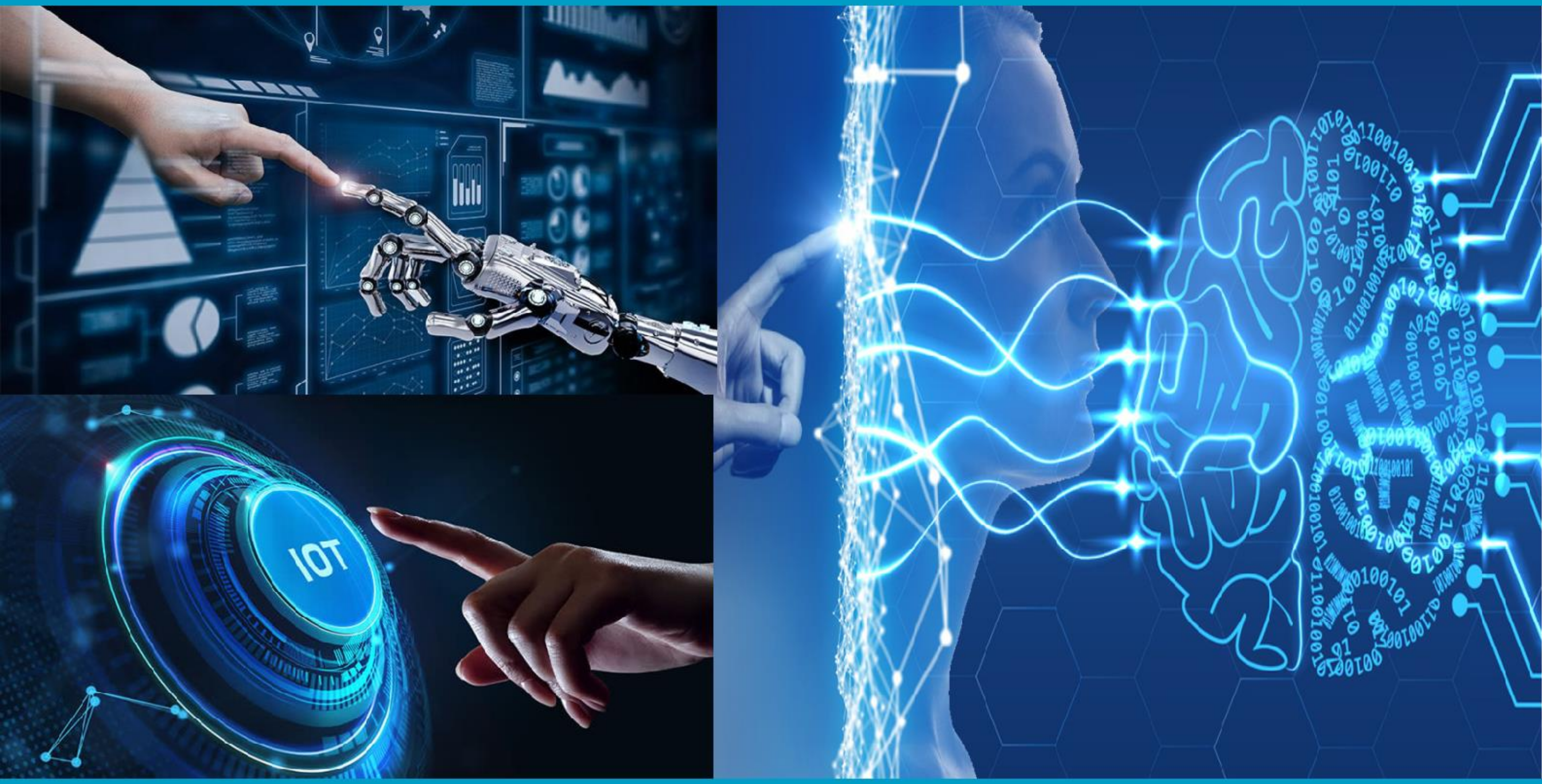
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 6, June 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.580

