World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity in Artificial Intelligence

Quiana Bradshaw *

Department of Doctor of Education in Computer Science, Judson University. Elgin, Illinois, United States.

World Journal of Advanced Research and Reviews, 2025, 27(01), 1735-1744

Publication history: Received on 10 June 2025; revised on 15 July 2025; accepted on 17 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2703

Abstract

We are currently living in an emerging technological society in today's society. AI has grown to a level where it is being used in a variety of fields, including banking, customer service, education, and law enforcement. What are some of the risks with cybersecurity issues and artificial intelligence? What kind of impact does artificial intelligence have on cybersecurity? Are there some drawbacks and limitations when using AI for cybersecurity? When using Artificial intelligence, it has provided many profound ways to implement measures of cybersecurity. There are some ways that AI improves the area of cybersecurity and helps manage the vulnerability of security issues. Granted, many cyber-attacks occur today, and data breaches are costing corporations millions of dollars for each incident. Cybersecurity efforts can help strengthen the validity of artificial intelligence and give it a new predictive perspective to safeguard information. When using AI Neural Nets can it be combined with absolute resolve to provide solutions to cyber security in AI issues? Furthermore, as society technologically evolves the need and use of AI helps one automate ideas and the way business is conducted. Hence, the push to adapt to AI needs to open up a door for improvement with cyber-attacks and vulnerabilities that may cause a hindrance. AI utilizes cybersecurity efforts and since there are new security risks cybersecurity needs to be revamped and have a broad level of playbook protection when the implementation of AI is complete.

Keywords: Artificial intelligence; Threat intelligence; Cybersecurity; AI Vulnerabilities; Privacy risks

1. Introduction to Cyber Security in Artificial Intelligence

In our emerging technological society, the growing rise of artificial intelligence has been implemented in almost every industry that you see today. Artificial intelligence is used in a variety of industries that have some form of interaction with individuals across the globe. Some of these industries include the following: The financial industry, supply chain, healthcare, construction, and aerospace just to name a few. Hence, with that emersion of AI, how can we keep those areas secure and how will it help us by doing exactly just that? The expansion of machine learning and artificial deployments in our society is growing at an exponential rate. Think of the AI assistants that are used when accessing our smartphones like Siri and Alexa among others when requesting help with things in our homes or products that are needed. Yet, along with the growing rate of security risks and cyberattacks that occur each day is becoming increased implementation of AI and less methods to secure it. AI initiates machines to learn from experiences and inputs from its human creators.

Improving efficiency is a top priority in many industries, and AI has the potential to help in several ways: - Automation: AI can be used to automate repetitive and mundane tasks, freeing up human workers to focus on more complex and creative work. - Predictive analytics: AI can help predict future trends and outcomes, allowing businesses to make more informed decisions and optimize their operations. - Optimization: AI algorithms can be used to optimize complex processes, such as supply chain management, to reduce waste, improve efficiency, and save time and money.

* Corresponding author: Quiana Bradshaw

There have been a number of threats and cybersecurity concerns and crimes that have threatened the way in which we do business. Many cyberattacks to the United States Infrastructure, Electrical grid and pipelines have been the concerns of many Americans. There is a legitimate amount of AI crime detection software that is for not only crime detection and prevention of crime using. (Caldwell, Andrews, Tanay, Griffin, 2020). Some of the features and AI detection are facial recognition, AI used to prevent fraudulent trading in financial markets, and AI deepfake videos to prevent crime. Cybersecurity is something that needs to be implemented with the increasing use of AI.

AI will continue to increase in our society today and is often used in a variety of business sectors that expand the use of it. (Khisamova, Begishev, Sidorenko, 2019) Artificial intelligence is widely used in education, healthcare coordination, retail, and pensions. The term artificial intelligence (AI) was presented by American computer scientist A. Turing. The acceptance of AI is continuing to grow but it raises questions for the security of it. The issue of securing confidentiality and security for individuals using AI and there have been problems when applying cybersecurity with AI. Some of the concerns with AI are the ethics and humanity and AI decision-making process. How can this be essential when establishing cybersecurity to AI? Is it something that can be prepared for when using the AI infrastructure or should something else be implemented just in case?

Robots are created for everyday use with households in the form of vacuum cleaners and AI is used for self-autonomous driving cars. This can very well prove as a necessity to help anyone that is a senior citizen that needs help or is disabled and cannot drive a vehicle themselves. Having AI in cars can along them to become a hub for hackers to infiltrate the AI systems infrastructure. Assessing the very validity of the system that was created to assist the individual. The vulnerabilities with AI have left gaps in the research for self-driving cars. The question arose and notion of the AI self-driving car would inherently run down a pedestrian and the ethics of the AI is autonomous cars are still a question for AI.

