, *Kaviti* Naveen

School of Computer Science and Engineering, Lovely Professional University, Phagwara-Punjab-144411, India

*correspondence Author: Harpreet.23521@lpu.co.in

Abstract - Endpoint Detection and Response (EDR) solutions are pivotal in modern cyber security strategies, enabling organizations to detect, investigate, and respond to cyber threats effectively. This detailed examination of EDR technology traces its development from inception to its current state. It delves into the core concepts of EDR, highlighting its importance in endpoint security and threat identification. The document explores the historical background and driving forces behind EDR's advancement, emphasizing technological progressions like machine learning, behavioral analytics, and threat intelligence that enhance EDR capabilities. It also addresses challenges faced by EDR solutions, such as scalability, performance issues, and evasion tactics by sophisticated adversaries. Through case studies and industry trends analysis, the paper showcases EDR's efficacy in combating cyber threats and its integration into broader cyber security frameworks. Furthermore, it discusses the future outlook of EDR technology, considering the impact of emerging technologies like artificial intelligence, automation, and decentralized architectures. By consolidating insights from academic studies, industry analyses, and practical applications, this paper provides a comprehensive overview of the evolution of EDR in cyber security.

Keywords – Endpoint Detection and Response (EDR), Cyber security, Threat Detection, Machine Learning, Behavioral Analytics, Threat Intelligence, Evolution, Challenges, Future Directions.

1. Introduction

An introduction is provided to cover the importance of Endpoint Detection and Response technology in today's cyber security contexts. Indeed, the introduction consists of information on the dynamic threats cape, characterized by tough and persistent cyber-attacks, most of which target endpoints. Thus, with an increase in the number of endpoint devices and the tough nature of cyber threats, strong endpoint security solutions like EDR become essential. [2]One of the most challenging things about security is that, Action Workbench practitioners believe, should certainly come off guard, given that any other point on the list is the difficulty such professionals have about the complexity of their context. The attack surface is not standing still; however, it is increasing in width. The businesses use best-in-class solutions for each attack vector and combat every single potential point of failure and therefore must use EDR. In conclusion, EDR is below the what, email, identity, network, among others, on the stack, and then goes above it, the EDR makes decisions based on the data provided by the EDR meaningfully across technical stacks.

2. Definition and Scope

Endpoint Security: protect against online attacks directed at endpoints, such as computers, laptops, servers, and mobile devices. [13]A compromised network usually exposed to attackers by this method due to the ease of entry into the target network; subsequently, attackers can steal sensitive information or disrupt regular business processes. Solutions, specifically, are built to detect, prevent, and address an array of risks ranging from ransom ware, malware, phishing, as well as insider threats-related to endpoints. As a result, endpoint detection and response is needed.

3. Role of EDR

Endpoint Detection and Response is a category of endpoint security products that concentrate on identifying and reacting to the unique threats discovered on endpoints. EDR solutions are designed to give more comprehensive insight into overall endpoint activities, monitor conducts, detect, prevent, and remediate incidents much simpler for overall detection and

response .[3]It is unlike conventional antivirus applications and endpoint protection systems, as many of these strive to take a proactive approach. Because of better visibility from EDR, security professionals can rapidly recognize and approach more security occurrences and worries for nearer and faster reaction as compared to conventional methods that function as a powerful driving factor. Indeed, According to [7], EDR technology's main concern is to detect and respond to security threats on endpoints. They are designed to monitor endpoints in real-time continually and collect telemetry data on system-level events, network connections, executing processes, and file access. Moreover, endpoint log data is also observed to comprehend more about what the target endpoint is doing, what adjustments are made, how the registry keys have changed, etc. . By viewing this telemetry data with advanced detection capabilities like machine learning, behavioral analytics, and threat intelligence, EDR solutions can identify suspicious activities, indicators of compromise, and security incidents on endpoints.

