iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59803

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

AI Driven Innovations in Cyber Security

Rugved Lav Nikam[1], Manisha Patil[2]
[1]*Dept of MCA, Trinity Academy of Engineering Pune, India*
[2]*Asst Prof Dept of MCA, Trinity Academy of Engineering Pune, India*

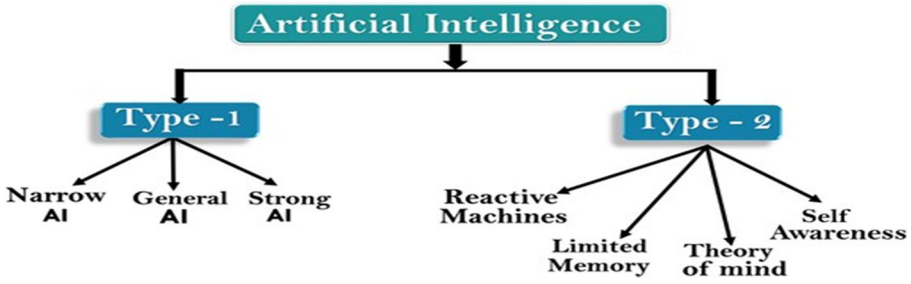
Abstract: ***The explosion of cyber threats presents a huge challenge to traditional cyber security methods, requiring the integration of advanced technologies such as artificial intelligence. This research paper provides an in-depth analysis of the current landscape of AI applications in cybersecurity. We will look at different AI techniques, such as machine learning, deep learning, natural language processing and anomaly detection, and explain their role in improving threat detection, incident response and vulnerability management. In addition, we explore AI-based cybersecurity challenges such as competitor attacks, data protection issues, and model interpretability. Based on recent advances and emerging trends, we propose future research directions to address these challenges and realize the full potential of AI to protect digital assets and critical infrastructure. Our synthesis aims to inform policymakers, industry participants and researchers about the transformative impact of AI on cybersecurity and inspire collaboration to build resilient and adaptive defenses in the face of evolving cyber threats.***
Keywords: Artificial Intelligence (AI), cybersecurity, machine learning, deep learning, natural language processing, and anomaly detection

I. INTRRODUCTION

A. *What is AI?*

Definitions of AI

1) John McCarthy, a pioneer of AI, defined it as "the science and engineering of making intelligent machines." He underlined the goal of AI as developing computers capable of performing activities that would normally require human intelligence.
2) Marvin Minsky, a pioneer in the field of AI, defined it as "the science of making machines do things that would require intelligence if done by humans." Minsky focused on AI systems' ability to mimic human intelligence and behavior.
3) According to futurist and AI expert Ray Kurzweil, AI is "the art of creating machines that perform functions that require intelligence when performed by people." Kurzweil highlights the significance of AI in augmenting human capacities and allowing robots to accomplish jobs formerly identified with human intelligence.
4) In their textbook "Artificial Intelligence: A Modern Approach," Stuart Russell and Peter Norvig define AI as "the study of agents that perceive the environment and take actions to maximize their chances of success." Their definition focuses on the agent-based approach to AI, in which computers interact with their surroundings to achieve certain objectives.



B. *Types of AI*

Based on capabilities

1) *Narrow AI (Weak AI):* This sort of AI is designed to do certain tasks, such as facial recognition, online searches, or driving. Most modern AI systems, including those capable of playing difficult games such as chess and Go, fall under this group. They operate within a narrow predefined range or set of situations.
2) *General AI (Strong AI):* This sort of AI focuses on specific tasks, such as facial recognition, online searches, and driving. Most modern AI systems, including those capable of playing difficult games such as chess and Go, fall under this group. They operate within a narrow predefined range or set of situations.

3) *Super intelligent AI:* This represents a future form of AI where machines could surpass human intelligence across all fields, including creativity, general wisdom, and problem- solving. Superintelligence is speculative and not yet realized.

II. BASED ON FUNCTIONALITIES

A. Reactive Machines

These AI systems do not retain memories or previous experiences for future use. They assess and respond to various situations. IBM's Deep Blue, which defeated Garry Kasparov in chess, is an example.