However, a study was conducted by MIT in 2016 to define whether or not the “Moral Machine” can be adaptive for the ethics that are instructed for the AI in the self-driving cars. This can help facilitate the need to not run down a pedestrian and help the system to define the rational thought (or deep learning) of using the proper safety precautions. (Khisamova, Begishev, Sidorenko, 2019).

Safety concerns will continue to play a pivotal role in the design and creation of additional autonomous self-driving cars. Will AI slow down on busy streets with fellow drivers and pedestrian crossings? The more the challenges are for AI and cybersecurity is what researchers are determined to explore and share with society. When you think of the threats and sovereignty of extensive risk prevention with AI, think of the benefits that can occur with that? Are AI systems in some way autonomous and can it provide some sort of risk management for technological systems in the coming future? Artificial Intelligence in nearly every aspect of our lives now. With the expansion of knowledge, there has to be increased methods of security and this is what needs to be thoroughly implemented with AI.

Cybersecurity efforts are equally important as implementation of AI systems itself. With the increase of individuals getting connected online there are a plethora of ethical issues that can occur with both artificial intelligence and cyber security. Innovation and diverse cyber security defense mechanisms are necessary for using AI systems. That preparedness for the release and efficiency of AI is not prepared in with the realms of cybersecurity. Cybersecurity has to stay one step ahead of AI and formulate a strong counterattack measures. Markevych & Dawson (2023) “ Enhancing intrusion detection systems for cybersecurity using artificial intelligence and some of the methods were mentioned. There is AI enhanced honeypots, ChatGPT IDS design, banking and financial systems, and deep learning in network intrusion detection.

Each of these methods can be evaluated to help with the defense when using AI systems. Cyber security can be applied to each of these methods examining the threats and vulnerabilities that is associated with it. There are a variety of mechanisms that scientists are working on to make AI safe and provide a sense of security for users. The effort and specifications that systems use is explained thoroughly. For instance, the enhanced AI honeypot system learns for attacks from and morphs networks into a protective state. It will remember those attacks and put a barrier up from the previous attack encounter. In ChatGPT IDS Design the advanced capabilities and functionalities of the AI IDS GPT-4 was the example that was selected for its broad knowledge and accuracy. One of the suggestions is that the tcpdump can be used for the counterattack when intrusion is performed again using the AI ChatGPT IDS. Banking and financial systems have enhanced AI systems that they have to use to assist the millions and millions of customers that it contains. Artificial neural network was recommended to deal with the intrusive cyber-attackers. When using deep learning in network intrusion detection it can assess and review malevolent traffic on the network. (Markevych & Dawson, 2023).

1.1. Cybersecurity

Cybersecurity models are necessary to legitimize user authentication and minimize cyber security risks when using AI systems. Machine learning algorithms in cybersecurity focuses on learning and intrusion detection techniques. The model that is utilized with machine learning is evaluated and used as a prediction analysis for cybersecurity. The growth of the AI cybersecurity software market is increasing. The models and machine learning algorithms that are used for detecting attacks using AI is expected to grow in the coming years. The current market application span of AI in cybersecurity markets have sales of 3.92 billion in 2017 and it is expected to reach 34.81 billion dollars by the year 2025. (Sen, Heim, & Zhu 2020).

The complexity of cyberattacks is becoming increasingly diverse at every turn. In the world of cyberspace, especially since dial up was introduced to the world, there was a certain intrigue with being able to get connected even when it was through AOL. The advancement of emerging technology and AI there has to be defensive perimeters set to protect users from this kind of intrusion measure. The security methods that must be implemented when using AI and various other software technologies needs a comprehensive upgrade. There are many kinds of cyber-attacks that can occur even in the advanced AI systems such as viruses, worms, trojans, ransomware, spyware, and phishing. Each of these attempts can come about when using technologies and software. (Al-Hawamleh, 2023).

1.2. AI using social media Driven Cyber Threat Intelligence

Cyberattacks have a huge price tag and are estimated to cost a 10.5 trillion dollars in damage to the world's global economy. With the advancement of artificial intelligence, which can apprehend the contextual information of social media posts that relates to cyberattacks. The estimated growth of the costs of cyberattacks were projected to grow more than ten times that by the year 2025. Yet, deep learning (DL) is used to alleviate the overwhelming loss to the world's global economy during the cyberattacks. Cyber threat intelligence is used in defense of cyberattacks that can damage the world economy. (Sufi, 2023). Sufi (2023) "A New Social-Media driven Cyber Threat Intelligence article innovations such as artificial intelligence (AI) and natural language processing (NLP) was utilized to comprehend cyberattacks monitoring social media posts and its relation to cyberattacks.

