IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

# Survey of Artificial Intelligence Applications In Cybersecurity

**Sonu Velgekar[1], Harsh Khandve[2], Rajeshwari Gundla[3]**

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[1]

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[2]

Assistant Professor, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[3]

**ABSTRACT:** Artificial intelligence refers to the idea of programming computers to have human-like intelligence and the ability to imitate human behaviour. Machines show characteristics correlated with the human mind, such as learning and problem-solving. The current security systems are slow and insufficient. Artificial intelligence may aid in the improvement of these factors, as well as the detection rate of intrusion detection and prevention systems (IDPS).With the successful use of AI, the system would be more efficient and fast but this also brings some risks and concerns. Therefore, it is equally important to manage both risks as well as concerns. Artificial intelligence improves the overall performance of security systems. Our research paper will help you know the various challenges, risks, and ways to resolve the issues and how new technologies can help fasten cybersecurity and make it more secure. It also informs about the current works going on in the world and what are different companies offering as help.

**KEYWORDS:** Cybersecurity, Artificial intelligence, IDPS, Problem-solving, Machine learning

## I. INTRODUCTION

With the launch of the first denial of service (DoS) attack in 1988, there has been a significant increase in the sophistication, number, and impact of cyber-attack. Since then the cyber-attacks have become more targeted and powerful which has to lead to an increase in Cybersecurity measures [1].

Earlier the first security tool was limited to tracing the viruses and preventing their execution. Whereas today we have a wide range of security that protects from different attacks and a variety of target systems. It has become increasingly challenging to protect information assets in the virtual world. Due to the constant growth in this field, it is difficult for security systems to trace new attacks and protect them through traditional methods. Even human interactions are slow and insufficient and the security systems lack flexibility and robustness [1] [2].

To overcome these factors and problems, Artificial intelligence was introduced and since then it has been a great help towards the protection of data from different attacks. This has also helped with the faster detection of attacks.

AI has multiple branches such as machine learning and deep learning. Machine learning is the part of AI which teaches machines how to make decisions which have helped the researchers with better techniques to take preventive measures for their data. With the growth in use of Machine Learning (ML), it has been easier to detect malware in networks and phishing emails. Deep learning is a type of machine learning where it performs pattern recognition and predictions. It can handle huge datasets and improves cybersecurity areas such as intrusion detection and botnet detection [3].

This research paper provides the reader with all the important aspects of artificial intelligence in cybersecurity and how it is better than human interaction and improves the various part of cybersecurity. Including the parts where machine learning and deep learning are used by the security experts for detections. It also informs us of the risks and concerns in artificial intelligence which also requires attention and the challenges in this field.

## II. LITERATURE SURVEY

As we know, the internet has now become an important utility in the daily lives of people around the world. It is also growing at a faster rate, be it in terms of users, devices connected to the internet, or different types of applications or technologies. With this growth, there is an equal amount of risks that are increasing towards being exposed to all types of cyber-attack. To control/protect these internet–connected devices along with their users and their data, cybersecurity has become indispensable.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

Further, we had research on how Artificial intelligence (AI) is applied to strengthen cybersecurity for various application domains.

1. **The internet**
   From an AI perspective, malicious patterns that differ from reasonable internet traffic are cyber-attacks. Intrusion detection systems are developed using AI techniques because they have the capability to check a large amount of data easily and in fast pace and so they adapt to the changing nature of internet traffic. Some recent cyberattacks have been targeted to network infrastructure, business logic and users for their data and other ways to harm the systems [5].

2. **Network infrastructure (BOTNET)**
   Most Internet services involve client-server communications. Attackers can pre-empt access to servers or prevent the server from serving client requests, as in DoS attacks. During a botnet, the attackers first compromise several hosts (using Trojans or other sorts of malware), which are controlled by the attackers, and issue-specific requests to execute tasks. For instance , during a DoS attack, these jeopardized machines often want to overwhelm a server with an outsized number of requests, leaving no resources to handle requests from legitimate users. DoS attacks became a significant threat because the botnets want to grow in complexity and run on multiple platforms from computers, mobile devices, and IoT devices.

