*Article*

# The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML)

Hrishitva Patel
School of Management Acad, PO Box 6000, Binghamton, New York 139026000
hpatel51@binghamton.edu

## Table of Contents

Abstract ..... 1
Introduction ..... 1
Role of Artificial Intelligence in Cyber Security ..... 2
AI and ML within Cybersecurity ..... 2
Using AI for Cyber security ..... 3
Benefits of Using AI in Cybersecurity ..... 5
What AI and ML can do to improve cybersecurity .....**Error! Bookmark not defined.**
How AI is used in Cybersecurity ..... 7
How Machine Learning is used in Cybersecurity ..... 7
Data Privacy Classification and Compliance ..... 8
Future of Cybersecurity ..... 9
Conclusion ..... 9
References ..... 10

*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1

## Abstract

Although, Artificial intelligence (AI) helps experts with crime analysis, research, and understanding, it has a favourable influence on cyber security. It strengthens the tools that businesses use to safeguard their networks, clients, and workers against dangerous online behaviour. However, artificial intelligence is infamous for requiring a lot of resources. It may not, however, always be relevant. Additionally, it can provide hackers a new tool and advance their abilities. Actually, the VPN industry benefits from AI in the same way. The threat posed by machine learning in AI to user data privacy may be lessened by using a VPN on all of your devices. Because they use machine learning algorithms, VPNs are better equipped to shield their users from internet-based threats. Artificial intelligence (AI) has reportedly being investigated as a means of enhancing internet security for a considerable amount of time, according to Smart Data Collective. We anticipated that AI and machine learning will have a substantial impact on the future of cyber security around two years ago.

**Keywords:** Artificial Intelligence (AI); Machine Learning (ML); Cyber security; Uses of Cyber security; Future in Cyber security; AI and ML in Cyber security

## Introduction

The term "AI for Cybersecurity" refers to protective measures for computer networks that make use of artificial intelligence (AI) and machine learning (ML). The rise in prevalence of Internet-connected services and the trend toward working from home has brought with it an increased risk of physical violence. It is becoming an increasingly archaic strategy to fight against these assaults by using signatures or other antiquated methods. Because it takes too much time to notice and halt a danger after noticing it or to wait for someone else to report it, organizations are left vulnerable to attack because of this situation. During this time period, advancements are made in artificial intelligence. In order to defeat the many, complicated, and ever-evolving dangers, defense systems need to be able to identify and respond to dangers as they occur. In addition, it is feasible to make advantage of the "edge" of the system, also known as the endpoint. At this stage, getting rid of humans accelerates the process since AI can swiftly search through millions of data sets for any potential danger. Even without looking for particular software fingerprints associated with recognized threats, it may be able to recognize behaviours associated with malware, phishing, and "crypto-jacking," which is a kind of cybercrime in which compromised computers are instructed to mine bitcoin on behalf of the hacker. In the event that any of these flaws are discovered, AI may put this information to use to strengthen its defenses and protect the safety of humanity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



# Role of Artificial Intelligence in Cyber Security

## ➢ Artificial Intelligence

Artificial intelligence enables the design of a computer, computer-controlled robot, or piece of software to mimic human intellect. AI is developed via the study of human cognition, which includes how individuals learn, make choices, and approach problems. This study will help to shape the creation of AI-powered software and hardware. Intelligence is often defined as the capacity to absorb new information and apply it to the solving of complicated problems. Intelligent robots may be able to do many of the tasks presently performed by humans in the future. Artificial intelligence is concerned with the development and implementation of intelligent technologies and computer programmes with cognitive abilities equivalent to those of humans. Artificial intelligence differs from both psychology and computer science. It differs from psychology in that it focuses on perception, thinking, and action, while computer science focuses on perception, mind, and action. This encourages machine learning, which improves capabilities.

## ➢ The emergence of AI in cyber security

Increases in computing power, data gathering, and storage have resulted in a rise in commercial and industrial applications of machine learning and artificial intelligence. AI thrives on this abundance of data since it allows it to analyze and scrutinize everything acquired in order to uncover new patterns and subtle nuances. Further attacks may be avoided if new initiatives and issues are identified and investigated as soon as possible. It may make the task of security "partners" easier. They are told what to do and when to do it, but they are free to pursue other, maybe more rewarding pursuits if they so wish. Consider which of your team members has the most security-related experience. If you utilize it to train your machine learning and artificial intelligence programmes, they will eventually become as smart as your star employee. Prepare your machine learning and AI programmes with your 10 brightest staff, and the results will be as clever as all of them together. Furthermore, AI is never idle.

