e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

CYBERDEFENCE IN THE AGE OF ARTIFICIAL INTTELIGENCE

Bhaven Thalke*1, Sumiya Madoo*2

*1Student, Department Of Computer Science, B.N.N College, Bhiwandi, Maharashtra, India.

*2Asst. Professor, Department Of Information Technology And Computer Science,
B.N.N College, Bhiwandi, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS35092

ABSTRACT

This research paper investigates the role of artificial intelligence (AI) in cyberdefence and the challenges posed by the increasing sophistication of cyberattacks. The paper discusses the potential of AI for enhancing cyberdefence capabilities, including its ability to detect and prevent cyberattacks in real-time, as well as its use in developing effective response strategies. It also examines the ethical and legal considerations surrounding the use of AI in cyberdefence, including issues related to privacy, accountability, and bias. Additionally, the paper explores the need for training and development of AI systems for cyberdefence so highlights the importance of ensuring that AI systems are developed and used in an ethical and responsible manner.

Keywords: Cyberdefence, Artificial Intelligence, Cyberattacks, Cyber Threat.

I. INTRODUCTION

A. Background and Context

Cyberattacks have become increasingly sophisticated in recent years, posing significant threats to businesses, governments, and individuals. These attacks have resulted in large-scale data breaches, economic losses, and reputation damage. underscores the critical need for an effective cyberdefence strategy.

At the same time, artificial intelligence (AI) is transforming various industries, including cybersecurity. Use AI-based tools and techniques to predict and prevent cyberattacks, improve threat detection and response times, and improve your overall security posture.

However, using AI in cyberdefence is not without its challenges and limitations. There is a constant arms race between defenders and attackers as attackers also use AI for their malicious activities, making AI the newest weapon in the arsenal.

This research paper aims to explore the topic of "cyberdefence in the Age of Artificial Intelligence".

This paper discusses how AI can be used to strengthen cyberdefence and the challenges and limitations associated with using AI.

This study is critical because it aims to contribute to the growing literature on the use of AI in cyberdefence and provide insights that can help develop effective cybersecurity strategies. The paper is also relevant to businesses, governments, and individuals seeking to protect their assets and data from cyberattacks in the digital age.

B. Problems and Research Questions

The increasing frequency and sophistication of cyberattacks are exposing the vulnerability of traditional cyberdefence strategies. Attackers use advanced techniques such as machine learning and AI to evade detection and bypass security measures. This calls for innovative cyberdefence approaches that leverage AI to predict and prevent attacks.

The research questions for this study are:

How can AI be used to enhance cyberdefence capabilities and what are the challenges and limitations associated with its use?

To answer this question, this study examines the state of cyberattacks and the role of AI in cyberdefence. The paper also discusses the challenges and limitations of AI-based cyberdefence strategies, including issues related to data quality, model accuracy, and ethical considerations.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

By examining this question, this research aims to provide insights that can help develop effective cyberdefence strategies. The findings also contribute to ongoing discussions on the use of AI in cybersecurity and provide recommendations for future research and practice.

C. Purpose and Significance of the Survey

The goals of this research work are:

1. Explore the role of AI in cyberdefence and how it can be used to predict and prevent cyberattacks.
2. Identify challenges and limitations associated with AI-based cyberdefence strategies.
3. Provides recommendations for developing effective AI-powered cyberdefence strategies.

The significance of this research is that it may contribute to the growing literature on the use of AI in cybersecurity. By examining the challenges and limitations of AI-based cyberdefence strategies, this paper provides insights to help develop more effective and efficient cyberdefence strategies.

Additionally, the study is relevant to businesses, governments, and individuals who want to protect their assets and data from cyberattacks in the digital age. Research findings provide actionable recommendations for improving cyberdefence capabilities using the latest AI techniques and tools.

This research also contributes to the ongoing debate around the ethical implications of AI in cybersecurity. As AI-based cyberdefence strategies evolve, it is important to consider ethical considerations related to their use, such as issues related to bias, privacy, and accountability. Overall, this research paper has the potential to contribute to the advancement of cybersecurity in the age of AI and the development of more robust and effective defence strategies.

D. An overview of the structure and organization of this document

This research paper consists of several sections that provide a comprehensive overview of the topic of "cyberdefence in the age of artificial intelligence".

