Global Review of Business and Technology (GRBT)

Vol. 3, No. 1, January 2023 ISSN: 2767-1941

CYBER CRIMES PREVENTION USING ARTIFICIAL INTELLIGENCE: AN ANALYSIS

Kandisa Agarwal, K. R. Mangalam University, India (kandisaagarwal@gmail.com)
Shivam Rawat, K. R. Mangalam University, India (2201830003@krmu.edu.in)
Sarita, Amity University Haryana, India (sgulia@ggn.amity.edu)
Amar Saraswat, K. R. Mangalam University, India (amar.saraswat@krmangalam.edu.in)

ABSTRACT

Artificial Intelligence in machines has been demonstrated as both the cause and the cure of Cyber Attacks. AI has been a futuristic aspect that can replace manpower in many sectors of work as it is developing day by day. As it gets enlarged, consequences came into action, significantly, Cyber Attacks which are the root to problems such as cyber wars, malware, viruses etc. To safeguard the usage of AI, different techniques were put into use to start defending the systems and machines. How AI is used to secure the network was coined as a term Cyber Security. This genre is critical to consider as it has become an international issue nowadays. This paper investigates various studies performed on the link between AI and Cyber Security and finds out how techniques of AI & Machine Learning can be put into use to prevent cybercrimes and how they themselves become the reason for cybercrime. System Learning models, Automated programming techniques, Cyber-physical systems, Cyber warfare laws are some majorly discussed topics. In addition, the work concludes a few existing technologies that have been successful so far to bypass cyber-attacks.

Keywords: AI (Artificial Intelligence), Cyber Crime, Cyber Attack, ML (Machine Learning), Automated Programming

1. INTRODUCTION

The internet was an unknown genre just a few years back. For about the past two decades, an enormous transformation of the world has been observed, with the occurrence of not just Internet, but Cyber Attacks, Artificial Intelligence, Machine Learning, Robotics, Data Mining and the list just keeps on getting larger. Now, these industries have become so vast that life is unimaginable without them. Even though these sectors of technology are exciting and helpful, for example, AI is majorly associated with automation and advancement of technology in every field, but it also calls for major privacy and security threats, which opens up the opportunity of Cyber security. Cyber-attacks have existed since computers came into existence (Li et al., 2021) and researchers have formulated patterns and methods to identify these cyber threats.

1.1 Grassroots of Artificial Intelligence

Diversity of AI in every field and its efficient application is what many researchers are fans of. Artificial Intelligence has skills to solve many of the problems just like it is mirroring human intelligence, only just it's beyond that. It helps in saving human time through automation and replication of human tasks at a faster rate than a human can do. The author in (Kumar et al., 2016) states, “AI has links not only with Computer Science but with Math, Psychology, Cognition, Biology and Philosophy.” Machines with artificial intelligence are replacing the workers with the help of the method of replication of tasks that could be done by using suitable intelligent machines. Since AI has the potential to learn human skills, they are replacing humans in every field. It is used in the Medical Field where AI is capable of providing the best healthcare facility. In the finance sector, Robots are used for repetitive bank jobs. Industrial robots are used in manufacturing. NASA uses robots for space exploration in areas where it is difficult for humans. ‘Autopilot’ feature is used in aircrafts, both private and government. Artificially intelligent robots are used for household tasks for cleaning etc. (Kumar et al., 2016).

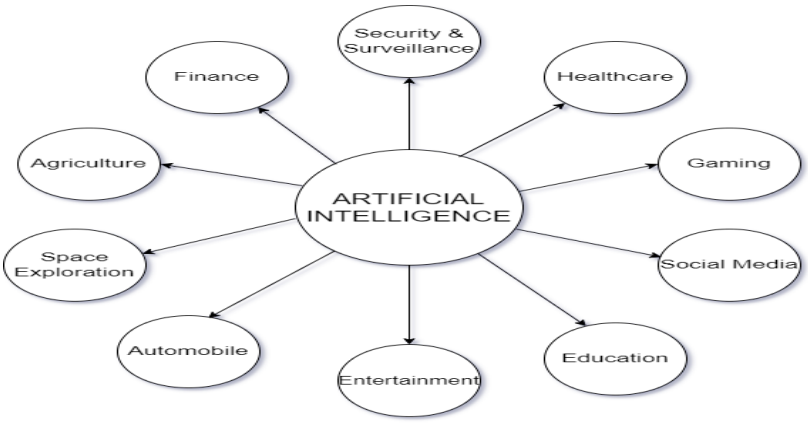

Figure 1: Usage of AI (Artificial Intelligence)

