OPEN ACCESS

KJMR

Kashf Journal of Multidisciplinary Research
Vol: 01 - Issue 12 (2024)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

Use of AI to Secure Network

Muhammad Obaid Ullah
Superior University Lahore

Zeeshan Ahmad
Superior University Lahore

Muhammad Azam
Superior University Lahore

Shumaila Iqbal
Superior University Lahore

Article Info

Abstract

In today's world, protecting our digital systems and data from cyber threats is a big concern. These threats are getting more advanced, with attackers using artificial intelligence (AI) to make their attacks even more effective. This means that we need to keep improving our defenses to stay safe. One of the main problems is that more and more devices are connected to the internet, like machines in factories. These connections create new opportunities for cyber attackers. This research looks at different types of cyber attacks and how we defend against them, especially in industries. We're also exploring how AI can help us with this, but there are pros and cons to using AI in security. While AI can be a powerful tool for enhancing our security, it's not a silver bullet. It needs constant training and human oversight because it has its limitations. Many companies are using AI for security, but it's important to make sure it's in the hands of ethical and knowledgeable people. AI is playing a growing role in monitoring and dealing with cyber risks. It can help detect and prevent different types of cyber threats, like viruses and phishing attacks. Although AI has its challenges, its advantages are greater. All in all, AI is changing the way we approach cyber security and helping us stay safe in our increasingly digital world.

Keywords: *artificial intelligence, cyber security, machine and deep learning, cyber attacks*

Introduction

A theoretical issue that has dominated in the field for many years is security. The issue of security has recently grown in importance last few years. Now a days it is the biggest challenge to secure the network because as the technology advanced day by day every secondgadget connect with the network e.g. house appliances, security system, different infrastructures and internet banking etc by this our life become more reliable and easy to access world is running on digital data but at the same time it is the challenging because if network is not secure and if it compromised then every second thing will also be on risk.[1] But at the same time it is gift for us that the Artificial Intelligence (AI) become the every task more easy our almost more than 50% working would be done by Artificial Intelligence (AI) that's why to complete the task is easy. [2]

Figure 1: AI in cyber security [9]

The Artificial Intelligence (AI) participate in every second thing that's why it is the need especially for secure the network. As we know Artificial Intelligence (AI) becomes the life more easy that's why we also get benefit from the Artificial Intelligence (AI) to secure the network in different aspects like to aware and secure the different viruses and attacks, multiple methods to secure the network, different layers of networks have different problems etc. [3]Security is an important component of networks. As the time become change with the passage of time and in the modern age the every one want to protect our self [4] which is not possible in past era but it is also very difficult now days because the problems become more tricky that's why the solutions that provides also become more complicated. [5] AI can swiftly search through millions of data sets for any potential danger.[6] But this is the time to with the help of Artificial Intelligence (AI) to secure our network. [3]To achieve this task we have different models, architecture and frameworks which we want to adopt. There are the multiple advantages like in the less time is productive output achieve but at the same time the challenges are also very complex like with passage of time the issues which we are facing changes day by day. Around 200 million personal records were exposed as a including high profile data releases.[7] As the multiple advantages the disadvantages are also there like as we increase the security the authentic approach of the authorized person also become more difficult because they crosses the multiple checks to required destination.[8]

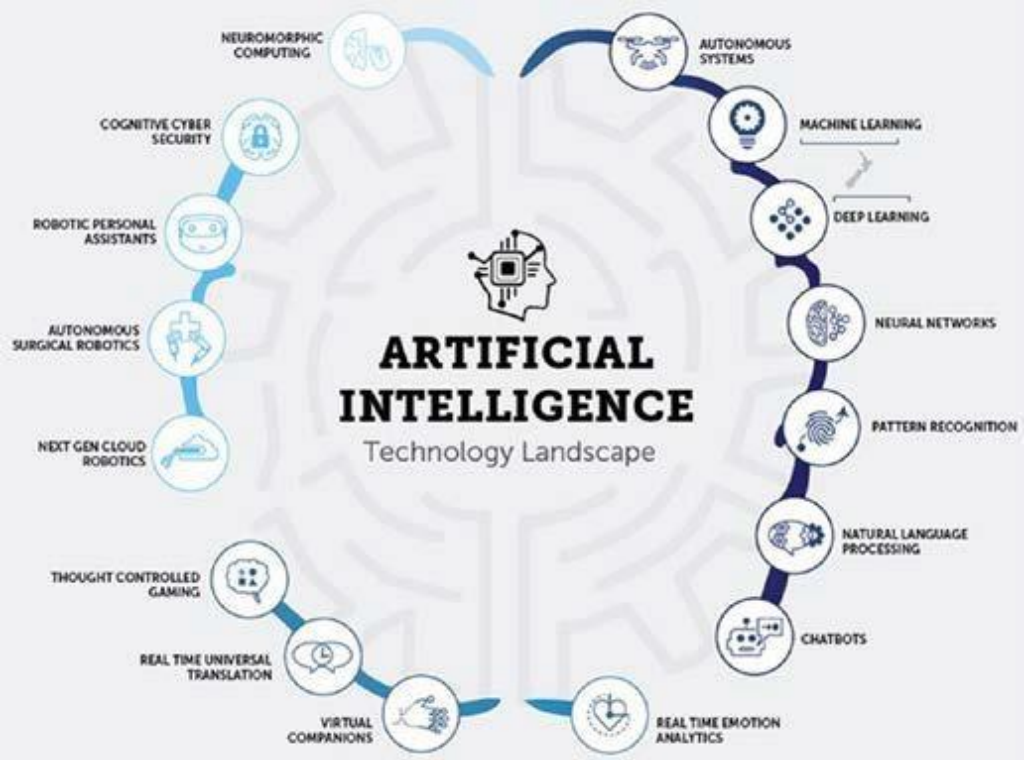

Figure 2: AI in cyber security [6]

The main issue is how we can accomplish this task of making the network more secure with the help of Artificial Intelligence (AI). As we know, there are multiple algorithms involved in Artificial Intelligence (AI) that are becoming more advanced day by day, so we can benefit from those algorithms to make the network more secure in a variety of ways. Artificial intelligence is a solution to "Internet threats", "Identify types of malware", "Ensure practical security standards", and "Help create better prevention and recovery strategies".[9]Existing solutions are not as trustworthy as we demand, therefore we employ advanced technologies such as Artificial Intelligence (AI) to address difficult scenarios, because hackers also use Artificial Intelligence (AI) to attack. AI systems may assist not only in danger detection, but also in taking proactive measures against cyber assaults, such as sorting and categorizing events and threats, therefore relieving technicians of repetitive chores. [10]Our goal is to become a more efficient means of securing our network with the use of Artificial Intelligence (AI).