After the introduction, the article continues with a literature review that examines the current state of cyberattacks and AI-based cyberdefence strategies. This section provides an overview of the relevant literature, including the latest research on AI in cybersecurity and the challenges and limitations associated with its use.

After a literature review, the paper presents the methodology used in the study, including study design and approach, data collection and analysis methods, variables and measurements, and ethical considerations. The results and analysis section then presents the results of the study, including a data summary and discussion of the results. In this section, we compare our results with previous studies and provide implications and recommendations for practice.

Finally, the paper concludes with a summary of the contributions, limitations, and future research directions of this study. Conclusions also include implications for the statement of conclusions and practice.

Overall, this research paper provides a comprehensive overview of the role of AI in cyberdefence, the challenges and limitations associated with its use, and its implications for developing effective cyberdefence strategies.

II. LITERATURE REVIEW

A. Overview of Cybersecurity and AI

Cybersecurity refers to protecting computer systems, networks, and data from unauthorized access, theft, and damage. With our increasing reliance on digital technology and the internet, cybersecurity has become a critical issue for businesses, governments, and individuals.

In recent years, artificial intelligence (AI) has become a powerful tool in fighting cyber threats. AI-based cyberdefence strategies use machine learning algorithms and other advanced techniques to detect and prevent cyberattacks in real-time.

AI is particularly useful in cybersecurity because it can quickly process large amounts of data and identify patterns and anomalies that could indicate an attack. AI-based systems can also learn from past attacks and adjust defence strategies, accordingly, thus more effectively defending against future attacks.

However, using AI in cyberdefence is not without its challenges and limitations. One of the biggest challenges is the need for high-quality data to effectively train AI models. Without accurate and representative data, AI

models can provide inaccurate or biased results, which can reduce effectiveness and undermine cyberdefence strategies.

Another challenge is that an attacker may use AI to develop new attack strategies that can evade detection by AI-based defence systems. This leads to a constant arms race between defenders and attackers, and AI is the newest weapon in the arsenal.

Despite these challenges, the use of AI in cyberdefence is advancing rapidly, with many businesses and governments investing in AI-based cyberdefence strategies. The next section of the literature review provides an overview of the latest research on AI in cybersecurity and its potential to improve cyberdefence capabilities.

B. State of Cyberattacks and their impact

Cyberattacks are becoming more frequent and sophisticated, posing significant threats to businesses, governments, and individuals. Phishing attacks, malware, ransomware, and denial of service attacks are among the most common types of cyberattacks.

Phishing attacks are one of the most common types of cyberattacks that use fraudulent emails, websites, or text messages to trick people into revealing sensitive information such as passwords and credit card details. According to a recent report from the Anti-Phishing Working Group, in the third quarter of 2022, APWG observed 1,270,883 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed., with businesses and individuals continuing to be targeted by these attacks.

Malware is another common type of cyberattack that uses malicious software to gain unauthorized access to computer systems and networks. Ransomware attacks that encrypt files and data and demand payment for the decryption key are also on the rise. According to the cybersecurity Ventures report 2023, the cost of ransomware attacks is expected to reach $8 trillion dollars worldwide.

A denial of service attack overloads a computer system or network with traffic, rendering it unusable to legitimate users. These attacks can start from a single computer or network of computers, making them difficult to detect and prevent.

The impact of cyberattacks can be severe, from economic loss to reputational damage to national security risks. For businesses, the costs of cyberattacks can include lost revenue, legal fees, and fines. For governments, cyberattacks can threaten critical infrastructure and national security.

In response to the growing threat of cyberattacks, businesses, and governments are increasingly investing in cyberdefence strategies leveraging AI and other advanced technologies.

The next section of the literature review provides an overview of the latest research on AI in cyberdefence and its potential to predict and prevent attacks.

C. AI Technologies and Applications in Cybersecurity

An AI-based cyberdefence strategy is an effective approach to detecting and preventing cyberattacks. This strategy utilizes a variety of techniques and applications that work together to identify and respond to potential threats in real-time.