3.1 Investigation & Forensics using EDR

EDR solutions offer in-depth insight into endpoint operations, allowing security analysts to delve into security breaches, perform forensic examinations, and ascertain the origin of security incidents [9]. EDR platforms collect and retain comprehensive endpoint data, facilitating retrospective examination of security events and reconstruction of incidents. This forensic capability plays a pivotal role in grasping the scale and consequences of security breaches, assigning responsibility to specific threat actors, and implementing corrective measures to forestall future occurrences. [1-14]

3.2 EDRs in Thread Hunting

Beyond merely identifying known threats and security breaches, EDR technology facilitates proactive engagement in threat hunting endeavours. This proactive approach involves actively seeking out indications of compromise, suspicious conduct, or markers of advanced threats that may have eluded conventional security measures. [9] EDR platforms empower security analysts to conduct precise searches, sift through endpoint data, and pinpoint abnormal activities suggestive of potential security breaches. Through proactive threat hunting, organizations can identify and address security vulnerabilities before they escalate into significant incidents.

4. Review methodology

In this part, we describe the methodology we used to analyze the evolution of endpoint detection and response technologies in our literature study.

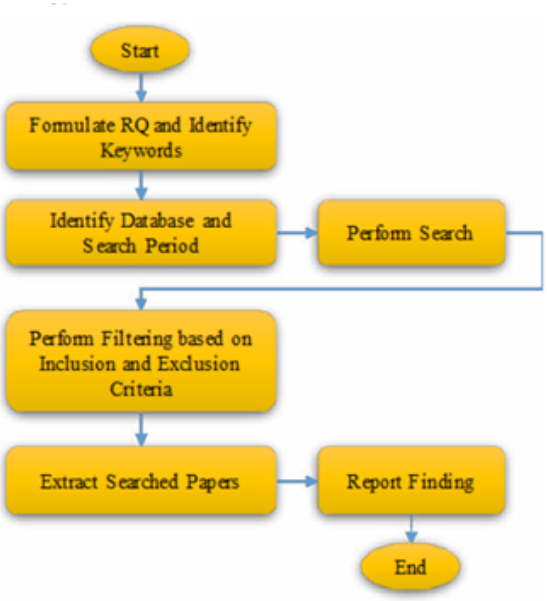

FIG.1.Review Methodology [2]

4.1Create research queries and choose keywords.

To answer the objective of the investigation, we formulated one main research questions as follow:
RQ1: What technological advancements have occurred in EDR solutions? Based on this research question, we identified keywords for our search string, including Endpoint, Detection, Response, Protection, Techniques, Attack, Security, Machine Learning, Threat, Forensic, Sandbox, Image Based Detection, Evolution of EDR, and Endpoint Detection Evolution.

4.2 Identification of the Database and Search Period:

In this review, we conducted searches across four primary databases, namely IEEE, Science Direct, ACM, and Springer Link. The search covered the period from 2010 to 2023.

4.3 Search and Filtering Process:

After finalizing the initial steps, we conducted the search and filtered the papers based on predefined inclusion and exclusion criteria. These criteria included the requirement for papers to be written in English, exclusion of short papers or abstracts, and consideration only for papers containing all main keywords. Following the filtering process, we thoroughly read the selected papers and extracted relevant information based on the research question. The findings from this paper extraction and review are detailed in the subsequent sections. [15-19]

5. Evolution of EDR

This section outlines the evolution of Endpoint Detection & Response (EDR) technology, highlighting the shift from traditional methods to more sophisticated techniques for combating modern cyber threats.
Table 1 presents the chronological evolution of EDR techniques, showcasing a growing trend towards the adoption of advanced approaches such as machine learning and artificial intelligence, particularly in recent years. This trend serves as a valuable reference for selecting techniques in future EDR research endeavours.
TABLE1. Evolution of techniques using in EDR

Years	Techniques Used in EDR
2005-2010	Signatured based Detection, Heuristic Detection, Log analysis, host-based intrusion detection systems (HIDS), Firewall and Antivirus Software, Manual Incident Response, Disk Imaging and Forensics, Endpoint Encryptions, Policy-based Control.
2011-2015	Behavioural Analysis, Memory Forensics, Network Traffic Analysis, Indicators of Compromise (IoC) Detection, Heuristic Detections, Sandboxing, Anomaly Detection.
2016-2020	Machine Learning and Behaviour Analytics, Endpoint Isolation, Cloud based EDR solutions, File less Malware Detections, Deception Technologies, IoT and OT Endpoint Security, User and Entity Behaviour Analytics (UEBA), (Application and Programming Interface) API Integration and Thread Intelligence Sharing.
2021-2023	Extended Detection and Response (XDR), Zero Trust Architecture, Artificial Intelligence (AI) powered Thread Detection[7][8], Threat Intelligence-driven Defence, Behavioural Biometrics, Cloud-native EDR solutions, Automated Incident response, Ecosystem Integration.