Until date, this strategy has only been used in a few businesses. Artificial intelligence (AI) is a new discovery in the realm of networks that has demonstrated the importance of networks. It will be challenging to adapt AI methodologies and tools to the new Cyber Physical System needs.[11] Artificial intelligence (AI) is a vital component that uses automation to boost an organization's output and efficiency. As a result of digital transformation, [12]

Security is an increasingly important issue in this era. Our motivation of this topic is the only one the burning issue of this present time Security and the security of networks through this world become the global village. Over the past century, there has been a major issue of security. [13] This study builds on the perspective of networks. Everything connected with networks and the protection of data is very important. Artificial intelligence (AI) has helped more organizations to improve the security posture effectively and reduce the breach risks.[12]

Figure 3: AI in cyber security [7]

Artificial Intelligence (AI) has the possible to be tremendously helpful in combating such dangers as Shown in Fig.2. In the above figure shows how the Artificial Intelligence (AI) helps us to secure network as well as in cyber security.

1. Literature Review

The increase in cyber attacks has outpaced the financial resources and people capacity of the cyber security sector threat. A growing amount of financial and personal data must be protected from cyber attacks as the digital world develops. Actually, cyber attacks have the potential to completely damage an organization's reputation. This study explores how artificial intelligence can be used to strengthen cyber security.

Artificial intelligence has developed to the point that it can now perform tasks like data analytics better than humans. The investigation revealed that there are advantages and disadvantages to utilizing artificial intelligence to control cyber attacks. The advantages outweigh the disadvantages. This study finds that because artificial intelligence systems require quick. These risks can be automatically identified and avoided thanks to artificial intelligence. Artificial intelligence methods can shorten the time between an attack and identification of malware since it changes too quickly to be identified or examined manually.

New, more adaptable, flexible, and scalable techniques are required due to the complexity of assaults and the quick expansion of cyber hazards. According to recent research, the main goals of AI based cyber security algorithms are malware detection, phishing detection, and spam detection. Several studies taken together. Although AI will inevitably play a role in addressing cyberspace issues, several issues with artificial intelligence's credibility as well as threats and attacks based on artificial intelligence will be concerning in the cyber environment.[2] Artificial intelligence techniques and how they can be used to identify network assaults. The depiction of models based on fuzzy, evolutionary, and neural computations is given special consideration. A binary classifier is the main component of the system and it matches each input object to one of two sets of classes. It is possible to create models trained on distinct subsamples by integrating binary classifiers according to a variety of different schemes. Many optimization strategies are put forth, both in terms of using aggregating compositions and parallelization. In order to make the assessed attack feature vectors less dimensional, principal component analysis is also taken into account. To cut down on false positives, a sliding window technique was created and used. The results of the trials utilizing the multifold cross-validation are reported, followed by the model efficiency indicators. The task of detecting network attacks is challenging, and there are numerous techniques for doing so in contemporary literature. Some of these are based on technologies like artificial intelligence, which is fast advancing. These consist of genetic algorithms, fuzzy logic, and neural networks. One of the most important aspects of assuring the security of network nodes is the creation of detection systems for attacks. As a result, it is critical to deploy cutting-edge methods, such as artificial intelligence algorithms, to identify network attacks. This study discusses binary classifier models used to identify network assaults. To improve the training of such classifiers, a parallel genetic technique based on the crossover, mutation, and permutation operators has been developed. We've gone through the sliding window approach for determining network parameters, which seeks to eliminate unusual network bursts. To combine binary classifiers when

developing multi-class models, many low-level approaches and aggregating compositions were considered. The studies revealed that the proposed strategy improved network record classification accuracy and true positive rates.[5]

Artificial intelligence increases corporate and individual security, but it also provides the wrong people more power. To give Artificial Intelligence more responsibility in the near future for security reasons, we must ensure that it is solely in the hands of white hat employees. Although artificial intelligence is unlimited, smart, and quicker than humans, it needs a human touch to get started. As a result, companies must focus their efforts largely on locating and training Artificial Intelligence agencies that can work with the machine to assureproduct safety. The combination of human intelligence and artificial intelligence would surely help in the fight against hackers. To recapitulate, Artificial Intelligence technology is becoming important in how corporations safeguard their networks and sensitive data. It's no surprise that cyber security is a top issue for all enterprises, especially now that the world is going digital. AI consultants and leading RPA providers are hard at work developing enhanced solutions to provide a comprehensive and robust protection mechanism. Here are some predictions on how Artificial Intelligence will improve cyber security with AI-powered technologies.