B. Limited Memory

By analyzing previously acquired data, these AI systems can make more informed and better decisions. Most modern AI applications, from chatbots and virtual assistants to self-driving cars, fit into this category.

C. Theory of Mind

This is a more advanced form of AI that researchers are still working on. It would include recognizing and remembering emotions, beliefs, and needs, and then making decisions based on them. This type requires the machine to properly understand people.

III. HISTORY OF AI.

A. Maturation of Artificial Intelligence (1943-1952)

Year 1943: Warren McCulloch and Walter Pits created the initial work that is today known as artificial intelligence in 1943. They proposed a model for artificial neurons.

In 1949, Donald Hebb presented an updating rule for altering the strength of neural connections. His guideline is now known as Hebbian learning.

Alan Turing, an English mathematician, pioneered machine learning in 1950. Alan Turing's book "Computing Machinery and Intelligence" includes a test proposal. A Turing test can be used to assess a machine's capacity to demonstrate intelligent behavior comparable to that of humans.

B. The Birth of Artificial Intelligence (1952– 1956)

In 1955, Allen Newell and Herbert A. Simon produced the "first artificial intelligence program," Logic Theorist. This program verified 38 of 52 mathematical theorems and discovered new and more elegant proofs for several of them.

In 1956, American computer scientist John McCarthy coined the term "artificial intelligence" at the Dartmouth Conference. For the first time, AI was defined as an academic field.

C. The golden years—early enthusiasm (1956-1974)

Year 1966: The researchers focused on inventing algorithms that could solve mathematical issues. In 1966, Joseph Weizenbaum invented the first chatbot, known as ELIZA.

WABOT-1, Japan's first intelligent humanoid robot, was constructed in 1972.

D. The First AI Winter (1974–1980)

The first artificial intelligence winter occurred from 1974 to 1980. AI winter refers to the period in which computer scientists faced a serious scarcity of government funding for AI research.

During AI winters, the interest of the public in artificial intelligence plummeted.

E. A boom in AI (1980-1987)

Year 1980: Following the AI winter, AI returned with "Expert System". Expert systems were created to mimic the decision-making capacity of a human expert.

In 1980, Stanford University hosted the American Association of Artificial Intelligence's inaugural national conference.

F. The Second AI Winter (1987–1993)

The second AI Winter took place from 1987 until 1993.

Again, investors and the government have ceased sponsoring AI research due to the exorbitant cost and ineffective results. The expert system, such as XCON, was extremely cost effective.

G. Deep learning, big data, and artificial general intelligence (2011–present)

Year 2011: In 2011, IBM's Watson won Jeopardy, a quiz show where it had to tackle complicated questions and riddles. Watson had demonstrated its ability to grasp natural language and solve complex queries fast.

Year 2012: Google introduced the "Google Now" function for Android apps, which may present users with information in the form of predictions.

Year 2014: In 2014, Chatbot "Eugene Goostman" won a competition in the notorious "Turing test." Year 2018: The "Project Debater" from IBM argued tough themes with two expert debaters and fared admirably.

IV. WHAT IS CYBER SECURITY?

Computer security, also known as cybersecurity, digital security, or information technology security (IT security), protects computer systems and networks from malicious attacks that could cause unauthorized information disclosure, theft, or damage to hardware, software, or data, as well as disrupt or misdirect services. The topic is significant because of the growing reliance on computer systems, the Internet, and wireless network technologies like Bluetooth and Wi-Fi. Also, due to the proliferation of smart gadgets, such as smartphones, televisions, and the many devices that comprise the Internet of Things (IoT).

Cybersecurity is one of the most pressing issues in the modern world, owing to the complexity of information systems and the society they serve. Security is particularly important for systems that regulate large- scale processes with far-reaching physical consequences, such as electricity distribution, elections, and banking.

V. COMMON CYBER THREATS

A. Malware

Malware, which stands for "malicious software," refers to any software code or computer program designed with the goal of causing harm to a computer system or its users. Almost every current cyberattack has some form of malware.