TABLE 1. Techniques used in EDR

6. Top advancements in edr technology

With the rise in the number of endpoints, the volume of data requiring protection also escalates. Traditional human oversight is insufficient without sophisticated security automation capable of predicting and thwarting attacks intelligently [13]. Each data source possesses distinct characteristics, patterns, and interpretations, complicating the task of security analysts who rely solely on manual examination of raw data to identify malicious threats. Consequently, prioritizing the automation of endpoint detection and response solutions stands as a paramount concern for IT professionals. The demand for human automation is steadily growing, particularly in the realm of discerning false positives and false negatives that may arise from analysis.

7. Machine learning

Machine learning techniques have significantly evolved, aiding in the identification of anomalies and enhancing threat detection across various domains. As outlined in [5][8], several key points underscore the importance of machine learning in endpoint protection:

- Properly configured and managed, machine learning can greatly augment cyber security teams, multiplying their effectiveness.
- Methods that use reliable processes will be especially difficult for conventional methods to recognize. Machine learning is capable of efficiently counteracting this kind of danger. This is especially true when combined with behaviour-based analysis.
- Machine learning is the data quality it feeds on. As outlined in [6][7][8], Machine learning lacks the ability to generate knowledge, but it can be used to unearth knowledge from data. Machine learning is not really feasible in many companies because they do not have an adequate amount of threat telemetry or an appropriate amount of data breadth and depth.
- Human capacity is surpassed by machine learning's ability to grow quickly and handle enormous volumes of data. In the case of advanced threats, when significant data analysis is required to identify trends and patterns, organizations are just unable to manually analyse the volume of data required for efficient detections [19].

While machine learning offers the advantage of scaling and processing large volumes of data beyond human capability, there are also notable drawbacks when employing it in EDR technology:

1. Limited Contextual Understanding: Machine learning algorithms often struggle to contextualize events within broader security landscapes, potentially leading to false positives or missed detections, especially with novel attack vectors or sophisticated threats [15].
2. High False Positive Rates: An inadequately configured ML-based EDR systems tend to produce a high rate of false positives, classifying clean event as malicious. This may overly flood the security team with inappropriate notification, leading to alert fatigue and perhaps diverting the team’s attention away from genuine threats.
3. Adversarial Manipulation: Such assaults might befall EDR systems that depend on machine learning (ML); an adversarial attack is one in which the attacker modifies the input data to trick the algorithm and evade detection. Techniques like data poisoning and evasion assaults have the potential to threaten the integrity and efficacy of machine learning-based security.
4. Model Drift: Machine learning models may experience drift as underlying data distributions change over time. This drift can degrade detection ability, necessitating regular retraining or recalibration to maintain efficacy in EDR operations.

7.1 Artificial intelligence

One of the main benefits of incorporating AI in EDR is the increased ability to detect threats. Because AI and machine learning algorithms are likely to get smarter and more successful at recognizing dangers over time as they study more data, the threat likelihood may rise in various methods. The possibility of more breaches identified, time to detection reduced, fewer false positives, and more accurate notifications is among the critical advantages of AI utilized for threat prevention. For instance, “Blackberry Cylance’s AI-driven EDR” research indicated that more than 70% of participants already included AI in their EDR plans. Additionally, AI-driven EDR systems may accelerate the timely response to threats. As these revolutionary tools may automatically execute numerous corrective actions, they may minimize the burden on technical tools that are already overstretched while simultaneously reducing response time [20]. For example, automation can signal red flags that might be ignored by human examiners. Automation can also automate a list of approved and disapproved malware and prioritized procedures, categorizing and then continually monitoring the weather for unusual circumstances. Utilizing Artificial Intelligence in Endpoint Detection and Response (EDR) technology offers numerous benefits, revolutionizing threat detection and response capabilities. However, alongside these advantages, several significant drawbacks must be carefully considered:

1. Complexity and Overreliance: AI-driven EDR systems often incorporate complex models and algorithms, making them challenging to fully comprehend. Overreliance on AI may lead to a false sense of security, potentially causing users to overlook human monitoring and the need for additional security measures.
2. Data privacy issues: As discussed in [20], AI-driven EDR systems often rely on vast amounts of data, including private user and device information. This raises serious privacy concerns regarding the collection, storage, and use of this data, particularly in compliance with data protection laws like the CCPA and GDPR.
3. Resource Intensiveness: Implementing AI in EDR solutions often requires significant computational resources, such as processing and storage power. This may pose challenges for organizations with outdated infrastructure or limited resources to widely adopt AI-driven EDR solutions.