   Network management through Software-defined networks (SDN) differs from ancient forwarding protocols. whereas ancient routers forward traffic consistent with their routing tables, SDN collects and programmatically analyzes network information before forwarding network traffic With Deep Learning algorithms, the work showed that it detected DoS attacks with 95.65 % accuracy. Deep Learning is seen as an acceptable answer for detection DoS attacks in SDN surroundings. SDN employs AI techniques to adapt to changes among the computing surroundings and learn from past network information to analyze new traffic patterns and predict security trends [5].

3. **Application layer**
   Until recently, application-layer attacks have focused on protocols like HTTP, name Service (DNS), or Session Initiation Protocol (SIP). For instance, novel DoS attack modelling and detection was proposed, when the remake of the online browsing protocol HTTP/2 was introduced, [16]. When the proposed HTTP/2 flood traffic was launched against an HTTP/2 service, AI techniques (Naïve Bayes, Decision Trees, and Rule Learning) showed a much better percentage of false alarms than when the equivalent AI techniques were employed to detect HTTP/1.1 DDoS attacks, which demonstrated that they bypassed known intrusion-detection systems. For detecting attacks, Support Vector Machines (SVMs) showed no false alarms, given a proposed set of features relevant to HTTP/2 detection [16].
   AI has proven to be a versatile technique to detect false information, as it can quickly analyze a large amount of data. For false information Automatic detection techniques improve human well-being and demonstrate AI's capability to use new features. Deep Neural Networks (DNNs) have shown their ability to detect hate speech in tweets with 93 percent accuracy [5].

4. **Human Link and Malware**
   Humans have probably been the weakest link within the field of cybersecurity being the end-user of the web. They're more focused over their business tasks rather than handling the daily increasing cyber-attack. One among the most reasons for the successful spread of malware attacks through modern phishing techniques is that the requirement of coaching supported past and modern issues to humans. This training is important in order that the machines are often re-engineered to mitigate a number of the well-known cyber threads.
   Malware is a type of software that has malicious intent and phishing is a method that tempts and tricks human users into clicking some malicious links or executing/ downloading a file in order to attack their devices and get some sensitive information. Once any human user clicks on any of such links or opens a file it triggers the spread of malware. This is one of the biggest problems that humans are facing nowadays too which to some extent has been brought under control but not extracted totally. Users must determine the target's credibility to avoid falling for phishing hooks, which can often be achieved by checking the code behind the links, which can take some advanced skills. This is a neighbourhood where AIs often want to augment human intelligence. These rules act as features in AI techniques to eliminate these malicious contents and links [5].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

5. **The Internet of Things**
   Computers became smaller, portable, and more powerful, and affordable. The ubiquity of mobile devices like phones and tablets became the dawn of the IoT era. Today, many devices (from toys, appliances, and vehicles to industrial control systems) are equipped with networking capabilities and Internet connectivity that creates the IoT possible. Other paradigms like cloud computing, big data, and fog computing are enabling mobile devices with limited resources to access a good range of services remotely. Researchers introduced fog computing services by provisioning the platform and application closer to the user as the demand for higher data rates kept on increasing. Fog computing distributes servers to attenuate network round trip delays, especially for Content Delivery Networks (CDNs). So, fog computing not only improves website performance, but also provides real-time energy and carbon footprint management [5].

6. **Privacy**
   As most folks are aware that some applications use a number of our device's features like voice, Geolocation, the surrounding temperature, and also our data and media in some applications. Traditionally, to take care of these data and privacy, secure authentication mechanisms like encryption and security certificates are into implementation. AI techniques are often wont to maintain private communications when routing paths dynamically change, and when a 3rd party stores the info. For instance, learning automata was adopted to distribute. Both biometrics and human behaviour metrics were employed by the secure authentication mechanisms, but the problems kept arising when the authentication devices were unable to seek out an honest fit under varying operating conditions. To beat these issues, AI techniques are wont to enable robust performance and accurate detection of face, fingerprint, and voice recognition in several operating environments. To facilitate blockchain applications, AI techniques are utilized in conjunction with blockchain which enables blockchain applications to ensure secure communication between two IoT devices [5]. Figure 1 gives an overview of how AI helps cyber security.

