*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. 21, Issue No. 7, October-2024, ISSN 2230-7540*

https://doi.org/10.29070/jkyjev53

# Improving Cybersecurity: The role of ai in identifying and preventing threats

**Kushagra Aditya Jha***

Class 11th, Sanskriti School, Chanakyapuri, New Delhi, India

Mail ID : kushagraadityajha@gmail.com

***Abstract— Cybersecurity is a major worry for individuals, corporations, and governments as digital technologies grow more prevalent. Cyberattacks are becoming more complex & dynamic, making traditional methods of threat identification and prevention inadequate. In the realm of cybersecurity, AI mostly serves to detect and prevent threats. By utilizing machine learning techniques & extensive data analysis, artificial intelligence may identify patterns and irregularities in network traffic and user behavior that could suggest a possible cyberattack. One way AI can help stop assaults is by using predictive modeling. Also, by looking at previous attacks and finding similarities, AI can anticipate such dangers and take precautions to avoid them. Artificial intelligence plays a crucial role in cybersecurity by enabling the creation of automated incident response systems. In order to minimize interruption and damage, these systems can analyze data, detect possible dangers, and then take action to either limit or lessen the impact of an attack. For cybersecurity purposes, businesses must use AI to safeguard their networks & confidential data from evolving cyber threats. In today's digital world, AI is quickly becoming an essential tool for effective cybersecurity due to its real-time data analysis capabilities and capacity to automate incident response. AI has several applications in cybersecurity, such as threat detection & prevention, which will be covered in this study.***

***Keywords: Artificial Intelligence, Cyberattack, Security, Threat Detection, Prevention***

---------------------------------x---------------------------------

## INTRODUCTION

Artificial intelligence is the ability to think, understand, find patterns, memorize, make judgments from several options, & learn from experience. The ultimate goal of AI research is to program computers to think and act like people, so they can complete complex jobs much more quickly. New developments in artificial intelligence have an effect on public life, politics, the media, & video games. During political campaigns, politicians utilized AI to assist them reach their intended audience more efficiently, saving time, energy, and resources. Institutions, businesses, & governments of today are all susceptible to cybercrime. There were data breaches at the FBI and DHS that exposed around 200 million personal records; these breaches included high-profile data releases. Finding out what other people are aiming toward is currently only a limited and slow process. By 2020, the worldwide market for computer security is projected to reach $170 billion, as reported by Forbes. The market is expanding at a quick pace due to two main factors: the increasing prevalence of new technologies and the constant effort to update security standards [G. A. Chandra 2021]. Nowadays, cyber security is all the rage, and it's being applied in tandem with AI. According to research [Li, K. Ota, M. Dong 2020], cyber security solutions that incorporate AI are superior at safeguarding digital information.

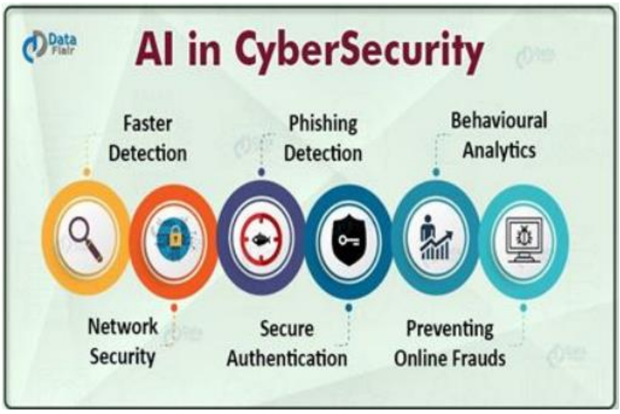


**Figure 1. AI in the field of cyber security**

Figure 1 shows that AI could be very helpful in preventing these kinds of threats. Building a protection against hackers can be made easier with the help of AI. Machines may be programmed to learn patterns & identify outliers with ease. One of the main components of AI is machine learning. It uses the data it gathers to enhance its operations & create preventative measures to fight future attacks. It is perfect for Cybersecurity because it can learn and comprehend human behavior, spot trends, and detect even small changes from those patterns. X. Qiu (2019) & J. Kuppala (2022) both state that AI can utilise this data to build its plans and functions. Creating tools that would enable computers to behave intelligently is the primary objective of AI research. When applied to cybersecurity, AI has the potential to detect new vulnerabilities with great accuracy, hence preventing future attacks [F. Farivar 2020, K. K. Srinivas 2022].