Making use of artificial intelligence Artificial intelligence is being used to track security incidents. To detect abnormalities, machine learning will be implemented into firewalls. Identifying the origins of cyber assaults using natural language processing (NLP) technologies Bots for robotic process automation (RPA) automate rule-based activities and procedures. Mobile endpoints are used to monitor and assess cyber hazards.[7] The fast rise in hostile cyber criminal activity has elevated cyber security to the status of a critical study area. as well as cryptography approaches, has demonstrated promising outcomes in combating adversary caused cyber dangers. As a result, the potential of Artificial Intelligence in boosting cyber security solutions is examined in this paper. Furthermore, the research included an in-depth review of several Artificial Intelligence-based strategies for detecting, analyzing, and preventing cyber threats. Finally, the current research has explored future research potential related to the development of Artificial Intelligence systems in the domain of cyber security. As the sophistication and speed of assaults have improved, artificial intelligence has become a critical weapon in cyber security. The present research report has demonstrated how cyber threats have evolved, become more complex, and are leveraging new technology to compromise security. The analysis indicates an increase in cyber security risk. Furthermore, as technology progresses, cyber assaults will increase, even if the cyber security sector develops measures to mitigate these dangers. Various Artificial Intelligence based approaches.[3] The reference article concentrated on the most significant facts concerning assault, Finally, AI applications of security threats in cyber attacks are discussed. who are not experts in the subject and need a quick and basic overview of the role of artificial intelligence in cyber assaults.[2]

Recent advances in artificial intelligence have been transformative, surpassing human competence in jobs such as data analytics. This study reveals that given the quick. ICT advancements have led in the rise of new cyber security challenges. Traditional tactics based on inferences from previous assaults no longer appear to be effective in combating security concerns. Because of the computational complexity of cyber assaults, innovative strategies.

[10] Technology is rapidly evolving; artificial intelligence has demonstrated promise outcomes in cyber security by evaluating data and making decisions. This article provides an AI method that is being employed in a variety of applications in the fight against cyber attacks.[12] Cyber assaults are continually evolving and changing, with the use of Artificial Intelligence technology boosting their malevolent performance. With technical innovation, the malevolent use of Artificial Intelligence has revolutionized the landscape of possible risksin the cyber environment. To guard thieves, technological progress necessitates current research. Manufacturing machines that are networked and connected to the Internet expose themselves to more cyber threats. Attackers take use of this interconnectedness to intensify their acts. This literature review discusses the many forms of cyber assaults, defense countermeasures, and the use as well as the benefits and drawbacks of employing AI for security. [8]

The usage of artificial intelligence is a powerful technology that may be utilized to identify weak places in cyberspace as well as the origins of attacks. This may be performed through the analysis of vast volumes of data. An artificial intelligence system designed with security in mind may continually sift through massive amounts of data in search of potential dangers and provide suitable suggestions. Despite its many valuable applications, artificial intelligence software is vulnerable to hacking, and the data it utilizes may be corrupted or poisoned, all of which can cause the programs to fail. To overcome these difficulties, specific changes will need to be made to the core procedures that are used to maintain and improve the operation of AI. Artificial intelligence, often known as machine learning, is quickly becoming a critical tool for increasing the efficiency of IT security teams. Because there are so many of them, a single human being working alone is incapable of providing appropriate protection for a contemporary company's potentially vulnerable points of entry. In terms of threat analysis and detection, artificial intelligence can meet the requirements set for security professionals. As a result, the probability of a security breach is reduced, and the overall degree of security is increased.[6] Standard computer algorithms are not always capable of dealing with, incorporating into cyber security is critical to improving. As a result, this study article focuses on artificial intelligence and its principles, which may be used in cyber security to increase data protection. A descriptive analytical technique based on previous research is applied. The inquiry is still ongoing, and some recommendations for improving cyber security are being made.

There are several difficulties that human intellect is expected to tackle in the modern world. However, in most circumstances, people lack the necessary intellect to comprehend certain difficulties and discover the best solutions. As a result, people choose to employ artificial intelligence, which has been shown to reduce mistakes competency.[13] Our post is aimed at the broader cyber security industry, and we keep technical words to a minimum in order to make our contribution intelligible to a wide readership. Furthermore, we dispel numerous myths that have arisen as a result of the rising amount of works that relate ML with cyber security applications. Following an introduction to the fundamental ideas of machine learning, we present a succinct overview discuss several more cyber security domains that might benefit from ML's self learning capabilities.[4] Improving cyber security through the use of artificial intelligence applications and methodologies we are able to the current state of cyber threats and viruses, an Intelligent Protection Infrastructure is

essential. Unlike existing cyber security solutions, Artificial intelligence approaches are durable and flexible, resulting in improved security implementation and stronger defense against an increasing range of sophisticated cyber threats. Comparable devices are not entirely prepared to adapt to changes in their surroundings, given the enormous shift that Artificial Intelligence has brought to the realm of cyber security.[9]

As cybercrime becomes more complex, cyber security methods must become more robust and sophisticated. This will allow defense systems to make real-time decisions, allowing them to respond to complex threats effectively. To help with this, researchers and practitioners must be conversant with existing cyber security measures. The use of artificial intelligence, namely in the fight against cybercrime. However, no summary of artificial intelligence techniques to combating cybercrime is provided.[1] This research quickly reviews several Cyber Physical Systems layers and their corresponding models in order to highlight growing safe Cyber Physical Systems research concerns. The neural networks under consideration here are intended to overcome the existing constraints of the most advanced static and adaptive detection and protection approaches, as well as the technologies' current level of development. This study presents a conceptual framework for future research on Cyber Physical Systems. AI based security techniques, in the end, employing intrusion prevention security systems, highlight some common Cyber Physical Systems layer dangers and unresolved research challenges in constructing intelligent Cyber Physical Systems security precautions. Aside from that, the suggested effort gives a look into the future and significance of Cyber Physical Systems safety research, inspiring assessments of research topics. A new strategy to estimating and correcting assaults launched by a forward link of nonlinear Cyber Physical Systems is proposed here using intelligent nonlinear system control.In the suggested strategy, neural networks are integrated with nonlinear control. Because all of the required technology is currently in place, it is clear from this assessment that cyber physical systems are on the verge of a sophisticated program. One of the problems of this new technology revolution is integrating several Cyber Physical Systems to conduct autonomous activities in a confined setting, which is a future scope. As applied in our Cyber Physical Systems AI is stressed as a critical instrument for improving the involvement of Cyber Physical Systems in an intelligent system that requires minimal human effort, with an overall performance of 96%. The proposed method evaluates overall effectiveness, accuracy, and loss in security analysis and confidentiality. More nodes can be added in the future to improve system efficacy in identifying threats and assaults connected to security andconfidentiality concerns.[11]

2. Methodology

The methodology used in this paper is a systematic literature review. It followed a four step process to identify relevant studies and extract insights. This conducted a search using specific keywords related to AI, machine learning, deep learning, cyber security, cyber attacks. This allowed them to retrieve a diverse range of relevant metadata for their research.

