INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 385-392

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Jaganath S[1], Navya Shree C[2], Pradeep D[3]

[1,2,3]Dept. of Electronics and Communication Engineering T. John Institute of Technology Karnataka, India.

DOI: https://www.doi.org/10.58257/IJPREMS32914

ABSTRACT

Over the past few decades, there has been a notable increase in the frequency and sophistication of cyberattacks. As a result, developing a cyber-resilient approach is critical. Con- ventional security measures are insufficient to stop data breaches caused by cyberattacks, as cybercriminals have mastered the use of sophisticated tools and new techniques to hack, attack, and breach data. Fortunately, Artificial Intelligence (AI) technologies have been introduced into cyberspace to create intelligent models for defending systems against attacks. Since AI technologies can quickly evolve to handle complex situations, they can be utilized as essential tools in the field of cybersecurity.AI-based methods can offer effective and potent cyber defense solutions to identify and notify security issues of many types, including malware assaults, network intrusions, phishing and spam emails, and data breaches. In this article, we examine the role of artificial intelligence (AI) in cybersecurity and provide an overview of the benefits of AI as it relates to cybersecurity.

Keywords— cybersecurity, artificial intelligence, machine learning, deep learning, bioinspired computing, cyberattacks

1. INTRODUCTION

The number of cyberattacks has increased dramatically as a result of the exponential expansion of computer networks. Our society's various sectors, including the government, business, and vital infrastructure, rely heavily on computer networks and information technology solutions. They are therefore clearly susceptible to cyberattacks. An attack against another computer or network, initiated from one or more computers, is referred to as a cyberattack. The usual objectives of a cyberattack are to either take down the target computer, disable it, or gain access to its data. The frequency and severity of cyberattacks have significantly increased since the first denial-of-service (DOS) assault in 1988. In fact, one of the hardest jobs in computer science today is cybersecurity, and it's predicted that both the volume and complexity of cyberattacks will increase dramatically over the coming years. More than ever, the modern world is reliant on technology. The widespread adoption of cutting-edge technologies like cloud computing and the Internet of Things (IoT) generates and gathers enormous amounts of data.

Even though data can be used to more effectively meet related business goals, cyberattacks frequently provide significant difficulties. An intentional and malevolent attempt to compromise the information system of another person or organization is known as a cyber-attack. These days, the region is frequently targeted by malware attacks, ransomware, denial of service (DoS), phishing or social engineering, SQL injection attacks, Man-in-the-Middle attacks, Zero-day exploits, or insider threats. Cybercrime and security incidents of this kind can disturb individuals and companies, result in severe financial losses, and affect both. For example, the IBM research states that a data breach in the US costs 8.19 million USD, and cybercrime is predicted to cost the world economy 400 billion USD annually. Generally speaking, cybersecurity refers to a group of tools, processes, and guidelines created to guard computers, networks, software, and data from intrusion, disruption, and attack. It is frequently referred to as "electronic information security" or "information technology security." The many needs of today may render the traditional, well-known security solutions such as firewalls, user authentication, encryption, and antivirus software ineffective.

The main issue with these conventional systems is that they are typically managed by a small group of knowledgeable security specialists, and as a result, data processing is done on an as-needed basis and cannot be intelligently adjusted to meet requirements. However, given its computational capacity and capabilities, artificial intelligence (AI), one of the main technologies of the Fourth Industrial Revolution (Industry 4.0), can be very significant for intelligent cybersecurity services and management.

