ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 4, July - August 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.028

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

Cyber Security and Risk Management in Modern World

Dr. M. Kundalakesi[1], G. Harshavarthini[2], Aadhi Keshav C[3], Sethuranga Skanthan P T[4]

Assistant Professor, Department of Computer Application, Sri Krishna Arts and Science College, India[1]

Student, Department of Computer Application, Sri Krishna Arts and Science College, India[2-4]

ABSTRACT: In an era of global connection and digital dependency, the convergence of cybersecurity and risk management is critical for enterprises looking to strengthen their digital infrastructure. This paper digs into the complex dynamics of cybersecurity and risk management, examining the changing threat landscape and critical tactics for effectively mitigating cyber risks. It also investigates the relationship between cybersecurity and risk management, with a focus on Artificial Intelligence (AI) as a critical tool for successful threat management. The incorporation of artificial intelligence into cybersecurity operations has emerged as a disruptive force, altering how organizations detect, assess, and manage cyber risks. The first section of the paper discusses the multidimensional nature of modern cyber threats, including malicious actors and sophisticated malware. It underlines the crucial importance of a comprehensive risk management approach that includes threat identification and robust incident response. Moving ahead, the conversation will focus on risk management frameworks and approaches customized to the digital realm. The article explains how AI-powered systems excel at spotting patterns associated with diverse cyber threats, allowing for a more proactive and adaptive cybersecurity posture. The study of AI's impact extends to risk management frameworks and adaptive decision-making. The study finishes by underlining the symbiotic relationship between AI, cybersecurity, and risk management, and arguing that AI should be integrated as a basic element in the current cybersecurity armory.

KEYWORDS: Cybersecurity , Risk management , Artificial Intelligence (AI) , Threat identification , Symbiotic relationship.

I. INTRODUCTION

In the digital age, cybersecurity and risk management are critical components of corporate resilience and success. Cybersecurity protects computer systems, networks, and data from unauthorised access, theft, and damage, whereas risk management identifies, assesses, and mitigates potential threats and vulnerabilities.

Businesses that rely heavily on digital technologies to foster innovation and optimize operations are more vulnerable to cyber assaults and data breaches. These accidents can have serious implications, such as financial losses, reputational damage, and legal liability. As a result, firms must prioritize cybersecurity and risk management in order to protect assets and maintain customer and stakeholder trust.

Cybersecurity and risk management are critical in today's linked digital landscape, as firms face constantly evolving threats from fraudsters looking to exploit loopholes. As technology improves, so do the techniques and sophistication of cyber assaults, making it critical for businesses to implement comprehensive security measures to protect sensitive data and systems. In this context, the use of artificial intelligence (AI) has emerged as a strong tool for improving cybersecurity measures and effectively mitigating threats.

Cybersecurity refers to a set of techniques and technology used to protect digital assets like as networks, systems, and data from unwanted access, breaches, and damage. To fight against attacks, it is necessary to adopt proactive measures such as firewalls, encryption, access controls, and intrusion detection systems. However, traditional cybersecurity approaches frequently struggle to keep up with the quickly evolving threat landscape, leading to holes in protection.

Here's where artificial intelligence comes into play. AI technologies, particularly machine learning algorithms, can analyze large volumes of data, recognize trends, and uncover abnormalities that could suggest possible security vulnerabilities. Organizations can improve their threat detection capabilities by adopting AI-powered solutions, allowing them to identify and respond to security problems in real time, reducing the impact of breaches.

Threat identification and response is one of the primary areas where AI is transforming cybersecurity. AI-powered systems can continuously monitor network traffic, user behavior, and system records for odd activity that may indicate a

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

cyber assault. These systems can evaluate data autonomously, identify potential threats, and even take proactive risk-mitigation measures like blocking suspicious IP addresses or isolating hacked endpoints.

Furthermore, artificial intelligence has the potential to significantly improve the efficiency and effectiveness of risk management processes.Risk management is the process of detecting, assessing, and prioritizing risks to an organization's assets, as well as putting mitigation techniques in place. AI can automate several parts of risk management, such as risk assessment, scenario analysis, and risk mitigation planning. Organizations can obtain deeper insights into their risk exposure by using AI-driven analytics, allowing them to make better decisions about resource allocation and risk mitigation methods.