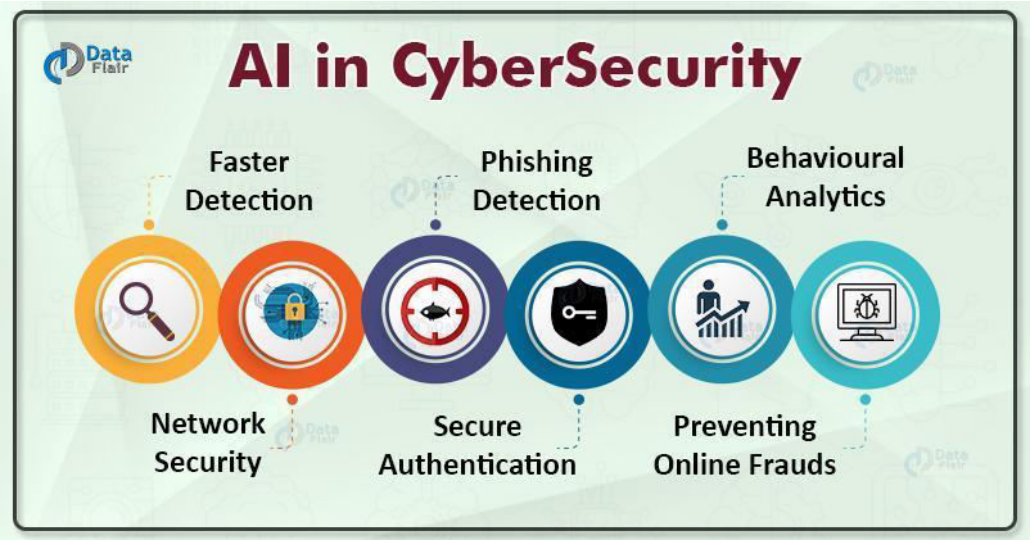


Fig.1. How AI helps in cybersecurity
(© Image Copyrights - https://data-flair.training/blogs/ai-and-cyber-security/ )

Some of the highest use cases of AI or ML or DL in cybersecurity:

1. To detect threats and Stop attacks: NHS agency of London spotted the attack within a seconds using their algorithms and therefore the threat was diminished without affecting the damage to the organization. They concluded that the recent ransomware issue infected quite 200 K victims across 150 countries. And stated that none of their customers were harmed by the WannaCry attack including those systems which weren't updated [9].
2. To analyze mobile endpoints: Google started using ML threats against mobile endpoints. In October 2018, MobileIron and Zimperium companies would integrate one another using the technology of ML-based threat detection and security compliance which might address challenges like detecting device, network and application threats immediately take automated actions and Protect organization data [9].
3. Enhance Human Analysis: In 2017, MIT's computing and AI Lab succeeded in building a model called AI2. It's an adaptive ML security platform that aids analysts to seek out key things during a larger database.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

Examining many logins every day, the system was capable to filter data and pass it to the human analyst. Decreasing watchful right down to 100 each day. This was practically administered by companies called CSAIL and PatterEx, and the attack detection rate rose to 85% [9].

There are currently quite 30 companies working by merging AI and cybersecurity to form the virtual world safer. A number of these companies are:

1. **Cybereason** (based in Boston, Massachusetts) may be a cybersecurity analysis platform that gives threat research, monitoring, and analysis. Cybereason's AI-powered hunting technology discovers whether or not a corporation is under fire. the standard sort of threat hunting significant resources, but this platform uses AI and automates this work in order that security teams of all sizes and skill levels can cash in on it [13].
2. **Fortinet (**headquartered in Sunnyvale, California) provides solutions for each part of the IT infrastructure. This company's AI-based product is named Fortiweb, which may be a firewall for web applications. It uses two levels of statistical probability and machine learning to accurately detect threats. Fortinet Cyber Security products are employed by most Fortune 500 companies [13].
3. **ImmuniWeb** (based in San Francisco, California) provides web and mobile security testing services through its AI and machine learning platform. The company's multiple AI-based products work alongside human intelligence to detect more vulnerabilities and risks within applications, open-source software, and other programs without returning false positives [13].
4. **SentinelOne** (based in Mountain View, California) could also be a comprehensive endpoint protection platform that provides defence against various kinds of attacks throughout the threat lifecycle. Between SentinelOne's static and behavioural AI engines, threats are detected and contained autonomously. From malware and phishing emails to Trojans and exploits within documents and files, the platform prevents, detects, and even reverses attacks [13].
5. **Shape Security** (based in Mountain read, California) provides software systems that combats imitation attacks like pretend accounts, papers stuffing, and application fraud for firms inside the retail, financial, government, technology, and travel industries. Shape's machine learning models accessed information that resembles attackers, permitting the system to grasp what human anti-fraud activity looks like. The company's solutions, Enterprise Defence and Blackfish use this AI to identify the variations between real and artificial users then block, direct or report the dishonest supply [13].
6. **The CUJO AI platform** (located in San Jose, California) uses machine learning to research and secure everything from browsers and smartphones to IoT devices. The method acknowledges patterns and proactively predicts attacks victimisation algorithms so malicious malware and phishing schemes are disappointed before they compromise a network [13].
7. **Deep Instinct** (based in New York), this threat bar platform prevents each file and file cyberattacks victimisation deep learning. Company protection will be applied to any platform (mobile devices, servers, terminals, etc.) and prevents script-based attacks, together with JavaScript and hypertext markup language [13].
8. **The Obsidian Security identity management platform** (located in Newport Beach, California) monitors and protects users across the enterprise. By providing one supply of trust for identity, DBAs recognize United Nations agency has access to what in the least times, considerably fast the method of preventing and containing information breaches. to boot, the company's AI helps managers build data-driven selections concerning that workers ought to access that permissions [13].