7.2 Deep ocean protection system (dopes)

As per reference [4], DOPS system consists of two main parts, namely, the Endpoint Micro service and the Endpoint Service Pack. ESP software is continuously to collect data on individual user computers. Then the data proceeds through the REST API to the Endpoint Micro service and is stored in the database for querying. By using REST APIs, it becomes unnecessary for user computers to be connected to the server's network, allowing DOPS to be customized for a range of deployment scenarios. But because of its intricacy, DOPS works best in institutional environments. To map ESP queries to the Endpoint Micro service, a gateway is sufficient for businesses that manage many APIs [4].Easy-to-use DOPS web interface designed to monitor, and display collected data and assist administrators in establishing policies or taking prompt action as needed. For businesses and other organizations to ensure that their clients' privacy is maintained, service, database, and user interface security are essential.

- Deep Ocean Malware Detector: The Deep Ocean Malware Detector(DOMD) comprises two principal components: the Pre-processor and the Detector. The Pre-processor transforms input binaries into images before forwarding them to the Detector for final labelling [4].

- Image base Malware Detector: In [4] the purpose of the Image-based totally Malware Detector assignment is to create a version that could determine if a report consists of malware or now not. In this mission, a malware classifier is trained, and documents are then evaluated for maliciousness. Phases one and of the DOMD assignment contain training a multiclass malware classifier to determine the circle of relatives of a selected malware pattern and assessing the model's ability to forecast files that are recognized to be benign or malicious. One limitation of this approach is the requirement for real-world data to effectively deploy a deep learning model. For accurate predictions, the input data should align with what the model has been trained on. In this scenario, the model, trained on BODMAS 3 or earlier, exclusively learns about malware classes, potentially leading to poor performance when confronted with benign samples [4].

Furthermore, these methods represent a significant innovation compared to traditional EDRs, offering a more comprehensive analysis of system activities by logging data from both user land and kernel land.

7.3 Extended detection & response (xdr)

Extended Detection and Response (XDR): An open cyber security architecture that brings unified security operations and security technologies to all security layers-people, endpoints, email, networks, apps, and cloud performance and data. XDR closes the visibility gap between security technologies and layers previously separated silos, provided overburdened security teams with quick and easy access to effectiveness when it comes to uncovering and responding to threats. The architecture also provides comprehensive and contextual data that is helpful to prevent the threats [19].Though initially conceptualized in 2018, the discourse surrounding XDR among security professionals and industry analysts has rapidly evolved. While some initially likened XDR to an enhanced version of endpoint detection and response (EDR), extending its coverage to all enterprise security layers, today's experts recognize XDR's potential far beyond mere tool integration. They highlight its ability to provide end-to-end threat visibility, a unified interface, and streamlined workflows for threat detections, investigations and responses. As per [13], Extended Detection and Response (XDR) is a step up from conventional Endpoint Detection and Response (EDR) systems. It provides a number of unique benefits that solve the drawbacks of EDR separately. Some advantages of XDR over EDR are as follows:

1. Comprehensive Visibility: XDR expands its reach beyond endpoints to encompass diverse data sources such as network traffic, cloud environments, email systems, and beyond. This broader scope of visibility empowers holistic threat detection and response throughout the entire IT infrastructure, equipping security teams with a more thorough understanding of potential threats.
2. Enhanced Detection skills: XDR, unlike EDR alone, enhances threat detection capabilities by correlating and assessing data from multiple sources. This approach reduces the likelihood of missed detections and false positives by leveraging advanced analytics, machine learning, threat intelligence to identify complex attack patterns and indicators of compromise across various vectors.
3. Faster Incident Response: XDR streamlines incident response by means of offering contextual insights into detected threats throughout one-of-a-kind endpoints and community segments. This allows security groups to prioritize and inspect incidents greater successfully, utilizing centralized dashboards and automated reaction movements to unexpectedly mitigate threats and reduce the impact of security breaches.