Malware is created and used by hackers and cybercriminals to obtain illegal access to computer systems and sensitive data, hijack and remotely operate computer systems, disrupt or damage computer systems, or hold data or systems hostage for significant sums of money (see Ransomware).

B. Ransomware

Ransomware is a sort of virus that encrypts a victim's data or equipment and threatens to keep it encrypted— or worse—until the victim pays the attacker a ransom. According to the IBM Security X-Force Threat Intelligence Index 2023, ransomware assaults accounted for 17% of all cyberattacks in 2022. "Or worse" is what distinguishes modern ransomware from its predecessors. The first ransomware attacks wanted a single ransom in exchange for the encryption keys. Today, the majority of ransomware assaults are double extortion, with a second ransom demanded to prevent the victim's data from being shared or published. Some are triple extortion attacks that threaten to launch a distributed denial of service assault unless ransoms are paid.

C. Phishing

Phishing attacks are email, text, or voice messages that fool users into installing malware, disclosing sensitive information, or giving money to the incorrect person. Most users are acquainted with bulk phishing schemes, which include sending bogus messages that look to be from a well-known company and ask recipients to reset their passwords or enter credit card information. However, more sophisticated phishing scams, such as spear phishing and business email compromise (BEC), target specific persons or groups in order to steal sensitive information or huge sums of money.

Phishing is simply one sort of social engineering, which is a collection of 'human hacking' strategies and attacks that use psychological manipulation to persuade or compel people into taking risky activities.

D. Insider Threats

Insider risks are those that originate with authorized users—employees, contractors, or business partners— who purposefully or unintentionally abuse their legitimate access or have their accounts hijacked by cybercriminals. Insider threats are more difficult to detect than external threats because they bear the hallmarks of authorized behavior and are invisible to antivirus software, firewalls, and other security systems designed to prevent external attacks. One of the most common cybersecurity myths is that all cybercrime stems from external sources. According to a recent study, 44% of insider threats are produced by hostile actors, with the average cost per occurrence for malicious insider incidents in 2022 being USD 648,062.3.

E. Man-in-the-Middle Attack

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, take place when attackers inject themselves into a two-party transaction. Once the attackers have interrupted the flow, they can filter and take data.

There are two common entrance points for MitM attacks:

1) Insecure public Wi-Fi allows attackers to implant themselves between a visitor's device and the network. The visitor unknowingly transmits all information to the attacker.

2) Once malware has infiltrated a device, the attacker can install software that processes all of the victim's data.

VI. COMMON CYBERSECURITY MYTHS:

A. Strong Passwords alone Provide Adequate Protection

Strong passwords can make a difference. For example, a 12-character password is 62 trillion times more difficult to crack than a 6-character password. However, because cybercriminals can steal passwords (or bribe unhappy employees or other insiders to do so), they cannot be used as the sole security safeguard for a company or individual.

B. The Biggest Cybersecurity Concerns are well Understood

In fact, the risk surface is always growing. Each year, thousands of new vulnerabilities are discovered in both old and new programs and devices. Opportunities for human error—particularly by careless workers or contractors who unintentionally create a data breach— are increasing.

C. 'My industry is safe'

Every industry faces cybersecurity concerns, with cyber attackers abusing the importance of communication networks in nearly every government and private-sector entity. For example, ransomware attacks are affecting more industries than ever before, including municipal governments, non-profits, and healthcare institutions. Threats to supply chains, ".gov" websites, and key infrastructure have all escalated.

D. Cybercriminals do not Target Small Businesses

Yes, they do. For example, in 2021, 82 percent of ransomware attacks targeted businesses with fewer than 1,000 employees, while 37 percent of ransomware assaults affected businesses with fewer than 100 employees.

VII. AI TECHNIQUES IN CYBER SECURITY

A. Machine Learning (ML)

Machine learning algorithms examine vast databases for patterns, anomalies, and correlations that indicate cyber dangers. Supervised ML models can categorize known hazards using labeled data, whereas unsupervised ML models can discover abnormalities or outliers in data without prior training. Malware detection, intrusion detection, and user behavior analytics are all examples of cybersecurity applications that use machine learning techniques.

B. Deep Learning

Is a kind of machine learning that trains artificial neural networks with several layers to recognize patterns and predict outcomes. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are used in cybersecurity for tasks such as image-based malware detection, natural language processing (NLP) for text-based threat analysis, and detecting network intrusions based on sequence data.

C. Natural Language Processing (NLP)

Helps computers understand, interpret, and generate human language. NLP is used in cybersecurity to analyze security logs, parse threat intelligence reports, and find indicators of compromise (IOCs) from unstructured text sources such as websites, forums, and social media platforms. Identifying phishing emails is a common concern to prevent personal information loss, such as bank account information, social security numbers, and user passwords. Contemporary ML models are inaccurate in this domain because they rely on human detection of representative features, and DL models face similar issues due to a lack of embedding words in the model for adequate content representation in an email exchange. NLP may be coupled with ML and DL models to efficiently classify email contents and identify phishing assaults.

D. Reinforcement Learning (RL)

Is an AI technique that teaches an agent to make decisions based on trial and error, with the goal of maximizing cumulative rewards. In cybersecurity, RL can be used to create adaptive security systems that dynamically alter defense mechanisms in response to new threats and changing network conditions, hence optimizing security posture over time.

E. Expert System

The most often used AI approaches are specialized programs. An expert program aims to solve challenges posed by customers or specific technologies in a certain field. This can help with decision-making in areas such as healthcare, banking, and virtual worlds. Optimization strategies can solve complex challenges ranging from small analytical medical diagnosis to advanced hybrid systems.
A scheme of expertise is a knowledge foundation that includes specialized study of a certain application area. In addition to the knowledge base, a deduction engine provides solutions based on this understanding.

VIII. AI BASED APPROACHES IN CYBER SECURITY

Advancements in computing technologies have significantly impacted people's daily lives and employment, causing rapid societal change. Some of these technologies have enabled machines to think, learn, make decisions, and solve problems in the same way that humans do. AI, for example, uses intelligence to perform real-time analysis and decision making while processing massive volumes of data to solve problems.
AI approaches have applications in a wide range of scientific and technological sectors. It is no secret that the Internet has a wealth of personal information, which presents numerous cybersecurity difficulties. Manual analysis is impractical owing to large data sets. Second, risks are increasing, and AI-based threats may occur. Additionally, hiring specialists raises the expense of threat prevention efforts.
Developing and implementing algorithms to identify risks requires significant time, money, and effort. AI-based technologies offer a potential solution to these difficulties.
AI is capable of quickly and accurately analyzing massive amounts of data. AI-based systems can predict future assaults based on past threats, even if trends change.
AI can be employed in cyberspace for the following reasons: AI can detect new and significant changes in attacks, AI can manage large amounts of data, and AI security systems can train continuously to better respond to threats. AI has limits, including the need for large amounts of data that might take time and resources to handle. False alarms can also be an issue for end-users, and delayed responses can reduce efficiency. Researchers have developed AI approaches for detecting, stopping, and responding to cyberattacks. Cyberattacks often fall into four categories:

A. Software Exploitation and Malware Detection

1) Software Exploitation

Vulnerabilities can be exploited by attackers who are aware of the defect, allowing them to target the underlying program. Some common software vulnerabilities include buffer overflow, integer overflow, SQL injection, cross-site scripting, and cross-site request forgery. Some vulnerabilities are identified and resolved. It would be wonderful if software developers have identified and addressed all vulnerabilities. Designing and developing software can be challenging due to high expenses and pressure to meet market demands. As a result, problems are constantly identified and addressed.
Bruce Schneier describes the internet as "the most complex machine mankind ever built." We don't fully grasp how it works or how to secure it. To correct software defects, it's time-consuming to read through each line of code. However, computers can automate this process if they are trained to recognize vulnerabilities. AI appears capable of completing these tasks. Benoit Moral explained how AI approaches increase application security.