1.2 Unavoidable Cybercrimes and Cyber Security

Cyber Crimes are a big threat. They put the matter of privacy of people and furthermore, become a factor of national security. Although there are laws against these cybercrimes, criminals don't restrict themselves. Everyone uses the Internet nowadays to connect, share, and gather information, including personal information that, in the wrong hands, might cause disruption. To avoid this, cyber security is a crucial part of internet management. Different nations set their Cyber Army to protect their country from foreign cyber-attacks. "Battlefields are now shifting from actual places to virtual areas" (Sevis et al., 2016). Cyber threat is present due to many different sources present in the world, sitting in different corners of the world. Since the internet is omnipresent, it is close to impossible to predict where and how the cybercrime is being planned. There are hackers, organisations, terrorists, foreign countries and many more sources of such cybercrimes. There are methods, patterns, and models which explain possible aspects of cyber security, however, new problems ask for new solutions (Li et al., 2021).

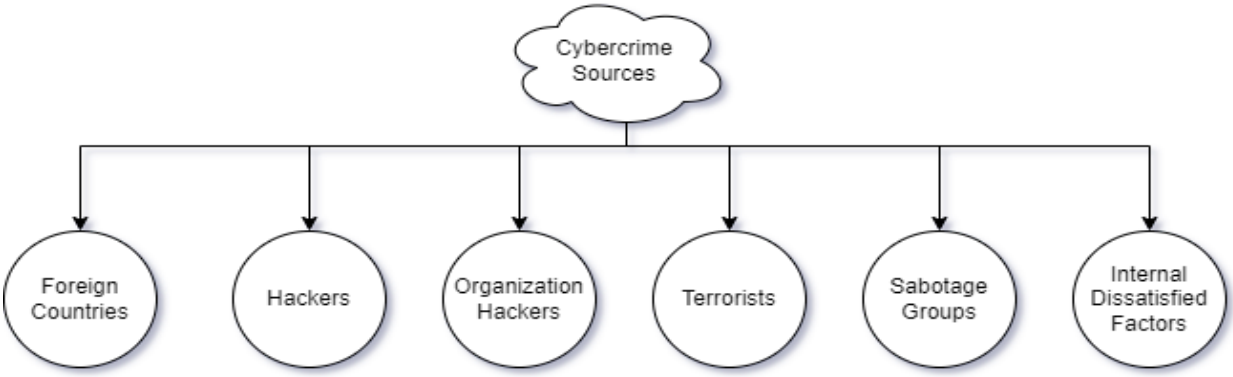

Figure 2: Sources of Cybercrime

1.3 Bridge Linking AI and Cyber Security

With time, cyber-attacks have become so recurring, but also highly progressive as technologists pave the path to newer and rather more complex forms for them. And securing ourselves from these cyber-attacks becomes trivial if done manually, hence, incorporating AI into identifying cyber security becomes a fascinating solution to this problem. "The participation of artificial intelligence in the cyber world is constantly growing" (Kumar et al., 2016). In a standard cyber-attack, a compromised device is involved, which has some loopholes, and the hackers take advantage of these loopholes to conduct the cybercrime (Das et al., 2017). It is proposed that using AI in cybersecurity will produce tremendous results in handling cyber threats, however, research also shows, and it is argued that AI is itself a cyber threat, so how can it be helpful in preventing it. "Over 60 percent of AI businesses recognise that AI creates the most significant cybersecurity concerns.", says the author, Mohammed (2020). Furthermore, the biggest threat of cyber-attacks is on nations, and, ironically, it is said to have anomalies to use AI for cyber security for national concerns. Additionally, AI is not proficient enough to provide 100% accuracy with catching malware.

1.4 Machine Learning: Another benchmark towards Cyber-security

Machine Learning (ML) is the skill of a computer to learn skills on its own and adapt techniques through running data and algorithmic codes and drawing patterns. ML is the way that machines learn without programming them to know a certain activity (Mahesh, 2020). This takes place with the help of critical analysis of the data and drawing conclusions from it. It has been observed that ML has provided quick solutions to complex problems of security threats on the internet (Ford et al., 2014). Activities like spam detection, authentication, cryptography etc. can be done using ML. Cyberthreats and ML have a common link of datasets, which becomes an essential part of them being related and being used in a synchronised manner. There has been research on many methods to use ML in Cyber security (Das et al., 2017) and it is observed that it becomes a helping hand many-a-times, however it itself creates a cyber threat. Researchers have conducted their analysis on using some popular Machine Learning techniques on Cyber Security, and identified how each can be useful or not beneficial for controlling cybercrimes. Some of them are provided in Fig 3.