# AI and ML within Cybersecurity

AI cybersecurity will soon be a strong weapon as a consequence of machine learning. People remain the most valuable and irreplaceable asset in security, as they are everywhere. At the moment, cybersecurity is mostly dependent on humans, but robots are rapidly developing the capacity to perform crucial tasks. The more advanced our technology becomes, the more it can help workers with their daily tasks. Several scientific areas provide the basis for these shifts:

- The goal of **Artificial Intelligence (AI)** research is to develop computer systems capable of performing cognitive tasks on par with the human brain. This is a broad area that covers subfields such as machine learning and deep learning.

- The utilization of previously observed behavioural patterns to draw inferences and forecast the future is a critical part of **Machine Learning (ML).** People must still make some changes. Machine learning has proven to be the most prominent area of artificial intelligence-based cyber defense to date.

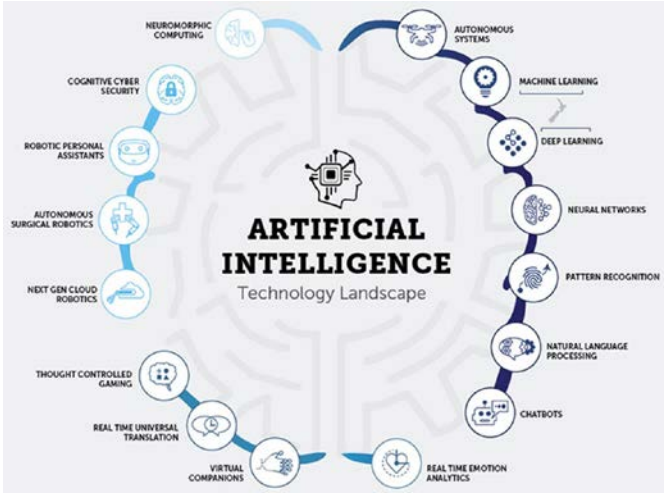
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



| Artificial Intelligence | Machine Learning |
|---|---|
| AI stands for Artificial intelligence, where intelligence is defined acquisition of knowledge intelligence is defined as a ability to acquire and apply knowledge. | ML stands for Machine Learning which is defined as the acquisition of knowledge or skill |
| The aim is to increase chance of success and not accuracy. | The aim is to increase accuracy, but it does not care about success |
| It work as a computer program that does smart work | It is a simple concept machine takes data and learn from data. |
| The goal is to simulate natural intelligence to solve complex problem | The goal is to learn from data on certain task to maximize the performance of machine on this task. |
| AI is decision making. | ML allows system to learn new things from data. |
| It leads to develop a system to mimic human to respond behave in a circumstances. | It involves in creating self learning algorithms. |
| AI will go for finding the optimal solution. | ML will go for only solution for that whether it is optimal or not. |
| AI leads to intelligence or wisdom. | ML leads to knowledge. |

## Using AI for Cyber security

Several areas of cybersecurity might benefit from AI's various features, including deep learning and unsupervised learning. Artificial intelligence (AI) can automatically analyze and fix vast volumes of potentially dangerous data and identify future problems. Unfortunately, threat actors may use the same AI technologies that are deployed to secure systems as a backdoor to compromise the targets' systems. A growing number of attacks are leveraging AI-powered technology, and malware is often altering its appearance to evade detection. To further their attacks, they use machinery that can generate large quantities of malware. AI and malware might be used by hackers to assess the target company's defenses and plan future attacks.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



### 1. Human Error in Configuration

Human error is the primary cause of poor cybersecurity. Even with a large IT staff, managing the process of creating the perfect system configuration, for example, may be tough. The fast adoption of new technologies has made computer security more difficult than ever. When network infrastructure is upgraded, repurposed, or otherwise updated, teams may use flexible technologies to detect and resolve issues that arise. Consider the possibility of building contemporary Internet infrastructure, such as cloud computing, on top of more conventional regional networks. To ensure the security of the company's data, the IT department must ensure that all systems are compatible. When teams must manually analyze the security of installations in addition to keeping up with the many upgrades that must be deployed and the numerous daily support chores, they get overwhelmed. Because of clever, flexible automation, the team may get assistance as soon as a new issue is recognized. They may get recommendations for future activities or have systems that make changes automatically.