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 6, June 2023 |

Artificial Intelligence in Cyber Security – Review and Applications

Miss. Sakshi A .Zawar, Mr Shripad S Bhide

Student, Department of M.C.A, P.E.S Modern College of Engineering, Pune, India

Assistant Professor, Department of M.C.A, P.E.S Modern College of Engineering, Pune, India

ABSTRACT: The rise in cyber hazards is a significant problem for both organizations and individuals as the digital landscape advances. Traditional cyber security techniques frequently fall behind the sophistication and breadth of today's threats. As a result, enhanced systems that can determine avert, and respond to cyber threats instantly are urgently required. The following research paper reviews the role of Artificial Intelligence in enhancing cyber security measures in depth.

The research begins by diving into the fundamental principles of artificial intelligence and its primary components such as neural networks, natural language processing and machine learning. It looks into the capability of AI to change cyber security by augmenting human capabilities. Automating routine tasks and enabling rapid response to emerging threats. Based on prior research this study intends to present a current overview of AI's use in cyber security and to assess the potential for improving cyber security through the expanded use of AI.

Anomaly identification, behavior analysis, predictive modeling, and threat intelligence are also investigated in the study. This study also tackles ethical concerns concerningAI's use in cyber security, emphasizing the significance of transparency, accountability, and justice. It explores the various biases and vulnerabilities of AI systems and proposes rules for responsible AI deployment to protect privacy and minimize unanticipated outcomes.

Finally, the study concludes with a vision on the future of AI in cyber security, noting new concepts such as an adversarial machine learning, explainable AI, and decentralized techniques.

Overall, this paper is a comprehensive resource for researchers, cyber security experts, and policymakers, delivering valuable insights into the potential of AI to strengthen cyber security measures, diminish risks, and guard information assets in an increasingly interconnected and vulnerable world.

KEYWORDS: cyber security, AI, Machine Learning, Neural Networks, Deep Learning, Cyber-attacks, Fraud detection

I. INTRODUCTION

The widespread interconnection of modern societies offers several benefits, but it also creates unprecedented levels of vulnerability to cyber threats. As cyber-attacks evolve and become more sophisticated, creative and smart countermeasures are needed to outsmart attackers. Artificial intelligence (AI), with its ability to make digital systems more resilient and protect sensitive data from unethical actors, is proving to be a promising solution here.

The purpose of the following research paper is to provide detailed review of the role of Artificial Intelligence in cyber security. We intend to analyze the usefulness and limitations of AI in securing digital assets by examining current AI-powered solutions and their influence on threat detection, incident response, and risk reduction. Furthermore, we will investigate the ethical implications of AI in cyber security and suggest potential solutions to these concerns.

To summarize, AI represents an enormous potential for the field of cyber security, helping organizations and individuals to effectively tackle the ever-changing threat landscape. We can proactively protect our digital frontiers, manage risks, and ensure the confidence and privacy of our linked world by utilizing the power of AI. To enable AI's responsible and successful incorporation into cyber security practices, a careful balance of innovation, ethics, and privacy must be struck.

II. OVERVIEW OF ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

2.1 Artificial Intelligence:

In the last decade, AI has experienced unprecedented popularity and widespread adoption as a subject ofcomputer science. In 1956 John McCarthy coinedthe term "AI" that represents the science of creating intelligent machines that simulates human intelligence. McCarthy's definition encompassed more than mathematical logic, extending to problem-solving, reasoning, learning, perception, and natural language processing. AI has evolved with advancements in the machine learning, neural networks, expert systems, computer vision, and robotics. Its ubiquity stems from increased computational power, large-scale datasets, and algorithmic progress. AI's applications span healthcare, finance, transportation, and entertainment, aiming to enhance efficiency and decision-making. While achieving artificial general intelligence remains a long-term goal, current AI technologies significantly impact society and will continue to shape our lives.