## LITERATURE REVIEW

Lysenko et al. (2024) Cyberattacks on information systems are on the rise around the world. Conventional defenses against cyberattacks are just not strong enough to handle the present threat. Consequently, technology based on AI is considered as a viable option for resolving the issue. The study's overarching goal is to give strong evidence that the cybersecurity system may benefit from using AI techniques to automate threat identification and protection. The study's methodology was based on standard scientific cognitive processes including reasoning, formalization, induction, deduction, comparison, abstraction, and logical & structural analysis. The essay demonstrates that AI enables very effective solutions to be implemented, cyberattacks to be identified efficiently & rapidly, security incidents to be optimally responded to, their repercussions to be assessed, and real-time responses to be determined. It is well-established that AI systems are crucial for enhancing information security standards and removing human error hazards. While designing the cybersecurity system, the writers took into account the most common forms of artificial intelligence. In terms of risk prevention, automation of protection, & threat identification, the article highlights the great efficiency of decision-making with the use of AI technology. The authors have brought attention to the difficulties and dangers of implementing AI into systems for protecting sensitive data. Evidence suggests that cybersecurity strategies that make use of AI capabilities are better able to thwart both internal & external attacks. Research findings can be used to the role of AI technologies in cybersecurity system design, taking into account their potential benefits and drawbacks. This is where their practical worth resides.

Iqra Naseer et al. (2024) AI has emerged as a crucial instrument in the fight against the proliferation & sophistication of cyber and phishing attacks. Through the use of ML, NLP, and pattern recognition, this study explores how AI-driven solutions could enhance cybersecurity by detecting potential risks in real-time. Artificial intelligence allows for the early identification of unusual activity in network traffic, such as phishing emails, harmful URLs, and other forms of email fraud that could otherwise go undetected. In addition, AI is always learning about new threats, which improves its defenses & ultimately leads to improved security standards with fewer false positives. To effectively manage risks, this study also evaluates AI integration with human oversight, highlighting the significance of integrating automated reactions with expert analysis. This paper shows that AI can revolutionize cybersecurity by providing a proactive & flexible method to resist cyber threats and protect personal data. It does this by analyzing current AI uses and future developments. In order to strengthen defense systems and proactively correct cyber vulnerabilities, AI is crucial, according to research.

Fazal Wahab et al. (2024) Methods for computer system security that rely on AI are called "AI for Cybersecurity." The linked digital world of today has made cybersecurity a top priority for governments, organizations, & individuals alike. Due to the increasing frequency and sophistication of cyberattacks, state-of-the-art technological solutions are required to adequately safeguard confidential information & computer systems. In the field of cybersecurity, AI has emerged as a powerful tool that offers numerous advantages in the fight against cyberattacks. AI has tremendous promise for revolutionizing cybersecurity processes. Its ability to sift through massive amounts of data, identify trends, & adapt to new dangers makes it an invaluable asset in the fight against cybercrime. By incorporating AI into their cybersecurity frameworks, organizations may boost security awareness & mitigation, optimize reaction to incidents, identify malware better, assess user behavior, control vulnerabilities, and exploit threat intelligence. In order to keep defense mechanisms strong & important assets protected from ever-evolving threats, AI integration into cybersecurity is essential. In this chapter, we will look at the role of AI in cybersecurity and how it could affect the safeguarding of digital data and systems. Additionally, this chapter provides a concise overview of the latest studies that have examined the cybersecurity implications & uses of deep learning and ML.

Rajashree Manjulalayam Rajendran et al. (2023) Cyber dangers have grown more difficult for experts to overcome in the past decade. More development is required for current security systems to withstand highly skilled cybercriminals. While using AI approaches can help identify scams, there are additional potential problems that come with their implementation. Intersections between cyber security dangers and their prevention by AI technologies are the subject of this research study. It provides a high-level overview of the uses of AI in various cybercrimes & provides an estimate of the likelihood of increasing cybersecurity through defense mechanism conservation. AI has opened up new possibilities for the future of our planet. Data security measures have impacted the development of AI in cybersecurity. The purpose of this article is to raise consciousness about the value of AI technology and how it may help with security on a bigger scale, in the context of a company or organization. The data presented in the report are based on reliable sources & support the findings of the investigation. One possible use of the study's findings is to highlight how AI will change the game when it comes to cyber defense.