A nationwide preparedness using convolutional neural network (CNN) which is an anomaly detection deep learning AI method. The method was used to detect anomalies on the following countries such as Australia, Russia, China, Ukraine, Iran, and India. (Sufi, 2023) Having a detection of this sort can help sniff out the potential dangers that are on the web as that can threaten the very safety of users that use the internet even social media. Social media cyber intelligence can very well identify potential threats and challenges along with the drawbacks during research. Some of the five challenges of social media driven solutions which includes the following:

- Legal & ethical concerns
- Bias and interpretation
- Data relevance
- Noise
- Data overload
- (Sufi, 2023).

The more it shows that the need for increased use of cybersecurity in AI has to take place to help defend users better with safety. Artificial intelligence uses a set of instructions to manage a variety of applications. Artificial intelligence is no stranger to using some type of cybersecurity and or cryptography in some sort of way. Some of the methodologies that are used can vary from machine learning, big data, Internet of Things (IoT), and other sectors. Meanwhile, some of the cybersecurity methods that are positioned to protect all kinds of electronics are essential. Protection is necessary for computer servers, networks, data centers, and cloud computing-based access centers. Cryptography protocols are generally used after the cybersecurity team evaluates the playbook. (Nitaj & Rachidi, 2023).

2. The use of Artificial Intelligence and Machine Learning as a Defense Mechanism

On the other hand, artificial intelligence has been used to help provide a prediction and knowledge of detecting a cyber security line of defense. The banking and finance industry heavily rely on the use of artificial intelligence and implementing cybersecurity in the foundation of it is also necessary. AI can assist with monitoring fraudulent purchases and suspicious account activity for banks across the world. This can help provide a sense of security with the ease of protection that banking customers can benefit from. Machine learning will act as a predictor and obtain which charges can potentially be fraudulent opposed from actual. Online retail customer support use automated machines to assist

customers and provide information from their website that interests them even more to purchase a product. This form of AI provides security for users and will help make the online experience even better. The basis of using it for customers can help them efficiently acquire the service by also using it as a predictor and extract information using natural language to help customers shop.

The vulnerabilities of AI are concerning and has to be addressed when providing implementation of cybersecurity with it. AI vulnerabilities go beyond coding errors and bugs so with that being said it also includes AI systems and how they can be manipulated. In the article " Cybersecurity for AI Systems (Sangwan, Badr, & Srinivasan, 2023) research has been done attackers launch attacks into AI systems often manipulating their input to produce an unintended outcome. Some of the attacks that were examined were biometric recognition systems defense mechanisms, machine learning models in 5G networks, AI based network intrusion detection systems and ML CAD systems. Each of these systems may have had an adversarial attack at one time or another. Each attack has been categorized with their vulnerabilities listed and their defense mechanisms. The defense mechanisms should be analyzed, and valid cybersecurity measures should be implemented accordingly.

How can AI cybersecurity become more reliable if it is not used efficiently and immediately? This is a question that should be asked when implementing a valid cybersecurity plan for AI systems. The goal is to ensure safety when using such a system and having the ease of security when accessing sensitive or even confidential data. Some of the ways that hackers use ChatGPT, AI bots that use (Deepfake voices), generative AI fake email exchange, and a variety of other tools to be intrusive and gain access to unauthorized accounts. These scenarios are often used and using new forms of smarter technologies and generative AI is something that creates increased challenges each time. A lot of times hackers will utilize a "one size fits all" approach to how they hack into systems and in AI it is more definitive. Makers of ChatGPT have released GPTZero and ZeroGPT which is more of a generative AI.

Some researchers feel that AI have been heavily used by criminals and have increased the public danger. Some of the threats that pose a threat to cybersecurity. AI has a mode of self-training and predictive measures for diagnosing or estimating what very well may or may not happen. Often times, A can be used for a variety of fields like education, healthcare, banking, and finance, among other things. According to Khisomova, Begishey, and Sidorenko (2019) Some of the IT threats in could be generated using AI in three particular ways:

- Malware attacks
- Physical attacks
- Social engineering attacks.
- (Khisomova, Begishey, and Sidorenko, 2019).
- The treats of using AI in cybersecurity can really have a huge impact on everyone that is involved.

3. Artificial Intelligence & Intelligence Automation (AI & IA)

Both AI and IA use AI enabled detection models, and these decision models helps deals with fraud and suspicious activity that may occur while online. The models will make inferences and receive evidence that will help it decipher unauthorized intrusions. The IA has a framework that is based off of six elements that including the 6 W's (who, what how, whom, where and when). IA compared to AI focused on the building and the dimensions that are necessary for the system ecosystem. (Zhou, Rudin, Gombolay, Spoherer, Zhou, and Soren, 2023). For example, it is like having to out together the puzzle with all the pieces in place. Each piece must align perfectly in order to build it properly and help it coexist in the right way.