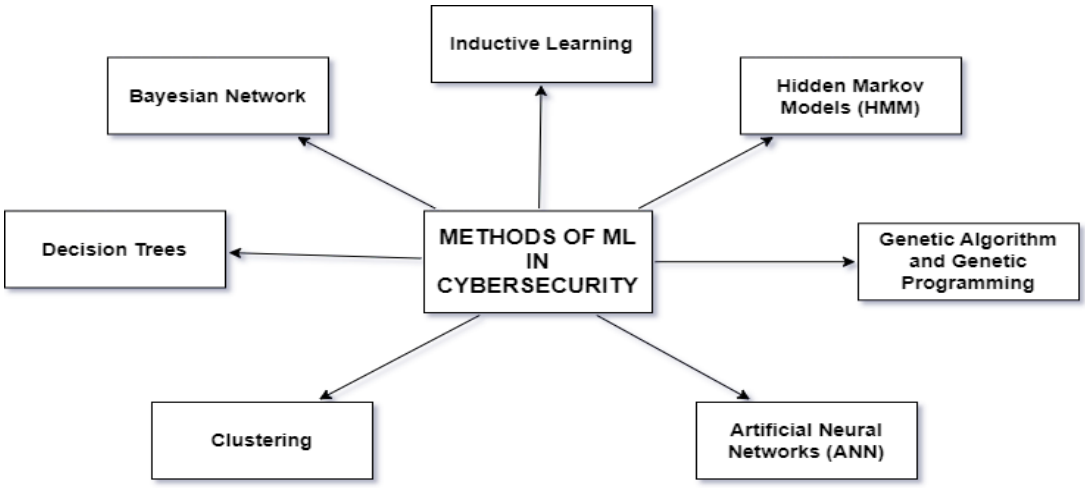

Figure 3: Machine Learning in Cyber security

1.5 Linking AI and ML

Machine Learning is the essence of Artificial Intelligence. A machine can't be programmed to gain its intelligence, the machine can learn on its own without being programmed. As mentioned above, various ML techniques can be deployed to control malicious activities on the internet. ML techniques have shown that AI can be threatening and become a cause for cybercrime. Similarly, ML has the potential to use "unusable data as a weapon" (Laato et al., 2020) which is why the data is the king. While the internet runs on data, it becomes crucial to keep it safe to avoid bad effects of ML and further on, AI.

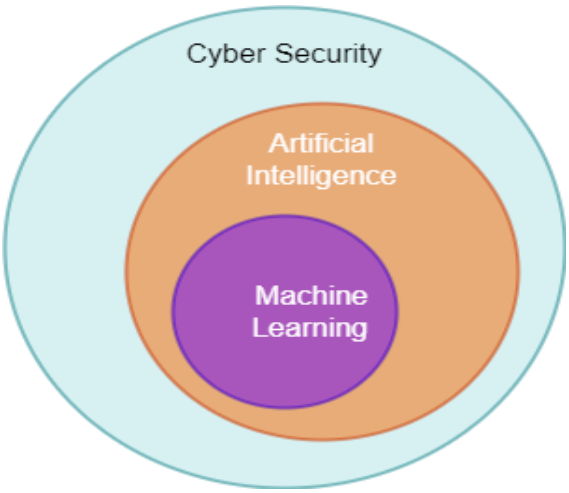

Figure 4: Linking Cyber security, AI & ML

This paper will discuss how artificial intelligence is put into use in cyber security. A literature survey will be conducted which would analyse the different forms in which AI is utilised in cyber security, how efficient it is and what are the drawbacks of using it. In the end, the paper will conclude whether the idea of AI included in cybersecurity is wise or alternatives can be found.

2. LITERATURE REVIEW

The research papers on which the literature survey is conducted have been picked up from authentic and official research websites. Some of them are IEEE Xplore, ResearchGate, ScienceDirect, Google Scholar etc.

The citations mentioned are published in either Journals or Conferences to ensure the relevance and authenticity of the content being used in this review paper. This paper has conducted a literature survey on research papers based on AI and Cyber security which have been published in recent years, 2019-2022. In addition to that, it also refers to papers from years before this timeline, to understand the progress of research, and changes in the results from one time frame to another. The literature ranges from the year 2009 to the latest 2022.