[16] According to the fig. 4 prism diagram After the initial search, it filtered out repeated publications, resulting in a total of 70 unique publications [17]. They then applied a critical analysis to evaluate these publications and exclude studies that did not. This step helped to narrow down the selection to 30 articles [17].In this critically analyzed the 30 selected articles to determine their relevance to the research topic. [8] And after that only 15

papers are left those are related to my article. They excluded certain document types, such as conference papers, review articles, and non-English publications, resulting in a final set of articles for further analysis [17].

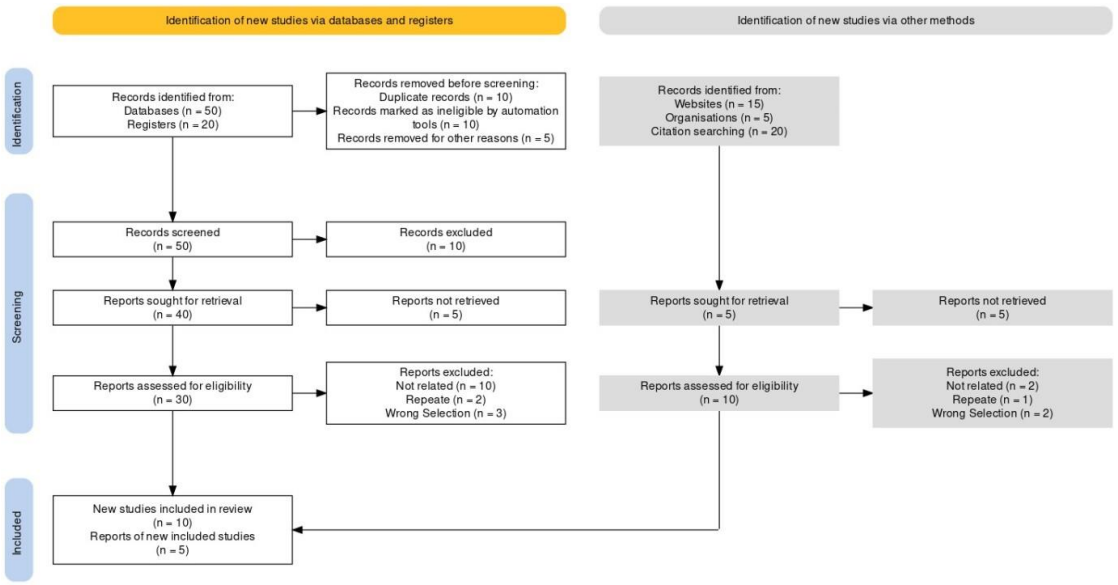

Figure 4: Prism Diagram

Its performed a thorough reading of the material identified in the previous. They extracted relevant information on AI-based cyber attacks and their applicability to cyber security. This critical reading allowed them to gain insights and develop. [17] Throughout the paper, its refers to the studies they identified and analyzed using appropriate. These provide references to the specific studies and sources that were used to support the findings and discussions presented in the paper. Overall, the systematic literature review methodology employed in this paper ensured a comprehensive and structured approach to gathering and analyzing relevant research within the networks. [8]

3. Results and Discussion

The paper discusses the growing significance particularly within the context of networks and industries. [19] It conducts a assess their relevance to industrial cyber security. The paper underscores the rising risks associated with cyber attacks in the industrial sector and stresses the need for robust defense mechanisms. It explores various applications of AI in industrial cyber security, such as detecting cyber security threats in Internet of Things (IoT) devices, leveraging block chain technology, employing AI, and enhancing fraud detection and network security. [20] These studies collectively emphasize the pivotal role of AI in addressing cyber security challenges within the industrial ecosystem. [21]In the fig. 5 visualize map it explain through the map of related papers with year.