In order to make cybersecurity computers more automated and intelligent than the industry's traditional security solutions, we thus concentrate on "AI-driven Cybersecurity." The article examines the need for cybersecurity strategies to evolve and describes how artificial intelligence (AI) may be used to improve cyber capabilities against cyber threats and provide the best possible solutions for cyber settings. Additionally, it gives a summary of a few AI subset technologies, including bioinspired computations, deep learning, expert systems, and machine learning.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 385-392

2. BACKGROUND OF ARTIFICIAL INTELLIGENCE

The process of giving a computer, a robot under computer control, or software the ability to think intelligently and similarly to intelligent humans is known as artificial intelligence. The process of creating artificial intelligence (AI) involves first understanding how the human brain functions and how people learn, make decisions, and collaborate to solve problems. The results of this research are then used to create intelligent software and systems. The capacity to acquire knowledge and use that knowledge to reason in order to solve complicated issues is a frequent definition of intelligence. Intelligent machines will soon take the place of humans in many tasks. The study and creation of intelligent hardware and software that can reason, learn, acquire information, communicate, operate, and see things is known as artificial intelligence. In 1956, John McCarthy first used the phrase to refer to the area of computer science that focuses on programming computers to behave like people. Perceiving and acting on reason is made possible by the study of computation. Artificial intelligence is distinct from psychology because to its focus on computing, but computer science differs from it in that it emphasizes perception, reasoning, and action. It gives machines more intelligence and utility.

This section provides a quick summary of learning algorithms, which are fundamental ideas in artificial intelligence. It also provides a brief overview of some of the AI subfields that are commonly used in the field of cybersecurity, including expert systems, machine learning, deep learning, and biologically inspired computation.

Machines may be trained using learning algorithms, which also help humans perform better by allowing humans to learn from their mistakes. Based on the definition provided by Mitchel. For the purpose of teaching machines, there are three common learning algorithms, which are described below:

A. Supervised learning

This kind uses a sizable labeled data collection during the training phase. Following the training phase, a test data set must be used to verify the system. These learning algorithms are often applied as regression or classification techniques. Based on the input, the regression method produces outputs, or prediction values, which are one or more continuous-valued integers. As opposed to regression, classification algorithms provide discrete outputs and classify data into groups.

B. Unsupervised learning

Using an unlabeled training set of 110 data points, unsupervised learning differs from supervised learning. Unsupervised learning techniques are typically applied to estimate density, minimize dimensionality, and cluster data.

C. Reinforcement learning

This kind of algorithm learns the optimal behaviors in response to incentives or penalties. One way to think of reinforcement is as an amalgam of unsupervised and supervised learning. In circumstances when data is few or unavailable, reinforcement learning can be helpful.

There are several subfields within AI technology, some of which are listed here.

1. The expert system, or ES

Another name for it is a knowledge-based system. The two primary parts of ES are an inference engine, which is used to reason about preset information and discover solutions to given issues, and a collection of knowledge, which forms the basis of knowledge-based systems and incorporates collected experiences. Expert systems are capable of handling two different kinds of problems: rule-based reasoning and case-based reasoning, according to the reasoning technique. ESs can aid decision-making in cyberspace. Generally speaking, altered security system data are assessed before the security expert system decides whether or not a system or network behavior is harmful. Security professionals can often scan and evaluate a sizable amount of updated data in a reasonable amount of time by using statistical approaches. Expert systems that monitor in real time in cyber settings can effectively assist these efforts. Security expert systems provide pertinent information and a warning message in the event of hostile breaches, allowing security experts to choose the best security actions.

2. Machine learning (ML)

An explicit collection of techniques that enable computers to learn without explicit programming is what Arthur Samuel defines as machine learning (ML). Through machine learning (ML), systems may learn from data, find and codify the underlying principles, and improve through experience without needing to be explicitly coded. In order to find patterns in the data and base future decisions on the provided examples, the learning process starts with monitoring the data through examples. Using this information, the system may infer the characteristics of cases that haven't been seen before.

ML makes use of statistics to analyze vast amounts of data in order to extract information, identify trends, and make judgments. Different kinds of machine learning algorithms exist.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 385-392

3. Deep learning (DL)

Usually referred to as deep neural learning, is the process of teaching computers how to perform activities that are normally performed by people using data. ML, or machine learning, which allows a computer to learn without human assistance via experience and skills, is fully included in DL.