## III. PROPOSED ANALYSIS APPROACH

There are multiple schemes planned with Deep learning and Machine learning (branches of AI) solutions in Net. Machine learning solutions embody k-nearest-neighbor (k-NN), Support Vector Machine (SVM), call tree, Neural Network, etc. Deep learning programs embody Deep Belief Network (DBN), repeated Neural Network (RNN) and Convolutional Neural Network (CNN). These schemes square measure as follows:

1. **K-nearest-neighbor-based cyber security:** SyarifANdGata (2017) has planned an intrusion detection theme mistreatment binary particle swarm improvement (PSO) and k-NN algorithms. They selected KDD CUP 1999 that could be a widely used customary dataset for researchers to simulate in IDSs. The experimental results show a two accuracy increase compared with those obtained mistreatment the k-NN formula alone.
   Hybridization of classifiers typically performed higher than individual ones. K-NN, SVM, and pdAPSO are hybridized for intrusion detection (Dada, 2017). Dada (2017) compared the performances of those 3 classifiers using KDD99 datasets, and therefore the experimental results showed that the fusion of the 3 classifiers will

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

cause a classification accuracy of ninety eight.55%. However, Dada (2017) centered on solely classification accuracy, and not the quality and potency of the model [13-14].

2. **Support vector machine based cyber security:** Shahid et al. (2012) proposed two techniques for fault detection and classification in power transmission lines (TL). Both approaches are based on the one-class quarter-sphere support vector machines (QSSVMs). The first approach, called "temporal-attribute QSSVM (TA-QSSVM)," tries to determine the attribute correlations of data measured in a TL for fault detection, and the second approach exploits attribute correlations for only fault classification. These convincing experiments showed that TA-QSSVM can obtain almost 100% fault-detection accuracy and A-QSSVM can achieve 99% fault classification accuracy, which are remarkable results. In addition to accuracy, these approaches had less computational complexity than multi-class SVM (from O ($n^4$) to O($n^2$)), making them applicable to online detection and classification [13-14].

3. **Decision tree based cyber security**: Vuong et al. (2015) used a call tree to get straightforward detection rules that were accustomed to defend against denial of service and command injection attacks on robotic vehicles. They thought-about cyber input options, like network traffic and disk information, and physical input options, like speed, power consumption, and change. Their experimental results showed that totally different|completely different} attacks have different impacts on automaton behaviors, together with cyber and physical operations, which the addition of physical input options may facilitate the choice tree, increase the general accuracy of detection and scale back the false positive rate [13].

4. **Neural network based cyber security**: Vollmer Associate in Nursing wild (2009) planned a computationally economical neural network rule to produce an intrusion detection alert theme for cyber security state awareness. The experimental results indicated that this increased version of the neural network rule reduced memory needs by seventieth, and reduced runtime from thirty sevens to ones [13].