Many can appreciate using both AI & IA to help break down the complexity of fraud and use it as a prediction model to keep it valid. What IA lacks is the lack of human interpretability being what causes a mishap in imperfect evaluation of users. Most AI model engineers often do not evaluate their models prior to release to see if they actually can cause a multitude of problems as a result. What can help in instances of prediction and human interferences is the creation of the IA and AI models and then evaluating them to ensure their work. Another solution would be to involve more human interaction with the creation of these models. Businesses should focus on putting more humans at the core of it to see if it can help with the model's construction. (Zhou, Rudin, Gombolay, Spoherer, Zhou, and Soren, 2023).

Intrusion detection systems can assist with the capability to detect suspicious activity that helps minimize the intrusion by users that test the system to see how they can manipulate it. With cybersecurity there is a certain thing as cyber-threat intelligence that can help detect deceptive technology and other intrusions that are used in the world of technology and AI. The cyber security domain consists of machine learning models that prevent and counterattack to

keep systems more secure. Some of the machine learning techniques (Ahsan, Nygard, Gomes, Chowdhury, Rifat, & Connolly, 2022) and can assist with threats and vulnerabilities that can occur. These techniques can detect any anomalies that are used for malicious intent and cause cyber security risks.

The security risks and consequences of the risks can be very daunting and there should be a variety of defense strategies in place. Having an intrusion detection system (IDS) will monitor suspicious computer network systems for malicious unauthorized activity. IDS can detect both internal and external threats that can wreak havoc if there was unauthorized activity. AI can extend the logical reasoning intrusion scenarios to evaluate attacks. (Ahsan, Nygard, Gomes, Chowdhury, Rifat, & Connolly, 2022). Thinking of the security risks can be mind-boggling and think about the some of the additional cybersecurity measures using AI. There is a phishing email detection model using deep learning is something that is used to track or minimize phishing attacks. Phishing types of crimes can very well affect everyone in the world and the sad thing is that it has increased increasingly each day. Just a few of the dangers that phishing can cause are some of the following:

- Identity theft
- Damage to the organization's reputation
- Financial loss
- (Atawneh & Aljehani, 2023).

The goal of using AI (Deep Learning) to understand in what ways to detect fraud and phishing attempts is something that is genuine and valid to do. Artificial intelligence can detect cybersecurity issues with little to no interaction with humans. Deep learning and machine learning is also used and could be used as an effective model for cybersecurity incidents. Cybersecurity metrics can be used when using AI and what would help is the fact that more advanced techniques of security efforts needs to be in place. The goal of using AI is to make systems more efficient and think of the ways that AI can detect various security issues. Think of the manner in which bullying can happen online, which is called cyberbullying. AI uses deep learning to detect machine learning algorithms to help decipher the security issues.

Deep learning can outperform the algorithms that ML has, and the deep learning network (DNN) will assist when modes of security and cyber bullying events occur. There are also concerns when it comes to both AI & robotics and the concern about data protection is embedded in AI and robotics. Artificial intelligence often tries to relate to humanlike or humanness types of human intelligence or technological growth. Think about the framework of AI linked technologies that reevaluates the features of today's technology. The technological growth of AI is growing increasingly each day. Our society is becoming increasingly connected as the days go by.

3.1. Challenges & Trust Issues in AI Cybersecurity

AI systems can perpetuate existing biases if the data they're trained on is biased. This can lead to inaccuracies and discrimination. Lack of transparency: AI systems can be difficult to interpret, making it hard to understand how they arrived at their decisions. This can lead to a lack of trust in the system. Cybersecurity threats: AI systems can be vulnerable to cyber-attacks, such as hacking and data breaches, just like any other system connected to the internet. How AI is being used to help prevent and detect cyber-attacks, the benefits, and challenges of using AI in cybersecurity. The role of AI in cyber defense vs cyber offense has the potential for AI to make cyber-attacks more sophisticated and dangerous. The ethical implications of using AI in cybersecurity.

Yet, there are a few key ethical implications to consider: - Bias: AI systems can perpetuate existing biases in the data they're trained on, potentially leading to discrimination or injustice. - Privacy: AI systems can potentially collect, analyze, and store sensitive personal information, raising privacy concerns. - Accountability: It can be difficult to hold AI systems accountable for their actions, as they may not have the same level of decision-making or moral reasoning as humans. - Autonomy: As AI becomes more sophisticated, there is concern about the level of autonomy it may have and the potential for it to make decisions without human oversight.

AI can help prevent and detect cyber-attacks in a number of ways: - Pattern recognition: AI can analyze large amounts of data and identify patterns of suspicious or malicious behavior. - Threat intelligence: AI can continuously learn and adapt to new threats by analyzing data from multiple sources, such as network logs, security system logs, and malware databases. - Real-time detection: AI can quickly identify and respond to emerging threats in real-time, helping to prevent or mitigate the damage of an attack. As for the challenges, some of the key ones include False positives: AI can sometimes generate false alarms, leading to wasted resources and a higher risk of missing actual threats. - Data quality: The effectiveness of AI systems depends on the quality and quantity of the data used to train them.