Like people, DL algorithms are able to learn from their experiences by repeating a job and making little adjustments each time to get a better result. DL simulates how the human brain processes information and forms patterns for use in making decisions. It takes on the signal processing systems of human brains and neurons. The performance of neural networks is continually improved by building larger neural networks and training them with a lot of data. The volume of data created daily in many applications is really large. One reason why DL is used in cyber settings is the rise in the quantity of data that is created every day. This is because DL algorithms need a vast amount of data to learn from.

The improved performance of DL over ML in big volumes of data is one of its benefits. DL techniques support reinforcement learning, unsupervised learning, and supervised learning, much like ML techniques do. DL techniques often utilized in cybersecurity include feed forward neural networks, convolutional neural networks, recurrent neural networks, deep belief networks, stacking autoencoders, generative adversarial networks, limited Boltzmann machines, and ensembles of DL networks.

3. CYBERSECURITY AND RELATED TERMS

Cybersecurity is the activity of defending systems, networks, and programs against digital threats. These intrusions are often intended to access, change, or delete sensitive information; extract money from users via ransomware; or disrupt regular corporate activities. In the past 50 years, our society has become more reliant on information and communication technology (ICT). As more smart gadgets rely on worldwide Internet access, the potential of data breaches and assaults grows. ICT security, or the prevention and protection of ICT systems from sophisticated cyber-attacks and dangers, has become a top priority for security experts and policymakers. Enterprises implement ICT security measures to safeguard the integrity, confidentiality, and availability of their data and systems. Cybersecurity involves safeguarding insecure information and communication technologies. Even though the phrase "cybersecurity" is widely used these days, there are a few related terms that are frequently used interchangeably, such as "information security," "data security," "network security," and "Internet/IoT security," which can be confusing to readers and industry experts alike. We define these phrases and provide their global popularity score in the sections that follow.

The main goal of Data security is to protect data, which might be specific data that is usually stored. Therefore, the prevention of illegal use, interruption, modification, or destruction of data while it is being stored may be defined as data security. Information security is the process of guarding against illegal use, interruption, alteration, and destruction of data. In a way, information security falls under the general category of cybersecurity, which is the larger practice of protecting IT assets from threats or assaults. Network security is the process of stopping and monitoring illegal access, abuse, modification, or denial of service to a computer network. Therefore, it may be viewed as a subset of cybersecurity, which generally guards data sent across networks. The phrases "cybersecurity" that have been discussed above pertain to the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data against harm, unauthorized access, malicious assaults, and cyberthreats. "cybersecurity" has the highest level of global popularity and is growing daily; its popularity indicator values were low in 2016 but are rising steadily.

We may thus determine that cybersecurity is all about protecting anything that exists in the cyberspace, including infrastructure, cloud, Internet of Things (IoT), network, information, application, and operational security, among other pertinent things. While network protection systems and computer security systems make up the majority of traditional cybersecurity systems.

4. AI'S DRIVEN STRATEGIES FOR CYBERSECURITY

The rapid progress of computer technologies has had a profound impact on people's daily lives and places of employment, contributing to the rapid change of our society. With the use of some of these technologies, machines are now able to reason, learn, make decisions, and solve issues just like people do. For instance, artificial intelligence (AI) absorbs intellect and can analyze massive volumes of data to solve problems while performing analysis and decision-making in real-time. Artificial intelligence (AI) has many applications in scientific and technological domains. It goes without saying that the Internet is a goldmine of personal data, which leads to several cybersecurity problems. First, the volume of data makes manual analysis all but impossible. Second, risks are evolving or they could be AI-based. Furthermore, the expense of mitigating dangers rises due to the high cost of hiring experts. The development and use of algorithms to identify those dangers likewise requires a significant investment of time, funds, and resources. The employment of AI-based techniques is one way to address those problems. AI is capable of quickly, precisely, and effectively analyzing vast amounts of data. An artificial intelligence (AI) system can forecast similar assaults in the

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 385-392

future, even if their patterns vary, by using threat history. The following are some of the reasons AI may be utilized in cyberspace [17]: AI can manage large amounts of data, AI can identify novel and significant changes in attacks, and AI security systems can train continually to improve their response to threats. However, artificial intelligence (AI) is not without its drawbacks. For example, an AI-based system needs a large quantity of data, which requires processing over time and using a lot of resources. Additionally, end users may experience false alarms frequently, which can negatively impact productivity. Attackers may also use model theft, data poisoning, and adversarial inputs to compromise the AI-based system.