Fake insights are the plan and arrangement of computer frameworks that can finish exercises that would habituallyrequire human insights. It is an interdisciplinary field that brings together principles and techniques from computer science, mathematics, statistics, cognitive science, and other disciplines. AI strives to construct intelligent machines that can learnreason, perceive, and interact with their surroundings.

Artificial intelligence technology can understand and learn from information from events and impacts and act accordingly. As per definition by Peter Norvig and Stuart Russell "AI aims not only to understand, but also to build intelligent entities."

By unraveling the workings of the human mind in learning, decision-making, and problem-solving, AI harnesses this knowledge to forge intelligent systems and applications.There are several components and approaches within AI like Machine Learning, Deep Learning, Expert Systems,Natural Language Processing, etc.

2.2 Cyber Security and different cyber-attacks (cyber threats)

Cybersecurity fortifies the digital realm, warding off trespassers and fortifying valuable systems, networks, and data against unauthorized intrusion, harm, and pilferage. It includes a number of techniques, technologies, and processes aimed at ensuring confidentiality, integrity, and availability (CIA Triad) of data in cyberspace.

The term "cyber" adverts to "related to computer culture, information technology, or/and virtual reality." This makes it apparent that we are articulating information security as well as computer network. Cybersecurity encompasses a range of techniques and safeguards aimed at safeguarding interconnected networks, software, equipment, and data from unauthorized access and malicious harm. In the realm of computing, safeguarding both the virtual domain of cyberspace and the tangible world of physical space hold equal importance, ensuring comprehensive security for digital systems and their tangible counterparts.

MAJOR CYBER ATTACKS

In today's interconnected world, there are several key cyber risks that individuals, organizations, and governments confront. Here are a few notable examples:

1. **MALWARE**: Malware encompasses harmful software variants like viruses, worms, the Trojans, ransomware, and spyware, posing threats of network and computer damage, data theft, system interruptions, and financial losses.
2. **PHISHING ATTACKS**: Phishing attacks employ deceptive messages, emails, or websites to deceive individuals into divulging classified information, such as personal data, credit card details, or passwords primarily with the aim of illicitly obtaining valuable data or unauthorized network entry.
3. **DISTRIBUTED DoS and Distributed Denial of Service (DDoS)**: DDoS attacks flood targeted websites or networks with traffic, causing them to become inaccessible to users. These attacks have the potential to disrupt services, tarnish reputations, and result in financial losses.
4. **DATA BREACHES**: A data breach occurs when unauthorised access to privileged data,like personal information, intellectual property, or financial recordsoccurs. Data breaches can be sold on the black market, used to conduct identity theft, or exploited for other malicious purposes.
5. **INSIDER THREATS**: Insider threats refer to employees leveraging their authorized access to breach networks, pilfer data, or disrupt operations. These threats might be intentional or unintentional, the result of negligence, displeasure, or coercion.
6. **MAN IN THE MIDDLE ATTACK**: About 95% MitM attacks occur when a cyber-attacker is between two parties.An attacker may interpret a message to steal sensitive data and then respond in a variety of ways.
7. **ADVANCED PERSISTENT THREATS**: "APTs employ intricate tactics to infiltrate target networks and ex-filtrate sensitive information, showcasing advanced levels of attack sophistication."

III. AI TECHNIQUES IN CYBER SECURITY

The following section provides a deep insightaboutvarious learning algorithms, which are fundamental AI concepts, as well as a brief introduction to AI branches like expert systems, machine learning, and deep learning which are often used in cyber security areas.

Learning algorithms train machines and improve performance through learning and experience-based training. In general, there are three primary learning algorithms commonly employed for training machines, each distinguished by its unique approach and characteristics:[1]

1. **Supervised learning**: Supervised learning is a machine learning technique that trains an algorithm to predict an output based on a labelled dataset. The system needs to be tested using test data set after the training phase. These learning techniques are often used for regression or classification. The regression algorithm utilizes input data to produce unique continuous-valued outputs or predictions. Classification algorithms, as opposed to regression methods, produce distinct results.