To find the relevant research papers, keywords like ("AI" or "Artificial Intelligence", ("Cyber security" or "Cybersecurity)", ("ML" or "Machine Learning"), ("AI and Cybersecurity"), ("ML and cybersecurity"), ("Cyber-attacks"), ("Internet security"). Thorough filtering of research papers was done to make our literature list become highly relevant to the topic of this review paper. Apart from sorting out the papers based on the keywords, timeline and conference/journals, abstracts were read to understand the base of the paper and scale it in order to add it to our pile of literature.

This review paper is based on the impacts of AI on cyber security. In other words, it will suggest how the occurrence of Artificial Intelligence affected the Cyber security field and using AI in cyber security as a solution is a way out for making cybersecurity more powerful than before.

Kumar et al. (2016) stated that artificial intelligence often delights us with major innovations. They have always been employed in a variety of occupations. It made our lives easier and better. The systems' built-in intelligence facilitates work in a variety of industries, military power, healthcare, technology and many more. The difficult tasks have become easier due to artificial intelligence. Additionally, it has helped to tackle the parallelism problem. In the upcoming years, AI will continue to advance. The ethical concerns should be considered while keeping in mind the changes that have occurred in this field. AI related ethical concerns ought to be addressed by writing an automated programmed tool code. It should develop more quickly by adequately testing ethical issues. Maintenance of conscience that would prevent calamities from happening in the future is important.

The phrase "artificial intelligence" has been around since 1956, when it was first used, as stated by Zhou et al. (2019) Artificial intelligence is a method for creating intelligent machines that can perform activities much like humans do. This concept is clearly quite broad and encompasses everything like Apple Siri, Google AlphaGo and much more powerful technologies that haven't even been created yet. To plan, learn, reason, solve problems, information extraction, vision, movement, and control, as well as, to a lesser extent, social competence, and creativity, are typical traits that AI systems exhibit when emulating human intelligence. However, AI development is highly dependent on the data, which can be either locally present, served through the internet (WAN) or a better & secure version, edge computing. Like for human intelligence, its neural system, learning in machines is based on Deep Learning models and each has their own precision and process.

Zeng (2022) stated that cybersecurity threats truly exist in both virtual and physical worlds, assigning significant risk of security to all countries' government, economy, societies, and national defence. Testing the security of network products in cyberspace would exacerbate current security problems, create fresh security dangers, and pose difficult challenges for any national safety. Artificial intelligence enables cyberattacks because as it develops, more data is needed, which in turn increases its demand. That made data the key of everything so as the data is increasing, cyber-attacks are increasing rapidly.

Hartmann et al. (2020) stated that due to their intrinsic stealthy, there were destructive effects on society, and widespread ignorance of Artificial Intelligence and ML accountability, attack paths against the systems are extremely

advantageous for rogue cyber user. The citizens have not yet been exposed to assaults, and the developers of the application are not yet acquainted with the threats posed by the use of AI. Despite the fact that assaults and attacks have already been noticed and are the topic of discussions in tech based and educational circles, they have not yet occurred. The use of AI or ML technologies enhances any application's risk, and it must be highlighted that AI systems are in fact vulnerable to cyberattacks. This calls for more tactful application of AI and ML techniques in security applications. To protect against cyber operations carried out with the help of AI, awareness of the vulnerabilities of AI systems may become essential. With limited current countermeasures available, such operations are being described in initiatives to spread misinformation, information warfare, and hybrid warfare. To maintain cyber sovereignty in the face of political obstacles and the continuous AI weapons race, a thorough understanding of Artificial Intelligence systems susceptibilities is necessary.

Before forming a strategic plan, every government consults with scientists. Most nations collect information from healthcare facilities (such as nursing homes, hospitals, and other social institutions), analyse it using formulas, and then use the results to create AI models that forecast potential development patterns and inform the development of their national strategies. It is now crucial to protect AI. The impact of AI on security is a major issue for the entire planet. Future study in social and natural sciences should also take this into account, as it is important. Security defences are crucial because many operations and services are running through the internet using devices. The outcomes must have sound data governance and security. A global AI security strategy should be given high attention in order to influence governments and their constituents. AI security will aid governments in their efforts to strategically balance politics, social issues, and technological advancements, as commented by Feng et al. (2020).