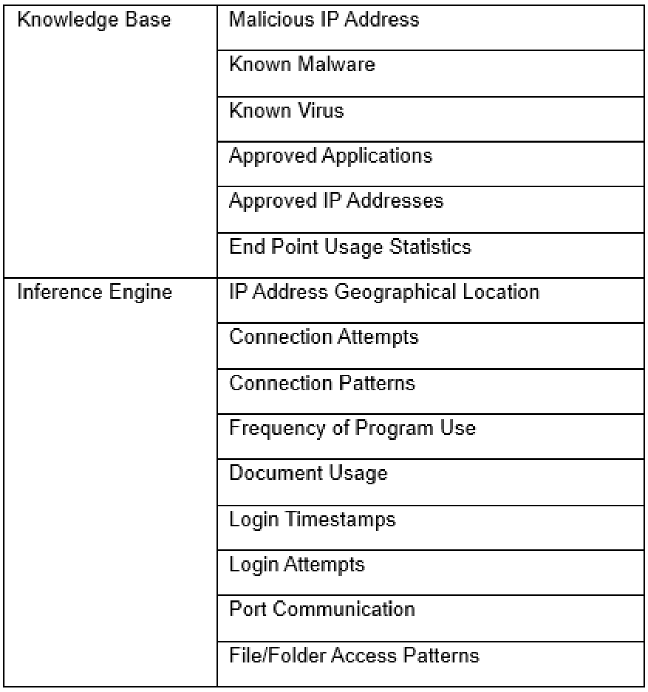
A. Anandita Iyer et al. (2023) Organizations and the ecosystems around them are changing at a breakneck pace due to the Industry 4.0 revolution. At the same time, new cyberattacks are becoming possible due to the expanding cyberattack surface, which cannot be stopped by human involvement alone. With its ability to quickly sift through vast amounts of data and identify multiple angles of attack, AI has quickly become an indispensable tool for security. Cyberattacks can take many forms, including active attacks like network exploitation & suspicious behavior like eavesdropping & traffic analysis. An AI's ability to identify various forms of assault is enhanced as it learns from datasets, refines its models using historical data, and applies its experiences. The cyber security business is greatly influenced by AI due to its ability to anticipate and avert threats prior to their occurrence. There were 450 million cyberattacks attempted against the Tokyo Olympics 2021 throughout the whole event. However, thanks to AI, the tournament was unaffected by any of these attempts because AI could foresee them a week in advance. Improved cyber security, which humans alone could not have accomplished, has been aided by AI. Human mistake accounts for 95% of security breaches, according to a new survey by IBM & Capgemini. While 48% of Capgemini executives utilize AI for threat detection, 18% for reaction, and 34% for prediction, the remaining 26% do not utilize AI at all. With the proliferation of connected devices and the complexity of cyberattacks, AI and ML have several potential uses in the field of cyber defense. These include automating threat detection, responding effectively to data exploitation, monitoring network vulnerabilities, creating useful incident and response reports, and compiling cyber threat intelligence. AI has its limits, just like any other technology. Even if it helps machines function better and more accurately, there are still risks, like as making mistakes when detecting threats in a network. An adversarial machine learning attack could trick an AI into thinking threat behaviors are regular data by manipulating its dataset.

## AI TECHNIQUES FOR CYBER SECURITY

### Expert Systems

The capacity of a computer system to mimic human decision-making is recognized as an Expert System. A knowledge-based system like this one is ideal. The Knowledge Base & Inference Engine are the two main components of these systems that rely on knowledge. The claims and examples in the actual world are represented in the knowledge base. A system that can reason automatically is known as the Inference Engine. It assesses the state of the knowledge base at the moment, applies the applicable rules to that state, and then asserts new knowledge into it. A knowledge base & inference engine are two parts of the Cyber Security Artificial Intelligence Expert System (CSIA).