5. **Deep belief network based attack defense**: Zhu et al. (2017) projected a unique DL-based approach known as "DeepFlow" to directly sight malware from the info flows in automaton applications. This theme is enforced by DBN (Fig. 3). supported the DeepFlow design, complicated attack feature knowledge is analyzed. DeepFlow design consists of 3 components: FlowDroid for feature extraction, SUSI for feature coarse-granularity, and also the DBN metric capacity unit model for classification. Crawler modules are accustomed to crawl malware from malware sources and benign ware from Google Play Store on an individual basis. The experimental results showed that DeepFlow outperforms ancient cubic centimeter algorithms, like Naïve mathematician, PART, provision regression, SVM, and multi-layer perceptron (MLP) [13].

6. **Recurrent neural network based attack detection**: Loukas et al. (2018) projected a cloud-based cyber-physical intrusion detection theme for the web of Vehicles (IoV) employing a deep multilayer perceptron associate degreed an RNN. They know that RNN, with associate degree LSTM hidden layer, proved terribly promising in learning the temporal context of assorted attacks, like DoS, command injection, and malware. This work jointly disclosed that detection latency, the key defect of DL-based schemes, could be a result of the multiplied process demands, which may be self-addressed by cloud-based machine offloading. They conjointly administered some experiments in an exceedingly real cyber atmosphere to verify their approach [13].

7. **Convolutional neural network based attack detection:**Based on a CNN, Meng et al. (2017) proposed a novel model, named "malware classification based on static malware gene sequences (MCSMGS)," for malware classification. First, the scheme extracted the malware gene sequences of both informational and material attributes. Second, it tried to determine the representation of correlation and similarity of each malware. Finally, to achieve accurate malware classification, a module named "static malware gene sequences−convolution neural network (SMGSCNN)" was employed to analyze the extracted malware gene sequences. They claimed that the classification accuracy was up to 98% with the proposed scheme, and it was more effective than the SVM model [13-14].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

## IV. CHALLENGES

Cybercriminals are adept at adopting any strategies or improvements that supply them with a foothold over cybersecurity defences. Early case research and studies imply in which defenders are already seeing the earliest effect: protecting towards 'strong' AI – in which criminals use structures that operate, assume and act as humans – and towards 'weak' or 'narrow' AI – in which structures are modelled on human behaviour to execute particular duties. Given its ability uses, AI is anticipated to pressure systemic modifications inside the cybersecurity landscape and may affect 4 key challenges in cybersecurity inside the close to destiny [6].

**Challenge 1: Increasing sophistication of attackers**

Attackers of various tiers of sophistication – from social activists to country states – make investments their efforts focused on possibilities that deliver the expectancy of maximum goes back on investment. Organizations can pressure change-primarily based manipulate investments to cut back their attraction to attackers. As groups mature their cybersecurity programs, they subsidize precious targets.

AI can boost up the number of assaults as automation of duties and enhancement of malicious offerings; in addition, lessen obstacles to access and execution of assaults. The AI-enabled era also can decorate attackers' competencies to keep each their anonymity and distance from their sufferers in surroundings in which attributing and investigating crimes is already challenging [15].

**Challenge 2: Asymmetry**

As defenders, we'd like to accumulate action at preventing assaults 100% of the time, whereas attackers handiest got to accumulate action once. Organizations have to be compelled to target constructing the correct capabilities and a gaggle in a shot to place effective procedures and era that reduce this imbalance.

While AI and automation are lowering variability and worth, enhancing scale, and limiting errors, attackers can also use AI to tip the soundness. Criminals are getting to be prepared to automatise the foremost resource-in-depth factors in their assaults and pass the controls deployed towards them. 'Narrow' AI predictions for the near to destiny imply that AI-enabled vulnerability scanners to accelerate discovery and exploitation of vulnerabilities through attackers might venture up to date vulnerability management and cybersecurity operations capabilities [15].

**Challenge 3: Increasing the attack surface / Digitalizing operations**

As groups nevertheless grow, so do the scale and complexity in their era and records estates, which means attackers have greater surfaces to discover and exploit. To stay earlier than attackers, groups can install superior technology like AI and automation to help create defensible 'choke points' in preference to spreading efforts similarly throughout the entire surroundings.

Additionally, the usage of AI in commercial enterprise procedures has the ability to differentiate the individual of cyber-dangers and belongings that require to be defended. Increasing reliance on the AI-enabled era can also additionally create new possibilities for attackers to intervene with vital commercial enterprise procedures, affecting each inner decision-making and relationships with customers [15].