The term "cyber warfare" was coined in response to the increase in cyberattacks on a large scale, particularly those between governments of different nations. Sevis et al. (2016) mentions that the International legal systems are constantly attempting to provide some guidelines and standards for this form of conflict. Due to the long-term internet vulnerability, it will be very hard to completely protect against cyberattacks, espionage, and sabotage. Therefore, it is essential for the nations that experienced cyberattacks to comprehend their legal rights and get a glance to respond to them lawfully in order to avoid turmoil or perhaps even something worse. In the case of a cyberattack or cyber warfare, there may be some instructions for how the law should be enforced, although they are insufficient and not needed by the international bodies. The new frontier in international law, and particularly in international war law, is cyber warfare law.

The author Ho et al. (2020) stated that the AI technique merely achieves 100% correctness, even for the most straightforward challenge, like MNIST. Additionally, the output of AI is typically inexplicable and is reliant on the training set of data. Cybercrimes typically occur when systems are used, either by careless users or foreign attackers. Network managers may not directly discover these malware-infected hijacked devices because the network environment typically hosts thousands of concurrently running internet services. Device malware that submits to itself without engaging in any activity is typically not discovered until an attack is launched. When a huge number of internet devices are being watched for ambiguous activity between harmless and harmful, it is difficult to identify the compromised devices in order for security to survive. It also states some limitations of artificial intelligence, some of the limitations stated by the author are - Lack of justification, online learning problems and issues that occurs during the updating of the AI model by training a new pattern that could be malicious.

Artificial intelligence is already changing our economy and culture, and the rise in AI decision making has sparked discussion about potential drawbacks and the need for enhanced transparency in AI decision-making. Self-building technologies are feasible even with our current level of technological development. It is also agreeable to create cognitive architectures that accurately mimic truly intelligent human behaviour, including "sentiment, motivation, charisma and other key qualities". The author, Radanliev et al. (2021) mentions that AI plays a major role in the security of Cyber-physical systems as it works to find drawbacks in the communication network. These systems work on huge data and this transfer of data is made secure using AI as it is programmed to detect any malicious activity which can be prevented.

In addition to the defence institutes around the world, the change to cyber operations represents a shift in cyber security research and teaching, said the author, Kallberg et al. (2012). Information assurance, as articulated in supporting domains like forensics, network security, and penetration testing, has historically served as the foundation for cyber security research and teaching. In the future of cyber security, both defensive data protection measures and engaged defence driven information operations will be used to execute the national cyber defence plan in a coordinated and

integrated manner. The National Security Agency (NSA) is very clear that cyber operations should be multidisciplinary, initially focusing on technical schools, but as time goes on, and the military of cyberspace will broaden the scope of collaboration. If the society is the target of a cyberattack, the country can be defended using advanced technology, but it will also become possible to reduce cyber vulnerabilities in societal behaviour, economic model, and institutional structures with the aid of other sciences. The ability to perform collection, exploitation, and response is necessary for cyber operations. Academic institutions train the personnel that will oversee the implementation, will manage and surveillance of cyber activities.

Both Artificial intelligence and Cyber Security are important for one of the widely used greatest innovations that is social media as argued by the author, Thuraisingham (2020). There are so many benefits as well as security threats of Artificial Intelligence. Over a billion people are connected through social media platforms like Facebook and Twitter, allowing them to converse and exchange information both among themselves and within a group of people. By spreading information about infectious diseases and proposing solutions to problems like ending child trafficking and violence against women, these social media networks could be of enormous use to humanity. Social media platforms may hurt people, though, by spreading misleading news and invading their privacy, among other things. The way social media platforms operate is changing due to the expansion of artificial intelligence (AI) technologies, strong machine learning techniques, and cyberattacks on information systems. Malicious malware may be used to assault social media platforms. Cyber Security and AI are just beginning to play a role in social media networks. Cyber Attacks on computer security and invasions of privacy complicate the issue of deploying Artificial intelligence.

The author Xue et al. (2009), explained the concept, importance, and primary approach of machine learning, as well as the fundamental components of a machine learning system. Many efforts have gone into developing new machine learning methodologies, including Rote learning, learning based on explanation, Instruction learning, deduction Learning and Inductive learning, among many others. Each of these techniques have their advantages and disadvantages, simplicity and complexity and Machine learning is indeed a fundamental method for giving computers intelligence. Its application, which primarily relies on synthesis and induction rather than deduction, has already penetrated a wide range of artificial intelligence fields.