**Table 1: Components of Expert Systems**



| | |
|---|---|
| Knowledge Base | Malicious IP Address |
| | Known Malware |
| | Known Virus |
| | Approved Applications |
| | Approved IP Addresses |
| | End Point Usage Statistics |
| Inference Engine | IP Address Geographical Location |
| | Connection Attempts |
| | Connection Patterns |
| | Frequency of Program Use |
| | Document Usage |
| | Login Timestamps |
| | Login Attempts |
| | Port Communication |
| | File/Folder Access Patterns |

### A. Security Expert System

As a defense against cyber threats, the security expert system adheres to a protocol. If the process is good and already known, the security system will let it run; otherwise, it will terminate it. The expert system determines the machine's status utilizing inference engine algorithms (rule sets) in the absence of such a procedure in the knowledge base. There are now three distinct machine states: safe, moderate, & severe. After inferring the machine's status, the system notifies the administrator or user and feeds the information into the knowledge base.

### Neural Nets

Artificial Neural Networks are a kind of deep learning. This area of artificial intelligence is quite sophisticated. It takes its cues from how the human brain normally operates. Many neurons in our brain are functionally generalizable and not specific to any one domain. Whatever data type, it can learn it. Frank Rosenblatt pioneered neural networks with his 1957 creation of the perceptron, an artificial neuron. When these perceptrons join forces with other neurons, they are able to gain knowledge and solve integration problems. Similar to how our brain learns autonomously from raw data using inputs from our sense organs, perceptrons learn to recognize the entity they are trained on by analyzing and interpreting high-level raw data. Applying this learned deep learning to the field of cyber security allows the system to autonomously determine if a file is malicious or not. When compared to traditional machine learning systems, our method significantly improves the detection of harmful threats. Speed is the key to neural nets' success in cyber security. Processing speeds are improved when they are implemented in hardware or graphics processors. When it comes to new malware threats, neural networks can help pinpoint them and close the holes that leave firms vulnerable to attacks.

### Intelligent Agents

An Intelligent Agent (IA) is a self-governing, sensor-based, agent-like organism that monitors its surroundings, responds to changes therein by means of actuators, and ultimately achieves predetermined goals. To achieve their goals, intelligent agents can also learn or draw on a knowledge base. They could be incredibly basic or incredibly complicated. Thermostats and other reaction machines are examples of intelligent agents. Agent interaction linguistic understanding, proactiveness, & reactivity are some of its behaviors. Their memory-based standard storage & recovery abilities allow them to adapt to real-time situations, communicate with their environment to quickly learn new things, and more. In preparation for a fight against DDoS attacks, intelligent agents are developed. Creating a "Cyber Police" force shouldn't be too difficult in the event of a legal or commercial crisis. Mobile intelligent agents should be part of the Cyber Police force. In order to achieve this, we need to set up the necessary infrastructure for intelligent agents to communicate and work together effectively. With multi-agent tools, the cyber police will seem much more like full-fledged operatives.

## ARTIFICIAL INTELLIGENCE-BASED THREAT DETECTION

When it comes to physical security, cyber security, or protecting the country. Keeping people and businesses safe relies heavily on threat detection systems. With the help of AI, it is now much easier to identify & eradicate dangers as they happen (Shamiulla, 2019b). With the use of AI-based threat detection systems, security systems may identify risks & threats with more efficiency, speed, and accuracy. By analyzing large datasets with the help of algorithms and machine learning, AI-powered threat detection systems can identify trends that may indicate impending threats (G. A., 2022). To train AI algorithms to detect and alert security staff of possible breaches or dangers, a variety of data types can be utilized, including network traffic, video surveillance footage, & social media feeds (Soni, n.d.).

By utilizing deep learning techniques, algorithms are able to sift through massive data sets in search of minute patterns. That could mean that potential dangers are a crucial part of AI-based threat identification. Algorithms trained with deep learning mimic the way the human brain learns by utilizing neural networks; this allows the algorithms to improve their performance with time as they identify & analyze more data (Rehman, 2022). AI based threat detection is highly successful at detecting threats in real time, allowing security teams to react quickly & prevent potential dangers from becoming major security events. In order to detect and follow threats across different systems and networks, these systems can evaluate data from multiple sources at once (Jenis 2021).

