WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Assorted Aspects and Implementation Patterns of Artificial Intelligence to Reduce Cyber Crimes

Prof. Dr. M . Randles[1]*

[1]School of Computing and Mathematical Sciences, Liverpool John Moores University, United kingdom

*Corresponding Author: Prof. Dr. M . Randles

DOI: https://doi.org/10.31185/wjcm.86

Received: September 2022; Accepted: November 2022; Available online: December 2022

ABSTRACT: Cyber crime was a major problem even before the epidemic, and it skyrocketed as the globe became increasingly digital after the pandemic began. It is crucial to think about how to make the web safer in the post-pandemic period, since the number of cyber scams is rising rapidly. With more people doing remote work and more people quickly embracing new technology, as well as with decreased monitoring and controls, hackers have more opportunities to attack weaknesses in the system. Individuals and businesses were rendered more vulnerable to cyber fraud as a result of each of these developments brought on by the epidemic. Since cybercriminals are just as technically savvy as their cyber security counterparts, a lot of effort and money must be spent on prevention. Professionals in the field of cyber security and cybercriminals nowadays share many of the same skills and use many of the same tools. Both cyber security experts and cybercriminals rely on them, but the former to protect their systems from the latter.

Keywords: Adoption of AI in Reducing Cyber Crimes, Cyber Crime, Avoidance of Cyber Crimes using AI Approaches

1. INTRODUCTION

The scarcity of cyber security specialists adds to the difficulty faced by hackers. According to the ISC2 - Cyber security-Workforce-Study-2020, the global need for cyber professionals is estimated at 3 million by 2020, with 2.05 million needed in the Asia-Pacific area alone [1].

An increasing number of people throughout the globe are now able to do their jobs from home, increasing the risk of cyber assaults. Cybercriminals are a threat to businesses of all sizes and their consumers because they are continually looking for new ways to generate money.

Though it's difficult to predict when and where these assaults will occur, many companies are relying on Artificial Intelligence (AI) to bolster their cyber security. We enjoy an unrestricted way of life, and the alternatives available to us in the digital sphere are almost limitless. However, the risk that our private data may be compromised due to Cyber crime is quite real [2].

The significance of cyber security has grown over the last several years. Keep in mind that cybercriminals may operate 24/7/365 from any location in the universe, and that they can use our personal information to steal our money [3, 4]. So AI and ML are becoming more and more important in the fight against Cyber crime. AI analyses patterns in data from past cyber occurrences to predict potential threats. Consequently, security officers will have more time for the tasks that really matter.

Recently, there has been a flurry of interest in using AI to improve cyber security. As was previously said, both the frequency and complexity of cyberattacks have increased. AI must be integrated with current cyber security strategies in

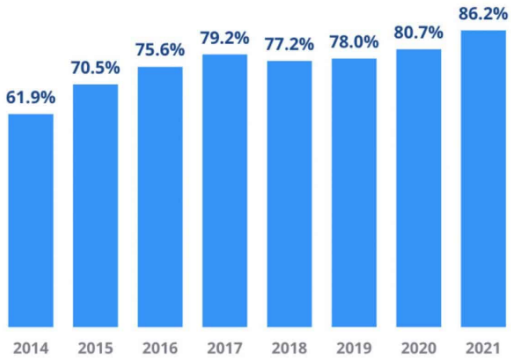

FIGURE 1. Organizations compromised towards cyber attacks

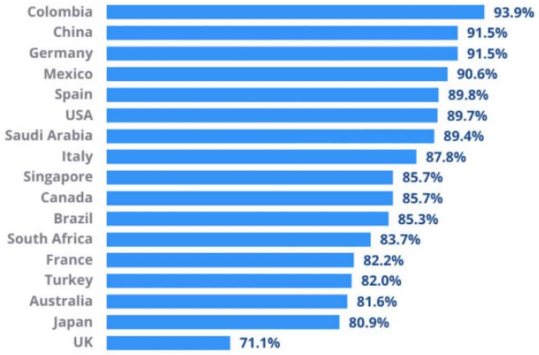

FIGURE 2. Penetration Levels of Cyber Crimes in Assorted Countries

order to provide accurate risk assessments and reduce the frequency of cyberattacks.