Some of them are:

1. Machine learning algorithms

Machine learning algorithms have become integral to modern cybersecurity systems that detect, prevent, and respond to cyber threats. These algorithms can be trained on large datasets of network traffic, user behaviour, and other data to learn patterns and identify anomalies that may indicate cyberattacks.

Supervised learning is a machine learning algorithm that trains an AI model on labelled data with a known desired output. For example, a supervised learning algorithm can be trained on a set of known malware samples and their associated signatures and can identify new malware based on those signatures.

Unsupervised learning, on the other hand, trains an AI model on unlabelled data where the desired output is unknown. This type of learning is useful when dealing with new or unknown threats where previous data or flags may not be available. Unsupervised learning algorithms can detect anomalies in network traffic and deviating user behaviour.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

Semi-supervised learning is a combination of supervised and unsupervised learning that uses small amounts of labelled data to drive the unsupervised learning process. This approach is useful when you have limited labelled data but some knowledge of the desired output.

In summary, machine learning algorithms are powerful tools in cybersecurity, and the choice of algorithm to use depends on the type and amount of data available and the specific problem to be addressed. By leveraging these algorithms, cybersecurity professionals can improve detection, prevention and response to cyber threats.

2. User Behavior Analytics (UBA)

User Behavior Analytics (UBA) is a cybersecurity approach that uses artificial intelligence (AI) to analyze user behaviour across an organization's network. With UBA, organizations can detect anomalies in user behaviour that can indicate cyberattacks and other security threats.

Traditional security solutions are often focused on protecting the perimeter of corporate networks but can be ineffective at detecting insider threats. This is where UBA comes in. Detect unusual user activity and behavioural patterns. This could indicate an insider threat or an attacker who has already gained access to your network.

UBA analyzes various data points such as login times, data access, and user activity logs to create a baseline of normal user behaviour. This baseline is then used to identify discrepancies or anomalies that may indicate security threats. For example, if an employee suddenly starts accessing files that they don't normally access, UBA can flag the activity as suspicious and alert the security team.

UBA helps organizations improve their overall cybersecurity posture by detecting insider threats and other types of attacks that traditional security solutions may miss. However, it's important to note that UBA must be carefully designed and implemented to avoid false positives and protect user privacy.

In summary, UBA is a key tool in modern cybersecurity that uses AI to detect anomalies in user behaviour and improve threat detection capabilities.

3. Natural Language Processing (NLP) and Anomaly Detection

In cybersecurity, Natural Language Processing (NLP) and Anomaly Detection are two AI techniques that have become increasingly important. NLP is used to analyze text-based data such as emails, social media posts, and chat logs to identify potential threats.

It can also analyze the language used in phishing attacks and other types of cyberattacks, enabling AI-based defence systems to more effectively identify and block these attacks. Anomaly detection is another important AI technique that identifies deviations from normal behavioural patterns that may indicate cyberattacks. Anomaly detection algorithms can be used to detect anomalous network activity, anomalous user behaviour, anomalous application behaviour, and more. By using these AI techniques, cybersecurity systems can more effectively detect and respond to cyber threats, including those that may be missed by traditional security solutions. As the threat landscape continues to evolve, NLP and anomaly detection will likely become even more important in protecting organizations from cyberattacks.

4. Cyber threat hunting

Cyber threat hunting is a proactive approach to cybersecurity that proactively looks for potential threats and vulnerabilities in an organization's systems and networks. This approach involves using a variety of tools and techniques to identify potential indicators of compromise (IoCs) that may indicate the presence of cyber threats such as malware and compromised access attempts. Cyberthreat searches are typically conducted by experienced cybersecurity professionals who have a deep understanding of corporate systems and networks and the latest threat intelligence and trends in the cybersecurity environment. By proactively searching for potential threats, organizations can detect and respond to cyberattacks faster, reducing the risk of data breaches and other security incidents. Scanning for cyber threats is becoming increasingly important as cyber threats become more sophisticated and traditional security solutions may not be sufficient to detect and prevent them.

5. Deception techniques

Deception techniques refer to a range of tactics used in cybersecurity to identify and respond to potential cyber threats. These methods involve creating realistic decoys, honeypots, and other traps designed to lure attackers

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

into revealing themselves or their methods. For instance, organizations can set up honeypots to detect and capture malware, and identify the techniques used by attackers. Additionally, bait files can be used to detect insider threats by creating false access points and credentials.