### 2. Human Efficiency with Repeated Activities

Another common issue in the cybersecurity sector is insufficient cooperation. It would be impossible to accurately duplicate a manual process in our fast-paced society. Setting up the equipment at each endpoint is one of the most time-consuming processes for any organization. IT staff must return to previously configured computers since misconfigurations and out-of-date settings cannot be corrected remotely. Furthermore, when individuals are tasked with reducing the danger, the degree of the threat might vary quickly. Unexpected impediments may break human attention, but a system built on AI and machine learning can respond rapidly.

### 3. Threat Alert Fatigue

Inability to handle danger warning fatigue correctly may be a cause of organizational risk. Exploitable entry points have risen as a result of the aforementioned proliferation and complexity of security layers. Many security systems are designed to flood administrators with notifications as soon as any of a number of common threats is detected. As a result, it is up to human teams to make sense of the myriad options presented by these autonomous impulses and to take appropriate action. Making judgements at this level is famously tough due to the massive amount of notifications. For cybersecurity experts, decision fatigue is a big source of worry. Although it is preferable to address these issues before they arise, many teams lack the resources to do so. It is common for teams to prioritize resolving huge issues above completing minor ones. More cybersecurity teams that utilize artificial intelligence to battle these attacks may be more productive and effective. Automated labelling may make group management of these hazards easier. However, the machine learning approach may be able to address additional issues individually.

### 4. Threat Response Time

The response time of a security team to a threat is an important performance parameter. Harmful assaults may happen swiftly, from discovery to distribution. Previously, attackers had to spend days or weeks dodging security measures and researching network permissions before launching an assault. Innovative technologies have the potential to assist more than only cybersecurity specialists. Cyber-attacks have gotten more automated since then. This is especially true with current LockBit ransom ware assaults and other types of malware, which have significantly reduced the period of typical attack windows. The current assault frequency ranges between every hour and every half hour. Even if the kind of attack is recognized, a human reaction may occur after the first assault. As a result, many organizations have prioritized reacting to attacks after they

 doi:10.20944/preprints202301.0115.v1



have occurred rather than preventing them. Attacks that are not documented, on the other hand, pose a risk in and of it. Security systems can swiftly acquire, organize, and analyze attack data by using machine learning to assist in incident response. When cybersecurity teams have more digestible and useable data, they have an advantage in processing and decision-making. This level of protection goes beyond just documenting incidents. It might also provide advice on how to prevent and minimize such assaults.

### 5. New Threat Identification and Prediction

The frequency at which new cyber threats are found and forecasted influences the time necessary to respond to an assault. It has been stated that there is already a lag in terms of current hazards. Teams may be hampered much more by attack patterns, behaviours, and instruments that they are unaware of. Data theft, for example, is a sneaky problem that frequently goes undiscovered. According to an April 2020 research, 84% of IT departments are concerned that their cloud-based systems may be compromised without their awareness. Adaptive attacks that take advantage of zero-day vulnerabilities are a recurring source of network security issues. The good news is that new types of cyber-attacks are seldom conceived from the ground up. Machine learning has a route to follow due to the prevalent practice of basing assaults on the behaviours, frameworks, and source codes of previous attacks. Similarities between a newly found danger and previously known threats may be highlighted using ML-based programming. This might aid in the detection of an assault. The fact that this is a task that people are incapable of doing well emphasizes the need for adaptive security solutions. Machine learning may improve danger prediction and reduce response times by raising team knowledge of potential risks.

### 6. Staffing capacity

Human resources shortages are a recurring issue for IT and cybersecurity organizations throughout the globe. There may not be a sufficient number of qualified personnel available to meet a company's demands. Firms, on the other hand, may be forced to pay large wages to their employees. To keep human workers, you must compensate them for their constant efforts and satisfy their continuing training and certification requirements. As discussed throughout this article, new products are always being developed, making it difficult for a cybersecurity expert to keep current. Intelligent security systems need less labour for operation and maintenance. The reduced employee required will result in a net savings of both time and money, but the remaining staff will need to stay current on AI and ML advances.