Recently, scientists have discovered ways to use AI approaches to identify, thwart, and respond to cyberattacks. The four primary categories that comprise the most prevalent forms of cyberattacks are as follows:

A. Exploitation of software and detection of malware

O Software exploitation: Software has flaws, some of which may be exploited by an attacker to target the underlying software program if they are aware of the vulnerability. Buffer overflows, integer overflows, SQL injections, cross-site scripting, and cross-site request forgeries are a few common software vulnerabilities. Certain vulnerabilities are found and addressed. The best scenario would have been for software developers to have discovered and addressed every vulnerability during the design and development phase. However, given the high expense of software development and the urgency to get products into the market, this is not always possible. As such, issue identification and resolution are ongoing processes.

The internet "can be regarded as the most complex machine mankind has ever built," claims Bruce Schneier. Going through code line by line to patch software defects is a laborious operation, but computers can accomplish it if they are taught what the vulnerabilities look like. AI seems to have the capacity to complete these jobs. Benoit Moral provided an explanation of how some AI methods enhance application security. This study recommended the use of knowledge-based systems, probabilistic reasoning, and Bayesian algorithms to identify software exploitations. It concentrated on online application security.

O Malware identification: This technique is often used in cyberattacks. Malicious software includes Trojan horses, worms, and viruses. Given the significant influence malware has on politics and the economy, it is imperative to detect and mitigate malware-related assaults. Thus, a lot of study has been done around the use of AI approaches. Here is a list of some noteworthy research. The authors established a system in which data mining and machine learning classification are used to categorize and detect malware.

The researchers employed support vector machines and k-nearest neighbors as ML classifiers to find unknown malware. To identify clever malware, an alternative method developed a deep learning architecture. Mobile malware was the subject of a recent malware detection study. For malware identification, a deep convolutional neural network was used. The authors developed a brand-new machine learning method called rotation forest to detect malware. Using bio-inspired computing to classify malware was another line of inquiry. This method was applied to categorize parameters based on their optimization. To improve malware detection efficiency, the authors employed genetic algorithms.

Network intrusion detection

O Denial Of Service (Dos): One Of The Most Prevalent Types Of Assaults Is When Hackers Prevent Authorized Users From Accessing Data, Hardware, or other network resources. The authors presented a system that combines two distinct methodologies: signature-based methodology and anomaly-based distributed artificial neural networks.

O Intrusion Detection System (IDS): An IDS guards a computer system against unauthorized access, unexpected activities, and potential dangers. The adaptability, speed of computation, and ease of learning of AI-based technologies make them suitable for the development of 112 IDS. Enhancing classifiers and optimizing features is the aim of AI-based algorithms in order to lower false alarms. The authors developed a model for IDS by combining a support vector machine with an altered version of k-means. The authors presented a reinforcement learning strategy for IDS that is based on fuzziness. To improve the performance, they employed supervised learning on unlabelled sample datasets.

Another method predicted network traffic over a certain time period using fuzzy logic and genetic algorithms for network intrusion detection.

B. Phishing and spam detection:

O Phishing attack: Phishing attacks aim to get the identity of the victim. Phishing attacks include, for example, dictionary and brute-force assaults.

Here are some noteworthy AI-based solutions to address this problem. They unveiled a phishing email detection system that used reinforcement learning and a tweaked neural network for detecting purposes. Feng used a neural network with the Monte Carlo method and a risk-minimization strategy to detect phishing websites.