According to the author Li et al. (2022), intelligence has emerged as both a new societal development and a new aspect of the advancement of information technology in recent years. Many smart products and devices like smart homes, robots, toys that are smart, and smart buildings have emerged with the quick development of technologies like artificial intelligence, the Internet of Things, big data, and cloud computing. These advancements have significantly changed how people live and go about their daily lives. The author develops an information-based English learning platform that can significantly increase the effectiveness of English learning in the conventional textbook mode and foster college students' interest and enthusiasm for learning the language through research constructively on different artificial intelligence algorithms. The informatization of a constructive English learning platform, which places the student at the centre and offers learning resources and methods, focuses on creating an ecological environment for autonomous learning by students, which can significantly improve students' ability to learn independently. It also respects and encourages the students as they actively construct their autonomous learning awareness.

Instances show that cyber threat intelligence is a valuable component of defensive security and cyber defence, concluded by the author Haass (2022). Today, automated techniques are required to keep up with the scope of attacks worldwide. If threat information is to be swallowed into computer-operated defence systems, it must be actionable, current, and credibly authenticated. False positives reduce the system's value. The problems of using machine learning to improve the flow of threat intelligence are the points discussed by the author along with some of the advancements made in the application of AI techniques. The development of learning models that can be combined with firewalls, rules, and heuristics has used a number of different techniques. Additionally, more work is required to efficiently support the few professional human hours available to assess the threat landscape that has been marked as dangerous in some kind of a SOC (Security Operations Centre) setting.

Gatti et al. (2019) stated that in addition to outlining the difficulties involved, there are three fundamental building blocks of any avionics platform of the future. Avionic systems are basically electronic systems. The term "Avionics Platform" refers to, firstly, all embedded systems necessary for an aircraft to operate (whether it be a commercial, fighter, transport, drone, or flying cab), and secondly, all embedded critical and less vital functions necessary for operating (flight command control, locomotion management, fuel economy, anti-icing, TCAS, TAWS, etc.), piloting,

utilities (slides and door, air conditioning, toilets etc.), maintenance and connectivity. The three pillars and key issues confronted in avionics are AI, Connectivity, and Cyber-Security.

The time now is one of fast progress. The author, Han (2021) stated that China's criteria and requirements for the advancement of internet-based information technology have increased as a result of the country's ongoing economic growth. This social environment served as the foundation for "artificial intelligence" to emerge. Additionally, artificial intelligence has improved the quality of our lives, made the globe a better place to live, and made the use of technology for computer networks more practical. People start pursuing a greater quality of life as the requirements of the social majority also continue to improve. Computer network technology slowly enters our lives as a type of high and innovative technology, becoming increasingly integrated into people's daily lives and developing into a sophisticated industry in the modern period. Through the conversation of artificial intelligence, the author demonstrated how modern artificial intelligence technology is applied to computer network technology. By doing so, readers will gain a better understanding of how artificial intelligence is used in computer network management, network security, categorisation and recognition services, and other areas.

Over the past ten years, particularly in relation to smart grids, cyber dangers have significantly increased. Author Hasan et al. (2019) are convinced that cybercriminals have improved their skills. Similar work has been done by Saraswat A. et al. (2020) and Sarita et al. (2022). Since there are so many highly experienced cybercriminals, networks cannot be protected with the current security procedures. Advanced Persistent Threat (APT) is virtually undetectable by current tools, and cybercriminals have mastered the art of dodging even the most complex techniques, like (IDPS) Intrusion Detection and Prevention Systems. (IDPS). Fortunately, the use of AI technology (AI) may boost IDPS systems' detection rates, and machine learning (ML) algorithms can mine data to identify various APT assault stages. Cybersecurity specialists must achieve a balance between threat and advantages because the introduction of artificial intelligence may bring additional concerns.

Table 1: Overview of Reviewed Sources

Serial No.	Author	Technology Used
1	Kumar, N. et. al	Lethal Autonomous Weapons Systems (LAWS)
2	Zhou, Z. et. al	Deep Learning Models & Machine Neural Networks
3	Zeng, Y.	AI Network Attack and Defense Technology
4	Hartmann, K., & Steup, C.	Attack Vector Techniques
5	Feng, X. et. al	ROS Cyber Security, DP3T –Decentralized Privacy-Preserving Proximity Tracing Tool
6	Sevis, K. N., & Seker, E.	Cyber Warfare Law
7	Ho, T. Y. et. al	Malicious behavior of AI and Malicious Levels
8	Radanliev, P. et. al	Anomaly Detection in Communication Channels
9	Kallberg, J., & Thuraisingham, B.	Survey on Cyber operations in CAE-R Academic Research centers
10	Thuraisingham, B.	Sentiment Detection and ML Techniques in Social Media
11	Xue, M., & Zhu, C.	Machine Learning System
12	T. Li & X. Zou.	English Learning with AI
13	Haass, J. C.	Cyber threat intelligence
14	Gatti, M., & Damien, A.	Avionic Control System