Here are a few examples of cyber security threats that AI systems can face: - Malware: Malicious software that can infiltrate AI systems and cause them to malfunction or leak sensitive data. - Phishing: Attempts to trick AI systems into revealing sensitive information or granting access to systems through social engineering tactics. - Distributed Denial of Service (DDoS) attacks: Overwhelming AI systems with traffic to make them unavailable to users. - Deepfake attacks: Using AI to create fake videos or audio recordings to deceive or manipulate AI systems.

Meanwhile, there are some instances of AI cybersecurity issues that include Anomaly detection: AI systems can be trained to detect unusual or suspicious activity in networks and systems, helping to identify potential cyber threats. Natural Language Processing (NLP): AI systems can analyze and understand text-based threats, such as phishing emails or social media posts, and alert cybersecurity teams. Intrusion detection: AI systems can monitor networks and systems for signs of intrusion, such as unusual login attempts or unusual traffic patterns. Cyber threat intelligence: AI can be used to analyze large amounts of data and identify patterns of malicious behavior, allowing cybersecurity teams to proactively identify and respond to threats.

On the other hand, some ways that AI systems can use intrusion detection to monitor cyber threat intelligence and protect users from unauthorized attacks: Network monitoring: AI systems can analyze network traffic in real-time and look for patterns that indicate a potential attack, such as unusual traffic patterns or communication with known malicious IP addresses. Behavior monitoring: AI systems can analyze user behavior and flag unusual or suspicious behavior, such as accessing sensitive data or attempting to bypass security controls. Vulnerability scanning: AI systems can scan for vulnerabilities in networks, devices, and applications, and identify potential weaknesses that attackers could exploit.

In addition to the points that were mentioned, AI can gain the trust of users in the following instances: Accuracy: AI systems that are highly accurate in detecting and preventing cyber-attacks can help build trust. If the system consistently performs well, users are more likely to trust it. Responsiveness: When AI systems are able to respond quickly to potential threats, it can show users that the system is working hard to protect them and their data. - Proactivity: AI systems that can anticipate potential threats and take proactive measures to prevent them can demonstrate their trustworthiness. For example, an AI system that automatically patches vulnerabilities or blocks suspicious activity can show users that it is actively working to protect them.

4. AI in Games that can Improve AI Systems

Gaming is actually a really useful way to develop and improve AI systems, for a few reasons: Huge amounts of data: Games generate enormous amounts of data, including player actions, strategies, and outcomes. This data can be used to train AI systems and help them learn more quickly and effectively. Unpredictable and complex environments: Games often feature complex and unpredictable environments, which can challenge AI systems and force them to adapt and improve. Fast iteration: Games allow AI systems to be trained and evaluated quickly and repeatedly, which can help them learn faster and become more effective over time. Virtual world environments are another excellent testing ground for AI development. Immersive environments: Virtual world provide a more immersive and realistic environment for AI systems to interact with, which can help them learn more effectively. - Complex interactions: Virtual worlds often feature complex interactions between characters, objects, and the environment, which can push AI systems to learn more sophisticated behavior. - Safe testing: Virtual worlds provide a safe and controlled environment for AI systems to be assessed and trained, without the risks associated with real-world environments.

4.1. Ways that AI can help the banking and finance industry

AI can help banking and finance: - Fraud detection: AI can analyze vast amounts of data to identify suspicious transactions and prevent fraud. - Personalized services: AI can help banks and financial institutions provide personalized advice and recommendations to customers based on their unique needs and financial goals. - Chatbots: AI-powered chatbots can provide 24/7 customer service, answer common questions, and even assist with account management tasks. - Risk management: AI can help banks and financial institutions assess risk and make more informed lending decisions.

4.2. Retail Online Customer Support

AI is already making big waves in retail customer support: - 24/7 customer service: AI chatbots can provide round-the-clock support to customers, answering questions and addressing issues outside of regular business hours. AI can provide Improved efficiency and can automate repetitive tasks, freeing up human employees to focus on more complex issues and provide better service. - Natural language processing: AI can understand and respond to customer queries

in natural language, making interactions feel more personal and natural. - Predictive analytics: AI can analyze customer data to predict future needs and provide proactive support, increasing customer satisfaction and loyalty.

4.3. Vulnerabilities in AI

While AI offers many advantages, it's not without its vulnerabilities. Here are a few to consider: Data bias, AI systems are only as good as the data they're trained on, and if that data is biased, the AI can perpetuate those biases. Security, AI systems can be vulnerable to hacking and cyberattacks, which could lead to sensitive data being compromised. Reliance on technology AI systems rely on hardware and software that can fail or be disrupted, which could lead to downtime or malfunction. To improve AI systems, it's important to address these vulnerabilities through. Comprehensive data collection and cleansing to reduce bias. Robust security measures, such as encryption and secure data storage. Redundant systems and backups to minimize downtime and ensure continuity of service.

4.4. How can AI be made more reliable in Cybersecurity?

There are several ways to increase the reliability of AI systems in cyber security. First, you have Adversarial training. This includes training AI systems to detect and defend against known and potential cyber threats, including cyberattacks that are specifically designed to fool AI systems. Second is Explainability, developing AI systems that are transparent and provide explanations for their decisions, so that security professionals can understand and trust the results. Third, is Human oversight. Having human experts review and validate the AI system's decisions, to ensure that they are accurate and appropriate. Finally, continuous improvement, regularly updating the AI system's training data and algorithms to ensure that it remains current and effective against evolving cyber threats.

4.5. How AI is emerging in our society today

AI is already playing an increasing role in our society, and it has the potential to positively impact many areas: *Healthcare*: AI can assist doctors with diagnosis and treatment recommendations and can help process vast amounts of medical data to identify patterns and improve care. *Transportation*-Autonomous vehicles and drones can improve safety and efficiency and reduce traffic congestion. *Education*: AI-powered tools can personalize learning and provide real-time feedback to students, allowing for more efficient and effective education. *Environment* AI can help monitor and mitigate environmental issues like climate change, deforestation, and pollution. All of these can help address pressing societal needs and improve quality of life.

Neural networks and AI can provide several advantages in cyber security, including, Improved accuracy. Neural networks and AI can analyze vast amounts of data and identify patterns that may be invisible to humans, leading to more accurate threat detection and incident response. Faster processing: AI can process data much faster than humans, allowing for real-time analysis and response to cyber threats. Increased efficiency, AI can automate many tasks, freeing up security professionals to focus on more complex and strategic issues. Better risk management: AI can help identify and prioritize the most significant threats to an organization, allowing for more effective risk management.

4.6. The Role of Intelligent Agents and their capabilities in AI

Intelligent agents are AI systems that can take autonomous actions on behalf of a user or organization. Here are some examples of how intelligent agents are being used in AI: Virtual assistants. Intelligent agents like Siri, Alexa, and Google Assistant use natural language processing and machine learning to understand user queries and provide relevant information or perform tasks like scheduling appointments or making purchases. Cyber security. Intelligent agents can be used to monitor networks, detect, and prevent cyber-attacks, and provide threat intelligence to security teams. - Supply chain management: Intelligent agents can analyze data from multiple sources to optimize supply chain operations, such as inventory management and delivery routing. - Financial trading: Intelligent agents are used to analyze market data and make trading decisions, often faster and more accurately than humans.

4.7. The Goal of using AI in our society

Here are some ways AI can improve cyber security and overall quality of life. Cybercrime prevention is a particularly important issue in society today. AI can detect and prevent cyberattacks, such as phishing frauds, malware, and ransomware, helping to keep personal and business information safe. Enhanced privacy: AI can be used to protect personal information by identifying and blocking unauthorized access to sensitive data, and by creating secure authentication methods. Smart cities: AI can help create smart cities, with improved transportation systems, optimized energy usage, and better resource management, leading to a more efficient and sustainable urban environment. Automated tasks: AI can automate repetitive tasks, freeing up time and resources for more creative and fulfilling work.

4.8. How AI can help with Data Loss Prevention and Leaks

Invasion of privacy can be quite daunting, and AI can assist in preventing and responding to data leaks. Data loss prevention can be assisted with AI and can be used to monitor and prevent the unauthorized sharing or exfiltration of sensitive data, both internally and externally. Automated data classification: AI can automatically classify, and label data based on its sensitivity and importance, making it easier to identify and protect sensitive data. Quick detection and response is what AI can detect data leaks quickly and alert security teams, allowing for a faster and more effective response, limiting the impact of the leak. Breach investigation, AI can analyze vast amounts of data and network logs to identify the source and nature of a breach, helping investigators to understand what happened and take action to prevent future incidents.

4.9. The Serious threat Hackers pose to AI

Hackers pose a significant threat to AI, and here's how they can 1) Malicious training data. Hackers can create or manipulate training data to make AI models produce biased or inaccurate results, or to trick AI systems into making bad decisions. 2) Data theft, hackers can steal data used to train AI models, compromising the security of the model, and potentially causing harm to individuals or organizations. 3) AI poisoning, Hackers can intentionally introduce flawed or misleading data into AI systems to corrupt their behavior or predictions, causing them to make mistakes or behave in unexpected ways. 4) Model hacking: Hackers can exploit vulnerabilities in AI models to hijack them and use them for malicious purposes, such as spreading misinformation or conducting cyberattacks.

Data manipulation by hackers can be dangerous because it can. Hackers can compromise the security of AI models and the decisions they make . As a result, it allows hackers to steal or alter sensitive data . Then hackers can cause the AI to enable the spread of misinformation or false predictions . It would directly cause AI systems to make biased or discriminatory decisions . Hackers can make AI systems vulnerable to adversarial attacks, where an attacker intentionally alters the input data to trick the AI system into making a mistake.

AI have been improving its models to help our society involves increasing accuracy. AI models can be fine-tuned to become more precise, reducing errors and improving performance. Improving interpretability, AI models can be designed to provide explanations for their decisions, making them more transparent and trustworthy. Building generalizability. AI models can be trained on more diverse data sets to make them more effective at handling new and unseen data. Implementing explainable AI, AI systems can be designed to explain their decisions and reasoning to humans, increasing transparency and reducing the risk of unintended consequences. Improving ethics, AI models can be developed with ethical considerations in mind, such as fairness, privacy, and accountability.

Ethical implications with AI and AI and fair use have a variety of elements that is included. Bias in AI algorithms, AI algorithms can perpetuate existing biases and create new ones if trained on biased data. Lack of transparency, AI algorithms can be opaque and difficult to understand, making it hard to know how they are making decisions and why. Job displacement. AI can automate tasks previously done by humans, potentially leading to job displacement and economic inequality. Privacy concerns, AI systems collect vast amounts of data, which can be used to invade people's privacy or used in unethical ways. Accountability, it can be difficult to hold AI systems accountable for their decisions, as it's not always clear who is ultimately responsible.

4.10. AI is a threat to some jobs in society

AI is a potential threat to some jobs. Here are some ways it could impact job security. Automation, AI can automate tasks that previously required human labor, such as data entry, customer service, and manufacturing. Skill shift, as AI advances, some jobs will become obsolete while new jobs are created that require different skills, such as data scientists and AI trainers. Productivity gains, AI can improve efficiency and productivity, allowing companies to do more with fewer workers. Upskilling required: Employees may need to acquire new skills to keep up with the changing job market, which could create barriers to employment for some people.

AI can never replace the human emotion that the world so thoroughly craves. AI can't replace the human touch in many areas. Think about the human emotion empathy. AI lacks the ability to understand and respond to human emotions, which is crucial in many jobs, such as healthcare and social work. Creativity is essential because AI may be good at replicating certain types of creativity, but it lacks the unique, abstract, and innovative thinking that humans can bring to the table. Ethics are important when using AI. AI systems are limited by the ethical frameworks they are programmed with and may not always make decisions that align with human values and morals. Human connection: Human interaction is an important part of many jobs, such as teaching, counseling, and sales. AI can't replicate the trust, rapport, and emotional connection that comes with human-to-human interactions.

Emotions and human intelligence are complex and nuanced, and AI simply can't grasp those aspects of human intelligence: Rationalization: AI lacks the ability to rationalize its decisions, which is an important aspect of human intelligence. It can explain its decision-making process but can't provide a full understanding of the thought process behind it. Emotional reasoning is something that human beings can make decisions based on feelings, values, and beliefs that are not necessarily rational. AI can't incorporate these types of non-rational thought processes into its decision-making. Intuition, human beings can often make decisions based on "gut feelings" or intuition. AI lacks the ability to tap into this subconscious level of reasoning, which can provide valuable insights.

AI can use security mechanisms that can help users feel more secure when going online, in a digital sense it can provide some type of rationale when it comes to surfing with ease. Security systems: AI can analyze surveillance footage, detect suspicious behavior, and alert authorities, helping to prevent crimes and protect people and property. Personal safety devices are good to have. AI-enabled wearables can detect and alert users to potential threats, such as falls or hazardous environments. A sense of Cybersecurity is what AI can detect and prevent cyberattacks, such as phishing swindles and malware, helping to keep individuals and organizations safe online. Decision-making: AI can help individuals and organizations make more informed and safer decisions by analyzing data and providing insights.

In society today, there are many uses for using advanced emerging technologies such as artificial intelligence. The growth of artificial intelligence should be monitored and controlled, not loosely disbursed, and let out of control. There are both advantages and disadvantages to using AI without any proper cybersecurity measures that should be in place. For instance, think about the self-driving car washing machines, and even the technologies that are in cars. These are products that can easily be attacked by hackers and taken over by them when they find a back door to get into them. All they need is your IP address and they can easily get in a cause catastrophic damage to your products. The scenario of safety and caution cannot be emphasized even more when it comes to using these products.

References

[1] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527. https://doi.org/10.3390/jcp2030027

[2] AL-Hawamleh, A. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2) Doi: https://doi.org/10.14569/IJACSA.2023.0140292

[3] Atawneh, S., & Aljehani, H. (2023). Phishing Email Detection Model Using Deep Learning. Electronics, 12(20), 4261. https://doi.org/10.3390/electronics12204261

[4] Bergadano, F., & Giacinto, G. (2023). Special issue "AI for cybersecurity: Robust models for authentication, threat and anomaly detection." Algorithms, 16(7), 327. Doi: https://doi.org/10.3390/a16070327

[5] Bhatt, H., Bahuguna, R., Singh, R., Gehlot, A., Shaik, V. A., Priyadarshi, N., & Twala, B. (2022). Artificial Intelligence and Robotics Led Technological Tremors: A Seismic Shift towards Digitizing the Legal Ecosystem. Applied Sciences, 12(22), 11687. https://doi.org/10.3390/app122211687

[6] Dawson, M. (2021). Cybersecurity Impacts for Artificial Intelligence Use within Industry 4.0. Buletin Stiintific, 26(1), 24–31. https://doi.org/10.2478/bsaft-2021-0003

[7] Dawson, M., & Szakonyi, A. (2020). Cybersecurity Education to Create Awareness in Artificial Intelligence Applications for Developers and End Users. Buletin Stiintific, 25(2), 85–92. https://doi.org/10.2478/bsaft-2020-0012

[8] Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. Applied Sciences, 13(13), 7507. Doi: https://doi.org/10.3390/app13137507

[9] Fisher, C. (2023). The Role of Ai in Cybersecurity. NZ Business + Management, 37(2), SP(12)-SP(13).

[10] Ivy, M., Brown-Liburd, H., & Miklos, V. (2020). The Ethical Implications of Using Artificial Intelligence in Auditing: JBE. Journal of Business Ethics, 167(2), 209-234. https://doi.org/10.1007/s10551-019-04407-1

[11] Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial intelligence and problems of ensuring cyber security. International Journal of Cyber Criminology, 13(2), 564-577. doi: https://doi.org/10.5281/zenodo.3709267

[12] Liu, X. M., & Murphy, D. (2020). A multi-faceted approach for trustworthy AI in cybersecurity. Journal of Strategic Innovation and Sustainability, 15(6), 68-78. Retrieved from https://www.proquest.com/scholarly-journals/multi-faceted-approach-trustworthy-ai/docview/2472179568/se-2

[13] Md, T. H., Hossain, M. A. E., Md Saddam, H. M., Akter, A., Mohiuddin, A., & Islam, S. (2023). A Review on Deep-Learning-Based Cyberbullying Detection. Future Internet, 15(5), 179. https://doi.org/10.3390/fi15050179

[14] Nitaj, A., & Rachidi, T. (2023). Applications of neural network-based AI in cryptography. Cryptography, 7(3), 39. Doi: https://doi.org/10.3390/cryptography7030039

[15] Renaud, K., Warkentin, M., & Westerman, G. (2023). From ChatGPT to HackGPT: Meeting the cybersecurity threat of generative AI. MIT Sloan Management Review, 64(3), 1-4. Retrieved from https://www.proquest.com/scholarly-journals/chatgpt-hackgpt-meeting-cybersecurity-threat/docview/2810212914/se-2

[16] Repede, Ş. E., & Brad, R., PhD. (2023). A comparison of artificial intelligence models used for fake news detection. Bulletin of "Carol I" National Defense University, 12(1), 114-131. doi: https://doi.org/10.53477/2284-9378-23-10

[17] Sangwan, R. S., Badr, Y., & Srinivasan, S. M. (2023). Cybersecurity for AI Systems: A Survey. Journal of Cybersecurity and Privacy, 3(2), 166. https://doi.org/10.3390/jcp3020010

[18] Sen, R., Heim, G., & Zhu, Q. (2022). Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for MIS academics. Communications of the Association for Information Systems, 51 Doi: https://doi.org/10.17705/1CAIS.05109

[19] Sousa, S., Cravino, J., & Martins, P. (2023). Challenges and Trends in User Trust Discourse in AI Popularity. Multimodal Technologies and Interaction, 7(2), 13. https://doi.org/10.3390/mti7020013

[20] Sufi, F. (2023). A new social media-driven cyber threat intelligence. Electronics, 12(5), 1242. Doi: https://doi.org/10.3390/electronics12051242

[21] Yu-Che, C., Ahn, M. J., & Yi-Fan, W. (2023). Artificial Intelligence and Public Values: Value Impacts and Governance in the Public Sector. Sustainability, 15(6), 4796. https://doi.org/10.3390/su15064796

[22] Zhou, L., Rudin, C., Gombolay, M., Spohrer, J., Zhou, M., & Souren, P. (2023). From artificial intelligence (AI) to intelligence augmentation (IA): Design principles, potential risks, and emerging issues. AIS Transactions on Human-Computer Interactions, 15(1), 111-135. doi: https://doi.org/10.17705/1thci.00185