### 7. Adaptability

Adaptability may not seem to be directly relevant to a company's security, but if handled properly, it may have a significant impact. Human teams may lack the flexibility required to meet your individual requirements. A team's performance may be hampered if its members lack competency in the utilization of certain resources. Even seemingly basic procedures, such as implementing new security standards, may take a long time when performed by human teams. This is how people work since it takes time to develop new skills. With enough data and a well-trained algorithm, you may create a custom solution from scratch.

## Benefits of Using AI in Cybersecurity

The purpose of AI research is to create a system with human-like intelligence. It has the potential to be used in cyber security. AI technologies, when used correctly, have the potential to serve as early warning systems,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



malware detectors, and data guardians for organizations. AI is the most effective way for a company to stay safe and lucrative in the digital era. Security professionals need significant assistance from intelligent machines and cutting-edge technology such as AI to do their tasks efficiently and safeguard their organizations from cyber assaults. The benefits of applying AI in this industry are explored.

### i. AI Learns More over Time

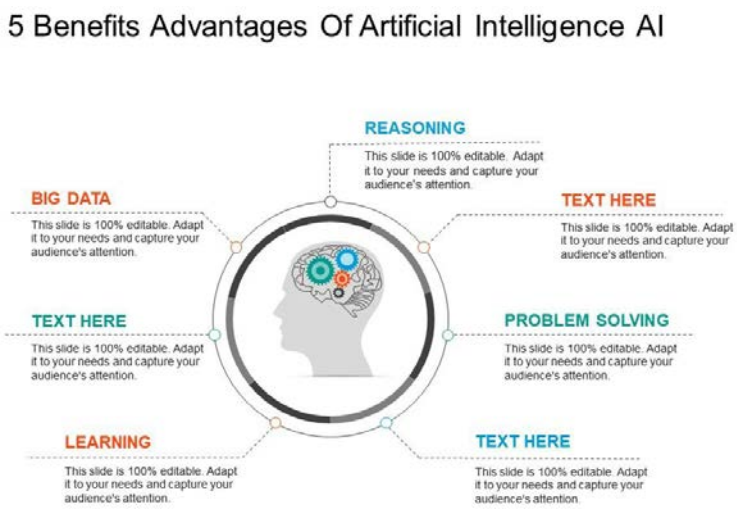
Self-learning artificial intelligence (AI) has the potential to improve network security in the long term. In order to detect and categorize network patterns, AI uses machine learning and deep learning algorithms. Then, it will keep an eye out for anything out of the norm in terms of security and take necessary action. These kinds of trends may assist to make the world a safer place in the future. Such dangers may be identified and eliminated in a timely way. Hackers are seldom successful against their intelligence since it is always evolving.

### ii. Artificial Intelligence Identifies Unknown Threats

There is a chance that no one individual can see every risk that their company confronts. Hackers may start an attack for a variety of causes and approaches. Unknown threats of this kind have the potential to inflict significant harm to a network. In terms of recognizing and mitigating previously unforeseen business threats from causing havoc, AI outperforms humans.

### iii. AI Can Handle a Lot of Data

Even when there is a large amount of data to analyze, artificial intelligence can detect potential hazards. Within and outside of an organization, people are always talking and exchanging ideas. This data must be protected against harmful humans and computer programmes. However, cybersecurity specialists' ability to evaluate all data for dangers is limited. In this circumstance, artificial intelligence is the most effective approach since it can identify any concealed threats in the traffic.



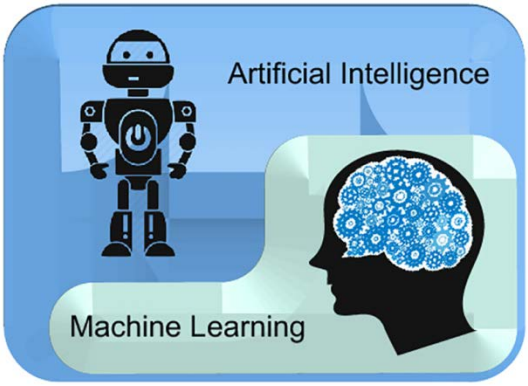

## What AI and ML can do to improve cybersecurity

It has been stated that revolutionary artificial intelligence and cyber security are closer than we believe. However, don't place too much faith in this since it only tells half the story. Significant changes may take

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



some time. In the grand scheme of things, what may seem to be a gradual progress toward a totally autonomous future is a significant advancement over what we were able to do in the past. As we consider the potential impacts of security on machine learning and artificial intelligence, it is critical that we solve the most pressing cybersecurity issues. Many of the objects and procedures that we take for granted on a daily basis may be studied using AI technology.