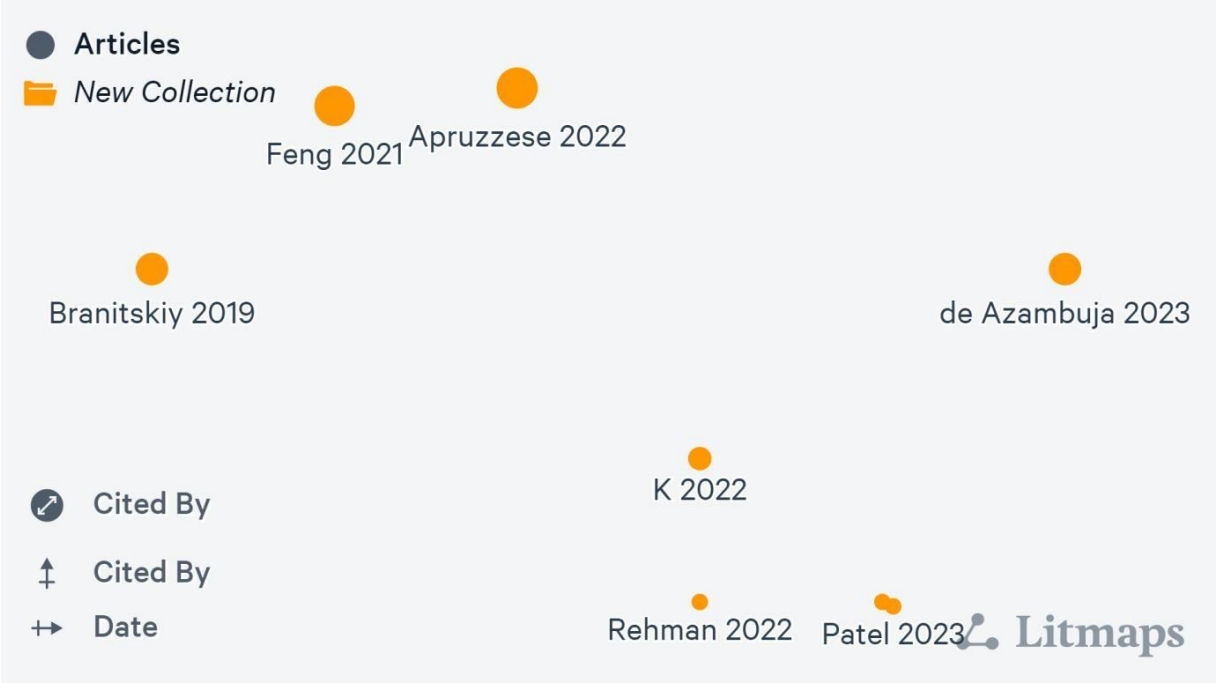

Figure 5: Visualize Map

Furthermore, the paper delves into the utilization of IoT architecture and machine learning techniques, particularly deep learning models, to detect and prevent cyber attacks in industry.
[22] It emphasizes the necessity for robust cyber security measures and provides insights into various types of cyber threats and their corresponding countermeasures. In the below Table no. 1 the search results of selected articles. [23]

Table 1: Search Results of Selected Articles

Title	Year of Publication	Publisher
Artificial Intelligence Techniques in Cyber security Manag.	2023	Springer
Applied Artificial Intelligence as Event Horizon Of Cyber Sec.	2022	IEEE
The role of artificial intelligence and machine learning	2022	Springer
Artificial Intelligence in the Field of Cyber	2022	IJRASET
Artificial Intelligence Techniques for Prevention of Cyber Attacks	2022	IJERA Journal
Deep Cyber security: A Comprehensive Overview from Neural Network and Deep Learning Persp.	2021	Springer
Deep Learning Algorithms for Cyber security Applications	2021	Elsevier
Artificial intelligence in cyber security: research advances, challenges	2021	Springer
A Survey on the Role of Artificial Intl.	2021	IEEE
Defense by Artificial Intelligence	2021	IJSES
Reinforcing Cyber World Security Lea.	2020	IEEE
Reviewing the effectiveness of artificial intelligence	2020	PEN
Survey On The Applications Of Artificial Intelligence	2020	IJSTR
Cyber Security Based on Artificial Intelligence	2020	IEEE
Cyber Threat Detection Using Machine Learning	2020	IEEE

In conclusion, it underscores the imperative need for ongoing research and development in the realm of AI driven cyber security to combat evolving cyber threats in the industrial sector.

[24] Additionally, it provides a comprehensive list of references covering predictive methods in cyber defense, distributed attack detection, industry readiness, industrial IoT architectures, artificial intelligence in cyber security,

and related topics, offering a framework for addressing cyber security challenges and underscoring the era. [25]

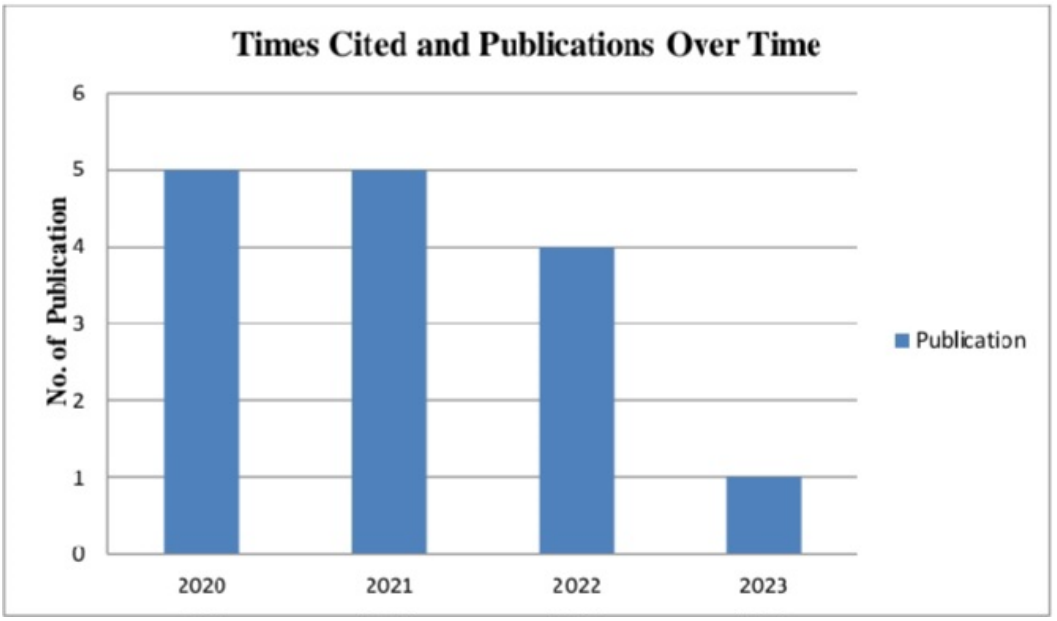

Figure 6: Times Cited and Publications Over Time

In the above fig. 6 its explains and illustrate the times cited and publication over time by column graph. The text highlights that AI-based techniques, including Machine learning (ML), decision trees, deep belief networks (DBN), artificial neural networks (ANN), and convolution neural networks (CNN) are all examples of artificial neural networks. demonstrated efficacy in detecting various cyber security threats, encompassing eavesdropping, malware. [26] They have consistently achieved high detection accuracy rates, surpassing 99% for DoS attacks. Similarly, DL based algorithms like CNN have shown promise in malware detection, attaining precision rates of up to 93% and accuracy rates of 99.41%. These findings underscore how AI techniques bolster cyber security practices, fortifying defenses against cyber attacks and cybercriminals while safeguarding valuable assets. [26] In the fig. 7 seed map its explain through the map of related papers with year by the seed the first paper how relate and site with others through all the papers which are related to this paper as well as literature review.