AI can also improve the robustness of cybersecurity defenses by providing adaptive and proactive approaches. AI-powered systems may learn from past security problems and adjust their defenses accordingly, keeping them one step ahead of cyber attackers. AI-powered threat intelligence solutions, for example, may scan massive volumes of data from numerous sources to detect emerging threats and vulnerabilities, allowing enterprises to patch or update their systems before they are exploited.

While AI has enormous potential for improving cybersecurity and risk management methods, it also introduces new difficulties and threats. Artificial intelligence algorithms may be subject to adversarial attacks, in which malevolent actors modify input data to trick AI systems and elude discovery. Furthermore, the use of AI in cybersecurity raises ethical and privacy problems, such as the possibility of algorithmic bias and the acquisition of sensitive personal data.

The use of AI into cybersecurity and risk management techniques has enormous potential for improving enterprises ability to effectively protect against cyber threats and reduce risks. Organizations may strengthen their security posture, improve threat detection and response capabilities, and make more informed risk management decisions by adopting AI-powered technology. However, companies must address the problems and risks connected with AI adoption in order to ensure that these technologies are used responsibly and ethically in the protection of digital assets.

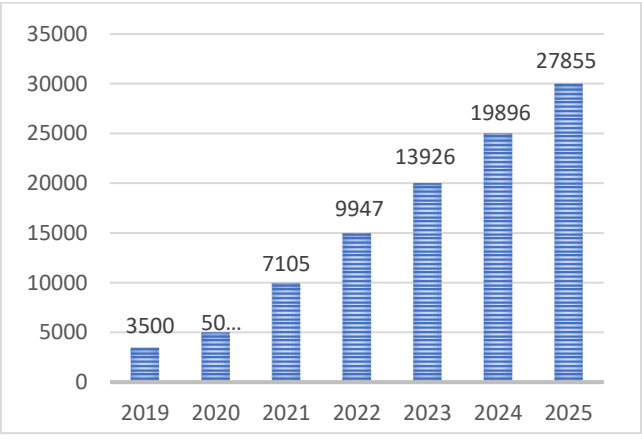
II. CYBERSECURITY

Cybersecurity may be a extend of procedures, advances, forms, and shields that secure computer frameworks, systems, gadgets, and information from unauthorized get to, robbery, harm, interference, or abuse. It comprises a wide extend of disciplines focused on at keeping up the privacy, integrity, and accessibility of advanced resources and assets within the confront of ever-changing cyber dangers. Cyber security may moreover be alluded to as data innovation security.

The Significance of Cyber Security:

Cybersecurity is basic since governments, militaries, organizations, monetary teach, and therapeutic organizations procure, handle, and store enormous sums of information on computers and other gadgets. A major sum of such information may be touchy data, whether it is money related information, individual data, or other shapes of information for which unauthorized get to or exposure could have extreme impacts. Organizations transmit delicate information over systems and to other gadgets within the course of doing trade, and cyber security portrays the teach committed to ensuring that data and the frameworks utilized to prepare or store it. As the volume and advancement of cyber assaults develop, companies and organizations, particularly those that are entrusted with defending data relating to national security, wellbeing, or monetary records, ought to take steps to ensure their touchy commerce and work force data. In today's interconnected society, cybersecurity has developed in importance.

Estimated cybercrime monetary damages,2019-2025 in million USD



| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

III. CYBER THREATS

Cyber dangers too allude to the likelihood of a effective cyber attack pointed at picking up unauthorized get to, causing harm, disturbing, or taking an data innovation resource, computer arrange, or any other touchy information. Trusted clients inside a company can posture cyber threats, as can obscure parties from farther regions.

For 2023 and past, the center ought to be on the cyber-attack surface and vectors to survey what can be done to restrain dangers whereas too progressing resiliency and recuperation. As client interest grows, so do dangers. As the Metaverse gets to be more widely available, it'll serve as a modern road for exploitation

Deep fakes are as of now being conveyed, and bots are still omnipresent. The geopolitics of Russia's intrusion of Ukraine have emphasized the vulnerabilities of crucial framework (CISA Shields Up) to nation-state dangers, counting expanded DDS attacks on websites and framework. The foremost concerning occurrence was the hacking of a Ukrainian satellite. Common cyber threats incorporate a assortment of unfriendly behaviors that endanger computer frameworks, networks, devices, and information. Here are a few of the foremost common sorts of cyber dangers.