15	Han, Z.	Modern Artificial Intelligence Technology is applied to Computer Network Technology.
16	Hasan, K. et. al	Advanced Persistent Threat (APT) is virtually undetectable by current tools

3. DISCUSSION

3.1 Key findings

This paper conducted a literature survey about two major headings: cyber security and artificial intelligence. It could be concluded about their linkage and the bridge that is joining both artificial intelligence and cyber security together and how each one is beneficial or problematic for each other.

The following conclusions were derived through this survey.

- Uses and limitations of Artificial intelligence
- AI is a futuristic need to help out the human race but as the progress rate increased, the stronger drawbacks are getting their roots nourished.
- Artificial intelligence became a basic need from a future asset.
- Improvement in cyber defence by creating patterns for APT control machine learning is possible.

3.2 Limitations

Artificial Intelligence is developing at a very fast pace. As AI became an emerging hot topic, paradox situations and problems started arising. Cyber-attacks, which are the main problem that every person is currently facing, are the most hazardous of all the issues caused by artificial intelligence. AI is the reason for the occurrence of Cyber Crime over the web. Cyber-attacks cause great damage to both government and private bodies, become a source for international wars and personal privacy threats. Different viruses came into action and many new ones are still developing and the process continues. Hence, even after being the liability and becoming the cause of Cyber Crime, AI with the help of its helping tools like ML, Data, Automation can become assets as well with a proficient compilation of them in order to beat cyber-attacks.

4. CONCLUSION

Summarising all the above findings, it can be concluded that Artificial Intelligence is the key of development and a futuristic approach that can be used to replace the hard work and man-power used by humans in the current era. It can develop furthermore and is developing day by day. Every new development is giving a helping hand to humans by Machine Intelligence.

Machines can replace mankind's work in the near future with the help of AI but as it is developing, everything has a consequence. Artificial intelligence has some major drawbacks like cyber-attacks, viruses, malware, cyber wars and so many other things. The most brutal of all are Cyber Attacks, which are the roots to all above mentioned drawbacks, and are happening at a rapid rate. Artificial Intelligence gave birth to Cyber Attacks due to which a new term came into action that is Cyber Security.

Skilled crimes as APT while currently being undetectable can be prevented using highly advanced artificial intelligence technology like data mining & complex machine learning models. And these programs can be used to secure cyber networks from loopholes that become the cause for these attacks. Hence, it can be concluded that Artificial Intelligence is yet in its development stage as it is bound to grow. Hence, the defence needs to be strong as the need for Cyber Security increases.

To conclude, the linkage of Cyber Security and Artificial Intelligence is that they work side by side to give a secured environment for work to the user in the internet world. In addition to this, it was learned how to secure our device or organisation from cyber-attacks.

REFERENCES

Anand, G., & Saraswat, A. (2022). Profitability Visualization in Catalog Management System. *2022 ECS Trans. 107 10693*. https://doi.org/10.1149/10701.10693ecst.

Das, R., & Morris, T. H. (2017). Machine Learning and Cyber Security. 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), 1–7. doi:10.1109/ICCECE.2017.8526232

Feng, X., Feng, Y., & Dawam, E. S. (2020, August). Artificial Intelligence Cyber Security Strategy. *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp.328-333). doi:10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00064

Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. *Proceedings of the 27th international conference on computer applications in industry and engineering* (Vol. 118). https://vford.me/papers/Ford%20Siraj%20Machine%20Learning%20in%20Cyber%20Security%20final%20manuscript.pdf

Gatti, M., & Damien, A. (2019, September). AI, connectivity and cyber-security in avionics. *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 35-38). doi: 10.1109/ETFA.2019.8869381

Haass, J. C. (2022, September). Cyber Threat Intelligence and Machine Learning. In *2022 Fourth International Conference on Transdisciplinary AI (TransAI)* (pp. 156-159). doi: 10.1109/TransAI54797.2022.00033

Han, Z. (2021, October). The application of artificial intelligence in computer network technology. *In 2021 2nd International Seminar on Artificial Intelligence, Networking, and Information Technology (AINIT)* (pp. 632-635). doi: 10.1109/AINIT54228.2021.00127