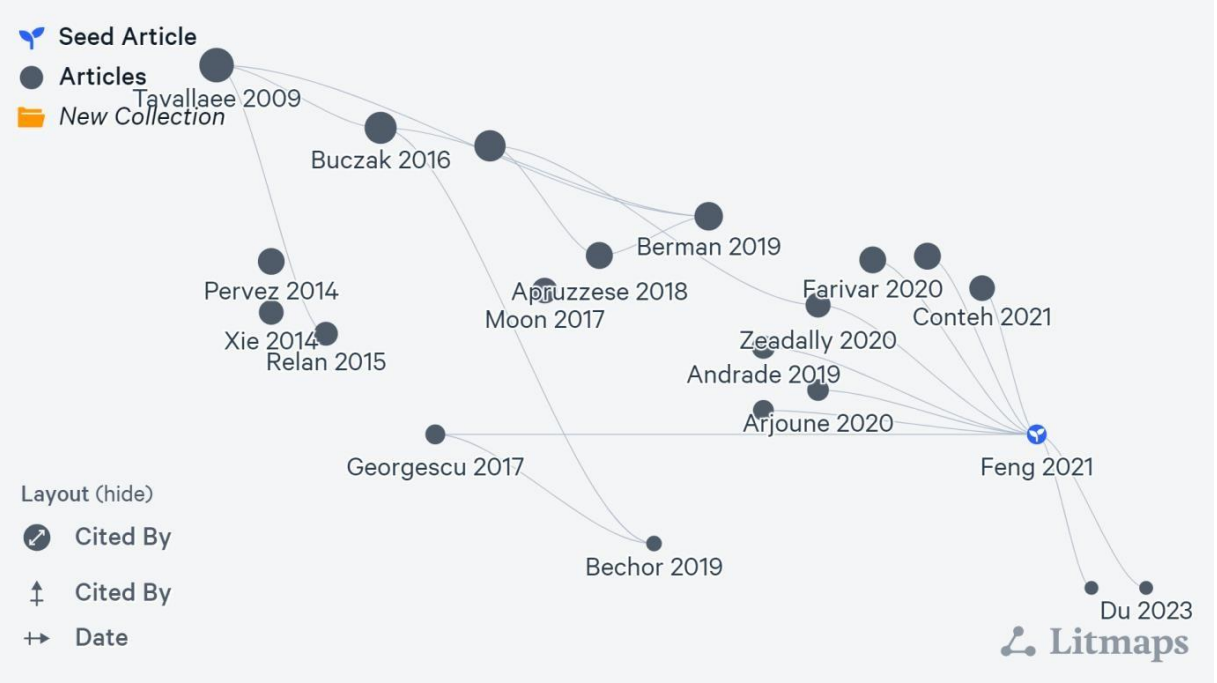

Figure 7: Seed Map

Nonetheless, the text cautions that AI tools are not a panacea and could potentially be exploited by malicious hackers. Limitations include the cost, resource intensity, and training required for AI in cyber security, rendering it impractical in certain applications. Absolute security in the realm of cyber security remains unattainable, and there is a risk that hackers may use AI to develop more sophisticated and harder to detect malware. The shortage of cyber security experts compounds these challenges, preventing AI from being the sole solution to cyber security. [27]

The research study adopts a systematic and descriptive approach to organize previous works and studies. It explores the potential use of machine learning, data mining, and deep learning in three primary areas: intrusion detection, spam detection, and malware analysis. However, it acknowledges limitations, such as the need for constant parameter adjustment and the variability in performance when applied to different threats. The paper also underscores the significance of deep learning, particularly unsupervised learning, as a leading machine learning method in cyber security. Deep learning algorithms offer advantages in automating the identification of patterns in suspicious behavior, enhancing cyber security effectiveness.

[28] In the fig. 7 discover map its explain through the map of related papers with year by the seed the first paper how relate and site with others through all the papers which are related to this paper as well as literature review and also add the 20 papers which are also related this research and this paper.