ZDNet reports that new security systems can identify threats like phishing schemes and new malware variants by collecting and analysing data from millions of cyber incidents [5].

There are cybercriminals that purposefully modify their malware's code so that antivirus programmes won't flag it as malicious. It's a huge challenge to find and eliminate all the many forms of malicious software. And now is the time to give thanks for artificial intelligence and machine learning systems, which provide formidable anti-malware protection.

The system may compare newly discovered malware with its database, analyse the code, and block attacks before they ever begin. This technique is effective even if the malicious code is hidden deep beneath a mountain of otherwise harmless or worthless code [6].

A monitoring system powered by AI can keep tabs on all of a user's typical activities and respond properly when it detects any out of the ordinary behaviour. To have such an edge in the present day is invaluable.

Applications aside, AI and ML are rising to prominence as key players because of their ability to prevent risks in real time without disrupting business as usual.

Data like the ever-increasing volume of communications (videos, chats, emails, etc.) may be tracked by this system even if they are not apparent to the human eye. Now that you have piqued my interest, let's examine the benefits of artificial intelligence in cyber security and see how they apply to this blog.

2. ISSUES TACKLED BY CYBER SECURITY TOOLS POWERED BY ARTIFICIAL INTELLIGENCE

All indicators of breach or exploit may be automatically analysed by AI, allowing security experts to be notified of potential threat events.

Cognitive reasoning may be used to establish connections between many types of threat entities related to real events, such as malicious entities, suspicious IP addresses, and hazardous files [7, 8].

No matter the specific implementation of AI, it's clear that technology has the potential to provide crucial insight into an incident and help a business comply and adapt.

3. USES OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

The creation of security policies and the design of the network architecture are two essential parts of network security. Traditional methods of doing these jobs took considerable time, but advancements in AI are shortening that time significantly.

This is achieved by keeping an eye on and analysing network activity and then suggesting security policies. Now that the security infrastructure is in place, experts may shift their attention to other areas of technological development [9, 10].

Up to 95% increases in detection rates are possible with the use of AI. Seeking to ascertain the source of the problem? False positives are a problem, therefore that's a yes. The best course of action here would be to combine AI with tried-and-true techniques. This integration of age-old and cutting-edge tools might increase detection rates by as much as 100 percent while also cutting down on false positives.

Danger hunting may be made better with the help of AI by including behaviour analysis. Application profiles may be developed for use inside a company's network by analysing data collected from endpoints [11].

FIGURE 3. **Global Market Size of A.I. in Cyber Security Market**

In the field of cyber security, Cylance is among the most prominent organisations that use AI. A consumer antivirus product, Cylance Smart Antivirus, offers businesses and homes the same degree of AI security often reserved for large organizations [12].

4. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial intelligence and machine learning are all that is required to detect malware in legitimate data. Thus, an antivirus is developed that watches for the moment a threat is ready to be carried out and then eliminates it automatically. An enormous number of users were shielded from the Wannacry ransomware attack thanks to it.

AI and ML have the potential to enhance the vulnerability management capabilities of existing vulnerability databases. Technologies like user and event behaviour analytics (UEBA), when fueled by AI, may monitor server and endpoint activity for anomalies that might indicate an attack. Before vulnerabilities are officially publicised and remedied, this may help organisations prepare a defence [13].

Present-day internet traffic is largely generated by bots, and they could pose security risks. Account takeovers via stolen passwords, bogus account creation, and data theft are all ways in which bots could pose a serious risk.

There is no way to successfully counter automated threats with purely human responses. Understanding the distinctions between benign and malicious bots, as well as humans, in website traffic is made easier with the help of AI and machine learning.

In order to keep track of everything that has access to every system, there must be an exhaustive list of IT assets. Under the hood, an AI system aids in calculating the IT asset inventory.

Artificial intelligence (AI)-based systems can predict how and where you are most likely to be hacked, enabling you to prepare for attacks and focus your defences on the weakest points. Prescriptive insights from AI-based analysis may help you establish and fine-tune policies and processes that will increase your cyber resilience.

Artificial intelligence (AI) automates mundane cyber security tasks that may otherwise drain your staff, while also mimicking the finest qualities of humans while eliminating their shortcomings. The ability to routinely monitor for and avert even the most basic security issues is a major benefit. It also does a complete scan of your network to identify any potential security vulnerabilities.

Artificial intelligence (AI)-driven endpoint security takes a different tack, educating the endpoint to conform to a certain standard of behaviour. Artificial intelligence has the ability to recognise anomalies and respond accordingly, whether that's alerting a technician or reverting to a secure state after a ransomware attack. This allows for preventative defence against assaults, rather than reactively waiting for signature changes. You may make better prioritisation choices based on what is most likely to be utilised to attack your systems with the help of AI-based cyber security solutions, which can provide the most up-to-date information on global and industry-specific threats [14].

By 2025, the world's workforce will have lost over 85 million jobs to artificial intelligence, according to estimates. As scary as it may appear, you need not worry. There will be an additional 92.1 million employment in the world as a direct result of technological advancements, say experts. Therefore, people will need to work along with machines.

5. NEGATIVE ASPECTS OF AI FOR CYBER SECURITY

One potential drawback of using AI for cyber security is the substantial investment of time, effort, and other resources required by enterprises to implement it.

In addition, hackers use AI to refine and enhance their malicious software. Malware built with artificial intelligence that can "learn" from other AI programmes is a serious threat.

Security firms need to use many data sets that include anomalies and malware codes to train the AI system. Creating reliable data sets may be a costly and time-consuming endeavour, which leaves some companies unable to do it.

Neural fuzzing is a method for finding bugs in software by testing it with massive amounts of random data. Combining neural fuzzing with neural networks allows a threat actor to learn about the target's software and its security flaws.

Cyber security firms may utilise AI to protect their customers, but the technology might also be exploited for unethical purposes. Criminals in the cyber world may utilise AI to modify their virus so that it is immune to the technology and behaves more erratically than usual.

The remedy for such flaws, After considering these drawbacks, it's evident that AI won't be the lone answer to cyber security problems anytime soon.

The most effective strategy employs a combination of both traditional methods and AI tools. Any company may improve its security by putting together a team of AI and cyber security experts that can work well together.

6. FUTURE OF ARTIFICIAL INTELLIGENCE HOLDS FOR CYBER SECURITY

As more approaches to cyber resilience use AI to enable adaptive protection against dynamic threat environments, there will be a greater need for people and technology to continue to exchange knowledge and insights. CyberGraph proves that AI might be useful in the field of cyber security.

Machine learning will be included into firewalls to identify abnormalities, and artificial intelligence (AI) will be utilised to monitor security incidents.

It's possible Locating the origin of cyberattacks via the use of natural language processing (NLP) tools. In addition, RPA bots are deployed to automate rule-based processes. There is a reliance on mobile endpoints for monitoring and assessing cyber threats.

The numbers show that by the end of 2020, there will be 5.8 billion IoT-connected automobiles and business gadgets. The potential for cyber assaults increases with the number of connected devices in the Internet of Things.

Therefore, AI may be used for a variety of purposes in the field of cyber security. As cloud-based solutions grow more common, there will be a greater need for AI-powered cyber security [15]. With this in mind, it is projected that the value of AI cyber security will increase from $4.89 billion in 2018 to $40.61 billion in 2026, a CAGR of 30.12 percent.

7. USAGE PATTERNS OF A I BASED PLATFORM OF OPENCV

More recent applications of computer vision and digital image processing include things like face recognition, biometric validations, the Internet of Things (IoT), criminal investigations, signature pattern detection in banking, digital document analysis, smart tag based vehicle recognition at toll plazas, and many more. All of these apps use real-time image and video processing to constantly amass a wide range of user feedback for in-depth analysis and prognostication.

Some of the many fields that benefit from HCI include: 2D and 3D image analytics; egomotion appraisal; feature points detection; human-computer interaction; facial recognition mechanism; mobile robotics; gesture control; object identifi-

cation; clustering recognition; motion understanding; stereopsis scene understanding; motion tracking; structure from motion; pattern classification; augmented reality; decision making scene reconstruction; and man-machine interaction.

When it comes to computer vision jobs, nothing compares to the speed and efficiency of the open-source framework known as OpenCV. Computer vision and predictive mining are both within its capabilities because to its large set of available characteristics and algorithms. OpenCV is an AI library built by Intel; W. Garage and Itseez both use it. OpenCV was developed in response to the growing need across several sectors for efficient, real-time image analytics and recognition.

Statistical Machine Learning library used by OpenCV

- Boosting (meta-algorithm)
- Convolutional Neural Networks (CNN)
- Deep Neural Networks (DNN)
- Gradient boosting trees
- Naive Bayes classifier
- Artificial neural networks
- Random forest
- Expectation-maximization algorithm
- Decision tree learning
- k-nearest neighbor algorithm
- Support vector machine (SVM)

8. IMAGE FORGERY ANALYSIS USING OPENCV

One of the most pressing issues in the current context is determining the authenticity of user-generated content in light of the widespread usage of digital authentications across a wide range of applications. Self-attestation is becoming more commonplace, with many companies requiring applicants to provide digital versions of signed papers and certifications. This is even occurring while providing new SIM cards for mobile phones. The forgers often use digital image editing applications like Adobe PhotoShop, PaintBrush, PhotoEditors, and others to copy and paste the scanned signatures of real people into the bogus documents. Some images may be improved by using one of the many accessible image editing software. The fresh forged copy of the document may be made using this implementation method without the target's knowledge or consent.

Here is how we see the process of identifying forged signatures in a newly created document play out.

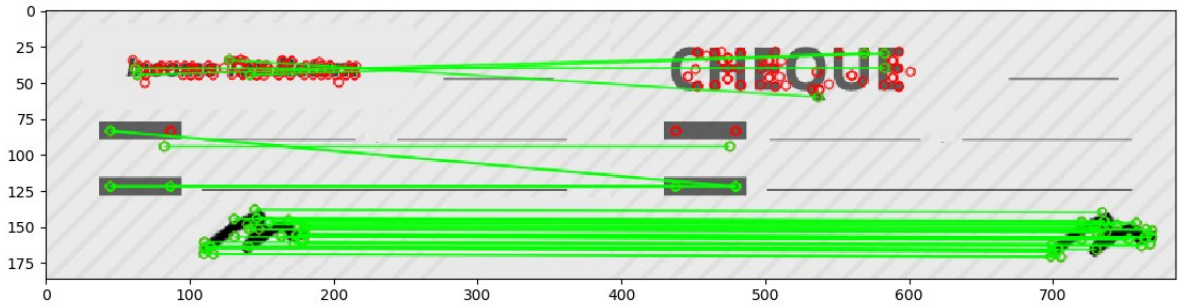

FIGURE 4. Forgery Analysis using OpenCV

The pixels in the new picture with the replicated signature are easily identifiable, as shown in Figure. Methods based on machine learning and OpenCV's built-in, highly accurate prediction mechanisms are used to label pixel values. The pixels can still pinpoint the source of the picture segment, even if the individual employs sophisticated image modification techniques. We have covered the growing role of AI in cyber security, as well as how AI may aid in the fight against Cyber crimes. Implications for the future of AI in cyber security are briefly examined, as are the benefits and cons of using AI in this field.

9. CONCLUSION

It's become clear that AI is a reliable option for countering cyber attacks. Artificial intelligence (AI) is often used to discern "good" from "bad" in security systems. This is achieved by the comparison of one entity's behaviours with those of other entities in the same environment. More sophisticated AI security systems can analyse massive amounts of data and help piece together associated behaviours that may signify questionable activity by anonymous entities, going well beyond just detecting good or negative behaviour. Businesses are utilising models based on AI and machine learning to build up network architecture that will deter and limit Cyber crime and assaults. Artificial intelligence (AI) security features, when presented with novel or unfamiliar information/behaviors, "learn" based on previous behaviour, allowing for rapid, actionable context and insights; such as drawing logical inferences based on potentially insufficient data subsets and providing multiple solutions to a known problem, empowering security teams to select the most appropriate course of action. When conventional security solutions are proven to be too sluggish or ineffectual, artificial intelligence-based technologies are improving the entire security architecture and its performance by offering stronger protection against a growing range of complicated cyber-attacks. Companies using AI to enhance both internal and external operations have had positive effects on business processes and financial results. Across addition, the use of AI-powered cyber security solutions has accelerated the development of data-driven security models in a variety of industries. We anticipate that artificial intelligence will soon be able to predict potential threats to cyber security systems and provide solutions to avoid them. It is also expected that countermeasures would be used extensively, giving companies peace of mind and helping them be ready for any potential cyberattacks. In addition, AI will be able to recognise sophisticated attacks, interrupt them, and prevent future efforts by hackers by establishing their identification and taking appropriate action, greatly enhancing cyber security. In addition, cutting-edge automated detection technologies will soon be available, allowing us to find attacks with a high likelihood and without the current astronomical running costs. Similarly, the arrival of automated software flaw root cause analysis — which can ascertain why a security weakness exists and how to fix it — is expected. Phishing detection neither misses a threat or issues a false alarm, and automated incident response may effectively boot an attacker from the network once they've been detected. While machine learning and artificial intelligence remain the favoured option for preventing Cyber crimes, many new breakthroughs are predicted to arise in the cyber security arena.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] 2021. https://www.technologyreview.com/2021/01/21/1016460/transforming-the-energy-industry-with-ai/.
[2] 2020. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.
[3] 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
[4] 2021. https://www.supplychaindigital.com/supply-chain-risk-management/lessons-learned-vaccine-supply-chain-attack.
[5] R. Prakarsh and Khanna, "Artificial Intelligence and Cyber crime- A curate's Egg", Medium," 2020. https://medium.com/the-%C3%B3pinion/artificial-intelligence-and-Cybercrime-a-curates-egg-2dbaee833be1.
[6] "The Dark Side of Latin America: Cryptocurrency, Cartels, Carding and the Rise of Cyber crime, 6," 2020. https://www.ozy.com/the-new-and-the-next/the-next-el-chapo-might-strike-your-smartphone-and-bank/273903/.
[7] "When Artificial Intelligence goes awry: separating science fiction from fact", without publication date." https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf.
[8] S. Energy, "Managed Detection and Response Service," 2020. https://assets.siemens-energy.com/siemens/assets/api/uuid:a95b9cd3-9f4d-4a54-8c43-77fbdb6f418f/mdr-white-paper-double-sided-200930.pdf.
[9] "Automated racism: How tech can entrench bias," *POLITICO*, 2021.
[10] "For a discussion on discrimination caused by algorithmic decision making on AI, see ZUIDERVEEN BORGESIUS, Frederik, "Discrimination, Artificial Intelligence and Algorithmic decision making". Paper published by the Directorate General of Democracy of the Council of Europe," 2018. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.
[11] "See the Special Report on Facial Recognition of the Center for AI and Digital Policy (CAIDP) that contains a summary of key references on this topic contained in the 2020 Report on Artificial Intelligence and Democratic Values/ The AI Social Contract Index 2020 prepared by CAIDP," 2020. https://caidp.dukakis.org/aisci-2020/.
[12] "the European Parliament adopted a resolution to ban the use facial recognition technologies in public spaces by law enforcement

authorities to ensure the protection of fundamental rights. See European Parliament," 2021. https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.
[13] "What are 'bots' and how can they spread fake news." https://www.bbc.co.uk/bitesize/articles/zjhg47h.
[14] "Fake News is Rampant, Here is How Artificial Intelligence Can Help," *FORBES*, 2021.
[15] "For a general review of policy implications in the UK concerning the use of AI and content moderation, see Cambridge Consultants, "Use of AI in Online Content Moderation," *Report produced on behalf of OFCOM*, 2019.