## How AI is used in Cybersecurity

Although machine learning and deep learning are important in cybersecurity, artificial intelligence is as important. The basic goal of artificial intelligence is "success," whereas "accuracy" is secondary. The purpose of handling difficult issues is to find intuitive answers. Decisions are made automatically in a real-world AI application. It seeks the most optimal solution to a problem rather than merely the one that follows logically from the available facts. To provide a more detailed explanation, it is necessary to first grasp the present state of AI and the subfields that feed into it. Highly mobile systems, particularly in the sphere of cybersecurity, seldom incorporate autonomous systems. The bulk of AI concepts revolve on fully autonomous systems. However, it is doable, and there are currently AI systems in place that might aid or supplement our security services. The nature of the patterns revealed by machine learning algorithms is an ideal cybersecurity task for artificial intelligence. Clearly, AI cannot interpret data as effectively as humans can. Despite efforts to shift the field toward more human-like frameworks, full artificial intelligence (AI) is still a long way off since it needs computers to apply abstract concepts in a range of situations. Artificial intelligence is not quite as sophisticated as some would have you believe in terms of creative and critical thinking.

## How Machine Learning is used in Cybersecurity

However, the public's perception of AI and machine learning-powered security solutions is significantly different. They are, nevertheless, the most effective artificial intelligence (AI) security solutions now available. This approach indicates the likelihood of an event using a series of data patterns. ML might be regarded the polar opposite of true AI. Machine learning is more crucial than success in order to obtain high levels of accuracy. This demonstrates that ML can learn from task-specific datasets. The technique closes by determining the most effective approach to do the specified assignment. Even if it is not the optimal option, it will pursue the one that makes the most sense given the facts provided. Because machine learning does not provide a means for comprehending data meaning, humans must continue to perform this function. Learning machines excel at activities that need repetition, such as pattern recognition and data adaptation. People are unsuitable for these vocations because they become bored easily and have a poor tolerance for monotony. As

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



a result, humans are still necessary to make sense of data analysis, but machine learning may aid in making the results more understandable.
Each of the many applications of machine learning in cybersecurity has specific advantages.

- Data Classifying

Data classification entails categorizing records based on predefined criteria. Identifying these locations is a vital step in developing a profile of threats, vulnerabilities, and other proactive security components. This is an important component of the connection between machine learning and cyber security.

- Data Clustering

In data clustering, data that does not conform to a set of criteria is grouped with data that has similar or unusual characteristics. For example, this may be used to analyze data about unskilled assaults. These data sets may be used to get a greater comprehension of what was attacked, how it was attacked, and what was left vulnerable.

- Recommended Courses of Action

The following approaches are offered to boost an ML security system's proactive operations. This is advice that takes previous choices into account and acts on them. They provide plausible courses of action. It bears repeating that this is not intelligent, self-operating artificial intelligence. It is, instead, an adaptable framework for generating conclusions that may use current data to identify causal linkages. This kind of device might be quite useful in dealing with hazards and reducing risks.

- Predictive Forecasting

Predictive forecasting is the most futuristic machine learning approach. This advantage is acquired through using previous data to forecast future events. This is an important component of many endpoint prediction systems, and it is often used for fraud and data breach prevention, as well as risk modeling.

## Data Privacy Classification and Compliance

It is perhaps more important than ever before for your company to comply with all applicable privacy regulations. California's Consumer Protection Act (CCPA) is modeled after the EU's General Data Protection Regulation (GDPR). To comply with these standards, you must appropriately maintain information and make it simple for customers and users to have their data removed upon request. If you violate these guidelines, your company may face severe fines as well as a loss of customer trust. You may use data categorization to determine if a set of data can be utilized to uniquely identify a person. This is particularly useful for larger or more established organizations since it eliminates the need to manually search through massive amounts of data.