2) Malware Identification

Malware identification is a common strategy for cyberattacks. Malicious software includes viruses, worms, and trojan horses. Malware has a significant impact on politics and the economy, making it crucial to avoid and mitigate assaults. Several studies have been conducted on the adoption of AI technology. Here is a list of noteworthy research. The authors developed a system for categorizing and detecting malware through data mining and machine learning. Scholars employed k- nearest neighbors and support vector machines as ML classifiers to detect unknown malware.

B. Phishing and Spam Detection

1) Phishing Attacks

A phishing assault aims to steal users' identify. Phishing attacks include brute-force and dictionary-based assaults. Here are some significant AI-based approaches for dealing with this issue. The authors developed a phishing email detection system that uses modified neural networks and reinforcement learning. Feng et al. used a neural network to detect phishing websites using the Monte Carlo technique and risk minimization approach.

2) Spam Detection

This refers to unsolicited mass emails. Spam emails may include unsuitable content, leading to security concerns. Artificial intelligence systems are now being used to filter spam emails. Feng et al. showed one system.

C. Network Intrusion Detection

1) Denial of Service (DoS)

Is a popular attack where fraudsters prevent authorized users from accessing network resources. The authors of suggested a system that combines anomaly-based distributed artificial neural networks and signature- based techniques.

2) Intrusion Detection System (IDS)

An intrusion detection system (IDS) safeguards a computer system against unexpected events, violations, or potential threats. AI-based technologies are ideal for constructing IDS due to their flexibility, speed, and ability to learn quickly. AI-based techniques enhance characteristics and classifiers to reduce false alarms.

IX. AI TECHNIQUES IN ENHANCING CYBERSECURITY MEASURES

A. Anomaly Detection

Providing information about AI techniques used to improve cybersecurity measures, including their formation and methodologies. Anomaly detection Statistical models are used to identify and minimize deviations from normal behavior based on specific organizational and resilience requirements. These models recognize attack vector patterns, allowing security personnel to make fast and efficient decisions.

However, the model is frequently used in conjunction with other methodologies to identify the true nature of the threat and conduct proactive analysis. A hybrid model using a Gaussian Mixture was presented for anomaly detection, along with the integration of network misuse detection via the decision tree model. The model accounts for inconsistencies in the dataset or logs, which might lead to misguided, or worse, high false rates.

To create a smart city with many ICT gadgets, IoT communications, and cloud-connected data storage systems, AI-integrated models can be implemented at various levels of the system to improve anomaly detection. A hybrid approach with centralized to distributed architecture demonstrates the importance of AI-based ML models for securing edge-to-cloud networks in smart cities. The design overcomes attacks on distributed computing devices with a facilitated ML- integrated SDN network that includes cloud-based services.

The combination of SDN, numerous controllers, and ML approaches at the edge networks improves security against malicious or aberrant data and identifies compromised system resources. Expert system cooperation often improves detector performance by providing feedback on accuracy and detection results from system analysts and operators, allowing the AI model to learn from the human in the loop system.

B. Signature-based Detection

The use of signatures as an attribute for detecting prominent aspects in time-dependent and urgent data patterns is widely used in literature. Signature-based models use two mechanisms: rulesets to protect against unknown or undefined actions in the network, and patterns to distinguish abnormal activity from typical traffic. Rule-based models filter data according on predefined rules, with common tools such as Snort, Suricata, and Zeek used for detection. In addition to open- source IDS software, various rule-based methodologies have been created, including a fuzzy rule-based model for identifying hazards in cross-country product pipeline systems.

C. Threat Intelligence and Deception

Technology Modern security management systems can capture hackers' behavior or data flow by identifying vulnerabilities in specific portions of the infrastructure or using tracking technologies. The strategy of attracting adversaries is commonly referred to as "HoneyPot," because it helps system analysts acquire crucial information about attacker attack signatures and methods. The Honey Pot analysis can also be used to simulate the IDS or to redirect the attack away from critical targets. The data collected by the Honeypot technique is a valuable source of real-time threat intelligence. Security analysts and forensic professionals can use this data to identify new attack patterns, malware injection strategies, and exploitation trends.