**Challenge 4: Balancing risk and operational enablement**

Organization's purpose to run their operations efficiently and securely. One smooth response to modifications to the chance and risk panorama is to undertake a heavy-passed protection way of life that in the end reduces competitiveness and suppresses the body of workers' morale. Instead, protection groups can use a chance-primarily based approach, through setting up governance procedures and materiality thresholds, informing operational leaders in their cybersecurity posture, and figuring out tasks to constantly enhance it.

Additional operational enablement is regularly finished through the usage of technology like AI to decorate how operational and era groups interact with protection. for instance, the usage of the era to be had today, the time required to complete habitual protection procedures are regularly decreased appreciably through the usage of AI to automate resource- or time-in-depth components of these procedures. For operational groups, upgrades in protection procedure performance lessen the friction associated with following protection requirements. Developments in the AI era are predicted to liberate greater possibilities to decorate cybersecurity operations and help the stability of chance and go back [15]. Fig.2. gives a brief idea about the different threats in AI.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

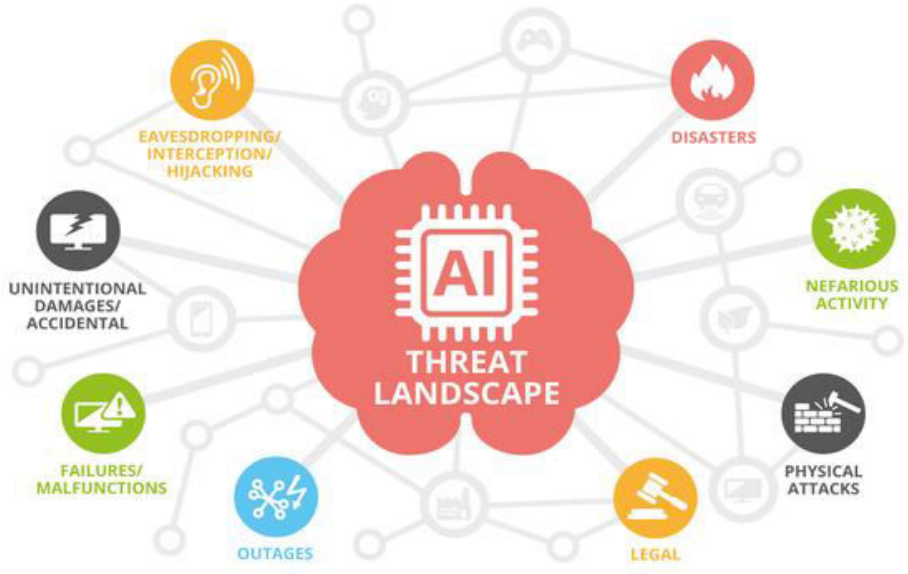


Fig. 2. AI threat landscape
(© Image Copyrights - https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges )

## V. RESULTS AND ANALYSIS

With today's ever-evolving cyber-attacks and proliferation of devices, machine learning and AI are typically accustomed to continue with the unhealthy guys. Automating threat detection and responding additional expeditiously than ancient software-driven approaches is however AI improves cybersecurity. AI is ideally matched to unravel a spread of our most troublesome issues and beneath this class falls cybersecurity. The results of implementing AI to the large and numerous classes of Cybersecurity is:

**IT plus Inventory**- Cybersecurity helps in knowing each device and user, and applications with access to any form of info systems. It additionally helps within the categorization and measuring of business criticality that plays an enormous role [11].

**Incident response** – Improved context for prioritization and response to security alerts may be obtained with AI-powered systems, AI surfaces root causes to mitigate vulnerabilities, offers quick response to incidents and avoid future problems [11].

**Explainability** – The explainability of recommendations and analysis is that the key to harnessing AI to enhance human InfoSec groups. this is often vital in obtaining buy-in from stakeholders across the organization, for understanding the impact of assorted InfoSec programs, and for reportage relevant info to all or any or any concerned stakeholders, as well as end-users, security operations, CISO, auditors, CIO, CEO, and board of administrators [11].

**Breach Risk Prediction**– AI-based systems will predict wherever and the way you're presumably to be broken so you'll be able to set up for resources needed and gear allocation towards areas of weakness and counter the attacks. AI additionally offers prescriptive insights derived from AI analysis, which might assist you piece associate degreed enhance controls to enhance an organization's cyber resilience effectively [11].