Deception techniques can be effective in detecting and responding to threats before they cause significant damage to an organization's systems or data. As a result, these techniques are increasingly critical in cybersecurity, particularly as traditional security solutions may not always be sufficient to detect advanced and persistent threats.

6. vulnerability management

The use of AI in vulnerability management can significantly enhance an organization's cybersecurity posture. By scanning systems and applications, AI algorithms can identify vulnerabilities and prioritize them based on risk. This allows organizations to patch critical vulnerabilities before they are exploited by attackers.

AI-based vulnerability management solutions can also provide real-time threat intelligence and automate the patching process, reducing the time and resources required to address vulnerabilities. This can help organizations stay ahead of potential cyber threats and minimize the risk of data breaches and other security incidents.

As such, vulnerability management is a critical component of any effective cybersecurity strategy, and AI can play a vital role in enhancing its effectiveness.

7. Zero-trust security

Zero-trust security is a security model that assumes all users and devices are untrusted and must be verified before being granted access to sensitive systems or data.

This approach is increasingly important as organizations face growing cybersecurity threats, particularly with the rise of remote work and cloud-based systems. AI can play a vital role in implementing zero-trust security by continuously monitoring user behavior and device activity, identifying potential threats in real-time, and responding automatically. With AI-powered zero-trust security, organizations can implement granular access controls, limit access to sensitive data, and systems only to those who need it. This approach can prevent lateral movement by attackers and reduce the risk of data breaches.

AI-based zero-trust security solutions can also provide real-time threat intelligence and automate the access management process, reducing the time and resources required to verify users and devices. As such, zero-trust security is an essential component of any effective cybersecurity strategy, and AI can significantly enhance its effectiveness.

8. Passwordless authentication

Passwordless authentication is a security model that eliminates the need for passwords, replacing them with alternative authentication methods such as biometrics or smart cards.

AI can play a critical role in implementing passwordless authentication, providing advanced authentication and verification capabilities that can significantly enhance an organization's cybersecurity posture. AI algorithms can analyze user behavior and device activity, identify anomalies or potential threats, and respond in real-time. This approach enables continuous authentication, eliminating the need for static passwords that can be easily compromised.

AI-powered authentication solutions can also use behavioural biometrics, such as keystroke dynamics or mouse movement patterns, to verify user identities without requiring passwords. Additionally, AI can be used to secure the underlying infrastructure of authentication systems, ensuring that they are not vulnerable to cyberattacks. As such, passwordless authentication is becoming an increasingly important component of any effective cybersecurity strategy, and AI can play a vital role in its implementation.

9. Security orchestration and automation

Security orchestration and automation are an integral part of cyberdefence, and AI is playing an increasingly important role in making them effective. AI-based security orchestration and automation tools can analyze vast amounts of data and identify potential threats faster and more accurately than humans can. This includes data from security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), and other sources.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

AI can also automate the incident response process, reducing the time it takes to respond to threats. AI-powered automation helps coordinate incident response and deploy appropriate response actions based on threat severity. This includes quarantining infected devices, gathering evidence, and deploying patches.

Additionally, AI can improve decision-making by providing greater insight into threat activity. This includes providing context around threats such as Tactics, Techniques, and Procedures (TTPs) used by attackers. This information helps security teams better understand the threat landscape and make informed response decisions.

In summary, security orchestration and automation are key elements of any modern cyberdefence strategy, and AI is a powerful tool to make them more effective. AI-powered security orchestration and automation tools help organizations stay ahead of evolving cyber threats by detecting and responding to potential incidents faster and more accurately.

AI-based cyberdefence strategies can be applied to a variety of cybersecurity challenges, including network security, endpoint security, and application security. For example, use AI-based defence systems to detect and block malicious network traffic, protect endpoints from malware and other types of cyber threats, and protect applications that can be exploited by attackers. vulnerabilities can be identified. Despite the potential benefits of AI in cybersecurity, the use of these technologies is not without challenges and limitations. One of the biggest challenges is the need for high-quality data to effectively train AI models. Without accurate and representative data, AI models can provide inaccurate or biased results, which can reduce effectiveness and undermine cyberdefence strategies. Additionally, attackers can use their AI to create new attack strategies that can evade detection by AI-based defence systems. Nonetheless, AI-based cyberdefence strategies have shown promising results in detecting and preventing cyberattacks and are expected to play an increasingly important role in the future of cybersecurity.