X. CASE STUDIES

A. Darktrace

Is a cybersecurity company using AI for attack detection and response. Their main product, the Enterprise Immune System, uses unsupervised machine learning algorithms inspired by the biological immune system to detect and respond to cyber threats in real time. Darktrace's AI algorithms continuously analyze network traffic and user activity to detect aberrant actions that may indicate cyber dangers, such as insider threats, malware infections, or advanced persistent threats (APTs). Darktrace assists enterprises in proactively mitigating risks and protecting their digital assets by responding to threats autonomously.

B. Cylance

BlackBerry purchased Cylance in 2019, which developed an AI-driven endpoint security solution that uses machine learning to combat malware assaults. Cylance's AI models examine file properties and behavior patterns to determine if a file is benign or malicious, without the need for signatures or prior knowledge of threats. Cylance's AI-based strategy offers enterprises proactive defense against changing cyber threats by detecting and blocking malware in real time.

C. Vectra AI

Vectra AI is a platform for network detection and response (NDR) that utilizes AI to identify and prioritize threats across enterprises. Vectra's AI algorithms examine network traffic and behavior patterns to discover anomalies that may indicate cyber threats such as lateral movement, data exfiltration, or reconnaissance activities. Vectra AI provides real-time visibility into network threats, allowing security teams to respond quickly and eliminate hazards before they become significant breaches.

D. FireEye Helix

FireEye Helix is a cloud-based security operations platform that uses artificial intelligence and machine learning to automate threat detection and response. FireEye's AI-powered algorithms sift through security alerts and event data from numerous sources to identify and prioritize threats based on severity and impact. FireEye Helix automates repetitive activities and correlates security events throughout the company, allowing security professionals to focus on significant threats and respond more effectively to cyber attacks.

E. Symantec AI-Powered Cyber Security

Symantec, a major cybersecurity business, incorporates artificial intelligence and machine learning into its security products and services to improve threat detection and response capabilities. Symantec's AI algorithms scan massive volumes of telemetry data, such as network traffic, endpoint activity, and threat intelligence feeds, to detect emerging threats and suspicious activity. Symantec uses AI-driven analytics to help enterprises stay ahead of cyber threats and secure their digital assets from evolving attack vectors.