- User Behavior Security Profiles

Creating personalized profiles of network personnel based on user behaviour allows you to tailor network security to the specific needs of your organization. Based on how individuals act when they breach the rules,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2023 doi:10.20944/preprints202301.0115.v1



this model may then be used to extrapolate what an unauthorized user could look like. Developing a threat model may need the use of information such as a person's typing style. With an understanding of the potential consequences of an unauthorized user's behaviour, ML security may offer strategies to limit the number of access points.

### ➢ System Performance Security Profiles

The optimal health of a computer, like a profile of a person's behaviour, permits the creation of a diagnostic profile that provides insight into the system's operation. Monitoring system resources such as CPU and RAM use, as well as other metrics such as network traffic, may aid in the detection of malicious activity. However, some users may consume a significant quantity of data on a regular basis due to activities such as video chatting and downloading several huge media files. It is possible to understand a system's expected behaviour by becoming familiar with its baseline performance. This is similar to the user behaviour criterion we discussed in the last ML example.

### ➢ Behavior-Based Bot Blocking

A website's available bandwidth may be depleted due to human or automated usage. Those whose only source of income is web traffic, such as online shops, should take this warning carefully. The website may be sluggish for heavy users, resulting in a drop in traffic and missed revenue prospects. Machine learning security solutions may prevent bots from accessing the internet by labelling their behaviours, even if the bots use privacy preservation techniques such as VPNs. A machine learning security tool may leverage information about harmful actors' online conduct to build prediction models, which may then be used to blacklist websites displaying the same suspicious behaviour.

## Future of Cybersecurity

Despite the optimistic predictions for the future of this kind of safety, there are several crucial factors to consider. Datasets are required for machine learning (ML), however privacy rules may provide a difficulty. The "right to be forgotten" clashes with the need for large data sets in order for software systems to make accurate predictions. Corrective steps will be required due to the likelihood of data breaches involving personal identifiers. One potential solution would be to make accessing the raw data needed to train the programme very difficult. Another way is to anonymize data points; however this requires extra effort to ensure that it does not impair the program's logic. Experts in AI and ML security who are comfortable with this kind of programming are in high demand. Machine learning-based network security would be significantly more effective if humans were in charge of making updates and modifications. However, the global demand for those who can deliver these answers far outnumbers the available supply. People working in groups will be necessary even in the far future. When it comes to making judgements, the ability to think critically and creatively will be advantageous. Long ago, it was claimed that ML and AI were incapable of doing any of these tasks. If you wish to continue this discussion, you must include these changes into your groups.

## Conclusion

The use of artificial intelligence is a strong technique that can be used to find weak points in cyberspace as well as the sources from which assaults originate. This may be accomplished by analyzing large amounts of

 doi:10.20944/preprints202301.0115.v1



data. An artificial intelligence system that has been developed with an emphasis on security may constantly scan through enormous volumes of data in search of possible threats and give recommendations that are appropriate. Software that uses artificial intelligence (AI), despite the many useful applications it has, is vulnerable to being hacked, and the data it uses may be damaged or poisoned, all of which can lead the programmes to fail to work properly. In order to address these issues, it will be required to make specific modifications to the basic processes that are done to maintain and enhance the functioning of AI. The use of artificial intelligence (AI), sometimes referred to as machine learning, is rapidly becoming into an instrument that is vital for enhancing the productivity of IT security teams. Because there are too many of them, a single human individual working alone is unable to provide adequate protection for a modern company's potentially susceptible ports of entry. Artificial intelligence can satisfy the standards placed on security specialists in terms of analysis and the detection of threats. As a direct consequence of this, the possibility of a security breach is decreased, and the level of security as a whole is elevated.