D. Challenges and Limitations of AI in cyberdefence

Although AI-based cyberdefence strategies show great potential in detecting and preventing cyberattacks, there are some challenges and limitations to their use.

One of the biggest challenges is the need for high-quality data to effectively train AI models. AI models rely on large amounts of data to learn and make accurate predictions, and the quality of the data used can have a significant impact on model effectiveness. Without accurate and representative data, AI models can provide inaccurate or biased results, which can reduce effectiveness and undermine cyberdefence strategies. Another challenge is that attackers may use AI to develop new attack strategies that can evade detection by AI-based defence systems. For example, attackers can use AI to generate sophisticated phishing attacks tailored to specific individuals and organizations, making them more difficult to detect and prevent. As AI technology continues to advance, attackers are likely to become increasingly sophisticated in their use of AI, increasing challenges to AI-based defence systems.

A related challenge is a need for AI-based defence systems to adapt to changing threats and attack strategies. AI models trained on historical data may not be effective at detecting new or emerging threats and may require constant updating and training to remain effective. Another limitation of AI-based cyberdefence strategies is the potential for false positives and false positives. A false positive occurs when an AI-based defence system identifies a threat that isn't a threat, while a false negative occurs when a threat is not identified by the defence system. Both false positives and false negatives can reduce the effectiveness of AI-based defensive strategies and lead to increased costs and risks for businesses and organizations.

Finally, there are ethical and privacy concerns related to the use of AI in cyberdefence. AI-based defence systems can collect and analyze sensitive data, raising privacy and data protection concerns. Additionally, AI-based defence systems can make decisions that have a significant impact on individuals and organizations, raising concerns about accountability and transparency.

Despite these challenges and limitations, AI-based cyberdefence strategies may play an increasingly important role in the future of cybersecurity. As the threat of cyberattacks continues to increase, businesses and organizations must continue to invest in advanced technologies such as AI to protect against these threats.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

III. METHODOLOGY

A. Research Design and Approach

This research paper adopts a qualitative research design, specifically a literature review approach. A literature review is an effective research methodology that provides a comprehensive and systematic overview of the existing literature on a particular topic. It allows for the identification of knowledge gaps and the synthesis of previous research findings to develop new insights and knowledge. For this research, a literature review approach is appropriate as it enables a thorough examination of the literature on the use of AI in cyberdefence.

B. Data Collection and Analysis Methods

The data for this study were obtained from a variety of sources, including articles, reports, books, and online resources. The search for relevant literature was conducted using various academic databases, including Google Scholar, and ScienceDirect. The search terms used included "cyberdefence," "artificial intelligence," "cybersecurity," and "cyber threats." The inclusion criteria for selecting the studies were that they focused on the use of AI in cyberdefence and were published between 2015 and 2023.

The collected data were analyzed using a thematic analysis approach. Thematic analysis is a common method used in qualitative research for identifying and interpreting patterns in the data. The analysis involved reading and re-reading the literature to identify themes and sub-themes related to the use of AI in cyberdefence. The themes were then coded and organized into categories to identify the key findings and insights.

C. Variables and Measures

This research paper explores the use of AI in cyberdefence and the challenges and limitations associated with its use. The key variables of interest are the use of AI in cyberdefence, the benefits of using AI, the challenges and limitations of using AI, and the implications of using AI for cyberdefence in the age of AI. The measures used to capture these variables include a review of the literature on the use of AI in cyberdefence, identification of the benefits, challenges and limitations of using AI, and the identification of the implications of using AI for cyberdefence in the age of AI.

Overall, this research paper adopts a qualitative research design and uses a literature review approach to explore the use of AI in cyberdefence. The data for the study were collected from a variety of sources and were analyzed using a thematic analysis approach. The key variables of interest were identified, and measures were developed to capture these variables. The methodology employed in this study is appropriate for achieving the research aims and objectives and for developing new insights and knowledge on the use of AI in cyberdefence.