**Threat Exposure**– hackers follow trends similar to everybody else therefore AI-based Cybersecurity systems will offer up-to-date information of worldwide and industry-specific threats. It'll additionally facilitate to form crucial selections supporting the information gathered from previous attacks and additionally from the previous patterns. It'll not solely provide us a counterattack however will facilitate us to see the way to defend ourselves from the attack [11].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005022

**Controls Effectiveness**– it's vital to know the impact of the many security tools and security processes merely that you just} merely simply have used to want care of a powerful security posture. AI will facilitate analysis wherever your InfoSec program has strengths, and gaps [11].
**Controlling Attacks**– AI area unit typically facilitates detection and preventing attacks as AI will notice common assaultive sources and will additionally acknowledge the distinction between a faux and bonafide web site in no time. AI additionally analyzes the phishing pattern in keeping with the precise geographical location [11].

## VI. CONCLUSION

In recent years AI has emerged as one of the best cutting-edge technologies for augmenting the efforts of human information security. Since cybercrimes are increasing day by day and it's been done on a large scale, humans can't control and defend the dynamic Enterprise attack surface. Hence Artificial Intelligence in Cybersecurity.
AI provides much-needed analysis and threat identification, it also identifies and prioritizes risks, instantly spots any malware on a network, guides incident response, and detects intrusions before they start so that Cybersecurity professionals can act on it to reduce breach risk and improve security posture.

## REFERENCES

1. Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." Cyber Intelligence, and Security Journal 1.1 (2017): 21-23.
2. Patel, Z., Senjaliya, N., & Tejani, A. (2019). AI-enhanced optimization of heat pump sizing and design for specific applications. International Journal of Mechanical Engineering and Technology (IJMET), 10(11), 447-460.
3. Patil, Pranav. "Artificial intelligence in Cybersecurity." International Journal of Research in Computer Applications and Robotics 4.5 (2016): 1-5.
4. Calderon, Ricardo. "The benefits of artificial intelligence in cybersecurity." (2019).
5. S.Jagadish, R.Sugumar, Optimal Knowledge Extraction technique based on hybridization of improved artificial bee colony algorithm and cuckoo search algorithm, International Journal of Business Intelligence and Data Mining, Volume 11, Issue 4, pp.221-232, November 2017.
6. Adi, Erwin, ZubairBaig, and Philip Hingston. "Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services." Journal of Network and Computer Applications 91 (2017): 1-13.
7. Zeadally, Sherali, et al. "Harnessing artificial intelligence capabilities to improve cybersecurity." Ieee Access 8 (2020): 23817-23837.
8. Chan, Leong, et al. "Survey of AI in cybersecurity for information technology management." 2019 IEEE technology & engineering management conference (TEMSCON). IEEE, 2019.
9. Geluvaraj, B., P. M. Satwik, and TA Ashok Kumar. "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace." International Conference on Computer Networks and Communication Technologies. Springer, Singapore, 2019.
10. URL = https://www.geeksforgeeks.org/significance-of-artificial-intelligence-in-cyber-security/accessed on 06th March 2021
11. URL = https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/accessed on 17th March 2021
12. URL = https://builtin.com/artificial-intelligence/artificial-intelligence-cybersecurityaccessed on 20th March 2021
13. URL = https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ accessed on 7 April 2021
14. Senjaliya, N., & Tejani, A. (2020). Artificial intelligence-powered autonomous energy management system for hybrid heat pump and solar thermal integration in residential buildings. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(7), 1025-1037.
15. **B.Murugeshwari,** C Jayakumar, , K Sarukesi, Preservation of the Privacy for Multiple Custodian Systems with Rule Sharing , **Journal of Computer Science**, Vol No 09 Issue 09, 1086-1091 Pages, 2013
16. URL= https://www.weforum.org/agenda/2019/09/4-ways-ai-is-changing-cybersecurity-both-in-attack-and-defense/accessed on 17th April 2021
17. Li, J. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462–1474. doi:10.1631/fitee.1800573
18. Apruzzese, Giovanni, et al. "On the effectiveness of machine and deep learning for cyber security." *2018 10th international conference on cyber Conflict (CyCon)*. IEEE, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details