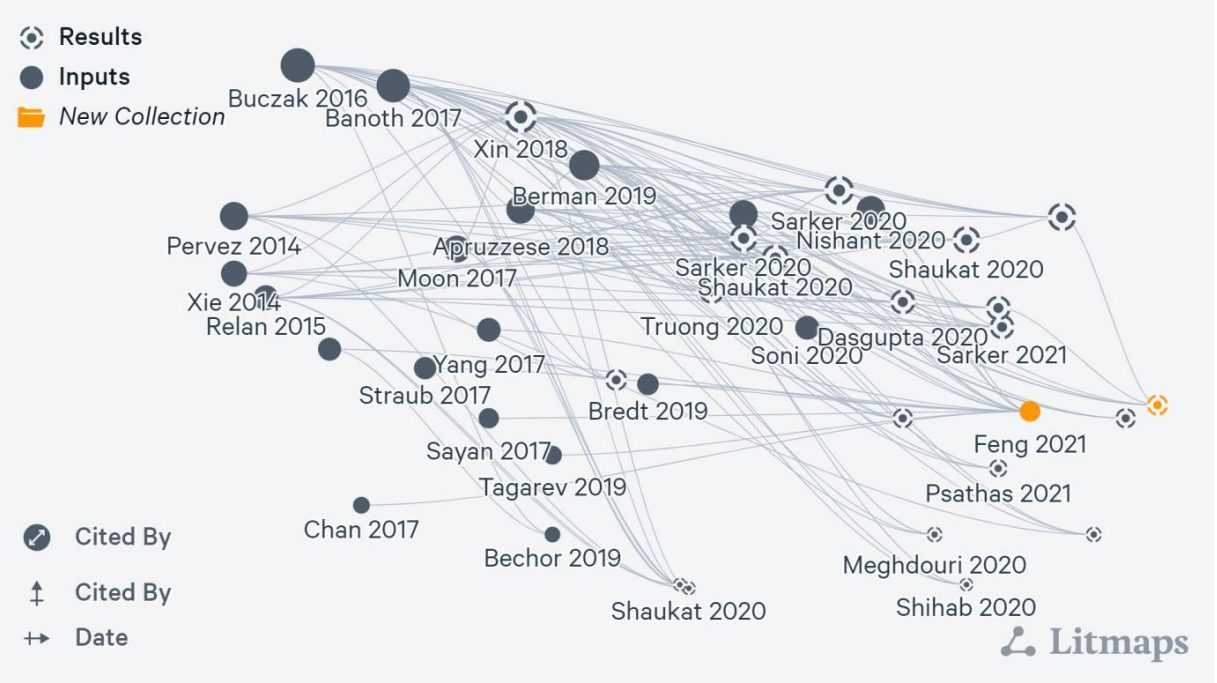

Figure 8: Discover Map

Additionally, the text discusses data mining techniques and algorithms for malware detection, including decision. These algorithms have their strengths and weaknesses, with challenges related to complexity, memory requirements, and computational intensity. The text concludes that while malware technologies evolve, there is a continuous need for the development of rapid and scalable mining algorithms to identify and categorize malware effectively. [29]

Privacy concerns and the "right to be forgotten" are also mentioned as challenges in the use of AI for cyber security, as they clash with the need for large datasets to train AI systems effectively. The text suggests potential solutions, such as making raw data access difficult or anonym zing data points. Additionally, it highlights the high demand for AI and ML security experts who can manage and update AI-based network security systems effectively, as the global demand for these skills exceeds the available supply. [30] In the bellow fig. 9 the prism diagram its shows that the total no. of 70 papers which are in literature review and totalstudy to write this paper then its filter to 45 and also filtered and in the final at the end total 15 papers are left which are fulfill the criteria of this paper.

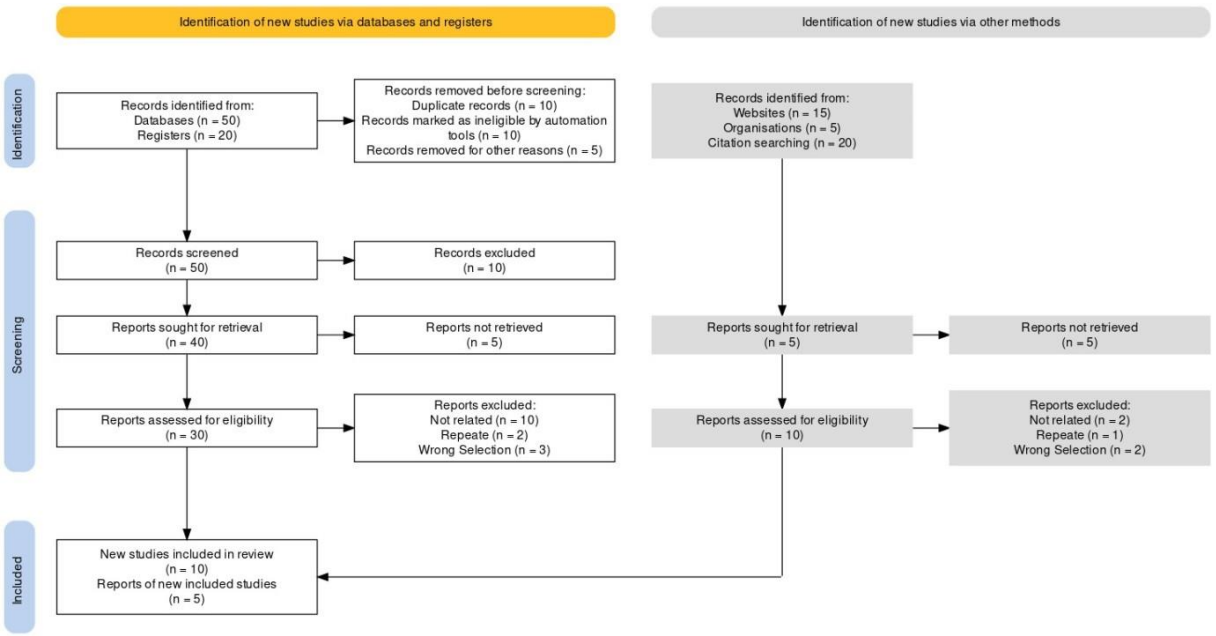

Figure 9: Prism Diagram

In summary, the text emphasizing its potential and challenges. It underscores the need for ongoing research and collaboration in this field to harness the power of AI while addressing its limitations in safeguarding our digital world. [31]

4. Conclusion

In the ever evolving world of cyber threats, the use of artificial intelligence (AI) has transformed the landscape of cyber security. Attackers are increasingly leveraging AI to create more sophisticated and potent cyber attacks, demanding continuous research and adaptation to defend against these malicious uses of technology. One critical concern is the vulnerability introduced. While AI has great potential in improving cyber security, it's not a one-size-fits-all solution. It requires ongoing training and human collaboration, and there are limits to its effectiveness. Cyber security experts are in high demand, and AI should be used judiciously to enhance human efforts in defending against cyber threats.