IV. RESULTS AND ANALYSIS

A. Summary of data and results

This literature review analyzed publications on cyberdefence in the age of artificial intelligence. The publications were drawn from academic journals, conference proceedings, and industry reports and covered various topics related to the use of AI in cyber defence.

The results of this literature review highlight the growing importance of AI in the field of cyberdefence and its potential benefits in preventing and predicting cyberattacks. A literature review identified many AI techniques and applications used in cyberdefence, including machine learning, natural language processing, and anomaly detection. These techniques are used to detect and prevent various cyber-attacks such as phishing, malware, and ransomware.

However, the literature review also highlighted some challenges and limitations related to the use of AI in cyberdefence. These include the lack of transparency and interpretability of AI algorithms, the potential for bias in AI systems, and the limited availability of qualified personnel to implement and maintain AI systems. These challenges and limitations must be carefully considered when designing and implementing an AI-based cyber defence system. Overall, the results of this literature review show that AI has the potential to significantly improve the effectiveness and efficiency of cyber defences. However, the ethical implications of using AI in this context require careful consideration, and ongoing research and development are needed to address the challenges and limitations associated with AI in cyber defence.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

B. Discussion of Results

The results of this literature review show that the use of AI in cyberdefence can significantly improve the effectiveness of traditional cyberdefence methods. The AI techniques and applications identified in the review, including machine learning, natural language processing, and anomaly detection, enable real-time monitoring and analysis of large amounts of data, helping detect and prevent various cyber-attacks.

However, the review also identified some challenges and limitations related to the use of AI in cyberdefence. A major challenge is the lack of transparency and interpretability of AI algorithms. The processes AI systems use to identify and prevent cyberattacks are often not fully understood, and this lack of transparency makes it difficult to identify and correct biases and errors within systems. can be difficult.

Another challenge is the potential for bias in AI systems. AI algorithms are only as good as the data they use to train them, and if the data used to train an AI system is biased or incomplete, the system will produce biased or inaccurate results. may generate This can have serious implications for cyberdefence, especially when AI systems are used to make decisions that can affect the security of individuals and organizations.

Finally, the literature review highlighted the limited availability of qualified personnel to implement and maintain AI systems in the context of cyberdefence. This is because effective use of AI in cyberdefence requires not only skilled data scientists and engineers, but also cybersecurity professionals who understand the unique challenges and risks associated with cyberattacks. is a serious problem.

In summary, the results of this literature review suggest that the use of AI in cyberdefence may significantly improve the effectiveness and efficiency of traditional cyberdefence methods. However, realizing this potential to its full potential requires ongoing efforts to address the challenges and limitations associated with AI in cyberdefence and to ensure that AI systems are designed and implemented in an ethical and responsible manner. necessary research and development.

C. Impact and recommendations

The results of this literature review have several important implications for the use of AI in cyberdefence and future research and development in this area. Based on these findings, the following recommendations are proposed.

1. Address AI challenges and limitations in cyberdefence:

Challenges and limitations associated with using AI in cyberdefence. Bias and lack of transparency should be addressed through ongoing research and development. This includes developing new techniques and approaches to reduce bias in AI systems, and increasing the transparency and interpretability of AI algorithms.

2. Increase the availability of skilled workers:

Effective use of AI in cyberdefence requires not only skilled data scientists and engineers, but also cybersecurity professionals who understand the unique challenges and risks associated with cyberattacks. To counter this, efforts should be made to increase the availability of qualified personnel in this field through education and training programmes, and through the development of new job profiles and career paths.

3. Promote collaboration and information sharing:

Collaboration and information sharing across organizations and industries are essential for effective cyberdefence. This includes sharing threat intelligence and best practices related to the use of AI in cyberdefence, and working together to develop new standards and guidelines for the ethical and responsible use of AI in this context.

4. Development of new indicators and evaluation frameworks:

Traditional cyberdefence metrics and evaluation frameworks may not be sufficient to assess the effectiveness of AI-based systems. New metrics and evaluation frameworks need to be developed that better reflect the unique capabilities and limitations of AI systems.