2. **Unsupervised learning**: On the contrary, unsupervised learning uses an unlabelled training data set. Unsupervised learning commonly serves the purpose of grouping data into clusters, simplifying its dimensions, or approximating its density.

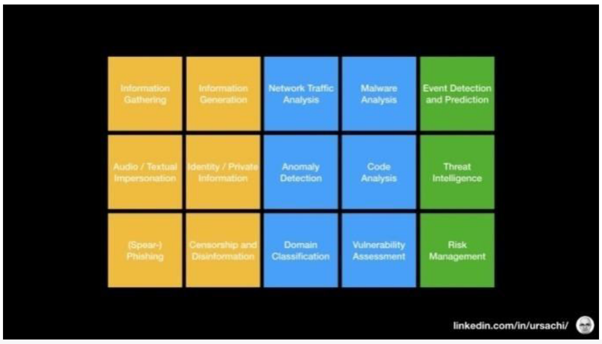
3.**Reinforcement learning**: This category of learning algorithms acquires optimal actions by considering rewards or penalties as guiding factors. Reinforcement is nothing but synthesis of supervised and unsupervised learning. This type of learning is useful when data is scarce or unavailable.[1]
AI techniques have become increasingly important in cyber security due to their ability to detect, prevent, and respond to sophisticated cyber threats. Here are some key AI techniques used in cyber security:

1. **Machine Learning (ML):** Arthur Samuel defined machine learning asa set of methods that provides computers with the ability to learn without being explicitly programmed. ML empowers systems to autonomously uncover and codify underlying data principles, acquire knowledge from the data, and enhance performance through iterative experience, all without explicit programming. At the onset of the learning process, the examination of data through examples facilitates pattern identification, enabling informed decision-making in subsequent instances. Equipped with this understanding, the computer harnesses the power of reasoning to infer attributes of previously unobserved instances.
Statistics are used in machine learning to gather information, recognise patterns, and draw conclusions from massive volumes of data. Machine learning algorithms are divided into following three categories: unsupervised learning, supervised learning, and reinforcement learning. Decision trees,Bayesian algorithms, KNN, association rule algorithms, k-means clustering, and principal component analysis are the most commonly used algorithms in cybersecurity.
ML algorithms are extensively used in cybersecurity for tasks such as anomaly detection, classification, and pattern recognition. Large datasets can be used to train machine learning models to discern patterns of normal and hazardous conduct, assisting in the detection and prevention of cyber-attacks.

2. **Deep Learning:** Deep learning is another type of machine learning that consists of training multiple-layer artificial neural networks to recognise complex patterns and characteristics. Deep learning models, among other things, can be used for image recognition, virus detection, and network intrusion detection.
Deep learning algorithms possess the ability to iterate tasks, introducing slight variations with each repetition to enhance the output, mirroring the human capacity to learn and improve through experiential learning.DL emulates the cognitive processes of the human brain, extracting patterns from data to inform decision-making. It simulates signal processing processes in human brains and neurons. The iterative process of constructing larger neural networks and training them with extensive data sets consistently enhances the performance of artificial neural networks. Every day, massive amounts of data are generated by numerous applications.
DL's adoption in cyberspace is driven by the surge in everyday data generation, as the algorithms rely on extensive data sets to facilitate learning. One advantage of DL is that it performs better with large volumes of data. In the realm of cybersecurity, various DL techniques find application, such as convolutional neural networks, feed-forward neural networks, recurrent neural networks, generative adversarial networks, restricted Boltzmann machines,deep belief networks, and ensembles of DL networks.