O Spam Detection: Unwanted mass email is referred to here.

Inappropriate material in spam emails might cause security problems. AI-based algorithms have been used to filter spam emails in the recent past. As an example, one system that Feng Support vector machines and the Naive Bayes algorithm were integrated by this system to screen spam emails.

AI may be used to examine data for attack detection and response in a variety of cyberspace domains. Processes may also be automated using AI, which makes it easier for security analysts to identify cyberattacks rapidly by utilizing semi-automated systems.

Below is a list of several well-liked AI cybersecurity strategies:

1. Threat categorization and detection: Artificial intelligence techniques are able to recognize potential dangers and stop assaults before they start. Usually, to do this, a model for evaluating large datasets of cybersecurity events and identifying patterns of harmful activity is created. In order to monitor, identify, and react to threats in real time, the model is usually composed of recorded Indicators of Compromise (IOC) and historical data monitoring.

Consequently, the models are used to automatically recognize similar behaviors if they are observed. IOC datasets are used by ML classification algorithms to recognize and categorize the various malware behaviors included in datasets. Moreover, behavioral-based research examines hundreds of malware's behaviors using ML clustering and classification algorithms. The patterns can also be used to automate the process of identifying and categorizing emerging risks. Security analysts and other automated systems can also gain a great deal. For example, machine learning algorithms may be trained to automatically recognize similar attacks by leveraging historical datasets that include specific occurrences of WannaCry ransomware outbreaks.

2. Network risk scoring: This is a quantitative metric that rates the risk of various network segments. Using the risk ratings as a basis, this metric is used to allocate cybersecurity resources. By examining historical cybersecurity records, AI can automate this process and identify network segments that are more susceptible to or participating in particular kinds of attacks.

3. Automating processes and human analysis optimization: Artificial intelligence (AI) can automate security analysts' repetitious security action-related activities. Analyzing historical action reports produced by security analysts to recognize and effectively counter specific assaults is one way to automate processes. With this information, AI systems create a model that may be used to subsequently identify similar cyber-activities. AI systems react to attacks using this approach without the need for human reasoning. It might be challenging to fully automate the security procedure at times. In this instance, AI may be integrated into the cybersecurity workflow, allowing computers and system analysts to collaborate on tasks.

5. THE FUTURE AND BENEFITS OF AI IN CYBERSECURITY

Although the exact future of AI is unknown, several sources provide their predictions and observations. Although there are numerous advantages to the rapidly expanding technology, there are also some worries in the cybersecurity sector. The market for artificial intelligence (AI) in the cybersecurity sector is anticipated to reach $46.3 billion by 2027, as per a study outlined in Hall's research, demonstrating the enormous increase anticipated for this technology. He identifies four key advantages of employing AI in business: the technology improves with time, can manage massive volumes of data, detects and responds to assaults more quickly, and improves overall security for the company using it.

He also discusses the worry that if there are insufficient diverse data sets, AI may produce false positives and erroneous findings. However, he suggests that another area of AI called deep learning may be able to help reduce these false positives.

Based on the second of Hall's four categorized advantages, there is ample evidence to suggest that AI is capable of handling massive volumes of data, something that would be unimaginable for a person to accomplish. In order to properly address any future cyberattacks, a vast quantity of data must be examined from past cyberattacks. This analysis is much beyond the capabilities of humans, which is where artificial intelligence (AI) comes in.

The importance of the caliber and volume of these data sources was emphasized by Addo et al. in both of their publications. This is necessary to teach the AI as effectively as possible, to support its ongoing development, and to help it understand how to respond to evolving cyberattack variants.

The question of whether AI will eventually replace humans is one that is hotly contested. There are differing views on this; some sources claim it will, while others claim that people will still be required. Of course, no one knows for sure, but this is a legitimate discussion that is emerging with the development of technology.

According to a study of IT executives, 41% thought AI will take over their position in their company by 2030, while 9% disagreed, saying AI "is not likely to replace humans." Hunter offers his thoughts on how, as an alternative to hiring people to perform this labor, AI algorithms might be used to evaluate vulnerabilities, locate ports of entry, and

other issues that need to be fixed in real time. Yampolskiy has an extreme stance, stating that a super intelligent AI (SAI) system breakdown would result in a worldwide catastrophe. He claims that Elon Musk, Bill Gates, and Stephen Hawking have all voiced concern about AI's ability to advance to the point that humans are unable to manage it.

On the other hand, a number of sites assert that despite the advancements in technology, people will still be required to write and maintain code. In his book, Addo et al. describe how artificial intelligence (AI) will identify dangers and evaluate unadulterated, unprocessed data, but that humans would still be required for error correction and attack protection. According to one of Labs' interview comments, software cannot identify everything on its own; at the very least, people will be required to adjust AI or ML to the specific context.

According to every source, businesses will spend more on cyber security in the next years as they become more aware of the hazards posed by the internet. For example, in three years, US spending is expected to surpass $63.5 billion, or 0.35 percent of GDP, according to the Technology Industry Association (TIA). Global expenditure is expected to increase by 8.2 percent between 2014 and 2015, according to Gartner Inc. The US $407 billion potential net benefit of block chain technology is the highest of any technology.

Product inventory management, sometimes referred to as provenance management, has the most economic potential (US$962 billion) and has become a new area of attention for many supply chains.

Block chain technology might help companies in a variety of industries, from mining and other heavy industries to fashion labels, in response to investors' and the public's growing interest in ethical and sustainable sourcing. The goal of banking and financial organizations is to lessen fraud and identity theft. Examples of this include the use of digital crypto currencies and the promotion of cross-border and remittance digital payments.

According to an analysis of artificial intelligence's benefits in the field of cyber security, organizations who use AI to improve cyber security have major advantages. The ROI of two out of three firms grew on cyber security products, demonstrating this. Siemens AG, a global leader in automation, digitalization, and electrification, for instance, employed Amazon Web Services (AWS) to build a high-speed, AI-based, self-controlled, and incredibly elastic platform for its Siemens Cyber Defense Center (CDC). 60,000 possible assaults may be estimated by the AI that was used in a given amount of time. This capacity was managed by a staff of less than twelve people thanks to the AI that was used, and system performance was not negatively impacted.

By using AI in cyber security, organizations may understand and use previous danger patterns to identify new risks. As a consequence, time and effort are saved when spotting, looking into, and addressing dangers. Approximately 64% of administrators report that the cost of finding and responding to breaches was reduced using AI. Reacting quickly is crucial to avoiding cyberattacks. Organizations may save costs by 12% on average. The cyber security environment is fast shifting from identification, manual reaction, and mitigation to automated mitigation, which is one of the main reasons AI presents prospects for cyber security. AI is able to recognize intricate and new changes in attack extensibility.

Because of the growing uses of AI, there has been a tenfold increase in the requirement for expertise in this field. Experts in cybersecurity are also encouraged to develop their AI skills. These all point to an increasing use of AI in cybersecurity in the future. Increasing awareness encourages cybersecurity developers to create AI protections. These methods will guarantee that cybersecurity defenses are soon fully automated. Consequently, the trend toward AI integration in cybersecurity points to a promising future for AI-based cybersecurity. Businesses are also encouraged to employ the technology due to how well it promotes security.

For the majority of users, implementing a certain kind of security is essential. The inclusion of these technologies will therefore raise the bar for creating AI systems that provide cybersecurity. AI algorithms have also been observed to be increasingly used in cyberattacks. AI is now required for cybersecurity protection as a result of this reason. This has to do with the idea that the strongest defense against an identical AI-based attack is the capabilities of AI technology. The creation of a federated learning system ensures the safety of personally identifiable information while using AI to combat cybercrime and address identity theft. The greatest protection in the current digitalization era is hence to use AI-based technologies to prevent cyberattacks.

6. AI'S DRAWBACKS AND LIMITATIONS IN CYBERSECURITY

- **Cost effectiveness:** Not everyone can benefit from artificial intelligence (AI) since it might often be too expensive to use.
- **Cyber threats:** These days, hackers can too easily exploit your data and privacy. If you don't take precautions, they may simply monitor your whereabouts and hack your personal information.
- **A machine taking over human control:** Oldest worry about AI is that machines would take control of people. This issue has been portrayed in several films and literature previously. Action needs to be done to stop this from occurring.

- **Job loss:** Artificial intelligence is viewed as a danger since some studies indicate that a sizable portion of the labor force will be displaced by machines and AI applications.
- **Not everyone is familiar with AI:** Not everyone is eager to learn about and wants to work with the newest, cutting-edge technology.
- **Lack of autonomy in maintaining cybersecurity:** Despite significant progress in integrating AI approaches into cybersecurity, security systems are still not entirely self-sufficient. There are still jobs that need human assistance since they can't yet fully replace human decision-making.
- **Data privacy:** Artificial intelligence (AI) systems, such as ANNs and DNNs, are constantly evolving and growing more sophisticated. However, there may be a drawback to the increased demand for big data in terms of data protection. Both public and commercial organizations may become reluctant to disclose personal data at all due to concerns about data privacy raised by the analysis of massive volumes of data. There may be unresolved questions and a lack of transparency for impacted companies regarding the usage of personal data, its purpose, and the decision-making process involved in AI-based solutions.

According to Charles Darwin's view of man's descent, man has always strived to guarantee that he has mastered the way nature treats him. The goal of humans has always been to ensure that they have a better environment to live in by having the power to alter what nature provides to suit their activities and survival. As the human revolution reaches the industrial stage, it is evident that they have made significant contributions to guaranteeing their broad use of the knowledge of technology that will support them in their daily tasks. Knowledge of physics and the ability to operate sophisticated technology allowed humans to completely replace animals in their daily routines. They were able to guarantee that their output and productivity had increased with the aid of the machinery. A guy discovers that machines are superior than people. Thus, the objective was to completely rethink the process of creating with a machine in order to get higher quality output and prevent any annoyance caused by human error. Additionally, they were able to enhance the gear and eventually arrive at modern computer technology.

One of the most commonly utilized technologies in existence today is computer technology, which means that many necessities of life are supported by it. As a result, certain technological criteria need to be put in place to guarantee that the effectiveness and security of the services provided are of concern. Financial institutions and other industries that own vital information about our lives have a right to utilize technology. Furthermore, our organization's technology includes information that other firms might utilize to gain a competitive edge. Computer technicians and developers must make sure they have included all the security measures to secure the protection of the data included in the system, given how important information is to the modern world.

Computer scientists were forced to encrypt their data before transferring it because they had to devise a method of guaranteeing data security. The encryption process will guarantee that the data remains unusable even in the event that it ends up in the wrong hands. It is challenging to utilize since one needs the decryption code in order to decode the relevant data. As data encryption technology developed, more individuals became aware of the underlying concepts.

Another problem emerged as a result of people realizing the procedure. Reverse engineering the procedure was made simple by people discovering the protocols utilized by the encryption applications and systems. The entire process of data security is considerably weakened by the potential to access the data being transported by having the protocol of detecting the encryption key. Computer scientists have to create more intricate procedures and processes to guarantee data encryption and proper operation.

The main objective of data security is accomplished. It makes sense to assume that robots will be the greatest at guaranteeing their security since, after all, they are trained to accomplish everything humans cannot. As a consequence, artificial intelligence technology is introduced, greatly enhancing the machine's security. There is never a situation when the information might be misused. The AI system works to make sure that all of the protocols it is designed to adhere to have been allocated in order to secure the security of the relevant data.

The fact that artificial intelligence is only a computer code designed to make sure that it has followed the procedures and improved itself in case of anything is one of its biggest limitations. This situation could seem reasonable because they have the ability to grow in any situation.

But since the system is fully coded, anyone may take control of it, manipulate it, and use it as a weapon. Just a few lines of code need to be changed, and the lengthy workdays might become a tool that is used against the company. Consequently, AI technology has the potential to be a weapon that destroys what it was designed to safeguard if it is utilized with the right skills and knowledge. One of AI's biggest barriers to cyber security is this element. Given their understanding of AI technology's potential, developers and computer scientists ought to take this into account.

7. CONCLUSION

Cyber threats and assaults are becoming increasingly sophisticated, necessitating the development of new, scalable approaches. According to recent study, phishing and spam detection, malware detection, and network intrusion detection are the three primary goals of AI-based cybersecurity algorithms. Numerous studies combined various AI techniques, such as ML/DL approaches with bioinspired computation, or diverse learning approaches, such supervised learning and reinforcement learning.

These pairings produce very good outcomes. While AI will undoubtedly play a part in resolving cyberspace challenges, there are concerns over AI trust as well as threats and assaults originating from AI. In addition to developing automated and intelligent cybersecurity solutions, our objectives included giving a thorough understanding of the significant role artificial intelligence may play in intelligent decision making. In order to do this, we have introduced security intelligence modeling, which uses a variety of AI-based techniques to intelligently address cybersecurity concerns. These techniques include machine and deep learning, knowledge representation and reasoning, and the idea of knowledge or rule-based expert systems modeling. Such artificial intelligence (AI) modeling may be used to a variety of issue areas, such as malware analysis and the identification of dangerous behavior that could result in a phishing attack or harmful code. Therefore, in this paper, we saw the significance of artificial intelligence in cyber security, as well as the many issues it raises and how to mitigate them. Even with its limitations, artificial intelligence is still very important to cyber security. Artificial Intelligence will help to enhance cyber security in order to overcome the shortcomings.

8. REFERENCES

[1] Morovat K, Panda B. A survey of artificial intelligence in cybersecurity. In2020 International Conference on Computational Science and Computational Intelligence (CSCI) 2020 Dec 16 (pp. 109-115). IEEE.

[2] Sarker, Iqbal H., Md Hasan Furhad, and Raza Nowrozy. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." SN Computer Science 2 (2021): 1-18.

[3] Shearstone, L., 2023. The Impact of Artificial Intelligence on the Cybersecurity Industry.

[4] Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." Cyber, Intelligence, and Security 1, no. 1 (2017): 103-119.

[5] Ansari, Meraj Farheen, Bibhu Dash, Pawankumar Sharma, and Nikhitha Yathiraju. "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review." International Journal of Advanced Research in Computer and Communication Engineering (2022).

[6] Dash, Bibhu, Meraj Farheen Ansari, Pawankumar Sharma, and Azad Ali. "Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review." International Journal of Software Engineering & Applications (IJSEA) 13, no. 5 (2022).

[7] Rjoub, Gaith, Jamal Bentahar, Omar Abdel Wahab, Rabeb Mizouni, Alyssa Song, Robin Cohen, Hadi Otrok, and Azzam Mourad. "A Survey on Explainable Artificial Intelligence for Cybersecurity." IEEE Transactions on Network and Service Management (2023).

[8] Zhang, Zhimin, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, and Kim-Kwang Raymond Choo. "Artificial intelligence in cyber security: research advances, challenges, and opportunities." Artificial Intelligence Review (2022): 1-25.

[9] Jenis Nilkanth Welukar, Gagan Prashant Bajoria, "Artificial Intelligence in Cyber Security - A Review", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 6, pp. 488-491, November-December 2021.

[10] Li, Jian-hua. "Cyber security meets artificial intelligence: a survey." Frontiers of Information Technology & Electronic Engineering 19, no. 12 (2018): 1462-14.