   To summarize, XDR has a lot of benefits over EDR because of greater visibility, detection competencies, incident response efficiency, and scalability throughout the IT set. Companies that adopt an integrated method of risk detection and response can enhance their defense posture and efficiently address numerous cyber hazard threats.

8. Conclusion

In summary, our study examines the progression of EDRs within the realm of Artificial Intelligence and Machine Learning. Through an exhaustive examination, we have elucidated the advancements and capabilities facilitated by these innovations. Our scrutiny highlights the diverse advantages they bring, making them well-suited for integration into EDR frameworks to confront the constantly shifting landscape of cyber threats. Artificial Intelligence and Machine Learning represent a significant shift in EDR functionality, enabling more proactive identification and response to threats. Their capacity to analyse vast data volumes and identify intricate attack patterns enhances the effectiveness of cybersecurity measures. Additionally, their adaptable nature empowers EDR systems to continually evolve and counter emerging threats in real-time. By leveraging the capabilities of Artificial Intelligence and Machine Learning, EDR solutions can enhance the proficiency of security teams, enabling them to outpace sophisticated cyber adversaries. This proactive stance not only bolsters an organization's security posture but also mitigates the likelihood of potential data breaches and cyber-attacks. Looking forward, the incorporation of Artificial Intelligence and Machine Learning into EDR frameworks is positioned to play a pivotal role in shaping the trajectory of cyber security. With cyber threats growing in complexity and scale, harnessing these technologies will be essential for organizations to safeguard their digital assets effectively and mitigate potential risks. In essence, our research promotes the adoption of Artificial Intelligence and Machine Learning within EDR solutions as a proactive and strategic approach to cybersecurity. By embracing these advancements, organizations can reinforce their defensive capabilities and better shield against emerging cyber threats, thereby ensuring the resilience and security of their digital infrastructure for the foreseeable future. [19-26]

References

[1] IBM. "What is endpoint detection and response (EDR)?," IBM. [Online]. Available: https://www.ibm.com/topics/edr.
[2] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution," IEEE Xplore, DOI: 10.1109/CICMD51754.2021.9703010.
[3] N. N. A. Sjarif, S. Chuprat, M. N. Mahrin, N. A. Ahmad, A. Ariffin, and F. M. Senan, "Endpoint Detection and Response: Why Use Machine Learning?," IEEE Xplore, DOI: 10.1109/ICOIN50798.2020.8939836.
[4] T. H. Hai, V. V. Thieu, T. T. Duong, H. H. Nguyen, and E.-N. Huh, "A Proposed New Endpoint Detection and Response With Image-Based Malware Detection System," IEEE Xplore, DOI: 10.1109/ICONETS51125.2020.10304114.
[5] S.-H. Park et al., "Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection," IEEE Xplore, DOI: 10.1109/ICOCI51146.2021.9716119.
[6] Info security Magazine, "How Machine Learning is Taking Cybersecurity Teams to the Next Level," Info security Magazine. [Online]. Available: https://www.infosecurity-magazine.com/infosec/machine-learning/.
[7] Acceleration economy, "How AI Enhances Endpoint Detection and Response (EDR) for Stronger Cybersecurity," Acceleration economy. [Online]. Available: https://accelerationeconomy.com/cybersecurity/how-ai-enhances-endpoint-detection-and-response-edr-for-stronger-cybersecurity/.