- Malware
- Phishing
- Ransomware

MALWARE:
Malware, brief for pernicious program, may be a term for program that disturb, harm, or pick up unauthorized get to computer frameworks, systems, gadgets, or data. Malware is produced and transmitted by cybercriminals with malevolent reason, and it can take numerous shapes and perform assortment of unsafe capacities. Here are a few major components of malware. Malware is classified into a few sorts, each with its possess set of characteristics and functionalities. Malware is commonly classified into:

VIRUS:
Viruses are antagonistic programs that taint records or programs and imitate themselves, spreading to other records or systems.

WORMS:
Worms are self-replicating computer program that spreads over systems and frameworks, habitually abusing vulnerabilities to do so.

SPYWARE: Spyware is implied to watchfully screen and collect data around users exercises, counting as keystrokes, surfing history, and individual data, which is along these lines communicated to attackers.

PHISHING:
Phishing may be a cyber assault in which assailants utilize false communications, such as emails, content messages, or websites, to dupe individuals into unveiling delicate data, such as login qualifications, money related data, or individual data. Phishing assaults are a sort of social designing that utilize human brain research and believe to trick casualties and accomplish hurtful objectives. Here are a few imperative highlights of phishing:

E-MAIL PHISHING:
Email phishing occurs when assailants send untrue emails showing up as authentic substances, such as banks, government offices, or respectable businesses, in arrange to trap beneficiaries into clicking on perilous joins, downloading pernicious connections, or disclosing touchy information.

SPEAR PHISHING:
Spear phishing is the targeting certain people or organizations with individualized and profoundly focused on messages in arrange to make strides the probability of victory. Aggressors as often as possible collect data approximately their targets from social media, company websites, and other places some time recently fitting their phishing emails.

SMISHING:
Smishing, or SMS phishing, involves sending false content messages to versatile phone clients, and large containing joins to phishing websites or instructions to contact a phone number from which assailants endeavor to get individual information.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

RANSOMWARE:

Ransomware could be a destructive program (malware) that scrambles records or locks computer frameworks, basically making them blocked off to clients unless a emancipate is paid. Ransomware assaults are a sort of cyber-extortion in which aggressors request installment from casualties in trade for decrypting their files or regaining access to their computers. Here are some important elements of ransomware:

ENCRYPTION AND LOCKING:

Ransomware often uses strong encryption methods to encrypt files stored on the victim's computer or network, rendering them unreadable without the attackers' decryption key. Some ransomware variants additionally lock the victim's computer screen, preventing them from viewing their desktop or data unless the ransom is paid.

RANSOM DEMAND:

After encrypting the victim's files or locking their machine, ransomware shows a ransom note or instructions requiring payment from the victim. Ransom sums can range from a couple dollars to thousands or even millions of dollars, and are frequently sought in cryptocurrencies like Bitcoin to permit anonymous transfers.

CYBER THREAT STATISTICS OF 2023:

- In 2023, there are an estimated 800,000 cyber attacks every year, and that figure is expected to increase annually.
- In 2023, the average cost of a data breach was $4.45 million, which was the most on record.
- In 2023, humans were responsible for 74% of breaches.
- Every 39 seconds, a threat actor attacks a company's cybersecurity infrastructure.
- Email is the primary mode of delivery for 92% of malware.
- In 2023, enterprises took an average of 49 days to detect a cyberattack.
- Malware affects about 4.1 million websites on the internet.

Since the beginning of the Russia-Ukraine war in 2022, 97 percent of enterprises have seen an increase in cyber attacks.

IV. TYPES OF CYBER ATTACK STATISTICS:

Ransomware and Malware:

- The average ransomware payment has risen considerably, from $812,380 in 2022 to $1,542,333 in 2023.
- In March 2023, the number of ransomware victims had nearly doubled from the previous year.
- Email is used to deliver 94 percent of all viruses. In the last year, ransomware affected 66% of firms. The average cost of ransomware recovery is approximately $2 million.
- In 2023, a ransomware outbreak affected 72.7% of all enterprises worldwide.
- Nearly half (47%) of organizations now have a policy to pay ransoms related with cybersecurity concerns, up 13% from the previous year.
- The average cost of a ransomware assault was $4.54 million.
- In 2023, 66% of organizations reported being targeted by ransomware, with the average ransom payout rising from $812,380 in 2022 to $1,542,333.
- Ransomware had the greatest impact on the construction business in 2023.

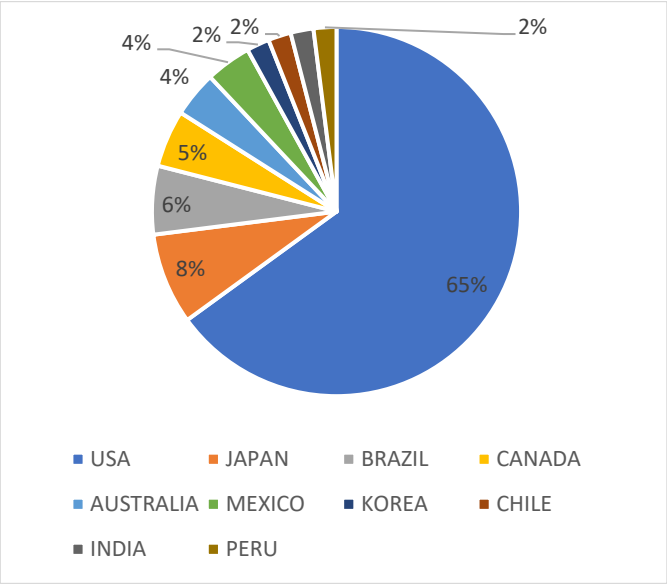
Phishing Attack Statistics:

- 57 percent of firms see weekly or daily phishing attempts.
- Phishing was the most common initial attack vector, appearing in 41% of instances.
- 26 percent of phishing assaults targeted public-facing applications.
- Phishing attacks are responsible for more than 80% of reported security problems.
- In phishing attacks, 62% employed spear phishing attachments, 33% used links, and 5% used a service.
- Phishing was recognized as the primary source of infection in 41% of cybersecurity incidents.

Here is a pie chart showing the countries affected by cyber threat

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |



V. HOW TO AVOID CYBER ATTACK

Cybersecurity is presently more significant than ever. With ever-increasing perils to businesses, having a solid security arrangement is exceptionally critical.We've all listened stories around businesses paying enormous fines or indeed going out of commerce as a result of a basic hack to their frameworks. There are essentially as well numerous risks out there to neglect the dangers; from ransomware to phishing, it might fetched your work. Avoidance is fundamental, and in this post, we are going to show you how to appropriately ensure your organization.

1. Keep your computer program and frameworks completely up to date: Cyber assaults regularly happen when your systems or computer program are out of current, uncovering vulnerabilities. So fraudsters take advantage of these blemishes to induce get to your organize. It's now and then as well late to require prudent measures after they've arrived. To address this, consider contributing in a fix administration framework that will oversee all computer program and framework overhauls, guaranteeing that your framework remains versatile and up to date.

2. Guarantee Endpoint Protection: Endpoint assurance shields systems that are remotely bridged to gadgets. Versatile gadgets, tablets, and portable workstation computers that are associated to corporate systems get to focus on security concerns. These ways must be ensured utilizing endpoint security software

3. Introduce a Firewall: There are various sorts of modern information breaches, and modern ones rise on a day by day premise, in some cases resurfacing.

4. Reinforcement your Data: In the occasion of a calamity (regularly a cyber assault), you must have your information sponsored up in arrange to maintain a strategic distance from major disturbance, information misfortune, and monetary damage.

5. Password: It can be hazardous to utilize the same secret word for everything. Once a programmer has figured out your watchword, they have total get to your PC and any applications you use.Having particular passwords for each application you employ is greatly useful to your security, and changing them on a customary premise can keep you secure from both inside and outside threats. It can be troublesome to know where to start when it comes to guarding your company from cybercrime and cyber dangers. There's so much data accessible that it can be overpowering, particularly when the data is inconsistent. There may be a of contrast between how humans deal with cyber risk and how fake insights bargains with cyber threat.