## References


1. *Tolani, M. G., & Tolani, H. G. (2019). The Use Of Artificial Intelligence In Cyber Defense. International Research Journal Of Engineering And Technology (Irjet), 6(7), 3084-3087.*
2. *Dalave, C. V., & Dalave, T. (2022). A Review On Artificial Intelligence In Cyber Security. In Proc. 6th Int. Conf. Comput. Sci. Eng.(Ubmk) (Pp. 304-309).*
3. *Bhere, R. R. Artificial Intelligence Based Cyber-Security Program.*
4. *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).*
5. *Atiku, S. B., Aaron, A. U., Job, G. K., Shittu, F., & Yakubu, I. Z. (2020). Survey On The Applications Of Artificial Intelligence In Cyber Security. International Journal Of Scientistic And Technology Research, 9(10), 165-170.*
6. *Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The Future Of Cybersecurity: Major Role Of Artificial Intelligence, Machine Learning, And Deep Learning In Cyberspace. In International Conference On Computer Networks And Communication Technologies (Pp. 739-747). Springer, Singapore.*
7. *Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence And Cybersecurity: Past, Presence, And Future. In Artificial Intelligence And Evolutionary Computations In Engineering Systems (Pp. 351-363). Springer, Singapore.*
8. *Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The Future Of Artificial Intelligence In Cybersecurity: A Comprehensive Survey. Eai Endorsed Transactions On Creative Technologies, 8(28), E3-E3.*
9. *Haider, N., Baig, M. Z., & Imran, M. (2020). Artificial Intelligence And Machine Learning In 5g Network Security: Opportunities, Advantages, And Future Research Trends. Arxiv Preprint Arxiv:2007.04490.*

 doi:10.20944/preprints202301.0115.v1




**10.** *Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications Of Artificial Intelligence And Machine Learning In Smart Cities. Computer Communications, 154, 313-323.*

**11.** *Juneja, A., Juneja, S., Bali, V., Jain, V., & Upadhyay, H. (2021). Artificial Intelligence And Cybersecurity: Current Trends And Future Prospects. The Smart Cyber Ecosystem For Sustainable Development, 431-441.*

**12.** *Turransky, A., & Amini, M. H. (2022). Artificial Intelligence And Cybersecurity: Tale Of Healthcare Applications. Cyberphysical Smart Cities Infrastructures: Optimal Operation And Intelligent Decision Making, 1-11.*

**13.** *Li, J. H. (2018). Cyber Security Meets Artificial Intelligence: A Survey. Frontiers Of Information Technology & Electronic Engineering, 19(12), 1462-1474.*

**14.** *Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand Challenge: Applying Artificial Intelligence And Machine Learning To Cybersecurity. Computer, 52(12), 45-52.*

**15.** *Dalal, R., Varahamurthy, R., & Talegaon, R. (2020). A To I Of Artificial Intelligence. Work, 7, 8.*

**16.** *Ravi, V., Zheng, J., Subramaniam, A., Thomas, L. G., Showalter, J., Frownfelter, J., & Miller, K. (2019). Artificial Intelligence (Ai) And Machine Learning (Ml) In Risk Prediction Of Hospital Acquired Pressure Injuries (Hapis) Among Oncology Inpatients.*

**17.** *Li, J. H. (2018). Cyber Security Meets Artificial Intelligence: A Survey. Frontiers Of Information Technology & Electronic Engineering, 19(12), 1462-1474.*

**18.** *Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The Future Of Cybersecurity: Major Role Of Artificial Intelligence, Machine Learning, And Deep Learning In Cyberspace. In International Conference On Computer Networks And Communication Technologies (Pp. 739-747). Springer, Singapore.*

**19.** *Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand Challenge: Applying Artificial Intelligence And Machine Learning To Cybersecurity. Computer, 52(12), 45-52.*

**20.** *Ghillani, D. (2022). Deep Learning And Artificial Intelligence Framework To Improve The Cyber Security. Authorea Preprints.*

**21.** *Hemberg, E., & O'reilly, U. M. (2021). Using A Collated Cybersecurity Dataset For Machine Learning And Artificial Intelligence. Arxiv Preprint Arxiv:2108.02618.*

**22.** *Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence And Cybersecurity: Past, Presence, And Future. In Artificial Intelligence And Evolutionary Computations In Engineering Systems (Pp. 351-363). Springer, Singapore.*

**23.** *Proko, E., Hyso, A., & Gjylapi, D. (2018). Machine Learning Algorithms In Cyber Security. In Rta-Csit (Pp. 203-207).*

**24.** *Haider, A., Khan, M. A., Rehman, A., Ur, R. M., & Kim, H. S. (2021). A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System.*

**25.** *Calderon, R. (2019). The Benefits Of Artificial Intelligence In Cybersecurity*