Hasan, K., Shetty, S., & Ullah, S. (2019, December). Artificial intelligence empowered cyber threat detection. and protection for power utilities. *In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 354-359). doi: 10.1109/CIC48465.2019.00049

Ho, T. Y., Chen, W. A., & Huang, C. Y. (2020, December). The Burden of Artificial Intelligence on Internal Security Detection. *In 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)* (pp. 148-150). doi: 10.1109/HONET50430.2020.9322823

Hartmann, K., & Steup, C. (2020, May). Hacking the AI-the Next Generation of Hijacked Systems. *In 2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 327-349). doi: 10.23919/CyCon49761.2020.9131724

Kumar, N., Kharkwal, N., Kohli, R., & Choudhary, S. (2016, February). Ethical aspects and future of artificial intelligence. *In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (pp. 111-114). doi: 10.1109/ICICCS.2016.7542339

Kallberg, J., & Thuraisingham, B. (2012, June). Towards cyber operations-The new role of academic cyber security research and education. *In 2012 IEEE International Conference on Intelligence and Security Informatics* (pp. 132-134). doi: 10.1109/ISI.2012.6284146

Li, Y., & Liu, Q. (2021, November). A comprehensive review study of cyber-attacks and cyber security. Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, T., & Zou, X. (2022, June). Informatization of Constructive English Learning Platform Based on Artificial Intelligence Algorithm. *In 2022 International Conference on Frontiers of Artificial Intelligence and Machine Learning (FAIML)* (pp. 71-74). doi: 10.1109/FAIML57028.2022.00023

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020, July). AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs. *In 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 6-10). doi: 10.1109/ICALT49669.2020.00009

Mohammed, I. A. (2020). Artificial Intelligence For Cybersecurity: A Systematic Mapping Of Literature. *International Journal Of Innovations In Engineering Research And Technology [IJIERT]*, 7(9).

Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).* [Internet], 9, 381-386. doi: 10.21275/ART20203995

Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. (2021). Artificial intelligence in cyber physical systems. *AI & society*, 36(3), 783-796. https://doi.org/10.1007/s00146-020-01049-0

Saraswat, A., & Gupta, K. (2013, September). Simulation of Endpoint Based Call Admission Control Using Retransmission Timer. In *2013 5th International Conference and Computational Intelligence and Communication Networks* (pp. 220-224). IEEE. doi: 10.1109/CICN.2013.53.

Saraswat A., & Kalra B. Safe engineering application for detection of medical image using deep convolutional. neural network. *Journal of Green Engineering*, *2020*, 10(11), pp. 12523–12535

Saraswat, A., & Sharma, N. (2022). Bypassing Confines of Feature Extraction in Brain Tumor Retrieval via MR Images. *CBIR. ECS Transactions*, 107(1), 3675. doi: 10.1149/10701.3675ecst.

Saraswat, A., & Sharma, N. (2022). Salvaging tumor from T1-weighted CE-MR images using automatic segmentation techniques. *International Journal of Information Technology*, 14(4), 1869-1874. doi: 10.1007/s41870-022-00953-6.

Sarita, Mukherjee, S., Choudhury, T., Kulshrestha, K., Singh, R., Diagnosing Alzheimer's Disease using Convolution Neural Networks, *Journal of Computer Science*, *2022*, 18(2), pp. 67–77

Sarita, Mukherjee, S., & Choudhury, T. (2020). An Android-Based Mobile Application to Help Alzheimer's Patients. In *Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018* (pp. 889-904). Springer Singapore.

Sarita, Mukherjee, S., Sharma, A., A review paper on cognitive neuroscience, Communication and Computing Systems. *Proceedings of the International Conference on Communication and Computing Systems, ICCCS 2016, 2017*, pp. 1065–1070.

Sevis, K. N., & Seker, E. (2016, June). Cyber warfare: terms, issues, laws and controversies. In *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)* (pp. 1-9). doi: 10.1109/CyberSecPODS.2016.7502348

Thuraisingham, B. (2020, May). The role of artificial intelligence and cyber security for social media. *In 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)* (pp. 1-3). doi: 10.1109/IPDPSW50202.2020.00184

Xue, M., & Zhu, C. (2009, April). A study and application on machine learning of artificial intelligence. In *2009 International Joint Conference on Artificial Intelligence* (pp. 272-274). doi: 10.1109/JCAI.2009.55

Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE*, 107(8), 1738-1762. doi: 10.1109/JPROC.2019.2918951

Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science*, 208, 170-175. https://doi.org/10.1016/j.procs.2022.10.025