IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

# Artificial Intelligence in Cyber Security

**Aman Dakhare, Prof Vijay.M. Rakhade, Prof Ashish Deharkar**

Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Chandrapur, India

Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Chandrapur, India

Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Chandrapur, India

**ABSTRACT**: Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against various security issues and cyberattacks. AI primarily monitors and analyzes behavior patterns. Using these patterns to create a baseline, AI can detect unusual behaviors and restrict unauthorized access to systems. AI can also help to prioritize risk, instantly detect the possibility of malware and intrusions before they begin.

**OBJECTIVES:** AI-powered solutions can sift through vast amounts of data to identify abnormal behavior and detect malicious activity, such as a new zero-day attack. AI can also automate many security processes, such as patch management, making staying on top of your cyber security needs easier. The central aims of AI is to develop systems that can analyze large datasets, identify patterns, and make data-driven decisions. This ability to solve problems and make decisions efficiently is invaluable across various industries, from healthcare and finance to transportation and manufacturing.

## I. INTRODUCTION

AI for cybersecurity uses AI to analyze and correlate event and cyberthreat data across multiple sources, turning it into clear and actionable insights that security professionals use for further investigation, response, and reporting. If a cyberattack meets certain criteria defined by the security team, AI can automate the response and isolate the affected assets. Generative AI takes this one step further by producing original natural language text, images, and other content based on patterns in existing data. AI plays a crucial role in Cybersecurity. AI can be utilized both defensively and offensively by enabling the development of new attack methods as well as the creation of effective defense mechanisms.

Currently, AI is already being employed in the security sector, and its significance will only grow with time. AI is particularly well-suited for gathering and analyzing vast amounts of data, extracting valuable insights, and responding accordingly. These capabilities greatly enhance an organization's ability to detect and respond to cyberattacks and ultimately minimize the potential damage inflicted by attackers.

### How AI Works in Cybersecurity?

AI in cybersecurity is like having a smart guard dog that can learn and adapt to new tricks to protect your house from intruders.

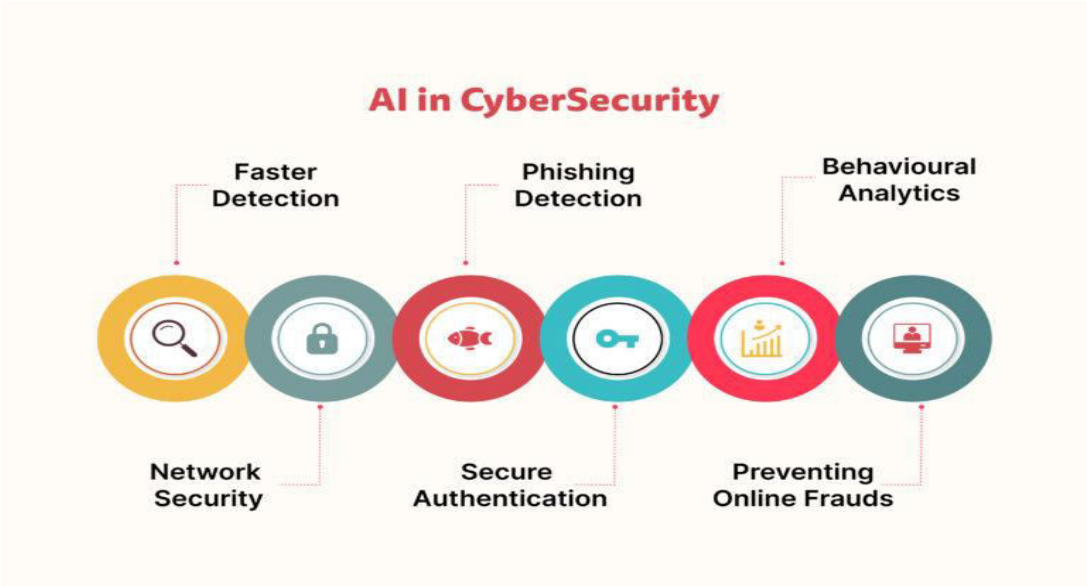
1. **Detection:** Imagine you have a pet dog that knows the smell of your family members. Similarly, AI in cybersecurity learns to recognize patterns in data to identify potential threats. For example, it can spot unusual activities like multiple failed login attempts or suspicious file downloads.
2. **Prediction:** Just like how experienced security guards can anticipate where burglars might strike next, AI algorithms can analyze data to predict potential cyber threats before they happen. They do this by looking at historical data and identifying trends that could indicate a future attack.
3. **Adaptation:** Your smart guard dog learns from experience. If it notices a new way burglars try to break in, it adapts its behavior to better protect your home. Likewise, AI systems in cybersecurity can evolve over time, learning from past incidents to improve their ability to detect and prevent future attacks.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