Several organizations and companies are adopting AI in cyber security, but it's important to ensure that it remains in the hands of ethical practitioners. AI can be a powerful ally in safeguarding networks and data, but it needs human oversight. AI's role in cyber security is expected to grow, with artificial intelligence, natural language processing, and robotic process automation playing key roles in monitoring and analyzing cyber risks. These technologies are enhancing cyber security by efficiently handling vast amounts of data and automating tasks. As cyber threats continue to evolve, AI is becoming increasingly essential for cyber security. It's being used to detect and prevent various cyber threats, such as malware and phishing attacks. While AI has its challenges, its benefits far outweigh the drawbacks. Overall, AI is revolutionizing cyber security, and its integration into security operations centers is seen as a significant step forward. It's helping organizations stay ahead of cyber threats and bolster their defenses in an era of digitalization.

5. References

1. F. Tao, M. Akhtar, and Z. Jiayuan, "The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey," EAI Endorsed Trans. Creat. Technol., vol. 8, no. 28, p. 170285, Aug. 2021, doi: 10.4108/eai.7-7-2021.170285.
2. A. H. S. Alt. , Samah Mohammed S. ALHusayni and Sabah M. Alzahrani, "Defense by Artificial Intelligence in Cyber Attack," Int. J. Sci. Eng. Sci. IJSES, vol. Volume 5,no. Issue 2, p. Page # 35-40, 2021.
3. Mohammed. I. Alghamdi, "Reviewing the effectiveness of artificial intelligence techniques against cyber security risks," Period. Eng. Nat. Sci., vol. Vol. 8, no. No. 4,p. pp.2089-2095, Oct. 2020.
4. G. Apruzzese et al., "The Role of Machine Learning in Cybersecurity," Digit. ThreatsRes. Pract., vol. 4, no. 1, pp. 1–38, Mar. 2023, doi: 10.1145/3545574.
5. A. Branitskiy and I. Kotenko, "Applying Artificial Intelligence Methods to Network Attack Detection," in AI in Cybersecurity, L. F. Sikos, Ed., in Intelligent Systems Reference Library, vol. 151. Cham: Springer International Publishing, 2019, pp. 115–149. doi: 10.1007/978-3-319-98842-9_5.
6. H. Patel, "The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML)," MATHEMATICS & COMPUTER SCIENCE, preprint, Jan. 2023. doi: 10.20944/preprints202301.0115.v1.
7. Kandala kalyana Srinivas (last), D. V. Sai, N.Saketh, and I. Neelima, B.Alekhya, "Artificial Intelligence Techniques for Prevention of Cyber Attacks and Detection of Security Threats," IJERA J., vol. Volume 12, no. Issue 6, p. Page # 37-44, 2022, doi: 10.9790/9622-1206053744.
8. A. J. G. De Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," Electronics, vol. 12, no. 8, p. 1920, Apr. 2023, doi: 10.3390/electronics12081920.
9. Dr. K. R. Dr Lendale Venkateswarlu and Sneha Yerram, "Applications and Techniques of Artificial Intelligence in Cyber Security," Turk. J. Comput. Math.Educ., vol. 12, no. 14, pp. 332–339, 2021.
10. S. B. A. Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu, and Ismail Zahraddeen Yakubu, "Survey On The Applications Of Artificial Intelligence In CyberSecurity," Int. J. Sci. Technol. Res., vol. 9, no. 10, 2020.
11. M. Alowaidi, S. K. Sharma, A. AlEnizi, and S. Bhardwaj, "Integrating artificial intelligence in cyber security for cyber-physical systems," Electron. Res. Arch., vol. 31, no. 4, pp. 1876–1896, 2023, doi: 10.3934/era.2023097.
12. Ms. J. K, H. R, and V. S, "Artificial Intelligence in the Field of Cyber Security," Int.
    a. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 10, pp. 1243–1246, Oct. 2022, doi: 10.22214/ijraset.2022.47155.
13. S. F. U. Rehman, "Practical Implementation of Artificial Intelligence in Cybersecurity – A Study," IJARCCE, vol. 11, no. 11, Oct. 2022, doi:10.17148/IJARCCE.2022.111103.
14. Dr. K. Ramasubramanian, "Applications and Techniques of

Artificial Intelligence in urity" Turkish Journal of Computer and Mathematics Education, vol. 11, no. 11, Oct.2022, doi: 10.17148/IJARCCE.2022.111103.

15. Al ghamdi, "Reviewing the effectiveness of artificial intelligence techniques against cyber security risks," Period. Eng. Nat. Sci., vol. Vol. 8, no. No. 4, p. pp.2089-2095, Oct. 2020.
16. Zhong, R.Y.; Xu, X.; Klotz, E.; Newman, S.T. "Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering" **2017**,3, 616–630.
17. Kaloudi, N.; Jingyue, L.I. "The AI-based cyber threat landscape: A survey.ACM Comput. Surv." **2020**, 53, 20.
18. H. Shapoorifard and P. J. I. J. C. A. Shamsinejad, "Intrusion detection using a novelhybrid method incorporating an improved KNN," vol. 173, no. 1, pp. 5-9, 2017.
19. E. Hodo, X. Bellekens, E. Iorkyase, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Machine learning approach for detection of nontor traffic," in Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, pp. 1-6.
20. M. V. Kotpalliwar and R. Wajgi, "Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP'99 IDS Database," in 2015 Fifth International Conference on Communication Systems and Network Technologies, 2015, pp. 987-990: IEEE.
21. I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, "Innovative technologies of wireless sensor network : The applications of WBAN system and environment," Sustain. Eng. Innov., vol. 1, no. 2, pp. 98–105, 2020.
22. B. Kolosnjaji, G. Eraisha, G. Webster, A. Zarras, and C. Eckert, "Empowering convolutional networks for malware classification and analysis," in 2017 International Joint Conference on Neural Networks (IJCNN), 2017, pp. 3838-3845: IEEE.
23. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in 2017 International Conference on Information Networking (ICOIN), 2017, pp. 712-717: IEEE.
24. D. Palmer, "AI is changing everything about cyber security, for better and for worse.Here's what you need to know," March 2020, https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you- need-toknow/