AI threat detection systems may identify a wide range of threats, depending on the data & algorithms used. One example of a threat that these technologies can identify is phishing & malware (Kuzlu et al., 2021). By analyzing video surveillance footage, AI can identify suspect activity or behavior, such as theft or unlawful entry, in terms of physical security. In the realm of homeland security, AI can scour social media feeds for signs of possible terrorist threats. AI has numerous benefits when it comes to danger detection. Because security professionals can spot risks instantly with the help of AI-based solutions, which are incredibly effective & precise. Because of their speed and ability to handle large datasets, these systems are ideal for multi-source data analysis. Learning from new data and adjusting to it can also increase AI systems' accuracy over time, minimizing the risk of false positives (Sadiku et al., 2020b).

## METHODS IN CYBER SECURITY BASED ON ARTIFICIAL INTELLIGENCE

Computing revolutions are causing societal shifts at a dizzying rate (Mehra 2021). This has a major influence on people's daily lives and their jobs. Computers with human-level cognitive abilities, such as learning, decision-making, and problem-solving capabilities, have recently emerged, due to a number of these technologies. For example, AI is capable of analyzing massive volumes of data & making intelligent decisions in real-time. The application of AI approaches has numerous positive effects on research & technology across many domains (Achi et al., 2021). There are a lot of cybersecurity issues because the Internet is full with personal data. To start, manually analyzing all of that data would be an enormous undertaking. Secondly, there can be risks associated with AI or emerging dangers. Ansari et al. (2022) note that the high cost of employing specialists drives up the expense of threat prevention.

It also takes a lot of resources (time, money, & effort) to design and implement algorithms that can detect those risks. An approach that makes use of AI-based methods could solve those issues. When it comes to processing large datasets, AI can do so fast, accurately, & efficiently. Even if the patterns of attacks change, an AI-based system can use threat history to forecast future attacks that will be similar to those that have previously happened. AI has the ability to process massive amounts of data, detect novel and noteworthy changes in attacks, & enhance the reaction of its security system to threats in an ongoing manner. AI in cybersecurity has helped shift the focus from reactive to proactive measures, allowing for the detection & elimination of threats in real-time (Rawat et al., 2022). A few examples of cybersecurity methods that use AI are these:

- **Threat Detection and Analysis**

Automatic analysis of massive data sets can be accomplished by threat detection systems powered by AI. In order to identify suspicious behaviors, ML algorithms can evaluate user behavior, spot patterns in network traffic, & detect malicious code in files (Bishtawi 2022).

- **Preventing Fraud**

AI fraud detection systems can sift through mountains of data in search of signs of suspicious activity. These systems have the ability to spot suspicious tendencies, patterns, and trends in monetary transactions and aid in the immediate detection of fraud (Benzạd 2020).

- **Analytics for Data Entity & User Behavior**

UEBA is an AI-powered method that detects questionable actions on user devices & accounts by utilizing ML techniques. It finds compromised accounts or malevolent insiders, which are hard to find using conventional security measures.

- **Response to Incidents**

When it comes to cyber risks, incident response systems powered by AI can automate the reaction, cut down on response time. According to Bhatele et al. (2019b), these systems can swiftly analyze data from several sources and give the security team relevant information.

- **Virtual assistants and chatbots**

Automating common security processes like account management and password resets is possible with the help of chatbots & virtual assistants powered by artificial intelligence. Users can also receive immediate support, which speeds up the resolution of security-related concerns.

- **Threat Intelligence**

Threat intelligence systems powered by AI can sift through mountains of data from all over the place in search of new vulnerabilities & threats (Li, 2018). Organizations can benefit from their real-time threat intelligence in taking proactive measures to safeguard themselves against cyber threats.

## DISCUSSION

The use of AI has grown in cybersecurity in recent years (Rekha et al., 2020). Due to the ever-increasing volume and sophistication of cyber threats, organizations have begun utilizing AI-based systems to detect & mitigate cyberattacks.

### a) AI-Based Threat Detection

With AI, threat detection takes center stage in cybersecurity. Historically, threat detection systems have relied on signature-based tactics, which are limited to identifying already identified threats. But as cyber attacks have gotten more sophisticated, traditional measures have become ineffective. But with the help of complex algorithms & ML models, AI-based systems can spot threats both old and new. When it comes to artificial intelligence methods used for threat detection, ML is among the most popular (Ghillani, 2022). By sifting through mountains of data, ML models can spot trends that could indicate danger. In order to teach the models to correctly detect possible dangers, they are trained on datasets that contain both hostile and benign traffic. If ML models notice anything out of the ordinary happening on a network, it could be a sign of a cyberattack. Another artificial intelligence method utilized in threat detection is deep learning. When it comes to data analysis and classification, Deep Learning models rely on deep neural networks. Intricate patterns can be identified and classified as good or undesirable by these models. Malware, phishing schemes, and other forms of cybercrime can be identified & categorized by Deep Learning models. Another artificial intelligence method, Natural Language Processing (NLP), is used for threat detection. Natural language processing methods can uncover possible dangers by analyzing unstructured data sources such as internet forums & social media feeds. Alhayani et al. (2021) found that the models might increase threat detection accuracy by extracting information from text data.

### b) AI-Based Threat Prevention

In addition to threat detection, AI can also be employed to prevent threats. Computer programs powered by artificial intelligence can detect danger & stop it in its tracks. Some ways AI is being used to combat risks are as follows:

- **Intrusion Prevention Systems:** These systems, powered by AI, may identify and thwart potential network invasions.

- **Malware Prevention:** Antimalware systems powered by AI can identify malicious software and stop it from being installed.

- **Phishing Prevention:** Anti-phishing systems powered by artificial intelligence may scan emails for malicious content and flag them as potential phishing attempts.

- **Vulnerability Evaluation:** Computer programs that use artificial intelligence can find security holes in a network and fix them before they cause any damage.

- **Access Control:** Systems that employ artificial intelligence to detect danger & prevent unauthorized people from entering can be very useful.

## CONCLUSION

In the ever-changing world of cybersecurity, AI is playing an essential role. The ever-evolving complexity & sophistication of cyber attacks has rendered traditional threat detection and prevention methods ineffective. Advanced and state-of-the-art countermeasures to cyberattacks are provided by AI-based systems. Systems powered by artificial intelligence use techniques like deep learning, ML, NLP, predictive analytics, & behavioral analytics to detect and prevent cyber threats. In addition, incident response has been improved by AI-driven automation, which has reduced the impact of hacks. Malware detection has also become an area where AI is crucial, especially for finding new types of malware & vulnerabilities (such as zero-day vulnerabilities). As new technologies emerge, AI's use in cybersecurity will evolve as well. Organizations must change and use these state-of-the-art technologies if they want their systems to be secure against cyber-attacks. Companies who invest in AI will be better prepared to defend against internet attacks.

## REFERENCES

1. Achi, A., Kuwunidi Job, G., Shittu, F., Baba Atiku, S., Unimke Aaron, A., & Zahraddeen Yakubu, I. (2021). SEE PROFILE Survey On The Applications Of Artificial Intelligence In Cyber Security. Survey On The Applications Of Artificial Intelligence In Cyber Security Article in International Journal of Scientific & Technology Research. www.ijstr.org

2. Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.02.531

3. Anandita Iyer, A., & Umadevi, K. S. (2023). Role of AI and its impact on the development of cyber security applications. In *Artificial Intelligence and Cyber Security in Industry 4.0* (pp. 23-46). Singapore: Springer Nature Singapore.

4. Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. IJARCCE, 11(9). https://doi.org/10.17148/ijarcce.2022.11912

5. Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? IEEE Network, 34(6), 140–147. https://doi.org/10.1109/MNET.011.2000088

6. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019a). The Role of Artificial Intelligence in Cyber Security (pp. 170– 192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

7. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019b). The Role of Artificial Intelligence in Cyber Security (pp. 170– 192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

8. Bishtawi, T., & Alzubi, R. (2022). Cyber Security of Mobile Applications Using Artificial Intelligence. 1st International Engineering Conference on Electrical, Energy, and Artificial Intelligence, EICEEAI 2022. https://doi.org/10.1109/EICEEAI56378.2022.10050484

9. F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear CyberPhysical Systems and Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, April 2020, doi: 10.1109/TII.2019.2956474.

10. G. A. Chandra, K. K. Srinivas, P. Anudeep, S. R. Prasad, Y. Padmasai and P. Kishore, "Mental Health Disorder Analysis Using Convolution Neural Network Based Speech Signal Model With Integration Of Artificial Intelligence," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 544-547, doi: 10.1109/RDCAPE52977.2021.9633637.

11. Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. American Journal of Artificial Intelligence, x, No. x, x–x. https://doi.org/10.22541/au.166379475.54266021/v1

12. J. Kuppala, K. K. Srinivas, P. Anudeep, R. S. Kumar and P. A. H. Vardhini, "Benefits of Artificial Intelligence in the Legal System and Law Enforcement," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 221-225, doi: 10.1109/MECON53876.2022.9752352.

13. Jenis Nilkanth Welukar, & Gagan Prashant Bajoria. (2021). Artificial Intelligence in Cyber Security - A Review. International Journal of Scientific Research in Science and Technology, 488–491. https://doi.org/10.32628/ijsrst218675

14. K. K. Srinivas, P. Vangara, R. Thiparapu, R. Sravanth Kumar and K. A. Bhagavathi, "Artificial Intelligence based Forecasting Techniques for the Covid-19 pandemic," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 297-301, doi: 10.1109/MECON53876.2022.9752240.

15. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things

(IoT) cybersecurity. Discover Internet of Things, 1(1). https://doi.org/10.1007/s43926-020-00001-4

16. Li, J. hua. (2018). Cyber security meets artificial intelligence: a survey. In Frontiers of Information Technology and Electronic Engineering (Vol. 19, Issue 12, pp. 1462–1474). Zhejiang University. https://doi.org/10.1631/FITEE.1800573

17. Li, K. Ota, M. Dong, J. Wu and J. Li, "DeSVig: Decentralized Swift Vigilance Against Adversarial Attacks in Industrial Artificial Intelligence Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3267-3277, May 2020, doi: 10.1109/TII.2019.2951766.

18. Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, *69*, 43-51.

19. Mehra, A., & Badotra, S. (2021). Artificial Intelligence Enabled Cyber Security. Proceedings of IEEE International Conference on Signal Processing,Computing and Control, 2021-October, 572–575. https://doi.org/10.1109/ISPCC53510.2021.9609376

20. Naseer, I. (2024). The role of artificial intelligence in detecting and preventing cyber and phishing attacks. *European Journal of Advances in Engineering and Technology*, *11*(9), 82-86.

21. Onih, V. A., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. *International Journal of Scientific and Management Research*.

22. Rajendran, R. M., & Vyas, B. (2023). Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology. *International Journal For Multidisciplinary Research*, *5*(6), 1-18.

23. Rawat, B. S., Gangodkar, D., Talukdar, V., Saxena, K., Kaur, C., & Singh, S. P. (2022). The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 247–250. https://doi.org/10.1109/IC3I56241.2022.10072877

24. Rehman, S. F. U. (2022). Practical Implementation of Artificial Intelligence in Cybersecurity – A Study. IJARCCE, 11(11). https://doi.org/10.17148/ijarcce.2022.111103

25. Rekha, G., Malik, S., Tyagi, A. K., & Nair, M. M. (2020). Intrusion detection in cyber security: Role of machine learning and data mining in cyber security. Advances in Science, Technology and Engineering Systems, 5(3), 72–81. https://doi.org/10.25046/aj050310

26. Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020a). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

27. Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020b). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

28. Shamiulla, A. M. (2019a). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119

29. Shamiulla, A. M. (2019b). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119

30. Soni, V. D. (n.d.). Role Of Artificial Intelligence In Combating Cyber Threats In Banking. www.iejrd.com

31. Wahab, F., Shah, A., Ullah, I., Khan, H., & Adhikari, D. (2024). The significance of artificial intelligence in cybersecurity. In *Artificial Intelligence for Intelligent Systems* (pp. 105-119). CRC Press.

32. X. Qiu, Z. Du and X. Sun, "Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks," in IEEE Access, vol. 7, pp. 172004- 172011, 2019, doi: 10.1109/ACCESS.2019.2956480.

**Corresponding Author**

**Kushagra Aditya Jha***

Class 11th, Sanskriti School, Chanakyapuri, New Delhi, India

Mail ID : kushagraadityajha@gmail.com