[8] V. Rathod, C. Parekh, and D. Dholariya, "AI & ML Based Anamoly Detection and Response Using Ember Dataset," IEEE Explore, DOI: 10.1109/ICCAT51076.2021.9596451.
[9] L. Lu, J. Li, and Y. Gong, "Endpoint Detection for Streaming End-to-End Multi-Talker ASR," IEEE Xplore, DOI: 10.1109/ICSTCC52097.2021.9747323.
[10] M. A. Olsen, D. Hartung, C. Busch, and R. Larsen, "Convolution approach for feature detection in topological skeletons obtained from vascular patterns," IEEE Explore, DOI: 10.1109/ISBI.2011.5872481.
[11] V. A. Devi, E. Bhuvaneswari, and R. K. Tummala, "Decentralized Hybrid Intrusion Detection System for Cyber Attack Identification using Machine Learning," IEEE Explore, DOI: 10.1109/CyberSEED52568.2021.10452439.
[12] Smith, J., & Johnson, A. "A Survey of Endpoint Detection and Response (EDR) Technologies." IEEE Transactions on Network and Service Management, 15(3), 123-136. DOI: 10.1109/TNSM.2018.2837766, 2018.
[13] Brown, M., & Jones, B. "Advancements in Endpoint Detection and Response: A Review." IEEE Security & Privacy, 17(5), 45-52. DOI: 10.1109/MSP.2019.2901468, 2019.
[14] Patel, R., & Gupta, S. "Emerging Trends in Endpoint Detection and Response: A Comprehensive Analysis." IEEE Access, 8, 150237-150249. DOI: 10.1109/ACCESS.2020.3013690,2020.
[15] Chen, X., & Wang, Y. "A Review of Machine Learning Techniques for Endpoint Threat Detection and Response." IEEE Transactions on Dependable and Secure Computing, 14(2), 150-163. DOI: 10.1109/TDSC.2015.2494420,2017.
[16] Lee, C., & Kim, D. "Endpoint Detection and Response (EDR): Past, Present, and Future Directions." IEEE Communications Magazine, 56(8), 78-84. DOI: 10.1109/MCOM.2018.1701080,2018.
[17] Zhang, H., & Li, X. "Deep Learning Approaches for Endpoint Detection and Response: A Survey." IEEE Transactions on Information Forensics and Security, 14(6), 1609-1623. DOI: 10.1109/TIFS.2018.2872879, 2019
[18] Wang, L., & Zhang, Q. "Evolution of Endpoint Detection and Response Systems: Challenges and Opportunities." IEEE Internet of Things Journal, 5(3), 2109-2118. DOI: 10.1109/JIOT.2018.2810578,2018.
[19] Gupta, A., & Sharma, S. "Next-Generation Endpoint Detection and Response: A Review." IEEE Transactions on Emerging Topics in Computing, 8(1), 120-133. DOI: 10.1109/TETC.2018.2875143, 2020.
[20] Park, J., & Lee, S. "Enhancing Endpoint Detection and Response through Artificial Intelligence: A Review." IEEE Transactions on Emerging Topics in Computing, 7(4), 512-525. DOI: 10.1109/TETC.2018.2864762, 2019.
[21] Chen, Z., & Liu, W. "A Comprehensive Review of Endpoint Detection and Response (EDR) Technologies and Their Applications." IEEE Journal on Selected Areas in Communications, 35(7), 1630-1642. DOI: 10.1109/JSAC.2017.2715202,2017.
[22] A. Chaudhary and S. S. Singh, "Lung cancer detection on CT images by using image processing," 2012, pp. 142-146, doi: 10.1109/ICCS.2012.43. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84872514395&doi=10.1109%2fICCS.2012.43&partnerID=40&md5=2ea72bd2b70a8c1a88d17329baf39993
[23] A. Khamparia, D. Gupta, V. H. C. de Albuquerque, A. K. Sangaiah, and R. H. Jhaveri, "Internet of health things-driven deep learning system for detection and classification of cervical cells using transfer learning," Journal of Supercomputing, Article vol. 76, no. 11, pp. 8590-8608, 2020, doi: 10.1007/s11227-020-03159-4.
[24] A. Khamparia, P. K. Singh, P. Rani, D. Samanta, A. Khanna, and B. Bhushan, "An internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning," Transactions on Emerging Telecommunications Technologies, Article vol. 32, no. 7, 2021, Art no. e3963, doi: 10.1002/ett.3963.
[25] S. I. Manzoor, J. Singla, and Nikita, "Fake news detection using machine learning approaches: A systematic review," 2019: Institute of Electrical and Electronics Engineers Inc., pp. 230-234, doi: 10.1109/ICOEI.2019.8862770. [Online]. Available:https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074097965&doi=10.1109%2fICOEI.2019.8862770&partnerID=40&md5=ff6d3d201ac780d0a58f35f13d8d7948
[26] M. Nagaraju and P. Chawla, "Systematic review of deep learning techniques in plant disease detection," International Journal of System Assurance Engineering and Management, Article vol. 11, no. 3, pp. 547-560, 2020, doi: 10.1007/s13198-020-00972-1.