XI. CONCLUSION

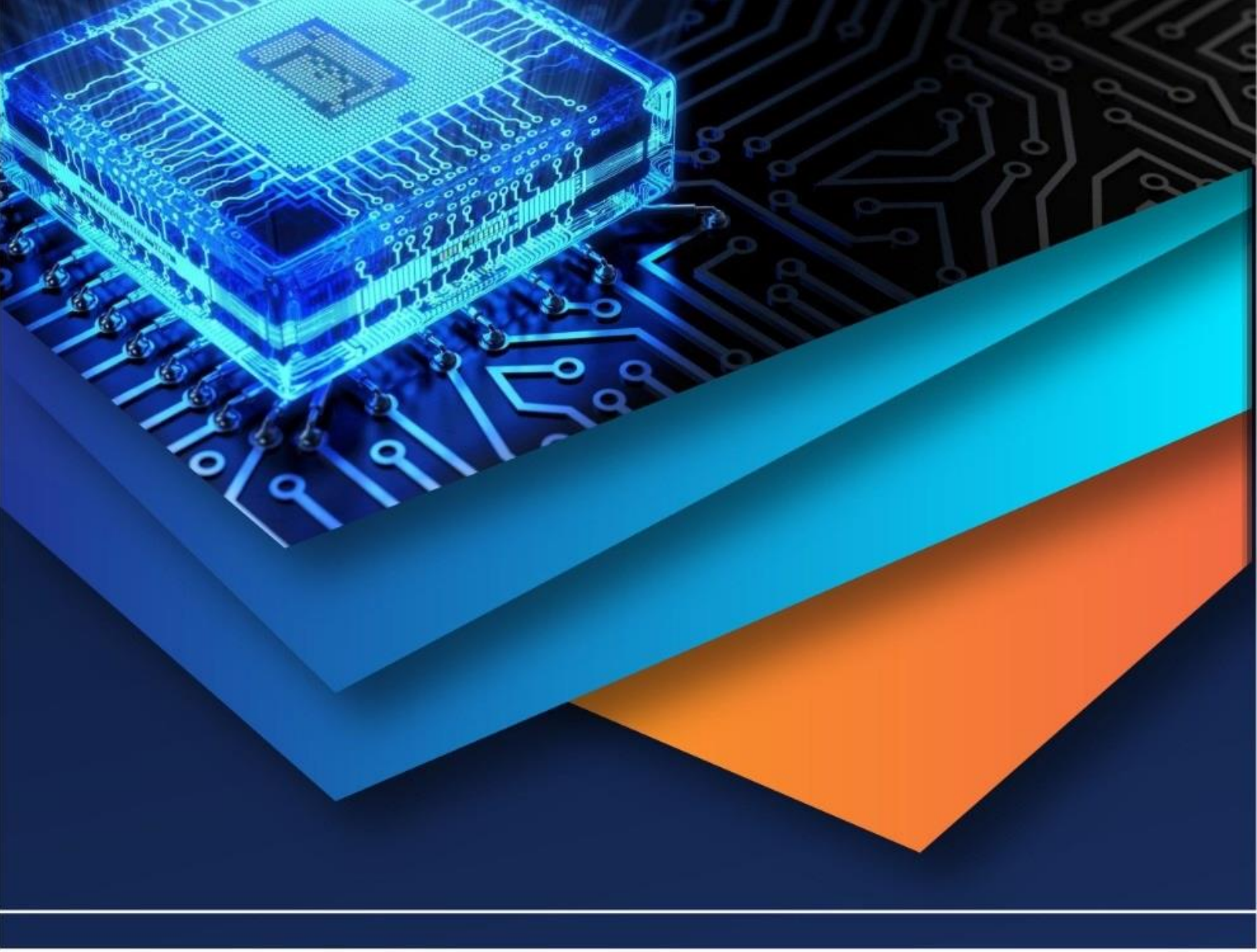
The use of artificial intelligence (AI) in cybersecurity has significantly improved threat detection, prevention, and response. The review of existing research and industrial implementations shows that AI-driven cybersecurity solutions have enormous potential in complementing human capabilities, improving the resilience of digital systems, and reducing emerging cyber threats.

One of the key benefits of AI in cybersecurity is its ability to analyze large volumes of data at unprecedented speeds, allowing for real-time threat analysis and proactive defense measures. Machine learning algorithms, in particular, have shown exceptional efficacy in detecting aberrant patterns and distinguishing sophisticated attack pathways, strengthening cyber defenses against both known and upcoming threats.

Looking ahead, researchers, practitioners, and governments must work together to address these difficulties while fully using AI's promise to protect digital assets and maintain cyberspace's integrity. Future research should prioritize the development of robust AI algorithms that are resistant to adversarial manipulation, as well as the creation of ethical frameworks for the responsible deployment and regulation of AI-driven cybersecurity systems.

REFERENCES

[1] John McCarthy, "Artificial Intelligence Logic and Formalizing Common Sense." Stanford University, California, USA. 1990
[2] Machine Learning Techniques for Malware Detection. Kaspersky Lab. 2020.
[3] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, and J. Wang, "A Novel Neural Network for Detecting Phishing Websites," Intelligent Humanizing Computation, 2018, 1-15.
[4] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abramo, M.L. Proenca, "Network anomaly detection system using genetic algorithm and fuzzy logic." Expert System Application, 2018, 92: 390–402.
[5] Sabah Alzahrani and Liang Hong, "Detection of Distributed Denial of Service (DDoS) Attacks Using Artificial Intelligence on Cloud." Proceedings of the 2018 IEEE Conference, San Francisco, CA, USA, July 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY