International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**2**, pp.**105-111**, February **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Review Article

A Study on Impact of Artificial Intelligence in Cyber Security

Nikhil S. Khamitkar[1*], Rajivkumar S. Mente[2], Bapu D. Chendage[3]

[1,2,3]School of Computational Sciences, Punyashlok Ahilyadevi Holkar Solapur University, Solapur, Maharashtra, India

**Corresponding Author:* ✉

Received: 26/Dec/2024; **Accepted**: 28/Jan/2025; **Published**: 28/Feb/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i2.105111

Abstract: Cyber security ensures the protection of devices, software, and data that are connected to the internet from potential risks, against attacks, damage, or unauthorized access. As maximum personal information and activities shift online, the significance of cyber security has grown. Various cyber security threats include hacking, malware, phishing, and ransomware. This paper reviews various Conventional methods of cyber security focus on protecting systems and data from digital threats., application of AI in cyber security, future of AI in cyber security, regarding AI in multiple area, intelligent techniques to facilitate security, disadvantages of using AI and machine learning in cyber security.

Keywords: Artificial Intelligence, Cyber Security, various conventional methods of cyber security focus on protecting systems, Application of AI in Cyber security, Future of AI in Cyber security, Concerning AI in Multiple Area, Intelligent Techniques to Facilitate Security.

1. Introduction

Artificial Intelligence and Machine Learning have quickly emerged as crucial technologies in the field of cyber security. As cyber threats become more advanced and data continues to grow, AI and ML play a key role in enhancing the security of both organizations and individuals. AI and ML assist in processing vast quantity of information and detecting arrangements that could signal the existence of a cyber-threat. For individuals, businesses, and governments, it is vital to secure personal data like financial information, IDs, and login credentials from cyber criminals. This article will highlight the crucial applications of AI in cyber security and look ahead to the potential future developments of these technologies. The recent rise in the intelligence of malware and cyber weapons makes it clear that only intelligent code can provide effective security against such advanced cyber threats.[1]

2. Regarding AI

A broad spectrum of methods has been developed within the AI field to solve challenging problems that require human-level intelligence. Some of these techniques have reached maturity, with well-defined algorithms. Visual networks, originating with Frank Rosenblatt's 1958 perceptron invention a synthetic neuron continue to be a popular element in neural networks. These are among the most widely used AI tools today.

Expert systems helps to answer queries within specific domains like diagnostics, finance, and networking. Intelligent agents possess traits such as proactivity, reactivity, and the understanding of agent communication languages. Search methods are essential when no other solution approaches apply, and learning processes improve systems by reorganizing knowledge or enhancing the reasoning engine [1]. Constraint satisfaction is another AI method for solving problems defined by specific constraints, such as equations or logical statements [2].

AI introduces a shift in cyber security practices, offering an approach that contrasts with traditional methods. Unlike conventional techniques, AI models learn from past events and evolve over time, becoming increasingly efficient. AI's self-learning ability helps to reduce false positives by better understanding normal behavior, enhancing threat detection accuracy.

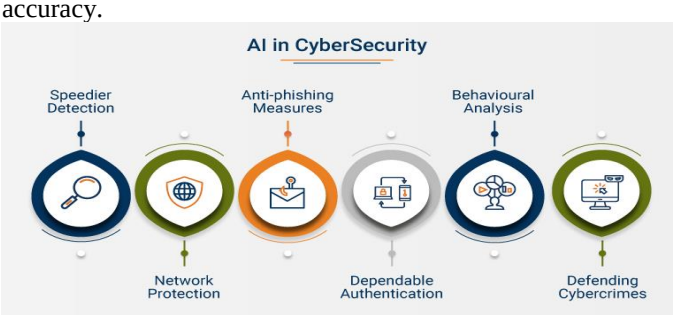


Fig.1 Artificial Intelligence in cyber security [2]

3. Literature Survey

AI-driven analytics allow for proactive threat hunting, identifying hidden threats that traditional methods might miss. By analyzing historical and real-time data, AI predicts potential threats, enabling organizations to take preventive action, while traditional approaches are more reactive.

Additionally, Using machine learning algorithms, AI can analyze extensive datasets and detect hidden irregularities, including new forms of threats, whereas traditional approaches are based on fixed signatures or rules. AI is particularly skilled at identifying complex attack behaviors across different data sources, even if attackers attempt to cover their tracks. Traditional methods, on the other hand, may overlook such disguised threats. Furthermore, Intelligent system decision are free from personal bias, offering equitable and unchanging threat assessments, while standard methods may be inspired by human judgment [3].

Cyber-attacks pose a growing risk to the functionality of businesses, financial institutions, government agencies, and network infrastructures. These attacks can be perpetrated by individuals or groups with malicious intent, including terrorist organizations. The spectrum of cyber threats includes malicious software (malware), phishing attacks, denial-of-service (DoS), social engineering, and man-in-the-middle attacks. Cyber security refers to the proactive measures taken to minimize the risks of these threats, with management playing a key role in mitigating potential impacts[1, 2, 3, 4, 5].

Among the technologies available for defense are firewalls, while AI has become an integral part of identifying and categorizing malware. By utilizing machine learning, AI systems can be trained to differentiate between various types of malware, such as trojans, worms, and viruses. Cyber security systems generally fall into two categories: expert-driven systems, where human analysts oversee operations, and automated systems, which rely on AI-driven tools. CAPTCHA serves as a prime example of an automated system that distinguishes between human and machine interactions [4,5].

The complexity and volume of data required for cyber security defense cannot be managed by humans alone, making automation indispensable. As networks grow, AI contributes by improving detection accuracy, enhancing biometric authentication methods, predicting potential threats, and reducing the need for human involvement in routine security tasks. Cognitive security, which blends human and artificial intelligence, offers a powerful combination for safeguarding networks. Cognitive computing, a form of advanced AI, replicates human cognitive processes and allows systems to exceed the limits of traditional computing architectures [4,5, 6].

AI has greatly advanced the field of cyber security, but it also poses risks when exploited maliciously, as demonstrated by DeepLocker. Unlike traditional forms of malware, DeepLocker is capable of concealing its malicious intent until it targets a specific individual. This is achieved through AI techniques such as face identification and location tracking, enabling the malware to accurately detect its victim. This illustrates the paradoxical nature of AI in cyber security: it serves as a tool for both enhancing defenses and creating highly sophisticated threats that are difficult to detect and counter [6,7].

Artificial intelligence, as a research domain, has existed almost as long as the advent of electronic computers. The fundamental aim of AI has always been to create machines or systems that surpass human intelligence. However, the timeline for achieving this has been fluid and has extended further as technology evolves. Early milestones, such as developing AI to play chess, were once considered prime examples of machine intelligence; though achieving such tasks is now viewed as less ground breaking than initially anticipated [8].

AI-based User and Entity Behavior Analytics (UEBA) leverages machine learning algorithms to continuously monitor and analyze the behavior of users and entities within a network, enabling the detection of anomalies indicative of potential security threats. This can help to identify insider threats and Advanced Persistent Threats (APTs). Furthermore, AI and machine learning are integral to network traffic analysis and anomaly detection, where algorithms detect traffic patterns that could signal intrusion attempts or malicious activities, such as an unusual increase in traffic from a specific IP address [6, 7, 8].

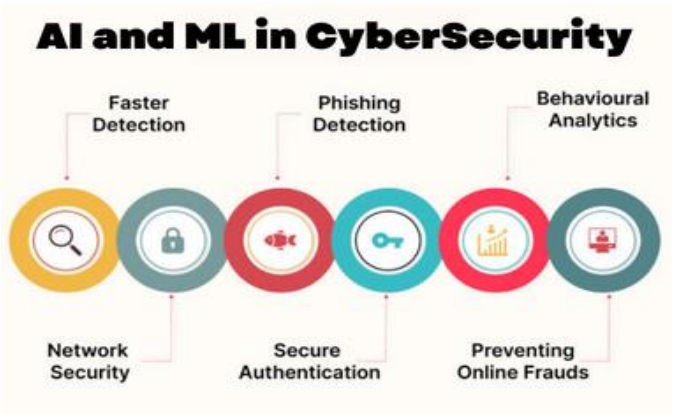


Fig 2: AI and ML in Cyber Security

Fig.2 shows, In cyber security, AI-powered automation is crucial for improving operational efficiency. Security automation and orchestration systems use machine learning to computerize routine operation, including patch deployment and response to disasters, allowing agency to focus their human resources on more critical functions. Additionally, penetration testing, which involves simulating attacks to discover system vulnerabilities, and vulnerability management benefit from machine learning's ability to automate both processes, increasing their effectiveness and speed[9].

Real-time threat intelligence systems leverage AI and ML to analyze and correlate data from multiple sources, providing organizations with real-time insights into potential threats and enabling faster responses. The integration of AI with blockchain technology could revolutionize areas like identity and access management, secure data sharing, and payment security. Lastly, AI and ML enhance the capabilities of Security Operations Centers (SOCs) by automating repetitive tasks, evaluating vast amounts of data, and delivering timely threat intelligence. AI, as a quickly advancing field within computer science, focuses on advancing systems efficient of simulating and expanding human intelligence through sophisticated algorithms and techniques [9, 10].

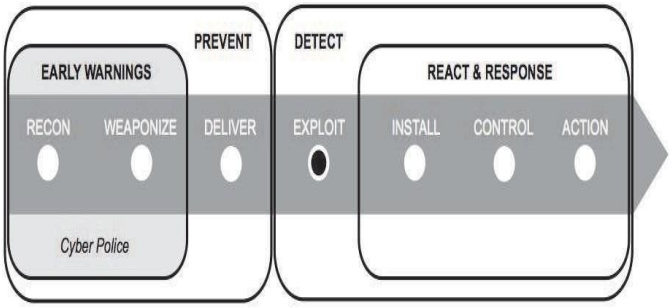


Fig.3 Interacting Intelligent Cyber Police Agents to Monitor Entire Networks

Fig.3 shows, A strong way to protect against distributed cyber attacks is to build a system of intelligent agents that act like cyber police. These agents work in a specific cyberspace to find and stop decentralized cyber threats. As shown in Figure 3, these agents can catch threats early on, preventing them from becoming bigger problems [11, 12].

Intelligent agents are also used in artificial immune systems (AISs) that mimic the human immune system. There are two kinds of agents: detection agents and counterattack agents. The detection agents monitor the environment for any unusual activities, while counterattack agents take action against the threats. This system helps protect against cyber-attacks by mimicking how the human immune system works [13, 14, 15]. To address distributed cyber-attacks effectively, a robust solution involves deploying intelligent agents that act autonomously as a cyber-police force. This system is decentralized, allowing agents to detect and respond to threats at the earliest stages of an attack, as illustrated in Figure 1. Additionally, artificial immune systems (AIS) use two categories of agents—detection agents and counterattack agents. Detection agents scan the network for anomalies and trigger counterattack agents when malicious activity is identified. These counteragents then take action to mitigate the impact or block the attack entirely, closely mimicking the human immune response to pathogens.

Search is a fundamental problem-solving method that is applicable across various domains, particularly when no other solution strategies are viable. It is used in everyday activities without conscious recognition. To formally implement a search process, one must generate candidate solutions and have a procedure for validating whether these candidates fulfill the problem's requirements. Search efficiency can be significantly enhanced when additional contextual information is leveraged. In intelligent systems, search plays a key role in performance, with its optimization often being critical. A variety of specialized search algorithms are designed to address specific problem domains and maximize efficiency. Numerous search techniques are incorporated in AI systems and applied in various programs, yet they are often not directly recognized as AI techniques.

For example, dynamic programming is widely used for solving optimization problems such as security, with the underlying search process concealed within the software code, making it invisible as a distinct AI application. In gaming software, search algorithms like αβ-search, minimax, and random search are crucial for decision-making, particularly in cybersecurity. The αβ-search algorithm, originally developed for chess, utilizes a "divide and conquer" strategy to efficiently evaluate possible moves by estimating both the minimum secured win and maximum possible loss, resulting in fewer choices and a faster search process.

Learning in artificial intelligence refers to enhancing a system by expanding its cognitive content or improving its inference capabilities. This field is under intense investigation and includes various machine learning methods aimed at acquiring new information, skills, or re-organizing existing knowledge. The complexity of learning tasks ranges from simple parameter adjustments to more complex forms such as symbolic learning, where concepts, grammars, functions, and behaviors are learned. AI supports both supervised and unsupervised learning techniques.

The latter is particularly valuable in scenarios where there is a large volume of data, which is common in fields like cyber security. Unsupervised learning, in particular, evolved from early AI techniques and plays a significant role in data processing. Neural networks, including self-organizing maps, are key implementations of unsupervised learning. Furthermore, parallel learning algorithms, represented by genetic algorithms and neural networks, are suited for parallel hardware execution and are used in applications such as threat detection systems in cyber security.

4. Case Studies of AI in Cyber security

4.1 AI-Driven Malware Detection

AI-driven malware detection systems have proven effective in identifying previously unknown types of malware that traditional signature-based antivirus systems might overlook. Unlike traditional methods that rely on known malware signatures, AI models can analyze the behavioral patterns of files and identify anomalous activities, enabling the detection of novel threats. For instance, the Falcon platform by CrowdStrike employs machine learning algorithms to track endpoint behavior and detect indicators of compromise (IOCs). Through continuous data learning, the system adapts to new threats, providing an evolving defense mechanism against emerging malware.

4.2 AI in Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are designed to detect unauthorized access or malicious activity within a network. AI-enhanced IDS can dynamically monitor real-time network traffic, learning from historical data to establish a baseline of normal behavior. Any deviations from this baseline are flagged as potential security incidents.

An example is IBM's QRadar, which uses machine learning and AI to analyze network traffic, detect intrusions, and adapt to emerging threat patterns. By continuously learning from attack data, it enhances the accuracy of detection while minimizing false positives.

4.3 AI in Threat Intelligence and Response

AI-driven systems are capable of automating the collection and analysis of threat intelligence from multiple data sources. These systems can correlate data to provide actionable insights for security teams, offering a more timely and proactive approach to threat detection and response.

Darktrace's Enterprise Immune System is an example, utilizing machine learning to detect abnormal behavior within a network. Once a threat is detected, the system can autonomously respond by isolating compromised entities or blocking malicious traffic, thereby reducing response time.

5. Growth of AI in Cyber Security (2015-2025)

Chart 1: AI Adoption in Cyber Security

Year	Adoption Rate (%)
2015	10
2018	25
2020	50
2022	75
2025	90

Bar Chart:

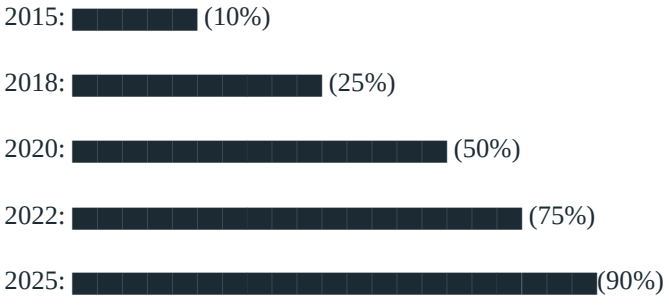


Chart 2: AI-powered Threat Detection

Year	Detection Rate (%)
2015	20
2018	50
2020	70
2022	85
2025	95

Bar Chart:

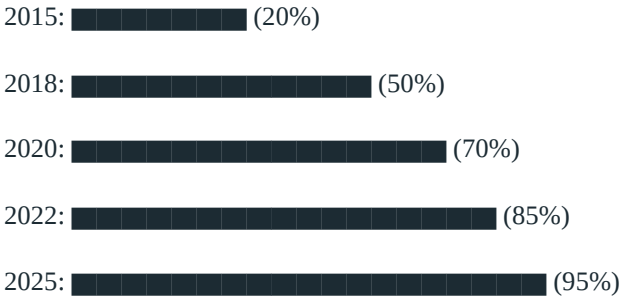


Chart 3: AI-powered Incident Response

Year	Response Time (minutes)
2015	60
2018	30
2020	15
2022	5
2025	1

Bar Chart:

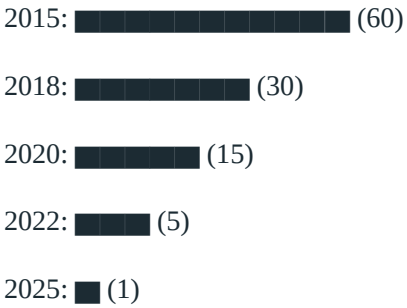
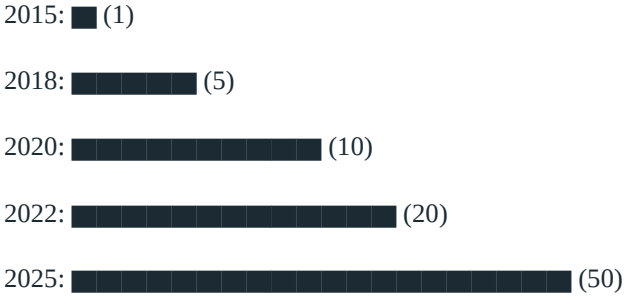


Chart 4: Investment in AI-powered Cyber Security

Year	Investment (billions USD)
2015	1
2018	5
2020	10
2022	20
2025	50

Bar Chart:



6. Overcoming the Challenges of AI in Cyber Security

Artificial Intelligence (AI) has changed the landscape of cybersecurity, offering new ways to protect against cyber threats. However, AI-powered systems face their own challenges. Overcoming these challenges is crucial to maximize the effectiveness of AI in safeguarding our digital environments.

6.1 Data Quality as the Backbone of AI Functionality

For AI-powered systems to work properly, they require high-quality data. Inaccurate or incomplete data can skew results, causing the AI system to fail. To ensure optimal performance of AI cyber security systems, it is essential that the data used is correct, comprehensive, and unbiased.

6.2 The Impact of Bias on AI Systems

AI systems can be affected by bias, leading to inaccurate decisions and unfair results. This bias can arise from several sources, including biased data, flawed algorithms, and human biases. It is crucial to recognize and address bias in AI-driven cyber security systems to maintain fairness and accuracy.

6.3 Making AI Decisions Transparent and Understandable

AI systems are often difficult to interpret, making it hard to understand the reasoning behind their actions. This lack of transparency can hinder the adoption of AI in cybersecurity. To overcome this, it is important to create explainable AI systems that clearly communicate how decisions are made, fostering trust and encouraging their use.

6.4 Explainable AI in Cyber security

The future of AI in cyber security includes the development of systems that provide clear, understandable, and interpretable decision-making processes. These "explainable" AI systems will allow cyber security professionals to trace the reasoning behind AI-driven actions, ensuring transparency and trust in automated security measures.

6.5 Adversarial AI in Cyber security

Adversarial AI focuses on creating systems that can identify and neutralize attempts to deceive or manipulate AI models. In cyber security, this means designing AI systems capable of detecting attacks that attempt to exploit weaknesses in machine learning algorithms, thus safeguarding security tools from adversarial threats[16].

6.6 Enhancing Cyber security with Human-AI Collaboration

The integration of AI with human expertise is a key future direction for cyber security. Instead of AI working in isolation, collaborative systems will enable AI to process and analyze data quickly while humans provide oversight, interpretation, and context for more informed decision-making in complex security scenarios.

6.7 AI-Driven Cyber security Frameworks

Future cyber security strategies will involve the creation of hybrid frameworks that combine AI technology with traditional security mechanisms. This will create adaptive, intelligent systems that enhance conventional methods like firewalls and intrusion detection, offering more comprehensive and proactive protection against evolving cyber threats.

6.8 Advancing AI Solutions for Cyber security

In the coming years, the focus of AI in cyber security will shift toward improving the clarity of AI decision-making through explainable models, counteracting adversarial AI attacks, fostering effective collaboration between AI systems and human experts, and building integrated frameworks that merge AI capabilities with traditional security tools to strengthen overall defense systems [17,18].

7. Cyber Attack Taxonomy Diagram

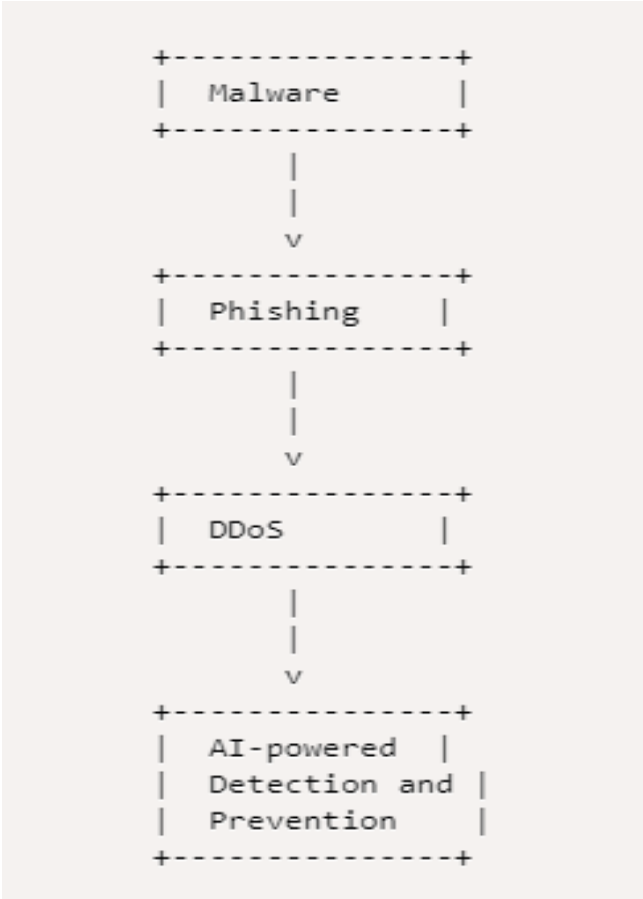


Fig4. Cyber Attack Taxonomy Diagram

A well-designed cyber attack taxonomy diagram can serve as a visual aid to categorize and illustrate the various types of cyber attacks that exist. By breaking down these attacks into distinct categories, it can help clarify the different tactics and methods used by attackers. Furthermore, such a diagram can highlight how artificial intelligence (AI) tools and techniques can be integrated into the process of detecting these attacks. Through machine learning, pattern recognition, and anomaly

detection, AI can proactively identify potential threats and prevent them from causing harm to systems or networks.

8. Privacy Concerns in AI-Driven Cyber security

8.1 Data Collection and Surveillance

AI systems used in cybersecurity often rely on massive datasets to train models and detect threats. These datasets can include personal information, user behaviors, and communication data, raising significant privacy concerns:

Excessive Data Collection: AI systems may collect more data than necessary for their tasks, leading to potential overreach and infringements on users' privacy rights. Collecting data on all users, including sensitive personal details, may be considered invasive and violate privacy laws like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

Surveillance and Monitoring: AI systems may inadvertently create pervasive surveillance environments, where users' online activities are continuously monitored and analyzed. This raises ethical concerns around the balance between security and individual freedom, especially when data collection is done without explicit user consent.

8.2 Data Security and Breaches

AI systems handling sensitive personal data in cybersecurity are at risk of being targeted by cybercriminals. A breach of such data can have severe consequences for individuals' privacy:

Data Theft: AI systems might become targets for hackers, with personal information potentially stolen in the process. If sensitive personal data is not adequately protected, there could be significant consequences for affected individuals, including identity theft or financial loss.

Data Misuse: Even if AI systems are not compromised, there is a risk that organizations using these technologies might misuse the data they collect for unauthorized purposes. This could lead to unethical surveillance or even discriminatory practices.

8.3 Informed Consent

The use of AI in cybersecurity often requires individuals to provide personal or sensitive data. However, ensuring informed consent is a critical issue:

Lack of User Awareness: Users may not fully understand the extent to which their data is being collected, analyzed, and stored by AI systems. In some cases, organizations may fail to communicate the full scope of data usage, which undermines the concept of informed consent.

Automated Consent Mechanisms: The automation of data collection for AI purposes may bypass the need for direct user consent, which can be seen as a violation of privacy rights.

9. Conclusion

In this paper, artificial intelligence (AI) and machine learning (ML) have become necessary tools in the evolving landscape of cyber security. As cyber threats grow more sophisticated, these technologies provide critical capabilities for detecting, analyzing, and mitigating attacks in real-time AI's ability to process large volumes of data and detect patterns allows it to uncover threats that traditional methods may overlook. Through applications such as User and Entity Behavior Analytics (UEBA), network traffic analysis, security automation, and real-time threat intelligence, AI enhances the security posture of organizations, businesses, and governments.

The integration of AI into cyber security systems also introduces new challenges, particularly when malicious actors exploit AI for harmful purposes, such as the development of advanced malware like Deep Locker. This paradox highlights the dual role of AI in both protecting and posing risks in the cyber domain. Nevertheless, the advancements in AI, coupled with emerging technologies like block chain, promise to significantly strengthen cyber security measures.

Looking forward, AI and ML will continue to reshape cyber security practices, with intelligent agent-based systems and artificial immune systems offering innovative approaches to threat detection and defense. As these technologies mature, the potential for AI-driven security to proactively identify and neutralize threats before they cause harm will play an essential role in safeguarding the digital infrastructure of the future. Ultimately, AI's ability to learn, adapt, and evolve makes it a powerful ally in the fight against increasingly complex cyber threats.

Conflict of Interest

Artificial Intelligence, Cyber Security, Digital Image Processing, Data Structure.

Funding Source

This research was entirely Self-funded by the Author's.

Authors' Contributions

All authors contributed equally to the conception, design, data collection, analysis, and interpretation of the study.

Acknowledgements

I would like to sincerely thank to the School of Computational Science for their invaluable support throughout the this research. The resources, expertise, and encouragement provided by the faculty and staff have been crucial to the completion of this work. I am deeply grateful for the opportunities to collaborate and for the academic environment that has greatly contributed to complete this work.

References

[1] Dr. Pranav Patil *"Artificial Intelligence In cyber Security"* International Journal of Research in Computer Applications and Robotics, **2016.**

[2] Narcisa Roxana Moşteanu, *"Artificial Intelligence And Cyber Security – Face To Face With Cyber Attack "*– A Maltese Case Of Risk Management Approach American University of Malta, BML 1013, Malta, Vol.**9**, Issue.2(22), **2020.**

[3] Mohiuddin Ahmed ·Sheikh Rabiul Islam ·Adnan Anwar · Nour Moustafa ·Al-Sakib Khan Pathan Editors Explainable *"Artificial Intelligence or Cyber Security Next Generation Artificial Intelligence"* Vol.**1025**, pp.**171-190, 2022.**

[4] Matthew N. O. Sadiku, Omobayode I. Fagbohungbe, and arhan M. Musa *"Artificial Intelligence in Cyber Security"* ,International Journal of Engineering Research and Advanced Technology (IJERAT) E-ISSN : 2454-6135, Vol.**6**, Issue.**5**, **2020.**

[5] Nadine Wirkuttis and Hadas Klein *"Artificial Intelligence in Cybersecurity, Cyber, Intelligence, and Security"*, Vol.**1**, No.**1**, **2017.**

[6] Sarvesh Kumar, Upasana Gupta, Arvind Kumar Singh, and Avadh Kishore Singh, "Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era" Vol.**2**, Issue.**3**, **2023.**

[7] Amit Rajbanshi, Shuvam Bhimrajka, C. K. Raina, "Artificial Intelligence in Cyber Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT, ISSN : 2456- 3307, Vol.2, Issue.3, **2017.**

[8] Bonfanti, Matteo E.; Kohler, Kevin CSS "Analyses in Security Artificial Intelligence for Cybersecurity" Policy 265 No.265, June **2020.**

[9] Hichem Sedjelmaci Hassnaa Moustafa Jiajia, Liu Shuai Han "Cyber Security Based on Artificial Intelligence for Physical Systems" IEEE Network May/June **2020.**

[10] Jian-hua LI, Cyber security meets artificial intelligence: a survey, School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China E-mail: lijh888@sjtu.edu.cn Received Sept. 16, 2018; Revision accepted Dec. 13, 2018; Crosschecked Dec. 24, **2018**

[11] Rammanohar Das and Raghav Sandhane, "Artificial Intelligence in Cyber Security", Journal of Physics: Conference Series 1964, 042072 IOP Publishing, **2021.**

[12] Jenis Nilkanth Welukar, Gagan Prashant Bajoria, "Artificial Intelligence in Cyber Security - A Review", International Journal of Scientific Research in Science and Technology Vol.**8**, Issue.**6** pp.**488-491, 2021**

[13] Syed Adnan Jawaid,Artificial Intelligence with Respect to Cyber Security University: Washington University of Science and Technology, Vienna, VA 22182, USA, **2023.**

[14] Petri Vähäkainu, Martti Lehto, "Artificial intelligence in the cyber security" University of Jyväskylä, Jyväskylä, Finland Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS, **2019.**

[15] Mohammed Rizvi Exelon Corporation, Chicago, IL USA, "Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention" International Journal of Advanced Engineering Research and Science (IJAERS) Peer-Reviewed Journal ISSN: 2349-6495(P) | 2456-1908(O), Vol.10, Issue.5, **2023.**

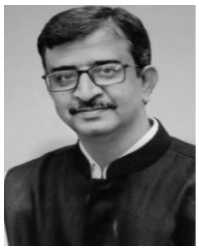
[16] Z. Chen, J. Xie, L. Zhang, and Y. Liu, "Artificial Intelligence for Cybersecurity: A Survey," *Journal of Computer Science and Technology*, Vol.**34**, No.**3**, pp.**497-511, 2020.**

[17] P. K. Manogaran and J. V. S. S. R. S. S. R. Dinesh, "Machine Learning in Cybersecurity: A Survey," *International Journal of Computer Applications*, Vol.**173**, No.**3**, pp.**13-20, 2021.**

[18] M. M. Uddin, K. R. Choo, and S. M. Y. S. Kumar, "AI-based Approaches for Cybersecurity," *Cybersecurity and Privacy Journal*, Vol.**4**, No.**1**, pp.**22-31, 2021.**

AUTHORS PROFILE

Mr. Nikhil S. Khamitkar has completed B.C.A. (Computer Application) from Punyashlok Ahilyadevi Holkar Solapur University, M.C.A. (Computer Application) from Punyashlok Ahilyadevi Holkar Solapur University, Solapur. His areas of interest are Artificial Intelligence, Data Structure, DBMS, Programming Languages, Digital Image Processing He has attended one International and two National Conference. Currently he is working as Assistant Professor at Punyashlok Ahilyadevi Holkar Solapur University Solapur.



Dr. Rajivkumar Mente is working as Director of School of Computational Sciences, Punyashlok Ahilyadevi Holkar Solapur University, Solapur, and Maharashtra, India. He is having total 29 years of teaching experience to Post Graduate, Under Graduate and Engineering Diploma. His areas of interest are Data Structure, DBMS, Programming Languages, Digital Image Processing, CBIR etc. He has published 55 research papers in various international and national journals. He has participated and presented research papers in 25 national and international conferences.

Mr. Bapu D. Chendage has completed B.Sc. (ECS) from Solapur University, M.Sc.(Computer Science) from Solapur University, He also Qualified National Eligibility Test (NET)-Dec. 2019 and State Eligibility Test (SET)- Jan. 2021. Currently he is research scholar and pursuing Ph.D. (Computer Science) from Solapur University. His research area includes Image Processing, Computer Vision and Pattern Recognition. He has published 12 research papers in various international and national journals. He has participated and presented research papers in 7 national and international conferences.