3. **Natural Language Processing (NLP):**
Within the realm of computer science and artificial intelligence, natural language processing (NLP) delves into the dynamics of computer-human communication using the medium of natural language. Its overarching objective is to enable computers to comprehend language on par with human understanding, fuelling advancements in virtual assistants, speech recognition, sentiment analysis, automatic text summarization, machine translation, and a wide range of other applications.
By merging linguistics and machine learning, NLP constitutes a computer science subfield with a unique interdisciplinary approach. The focal point of the field lies in facilitating natural language communication between computers and humans, as NLP revolves around imparting the ability to computers for interpreting and generating human language.
As the cyber security landscape encompasses every IT system or application, the role of NLP is expanding to cater to its demands, utilizing the continuous influx of research and algorithms to bolster a wide array of cyber security applications. The below diagram depicts the same and hence it is classified into three types of application as follows:

1.The yellow boxes symbolize applications that leverage automated information gathering and generation to either launch attacks or strengthen defence mechanisms in the context of human-machine collaboration.
2. The blue boxes are for applications that attackers can use NLP to amplify their attacks on a system or defenders can use to harden their system.
3. The green boxes symbolize applications that support human side of human-machine teaming.



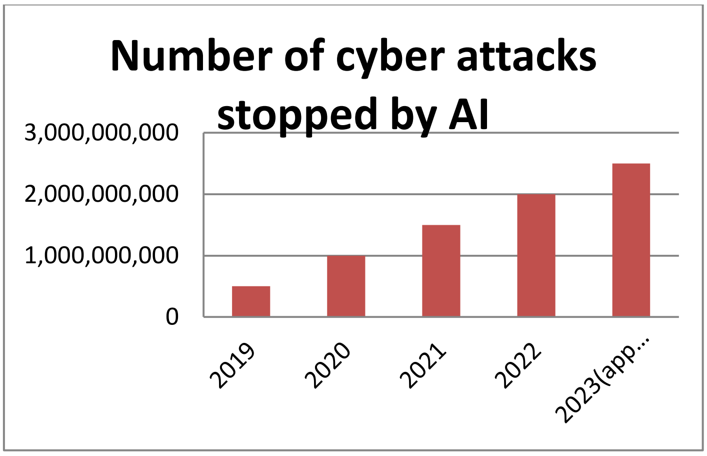
Information Gathering	Information Generation	Network Traffic Analysis	Malware Analysis	Event Detection and Prediction
Audio / Textual Impersonation	Identity / Private Information	Anomaly Detection	Code Analysis	Threat Intelligence
(Spear-) Phishing	Censorship and Disinformation	Domain Classification	Vulnerability Assessment	Risk Management

linkedin.com/in/ursachi/

Fig.NLP used in cyber security as per various researchers and algorithms.[8]

NLP techniques are used in cybersecurity to analyse textual information such as log files, network traffic, and social media content. NLP systems can analyse keywords, sentiment, and context to identify potential security risks and attacks.

IV. APPLICATIONS OF AI IN CYBER SECURITY



[10]

1. MALWARE CLASSIFICATION

With an ever-evolving nature, malware encompasses various forms of malicious code or software designed for intentional harm, and while traditional detection relied on signature-based systems, the advent of machine learning is now driving a shift towards inference techniques to enhance malware detection and prevention.
One potential answer to this threat is the use of AI in malware classification. AI can analyse and classify malware based on a multitude of factors, such as code, behaviour, and impact. This can help cybersecurity specialists identify and neutralise threats more quickly and efficiently.
There are several methods for using AI to categorise malware. One method is to use machine learning techniques to assess software code and determine if it is malicious or benign. This can be performed by training the algorithm on a large dataset of both malicious and benign software, allowing it to learn the characteristics that distinguish the two.
Another possibility is to use artificial intelligence to analyse programme behaviour. This is performed by running the software in a virtual environment and observing its behaviour. The software can then be classified by AI depending on whether its behaviour is typical of malware or innocent software.
The cyber security field has witnessed one of the most successful implementations of deep learning and AI, thanks to the availability of extensive, precisely labelled datasets consisting of tens of millions of samples from both malicious malware and benign applications, emphasizing the crucial role of large, accurately labelled data sets in training effective algorithms.

2. **Threat detection and classification**

AI systems possess the capability to identify and mitigate threats by developing models that analyze massive datasets of cyber security events, enabling the recognition of patterns indicative of malicious behaviour, ultimately preventing attacks from taking place. The construction of the model often relies on pre-existing data and recorded indicators of compromise (IOCs), enabling real-time tracking, identification, and response to threats, enhancing the effectiveness of threat detection and mitigation in cyber security. As a result, if identical activities are detected, the models recognise them automatically. ML classification techniques leverage IOC datasets to find and classify malware behaviours.

Innovative behavioral-based research leverages machine learning clustering and classification techniques to evaluate the behavior of numerous malwares, extracting patterns that can automate the detection and classification of emerging threats, offering significant benefits to security analysts and other automated systems in the cyber security domain.

3. **User Authentication and Access Control**

By assessing user behaviours, contextual data, and risk factors, AI may dynamically change authentication limitations and improve access control.

If suspicious behaviour is detected, AI systems can detect abnormalities in user behavioural patterns and initiate alerts or additional authentication processes.

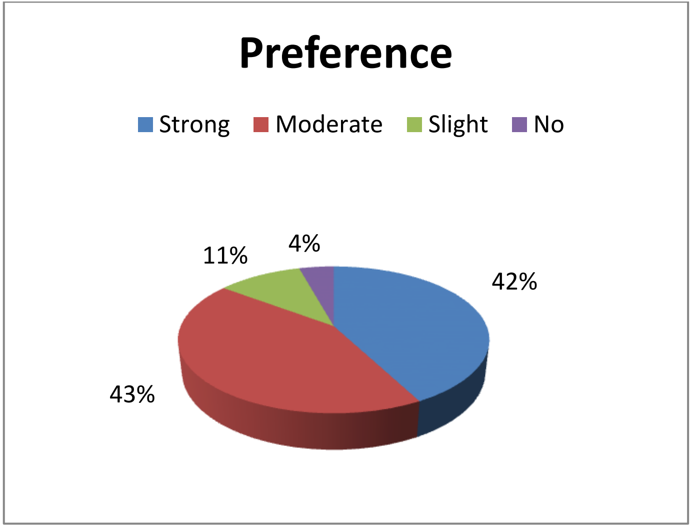
User access verification refers to the process of authenticating the identity of users attempting to access a system or network. This is an important part of ensuring cyber security because it helps prevent unauthorised access and secure sensitive data.

AI can examine user attributes such as login history, system behaviour, and other criteria to determine whether or not a person is who they claim to be. This could include using machine learning algorithms to study patterns of behaviour and detect anomalies that could indicate a cyber-attack attempt.

Biometric data, such as fingerprints or facial recognition, can be used to authenticate people. Installing sensors or other devices that collect data and use it to validate user identities is one example.

AI in Cyber Security -> Preference Statistics by Different Organizations [9]

(Statistics as per information from various websites)



V. ADVANTAGES AND DISADVANTAGES OF AI IN CYBER SECURITY

ADVANTAGES

In the sphere of cyber security, AI provides various advantages.
1.Improved threat detection
2. Real-time response
3.Daily Task Automation
4. Increased accuracy and decreased false positives
5.Adaptive authentication

These advantages demonstrate how AI may improve cyber security by increasing threat detection, response time, and overall resilience to cyber threats. However, keep in mind that AI has limitations and constraints, and human talent is still essential for interpreting AI-generated knowledge and making strategic decisions.

Extensive research on the advantages of artificial intelligence in cyber security unveils that organizations implementing AI in this domain experience substantial benefits, as evident from the increased return on investment (ROI) on cyber security products reported in two-thirds of enterprises; highlighting the tangible value AI brings to the field. A significant majority of administrators, 64% to be precise, affirm that artificial intelligence (AI) has effectively reduced expenses related to breach detection and response, while organizations save an average of 12% on costs. With the cyber security landscape rapidly shifting towards automated mitigation, AI holds immense potential by swiftly recognizing novel and intricate modifications in attack patterns.

DISADVANTAGES

While artificial intelligence has the potential to improve cyber security, it also has several downsides. Here are a couple of such examples:

Cost: Implementing AI-powered cyber security solutions can be costly, especially for small and medium-sized businesses. Obtaining technology, recruiting educated personnel to administer it, and staying current with technical advancements can be prohibitively expensive.

Lack of human oversight: If AI systems are not properly programmed or educated; they can make errors and overlook critical security threats. Without human oversight, AI-powered cyber security technology can be useless or even damaging to a company's security posture.

Cyber threats: The increasing vulnerability of data and privacy to cyber-attacks necessitates the implementation of robust safeguards to prevent unauthorized access and potential breaches, as cyber attackers can exploit vulnerabilities to trace locations and compromise critical information.

To fully leverage the benefits of AI in cyber security while mitigating risks, a comprehensive understanding of its limitations and potential drawbacks is essential for optimal deployment and utilization.

VI. CONCLUSION

To summarise, AI has the potential to greatly improve cyber security measures by automating procedures, detecting trends, and processing large amounts of data in real time. It can aid in the identification of threats, incident response, and decision-making. However, there are several disadvantages to adopting AI in cyber security.

Given the rapid proliferation and increasing sophistication of cyber threats, the need for novel, resilient, adaptable, and scalable approaches becomes imperative. AI-based cyber security algorithms are focusing on key areas such as virus detection, network intrusion detection, and phishing/spam detection, with studies exploring the fusion of ML/DL techniques with bio-inspired computation and reinforcement learning to yield remarkable results. These innovative combinations offer promising outcomes in bolstering cyber security defences.

To leverage the benefits of AI in cyber security while minimizing its limits, it is vital to combine AI with human experience and oversight. Human analysts and cyber security professionals play an important role in analyzing AI-generated insights, validating findings, and making essential judgments. Collaboration between humans and artificial intelligence can result in stronger cyber security defense.

Overall, artificial intelligence has the potential to improve cyber security by improving capabilities and lowering response times. However, it must be implemented with caution, taking into consideration its limitations and ensuring the necessary human interaction to enable effective and comprehensive cyber security measures.

REFERENCES

[1] “A Survey Of Artificial Intelligence in Cyber security” 2020 International Conference on Computational Science and Computational Intelligence , Katanosh Morovat, Brajendra Panda

[2] Novateur Publications International Journal Of Innovations In Engineering Research And Technology [Ijiert] Issn: 2394-3696 Website: Ijiert.Org Volume 7, Issue 9, Sep.-2020 “ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE“ Ishaq Azhar Mohammed

[3] ICACSE 2020 “Artificial Intelligence in Cyber Security” Rammanohar Das and Raghav Sandhane

[4]“Artificial Intelligence in Cyber Security“ Rammanohar Das and Raghav Sandhane

[5]”Artificial Intelligence in Cyber Security - A Review” Jenis Nilkanth Welukar, Gagan Prashant Bajoria

[6] REST Journal on Emerging trends in Modelling and Manufacturing Vol: 8(2), 2022 REST Publisher; ISSN: 2455-4537 “Artificial Intelligence in Cyber Security “ Swagat M. Karve, Arpit Yadav, Prateek Datt

[7] “The Role of Artificial Intelligence in Cyber Security” Kirti Raj Bhatele, Harsh Shrivastava, Neha Kumari
[8] https://www.masernet.com/project/role-and-applications-of-nlp-in-cybersecurity
[9] https://cyber-edge.com/resources/2020-cyberthreat-defense-report/
[10] https://bard.google.com

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com