VI. RISK MANAGEMENT

Risk management includes identifying, analyzing, and responding to risk factors that arise during the course of a company's operations. Effective risk management entails attempting to control future outcomes as much as possible through proactive rather than reactive actions. Thus, effective risk management has the potential to lower both the likelihood of a risk occurring and its potential impact. Risk management is an important activity because it provides a

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

firm with the tools it needs to detect and manage potential risks. Once a risk has been identified, it is simple to address it. Furthermore, risk management provides a foundation for businesses to make sound decisions.

What is the aim of risk management and how important is it? Simply expressed, risk management seeks to shield an organization from potential losses or threats to its continued functioning. This can entail financial losses, reputational damage, or employee hurt.Remember that there is no such thing as a one-size-fits-all risk management solution. Every organization is unique, and each will face distinct types of hazards.That is why firms need to have a risk management plan in place. A risk management strategy outlines all of the assessed hazards that the company faces, as well as the efforts that have been taken to minimize them.

CYBER SECURITY AND ARTIFCIAL INTELLIGENCE:

Artificial intelligence (AI) is transforming cybersecurity by improving threat detection, response, and prediction capabilities. With the rising sophistication and frequency of cyber attacks, AI-powered cybersecurity solutions play a critical role in helping enterprises better protect against emerging threats. AI's outstanding capacity to analyze data, discern trends, and predict risks has led to its widespread use in cyber security. Although AI has transformed the field, it is important to note that it does not replace human adversaries. Indeed, sophisticated fraudsters with specialized techniques may often dodge.AI technologies, demonstrating that the human factor in cyber security remains a serious concern. Human enemies are dynamic, not static dangers. They pose a continuous threat despite modern AI defenses due to their creativity, intelligence, and ability to change their techniques. AI systems can be manipulated using strategies like 'data poisoning' and 'adversarial attacks'. Artificial intelligence in cybersecurity is becoming increasingly important for protecting online systems from cyber criminal attacks and unwanted access attempts. AI systems, when utilized correctly, may be trained to detect cyber threats automatically, create alerts, identify new malware strands, and secure important company data.The benefits of artificial intelligence in cybersecurity include the ability to use AI techniques such as deep learning, machine learning (ML), knowledge representation and reasoning, and natural language processing to provide a more automated and intelligent cyber defense. This allows firms to uncover and mitigate the thousands of cyber events that occur on a regular basis. AI is already being used in the security sector, and its importance will only increase over time. AI is especially well-suited to collecting and analyzing massive volumes of data, extracting important insights, and responding appropriately. These features considerably improve an organization's ability to detect and respond to cyberattacks, hence reducing the potential damage caused by attackers. AI's defining feature is its ability to reason and make judgments with the highest probability of reaching a certain goal.

- Machine learning (ML), a subset of AI, is based on the premise that computer programs can learn and adapt to new data without the need for human involvement.
- Deep learning approaches help in autonomous learning by processing large volumes of unstructured data like text, photos, and videos.

Here's how artificial intelligence is transforming cybersecurity:

Threat Detection and Analysis: AI algorithms evaluate massive volumes of data from a variety of sources, including network traffic, logs, endpoint telemetry, and threat intelligence feeds, to identify trends, abnormalities, and indications of compromise (IOCs) linked to cyber threats. Machine learning (ML) techniques allow AI systems to detect known and new threats, including as malware, ransomware, and advanced persistent threats (APTs), with more accuracy and efficiency than traditional signature-based methods.

Pattern Recognition: To address complex security challenges, AI employs three primary approaches. For starters, it excels at pattern recognition, swiftly identifying and categorizing data patterns that would be difficult to analyze manually. These patterns are then provided to security experts for additional analysis.

Actionable Guidance: AI offers actionable counsel through intelligent agents. These agents make practical recommendations based on the detected patterns, providing security professionals with useful insights into the proper measures to take.

Automated Incident Response and Orchestration: AI-powered cybersecurity solutions automate incident response workflows, orchestrate security controls, and streamline incident investigation and remediation procedures. AI systems that integrate with security orchestration, automation, and response (SOAR) platforms may correlate and analyze security alarms, augment event context, and execute predetermined playbooks in real time to control attacks, remediate vulnerabilities, and respond to security incidents. Automated incident response capabilities assist firms in reducing reaction times, minimizing manual intervention, and increasing overall operational efficiency.