In summary, the results of this literature review suggest that the use of AI in cyberdefence may significantly improve the effectiveness and efficiency of traditional cyberdefence methods. However, realizing this potential to its full potential requires ongoing efforts to address the challenges and limitations associated with AI in cyberdefence and to ensure that AI systems are designed and implemented in an ethical and responsible manner. necessary research and development.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

V. CONCLUSION

A. Overview of the study and its contribution

The use of AI in cyberdefence is an area of growing interest and importance as organizations seek to improve their ability to detect and prevent cyberattacks. This literature review provides an overview of the current state of cyberattacks, the application of AI in cyberdefence, the challenges and limitations associated with using AI in this context, and recommendations for future research and development.

The results of this literature review highlight the potential benefits of using AI for cyberdefence, including improved threat detection accuracy and speed, and the ability to detect and defend against advanced attacks. However, this review also identified some challenges and limitations associated with using AI in this context. Bias and Lack of Transparency. It should be addressed through ongoing research and development.

Overall, the contributions of this study include providing a comprehensive overview of the current state of AI in cyberdefence, highlighting the potential benefits and challenges associated with this technology, and proposing recommendations for future research and development. included. It is hoped that overcoming these challenges and limitations will further improve the effective use of AI in cyberdefence, enabling organizations to better protect against the growing threat of cyberattacks.

B. Limitations and directions for future research

This literature review has several limitations that need to be recognized. First, this review is based on a limited number of studies and may not cover the full spectrum of research on AI in cyberdefence. Furthermore, the review only considered studies published in English and may have excluded relevant studies published in other languages. Finally, the field is evolving rapidly, so some of the results presented in this review may already be out of date.

Future research in this area could address some of these limitations by conducting a more comprehensive systematic review across a wider range of studies, including those published in languages other than English. Yes, future research could explore the potential of AI in cyberdefence in different industries and contexts, and examine the ethical and legal implications of using AI in this context. Finally, continued research and development is required to address AI-related challenges and limitations in cyberdefence, including: Bias and Lack of Transparency, and the Development of New Techniques and Approaches to Mitigate These Problems.

In summary, this literature review provides a comprehensive overview of the current state of AI in cyberdefence, but much remains to be done in this area. Future research and development is needed to fully realize the potential of AI in cyberdefence and to address the challenges and limitations associated with this technology. In this way, businesses can protect themselves from the growing threat of cyberattacks and ensure the security of their data and systems.

C. Conclusions and Implications for Practice

The use of AI in cyberdefence has the potential to significantly improve the security of organizations and their data and systems. However, it is important to note that AI is not a cybersecurity panacea and there are still many challenges and limitations to using AI in this context. Therefore, organizations should carefully consider the potential benefits and risks of using AI for cyberdefence and implement appropriate strategies and safeguards to ensure its effective and ethical use.

One of the implications for practice is that organizations will need to invest in developing the skills and expertise needed to effectively implement and manage AI into their cyberdefence strategies. This may include hiring or training staff with AI and cybersecurity expertise, and investing in the infrastructure and tools necessary to support the use of AI in this context.

Another implication for practice is the importance of continued research and development to address AI-related challenges and limitations in cyberdefence. This may include developing new technologies and approaches to reduce bias and improve transparency, and investigating the potential use of AI in combination with other cybersecurity technologies and strategies.

In summary, effective use of AI in cyberdefence requires careful consideration of its potential benefits and risks, as well as continued research and development to address the challenges and limitations associated with this

technology. In this way, companies can protect themselves from the growing threat of cyberattacks and ensure the security of their data and systems.

VI. REFERENCES

[1] B. Alhayani, H. Jasim Mohammed, I. Zeghaiton Chaloob et al., Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.02.531

[2] Paul-Jasper Dittrich and Björn Boening, More security in cyber space:: The case for arms control, Federal Academy for Security Policy, Security Policy Working Paper, No. 9/2017, http:// www.jstor.com/stable/resrep22197

[3] y Joseph Ogaba Oche, The Risk of Artificial Intelligence in Cyber Security and the Role of Humans, Texila International Journal of Academic Research Special Edition Apr 2019, DOI: 10.21522/TIJAR.2014.SE.19.01.Art001

[4] Batta Mahesh, Machine Learning Algorithms - A Review, International Journal of Science and Research (IJSR), Volume 9 Issue 1, January 2020, DOI: 10.21275/ART20203995