4. **Automation:** Think of having a robotic security system that can respond to threats automatically. AI in cybersecurity can automate certain tasks like blocking suspicious IP addresses or quarantining malware-infected devices, freeing up human security experts to focus on more complex issues.
5. **Response:** When your guard dog detects a threat, it barks to alert you. Similarly, AI in cybersecurity can trigger alerts or take action to mitigate threats in real-time, helping to minimize the impact of cyber attacks.




## II. USES OF AI IN CYBERSECURITY

1. Enhanced Threat Detection & Analysis

- AI algorithms have the ability to process data at a huge scale derived from many sources in real-time and flag out possible cyber threats by identifying patterns and irregularities.
- Algorithms in machine learning will be able to learn new data continuously to increase the detection exactitude and follow the dynamism of cyber threats progression.
- AI-enabled platforms for threat intelligence can be used to draw out different conclusions from different sources to ultimately give a broad and up to date risk picture.

2. Automated Incident Response (AIR)

- AI can streamline an initial response to the security issues with automating the incident triage and response, AI might increase the protection windows by allowing for faster detection and remediation of threats.
- With the machine learning, AI systems can take into account the parametricity and necessity of the alerts when they are working. This may relieve the employees from the burden of analyzing hundreds of alerts and by this will help them to target on the issues of greater involvement.
- AI-executed incident response systems can be designed to aggregate with other software tools to enforce protocol throughout the organization's IT infrastructure.

3. Enhanced Security Risk Assessment

- AI technologies provide a way to make the system deep intelligence-based analysis of the whole IT structure, applications, and data. Then, information is provided about all potential security risks and vulnerabilities.
- Through the sophisticated analytics performed by machine learning algorithms, security managers can identify both the probability and the level of impact of the possible security cases. This will allow the companies to focus their mitigation efforts on the most critical incidents.
- AI-embedded risk detection tools give pragmatic guidance for the security enhancement by tracking the historical data and using industry's best practices as their paradigm.

4. User Behavior Analytics (UBA)

- With AI algorithms, the behavior of the user can be analyzed from the usage pattern, that can reveal any suspicious behavioral pattern other than the regular use, which may be an insider threat or an unauthorized access.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

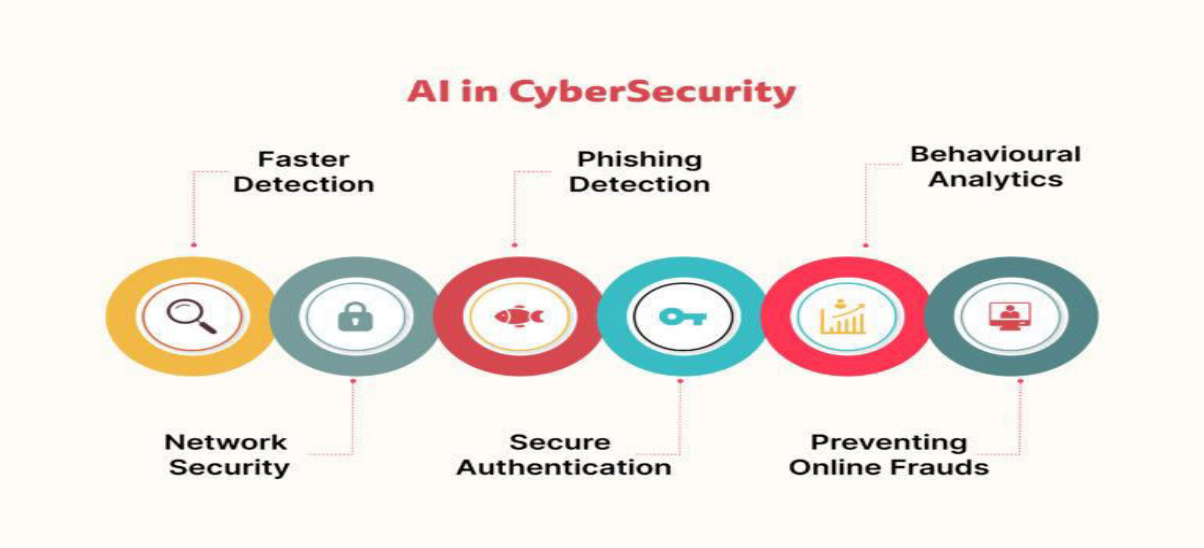
- Artificial intelligence algorithms can identify behavior peculiarities around lambda times, localities, and access manners across several dimensions.
- UBA services empower enterprises to uncover any anomaly about knowledge access by employees through auditing systems which in turn reduces the possibility of data breaches and insider risks.

5. Malware Detection and Prevention
- AI-powered malware scan systems can perform efficient pattern matching of a file such as its attributes and behaviors and hence can identify malware with accuracy.
- By observing and analyzing a range of malware samples, machine learning algorithms can form a pattern between previously unseen variants of malware and their characteristics and behaviors which they may have in common with known malware threats.
- AI-based programs of Watch Points may place different types of endpoints in quarantine or automatically remediate them when it sees that the devices are infected in order to block the spread of malware inside the network.

6. Phishing and Email Scam Detection
- AI algorithms are able to analyze email contents, the sender's behavior, and other metadata that will enable them to successfully detect phishing and email scam attempts.
- The most up-to-date ML models can identify hidden signs like the fake sender, attachments or domain names stated in the e-mails that help classify a message as a phishing attack.

7. Vulnerability Management and Patch Prioritization
- AI helps to identify more likely exploitation spot and the severity of the it on company's safety position.
- Algorithms of machine learning development can be used for analysing historical data and the threat intelligence feeds to determine a set of the most critical vulnerabilities needing to be fixed immediately.

.'




## III. CHALLENGES OF AI IN CYBERSECURITY

While AI holds tremendous promise for revolutionizing cybersecurity, its widespread adoption also presents challenges and considerations. These include:

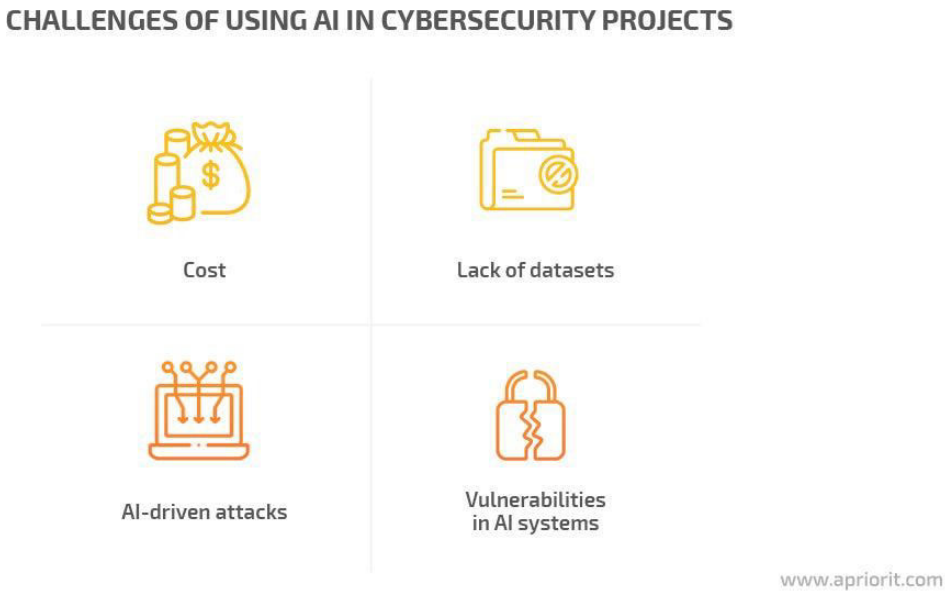
1. **Data Privacy and Ethics:** Modern cybersecurity which is AI-based is mostly based on the history of the data which is difficult to be obtained via the training process and analysis, thus people with the data privacy, confidentiality, and ethics are the same.
2. **Adversarial AI:** Some cybercriminals see AI systems as an opportunity to attack through the software vulnerabilities they may cause, for instance, the adversarial attacks that confuse machine learning and fool the detection.
3. **Algorithmic Bias:** There is the chance AI algorithms to be biased towards the data it is taught on which may lead to discriminatory actions against threats assessment or to inaccurate outcomes.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

4. **Human Expertise:** At the same time, AI as a cybersecurity tool brings about a high efficiency but, the human expert knowledge is more demanded in the complicated situation to assess the results, to validate the alerts, and to make right decisions.




## IV. ADVANTAGES OF AI IN CYBERSECURITY

Some of the benefits of AI in Cybersecurity that are as follow:

1. **Enhanced Threat Detection Accuracy and Faster Response Times:**
   a. AI algorithms excel in identifying patterns and anomalies in vast amounts of data, leading to more accurate threat detection. Automated Incident Response (AIR) systems powered by AI enable organizations to respond to security incidents swiftly and effectively, reducing the impact of breaches.

2. **Improved Ability to Identify Novel and Sophisticated Attacks:**
   a. AI's advanced analytics and machine learning capabilities empower cybersecurity systems to detect and respond to novel and sophisticated cyber threats that traditional methods may overlook. By continuously learning from past incidents, AI systems adapt to evolving attack techniques, enhancing overall security posture.

3. **Reduced Workload for Security Analysts:**
   a. AI automates routine security tasks, such as monitoring network traffic and analyzing security alerts, reducing the workload for human security analysts. This allows analysts to focus their expertise on investigating and mitigating complex security issues, improving overall efficiency and effectiveness.

4. **Continuous Monitoring and Automated Responses for 24/7 Protection:**
   AI-powered cybersecurity systems provide continuous monitoring and automated responses, ensuring round-the-clock protection against cyber threats. By leveraging AI's capabilities, organizations can proactively identify and respond to security incidents in real-time, minimizing the risk of breaches and data loss.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

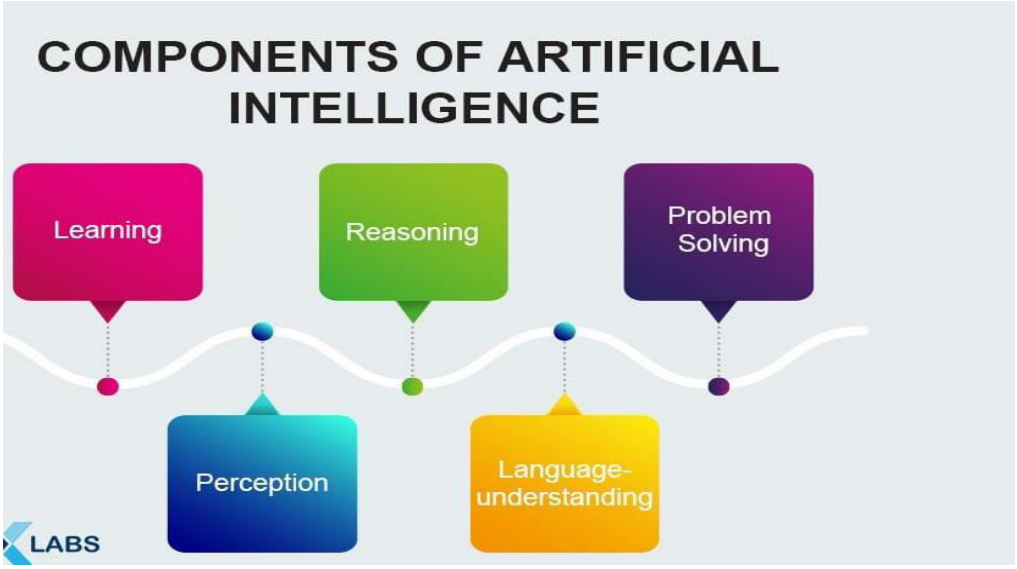

## V. KEY COMPONENTS OF AI IN CYBERSECURITY

- **Machine Learning Algorithms**: At the core of AI in cybersecurity is machine learning, a subset of AI that enables systems to learn from data and improve their performance over time without explicit programming. Machine learning algorithms are crucial in detecting patterns, anomalies, and potential threats in vast datasets.

- **Natural Language Processing (NLP)**: NLP allows machines to understand, interpret, and generate human-like language. In cybersecurity, NLP can analyze textual data, such as logs and threat intelligence reports, to extract meaningful insights and identify potential security issues.

- **Predictive Analytics**: AI utilizes predictive analytics to forecast future cyber threats based on historical data and ongoing trends. This proactive approach enables organizations to implement preventive measures before potential threats materialize.

- **Automation and Orchestration**: AI-driven automation streamlines routine cybersecurity tasks, allowing quicker response times and reducing the burden on human analysts. Security orchestration involves coordinating and automating various security processes to enhance overall efficiency.



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

## VI. CONCLUSION

AI is rapidly becoming an essential technology for boosting the effectiveness of IT security teams. The limitations of human scalability in adequately securing an enterprise-level attack surface are evident, and AI provides the crucial analysis and threat detection necessary for security professionals to mitigate breach risks and strengthen security measures. Furthermore, AI aids in the identification and prioritization of risks, guides incident response efforts, and detects malware attacks proactively. Despite the potential drawbacks, AI will undoubtedly propel the field of cybersecurity forward and enable organizations to establish a stronger security stance.

## VII. FUTURE SCOPE

As AI technology continues to advance, role of AI in cybersecurity will become even more crucial.

- **Autonomous Security Systems:** AI and ML have the potential to develop autonomous security systems that can function independently and make decisions without human intervention. This would empower organizations to promptly address threats, even in the absence of human operators.

- **Predictive Threat Intelligence:** AI and ML can be utilized to analyze data from diverse sources and offer predictive threat intelligence. This would empower organizations to anticipate and prepare for emerging threats before they materialize.

- **Advanced Threat Hunting:** AI and ML can be employed to create advanced threat-hunting systems capable of detecting and responding to unknown threats. This would enable organizations to stay one step ahead of attackers who continuously evolve their tactics.

- **AI-Driven Incident Response And Forensics:** AI and ML can automatically analyze data from various sources, such as network traffic, endpoint data, and logs, to swiftly identify and respond to threats in real time. This would enable organizations to promptly contain and investigate incidents.

- **Automated Compliance And Governance:** AI and ML can automate the compliance and governance process by continuously monitoring and reporting on security controls, as well as identifying potential violations.

- **AI-Powered Security Automation And Orchestration:** AI and ML can automate repetitive security tasks, including patch management and incident response, thereby freeing up human resources to focus on more critical responsibilities.

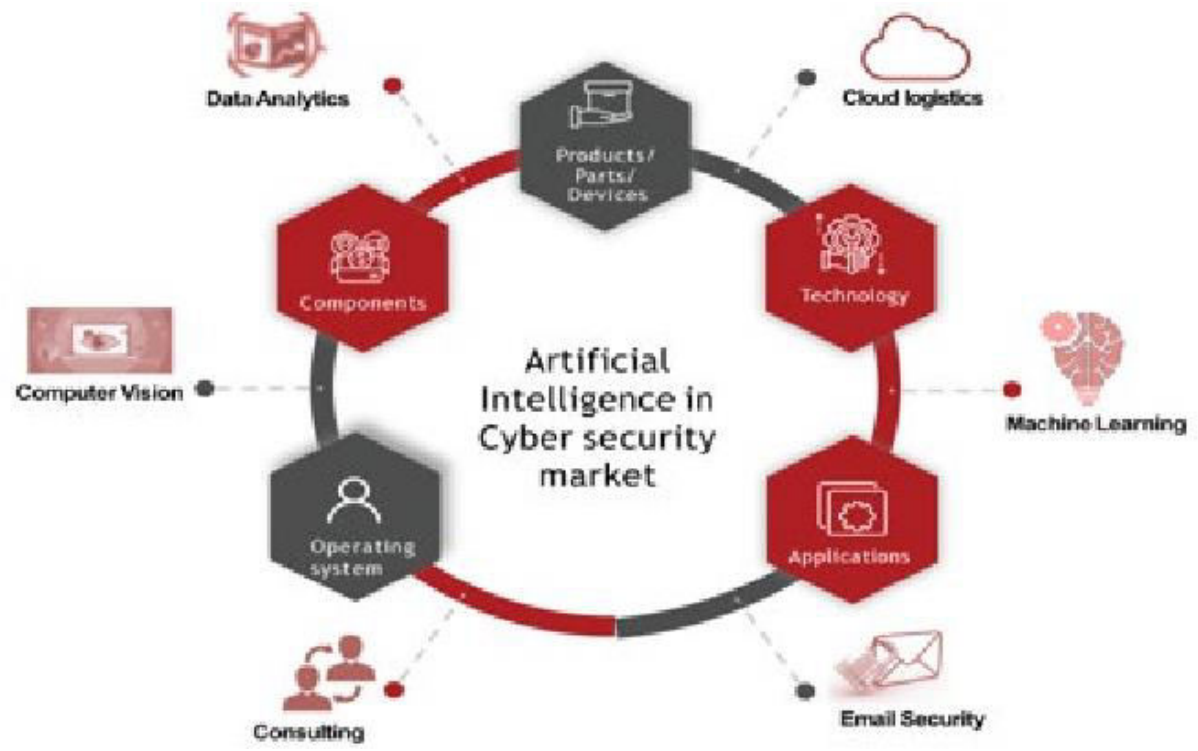
- **The Intersection of AI And Blockchain:** The combination of AI and blockchain technology can offer a more secure and decentralized approach to cybersecurity, particularly in the areas of identity and access management, secure data sharing, and secure payment systems.

- **AI-Driven Security Operations Centers (SOC):** AI and ML can enhance the efficiency and effectiveness of security operations centers **(SOCs)** by automating repetitive tasks, analyzing data from various sources, and providing real-time threat intelligence.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |




## REFERENCES

[1] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[2] Feyereisl, J., & Aickelin, U. (2009). S Elf -O Rganising M Aps. August, 1–30.

[3] Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1907, 93–109.
https://doi.org/10.1007/3-540-39945-3_7.

[4] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

[5] IOS Press. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithms-and-architectures-of-artificial-intelligence/.

[6] Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4476 LNAI, 212–228. https://doi.org/10.1007/978-3-540-72839-9_18.

[7] Kotenko, I. V, Konovalov, A., & Shorov, A. (2010). Agend-based Modeling and Simulation of Botnets and Botnet Defense. In Conference on Cyber Conflict (pp. 21–44). http://ccdcoe.org/229.html.

[8] Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. MODELSWARD 2013 - Proceedings of the 1st International Conference on Model- Driven Engineering and Software Development, 312–315. https://doi.org/10.5220/0004348203120315.

[9] Pachghare, V. K., Kulkarni, P., & Nikam, D. M. (2009). Intrusion detection system using self organizing maps. 2009 International Conference on Intelligent Agent and Multi-Agent Systems, IAMA 2009, 4(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074.

[10] Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322. [15] Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and perfor-mance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305158 |

[11 L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.
[12] L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.
[13] Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879, DOI: 10.13140/RG.2.2.15400.99846.
[14] Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY-MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details