Behavioral Analysis and Anomaly Detection: AI-powered cybersecurity systems use behavioral analysis approaches to monitor user and entity behavior, discover deviations from usual patterns, and flag suspicious activity that may indicate

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

a security problem. AI systems can better detect inside threats, account compromise, and illegal access by employing ML algorithms to construct baseline behavior profiles and detect anomalies in real time.

Malware Detection and Prevention: AI is useful in cybersecurity since it helps identify and prevent malware. AI-powered systems use machine learning algorithms to comprehensively examine the properties and actions of existing malware, as well as uncover potential indicators of unique and emerging threats.These systems excel at detecting and classifying malware using a variety of techniques, including file signatures, code analysis, behavioral patterns, and the detection of network traffic anomalies. AI improves its detection skills by adapting to the ever-changing landscape of malware methods through continuous learning.

Phishing And Email Scam Detection: AI can reliably distinguish between legitimate and fraudulent emails by analyzing the email's content, sender information, and user activity patterns. This has a significant influence on lowering the possibility of employees becoming targets of phishing attacks and putting personal information at risk.

VII. HOW AI IS DIFFERENT FROM NORMAL SCAM DETECTION

AI-powered cybersecurity solutions differ from traditional approaches in a variety of ways**.**
AI-based solutions employ machine learning algorithms to detect and respond to known and novel threats in real time. Machine learning algorithms are trained on massive volumes of data, including historical threat data as well as network and endpoint data, to detect patterns that people cannot notice. This enables AI-based solutions to detect and respond to threats in real time, eliminating the need for human intervention Machine learning algorithms, for example, can examine network traffic patterns to detect aberrant behavior that could suggest a cyberattack, inform security staff, or even take automatic action to mitigate the threat. As new threats develop, machine learning algorithms can be trained with new data to improve their ability to detect and respond to them. This means that AI-based solutions may evolve with the threat landscape, providing more effective cybersecurity protection over time.

VIII. HOW AI CAN CHANGE THE LANDSCAPE OF CYBER SECURITY INCREASED EFFICIENCY

AI-powered automation is also useful for tasks such as vulnerability screening and patch management. Artificial intelligence can automatically analyze systems and networks for vulnerabilities, discovering potential flaws that attackers could exploit. It can then prioritize and recommend patches or security upgrades, making patch management more efficient. This technology saves security analysts time and effort in manually identifying vulnerabilities and applying updates, allowing them to focus on more important security issues. Artificial intelligence can help to streamline incident response methods. When a security event happens, AI algorithms can assist in determining its severity and impact by analyzing pertinent data. They can generate real-time alerts and recommendations, allowing security teams to react quickly and efficiently.

IMPROVED ACCURACY: AI algorithms excel at detecting risks that people may miss, such as new and unknown malware strains and minor patterns in network traffic that suggest a potential cyber threat.AI exhibits its ability to detect new and evolving threats. Traditional antivirus software identifies threats using a database of known malware signatures. However, this method is limited to detecting just known malware strains. AI analyzes file and program activity with advanced machine learning techniques, allowing it to detect new and unknown malware strains.

IX. CONCLUSION

Finally, good cybersecurity and risk management are vital for defending against cyber threats, securing critical assets, and preserving trust and confidence in the digital economy. Organizations can effectively mitigate risks, strengthen resilience, and ensure the security and integrity of their digital assets and operations in an increasingly interconnected and vulnerable world by investing in robust cybersecurity measures, leveraging emerging technologies, and cultivating a culture of cybersecurity awareness. To summarize, the use of artificial intelligence (AI) in cybersecurity offers a huge step forward in the fight against developing cyber threats. This research report examined the numerous ways in which AI is transforming cybersecurity, from improving threat detection and analysis to automating incident response and orchestrating security policies. Organizations can improve their overall cybersecurity posture by implementing AI-powered solutions for detecting, mitigating, and responding to cyber threats.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 4, July-August 2025 |

REFERENCES

1. https://terranovasecurity.com/blog/cyber-security-statistics/
2. https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/
3. https://www.varonis.com/blog/cybersecurity-statistics
4. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=368814fd19db
5. https://www.cobalt.io/blog/cybersecurity-statistics-2024
6. https://www.capgemini.com/in-en/insights/expert-perspectives/five-cybersecurity-trends-for-2024/
7. https://www.ibm.com/ai-cybersecurity
8. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
9. https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/
10. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |