Sri Lanka Institute of Information Technology

Integrating AI in Cybersecurity along with its latest Developments

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20076498	Dias L.R.S

Date of submission: 23/05/2021

Table of Contents

Abstract 3

1. Introduction 4
2. Evolution of the topic 7
3. Future developments in the area 12
4. Conclusion 18
5. References 19

Abstract

This study addresses the use of AI in cybersecurity, as well as its potential innovations. The increase in cyber-attacks has outstripped the cyber security industry's budgetary resources and human capacity to evaluate and tackle any new type of cyber threat. With the growing digital presence, there is a large amount of personal and financial information that should be safeguarded against cyber-attacks. Since cybercrime is becoming more and more nuanced, we have a need for more efficient and intelligent cyber defense approaches. In the coming years, artificial intelligence (AI) is promising to transform cyber safety. As neither humans nor AI alone have shown general success in this field, it has become apparent that integrating AI into cyber security can only be resolved successfully with many problems in cyber security where AI techniques are used.

Keywords: security intelligence, cybersecurity, Integrated Security Approach (ISA), artificial intelligence (AI), Emerging trend

1. Introduction

Researchers have devoted over half a century improving computers' autonomous learning capability, starting with the invention of computers that involved human control in the 1950s. Not only in computers, but in industry as well as in human society this transition represents a breakthrough. Computers have developed in a way that allows new tasks to be completed on their own. Phrase "cyber security" provides the concepts, processes, and strategies used to protect devices, facilities, networks or information from being targeted, destroyed, as well as accessed without permission. Cyber security is also known as information technology defense. Many say that cybersecurity is an application for protection against unwanted malicious attacks by servers, cellular phones, machines, electronic systems, Records, platforms. The goal of cyber security is to develop security that protect computer infrastructures, networks, applications, and data from unauthorized access, alteration, or vandalism. The program also includes a series of methods used to protect networks, apps and stored information from damage, unlawful access and cyberpunk attack. Cyber security is a broad term that encompasses anything from personal computer information security to disaster recovery and end-user training.

However, Cyber security is strongly linked to artificial intelligence. “Intelligence” seems to be merely the quality which excludes humans from all other species on earth. And since machines cannot have that genetic intellect, the concept of getting that intelligence in man-made machines is very intriguing. The scientific and metaphysical disciplines working to comprehend the mind of the human being began considering this "Why cannot machines think?" instead of the normal human intellect. The concept of developing "Artificial Intelligence" started to draw the interest of researchers all over the world as a result of collaborative efforts in cognitive science, neuroscience, and computer science.

Artificial Intelligence (AI) became initially introduced mostly as methodology to simulate the human brain and examine serious issues with something like a comprehensive human approach. From imaginative film and literary works AI has become widely known. AI enables the intelligent storage and processing of large amounts of data. The development of usable tools is made easier by this processing. Artificial intelligence is often used to include expert systems in a range of contexts, including security and space travel. On a computer or machine, artificial intelligence is classified as artificially created intelligence that offers knowledge to solve deep and challenging issues. Artificial intelligence is a blend of IT and physiological intelligence that is used for computational purposes. Intelligence is the capacity to think about the development of memories and comprehension, patterns recognition, adaptive choices and knowledge learning. Machines can be programmed to act like humans, but they can be quicker and more humane.

With that, the risk of losing essential data is reduced by cyber protection but cyber-attacks have enhanced and increased. The biggest hole is the human element and the root cause of cybersecurity incompetence. All is vulnerable to a cyberattack. Malicious actors are more advanced and outpacing existing cybersecurity regulations as technology progresses. Experts are starting to counter this vulnerability, using artificial intelligence, in order to stay ahead of cybercriminals (AI).

In cyber defense, artificial intelligence is being used by organizations to in order supply stronger data privacy against increasingly professional attackers. Artificial intelligence is helping to automatically detect threats and respond to breaches of information technology in complex and complicated processes. By using artificial intelligence, these types of applications are evolving and becoming more sophisticated and detailed. Artificial intelligence technologies, with their adaptable and adaptive system behavior, will assist in overcoming the shortcomings of today's cybersecurity tools.

The goal of this report is to raise awareness of the term "AI integration in cyber security" as well as its future developments. Furthermore, this work summarizes the topic's historical review.

2. Evolution of the topic

Artificial Intelligence (AI) is becoming more critical in Cyber Security as a result of advances in research and the availability of cheaper computing and storage power from cloud providers. In the cybersecurity sector, AI is offering a new beginning. AI isn't a brand-new invention in the world of computing. **Early 1700s:** The representation of all-knowing devices, such as computers, started to appear in popular literature. Jonathan Swift's novel 'Gulliver's Travels' outlined a device called the generator, one of modern technology's greatest changes. With the assistance and expertise of a supernatural mind, the aim with this system, improve documentation and technological procedures to the point that even the least talented person appeared to be skilled.

John Vincent Atanasoff (scientist) as well as his doctoral candidate partner Clifford Berry created the Atanasoff-Berry Computer in 1939 with a $650 grant from Iowa State University (ABC). The ABC weighed over 700 pounds and could solve up to 29 linear equations simultaneously.

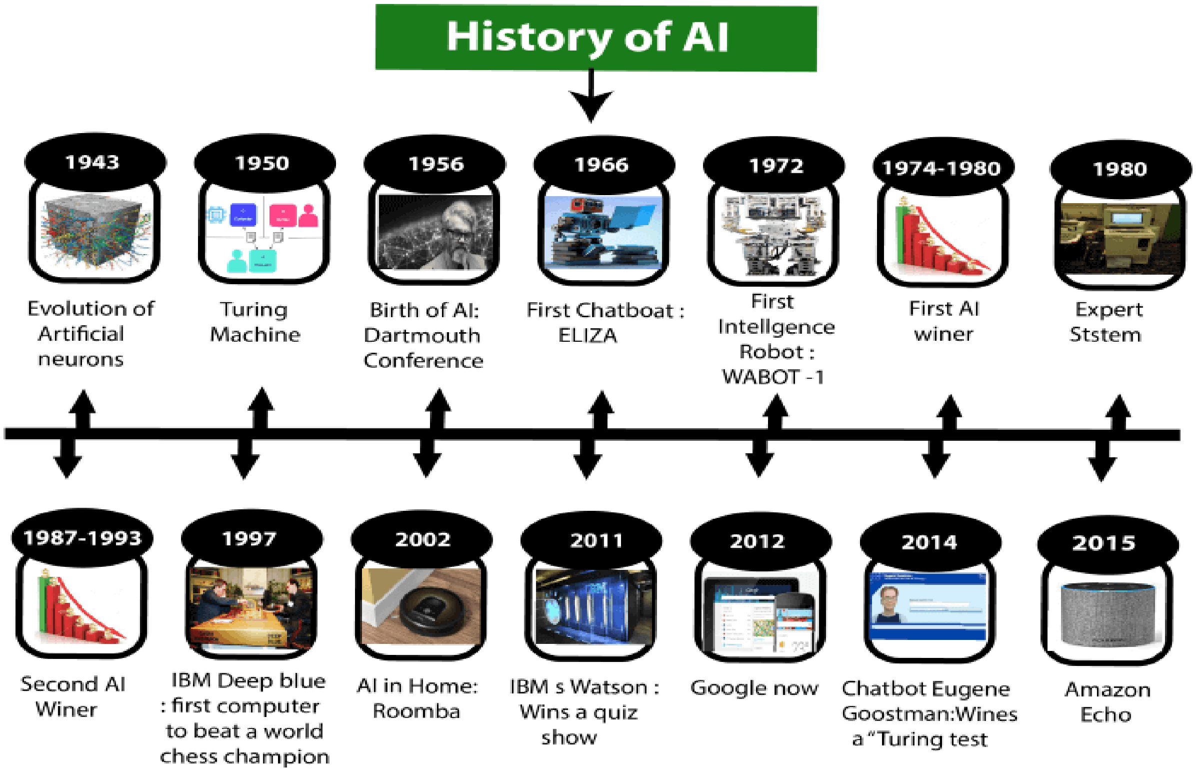
In 1956 it was characterized by computers as the ability to carry out human intelligence-type tasks. Learning, decision-making, problem-solving, and knowing and hearing speech were examples of such activities. Deep learning, reinforcement learning, and Bayesian networks are all examples of AI. In what might be the ultimate victory for the cybersecurity industry against cybercriminals, AI is poised to change the cybersecurity room in a variety of ways.

In the first half of the XX century, sci fi developed the concept of artificially smart robots. It began in the "heartless" Tin Man of the Wizard of Oz, and continued in Metropole with Maria's humanoid robot. And in 1950s, the idea of artificial intelligence (or AI) was culturally assimilated by a generation from scientific, mathematicians and philosophers. One of these people was Alan Turing, a British-born polymath who studied the theoretical capabilities of artificial intelligence. The logic theorist was a piece of software created by the RAND Corporation to simulate a person's conflict talents. Many consider the Dortmund Research Work for Artificial Intelligence (DSRPAI), hosted in 1956 by John McCarthy and Marvin Minsky, to be the first artificial intelligence program. McCarthy invited great collaborative scholars across specific sectors in this seminal conference to openly explore artificial intelligence.

AI flourished between 1957 and 1974. More knowledge could be saved by computers and quicker, cheaper, more usable. Machine learning algorithms have also advanced, and people have become more aware of which algorithm to use. A mountain of barriers was unveiled by the breach of the initial fog of AI. The biggest problem was a lack of computing resources to do something useful: machines couldn't store or process data quickly enough. For example, in order to communicate one must learn and accept several words in many varieties.

The extension of the computational framework and enhanced investment renewed AI in the 1980s. John Hopfield and David Rumelhart endorsed "deep learning" strategies that allowed machines to learn from experience. Edward Feigenbaum, on the other end, pioneered expert systems that mimicked the decision-making system of a human expert. Upon questioning an expert in such a profession how and where to respond at every case, the software may provide advice to non-experts. Non-experts may obtain guidance from the software until this was known in virtually each case. Deep learning were widely used in industrial applications.

Surprisingly, AI blossomed in the absence of government support and media attention. Most of artificial intelligence's milestone targets were accomplished in the 1990s and 2000s. Gary Kasparov, the reigning world chess champion and grand master, was defeated by IBM's Deep Blue, a chess-playing computer program, in 1997. This highly publicized match marked the first time a reigning world chess champion was defeated by a computer, and it was a significant step toward developing an artificially intelligent decision-making program.


History of AI
1943
Evolution of Artificial neurons
1950
Turing Machine
1956
Birth of AI: Dartmouth Conference
1966
First Chatboat : ELIZA
1972
First Intellgence Robot : WABOT -1
1974-1980
First AI winer
1980
Expert Ststem
1987-1993
Second AI Winer
1997
IBM Deep blue : first computer to beat a world chess champion
2002
AI in Home: Roomba
2011
IBM s Watson : Wins a quiz show
2012
Google now
2014
Chatbot Eugene Goostman:Wines a "Turing test
2015
Amazon Echo

Artificial Intelligence Maturation (1943-1952).

Year 1943: Warren McCulloch and Walter Pits published the first work on artificial intelligence (AI). They proposed an artificial neuron model. The model was explicitly targeted as a "nerve net" in the brain computational model. [eight] It used a threshold as a transition mechanism, which was like using the Heaviside phase function. At the beginning only a basic model with binary inputs and outputs, some weight constraints as well as a more versatile threshold value are suggested. It was discovered early on that any Boolean function could be implemented by networks of such devices, as evidenced by the fact that the AND and OR functions can be implemented and used in either the disjunctive or conjunctive normal form.

Year 1949: Donald Hebb has shown an update rule to change the intensity of neurons attachment. Hebbian learning is the name given to his law. A psychologist from Canada, Hebb helped to cross the field of psychology and neuroscience by pioneering studies into brain function. Eventually, the discipline we now know as neuropsychology was created. He is most renowned for his classical 1949 novel, "The Behavior's Organization: a Neuropsychological Theory," in which he suggested biological explanations of conduct and mind processes, especially the Hebb’s rule. **1. One of the 20th century's most cited scientists. 2. The work of Hebb opened the way for the interpretation of brain functions in order to explain important processes like learning and memory.**

Year 1950: Alan Turing, a mathematician of England and a pioneer of machine study in 1950. In his paper "Computing Machinery and Intelligence," Alan Turing proposes a test. A Turing test can be used to assess a machine's ability to demonstrate intellectual behavior comparable to human intelligence. The expression "The Turing Test" is most appropriately used as a means to answer the question of whether machines can think of a suggestion made by Turing (1950). The question whether machines may think that they themselves are "too pointless" to be discussed, according to Turing.

A computer scientist named Arthur Samuel created a checkers-playing computer program **in 1952**, making it the first computer program to learn how to play the game on its own. Samuel coined the term "machine learning" when he programmed a computer that perform chess smarter than its person which develop the code in 1959.

1961: Computer scientist and professor James Slagle created a heuristic problem-solving software called Symbolic Automatic Integrator which was based on symbolic integration into freshman calculus.

1966: The first general-purpose mobile robot, also known as the "first electronic human" was created by Charles Rosen with the help of 11 others, Shakey the Robot.

As in the 1960s**, the 1970s** led to rapid progress, in the area including automobiles as well as robotics. Artificial intelligence, on the other hand, encountered difficulties in the 1970s, including decreased authority funding for AI science.

1970: WABOT-1 was designed in Japan in Waseda University as the first anthropomorphic robot. It had flexible body parts, the capability to eye sight, and the potential to have a conversation.

The Creation of Intelligent Agents (1993-1999).

Year 1997: In the year 1997, IBM Deep Blue defeats world chess champion Gary Kasparov, becoming the first machine to do so.

Long Short-Term Memory (LSTM) is a type of cyclic neural network (RNN) defined work by computer scientists Sepp Hochreiter and Jürgen Schmidhuber in 1997 for writing and voice recognition.

1999: In the same vein as Furby, launched by sony, an Artificial Intelligence powered robot t, a $2,000 robotic pet dog designed to adapts by communicating with its surroundings, owners, and other AIBOs. It had the ability to pay attention to more than 100 voice commands, as well as interact with its human owner.

Deep learning, and artificial general intelligence (2000-present).

After the fears of Y2K were lost, the new millennium began – AI started to trend upwards. More artificially smart entities and creative media (in particular, film) were created, as forecasted, on the nature of artificial intelligence.

2000: A robot named as Kismet, that can identify and imitate facial expressions, has been created by Professor Cynthia Breazeal. That one was designed to look like a human face, complete with eyes, mouth, eyelids, and brows.

Honda launches ASIMO, a humanoid robot with artificial intelligence, in the year **2000.**

Year 2011: The IBM Watson won a challenge in 2011, a quiz shows in which the complicated issues as well as the riddles were to be resolved. Watson had demonstrated its ability to understand natural language and quickly solve difficult questions.

Year 2012: Google has released "Google now," an Android app feature that could predict user data.

Year 2014: Chatbot "Eugene Goostman" has won the notorious "During Test" competition in the year 2014.

Year 2018: The IBM "Project Debater" discussed and performed exceptionally well on complex issues with two keynote discussants.

In the past, AI and cyber security had no connection whatsoever. However, as time passed, the lines between the two became increasingly blurred. **Present era**, AI sounds promising. AI is perfect for solving some of our hardest challenges, and cyber security definitely falls under that category. In today's pace with the fast cyber-attacks and system expansion, AI can be employed to stay away from bad attackers to simplify threat detection and adjust efficiently than traditional technologies.

Cyber security solutions driven by artificial intelligence can aid cybersecurity teams at varying phases of protection. AI may be used to scan a threat intelligence database for a particular Indicator of Compromise, notifying the Security Operations Center when it detects a cybercriminal attempting to breach the system, while also automatically adjusting preventative security measures to prevent the breach in the first place. Artificial Intelligence-based security measures will, without a hesitation, provide intelligent advice to cybersecurity teams. As attacks targeted to mimic genuine results, not only at the human user level but also at lower device levels, the two fields grew closer over time. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a big part of how AI and protection are tied. This necessitates the end-user adding the letters of some unfair image, sometimes with the addition of a masked sequence of letters or digits that appears on the screen.

The sector may be driven by enhancements to the automatic character recognition software, which can be labeled a breakthrough in AI technology. The competitive security market is thus stimulating progress in the artificial intelligence in the practice of trying to safeguard assets, such as online reservations for tickets. Artificial Intelligence is one of the most important elements of our solutions and lets us easily find and evaluate new vulnerabilities and flaws to avoid many threats. Interference detection relies on Artificial Intelligence strategies, which allow for the analysis of even unidentified attacks before they spread. When it comes to understanding unique forms of cyber, artificial intelligence platforms that are designed to adapt and evolve and are capable of detecting even minute changes in environments, have enough capacity to intervene much earlier and based on a vast trove of data than humans.

3. Future developments in the area

AI and cyber security are considered futuristic and much closer than we might believe. But that is only a partial reality that needs to be addressed with reserved standards. The fact is that we will find ourselves facing reasonably progressive changes in the future. In view, what might seem progressive compared with a completely independent future is already springing beyond what we were able to do in the past. AI cybersecurity is set to be an important weapon for the future, with the assistance of machine learning. Human interaction has become important and indispensable for defense, as is the case in other industries. Although cybersecurity is obviously highly dependent on user input, technology is increasingly improving at certain aspects than we should be. It's probably an understatement to say that artificial intelligence (AI) has become a hype. The concept is widely misunderstood by the general public, although the C-suite can't get enough of it. A beginner might think of AI and its little sister, machine learning, as futuristic concepts like flying cars and drone grocery delivery, but in fact, AI and its little sister, machine learning, are present in most of the today's industrial and economic software (ML). Any software developer will tell you that these tools are nothing more than statistical probabilities. Depending on the statistics they have, they interpret current data, take measures, and make inferences.

As artificial intelligence (AI) is all-pervasive, a recent study anticipates that by 2031, technology in the field of cybersecurity would replace people as hackers use increasingly sophisticated instruments. In a new survey, a cloud-based protection company named 'Trend Micro,' said over two and a half (41%) of IT leaders considered AI as a substitute for 2030. Only 9% of participants believed AI will never overtake one ‘s career over the next century. Almost a third (32%) claimed AI will ultimately outsource all cybersecurity in detail. Almost one in five (19 percent) assume that AI criminals will be widespread by 2025 to improve their armaments. As a result, AI will play a critical role in addressing the cybersecurity skills gap in the future.

It's necessary to portray some latest specific problems in cybersecurity since humans investigate the potential repercussions of protection in machine learning and AI. We have long recognized numerous practices and factors that can be viewed in the framework of AI technologies. By 2020, life has turned, and the way entire workers function has been fully transformed. Digitalization has become necessary for survival from the emerging trend. Certain firms have not; some businesses have been brought to their knees, and others have prospered. Cybercrime was one of the industries that thrived. Organized crime, country, and skilled hackers alike abused the flaws as millions were rapidly assembled and transferred to work-from-home environments. In order to enhance threat detection, forecasting and security, most organizations have confidence in artificial intelligence (AI). Also, it includes the ongoing skill deficit in cyber security.

While AI has a strong potential, future AI attacks are probable. To combat hacker attacks, cyber-naive remote staff need security awareness training, as shown by the Covid-19 pandemic. Immature technology would be targeted by attackers, putting 5G communications, smart cities, and the Internet of Things (IoT) under threat. We've seen cybersecurity software companies use AI to classify security threats in software and networks during the last few years. Cyber criminals have almost the same modern technologies, that increased the likelihood that companies around the world might breach security. Artificial Intelligence (AI) is without a doubt the future of cybersecurity. In other words, Artificial Intelligence holds the key to the future of cybersecurity (AI).

AI and Biometrics

AI would be used to secure digital identity fraud, for example through providing better accuracy and speed to validate the identity of an individual, either by integrating biometric information to prevent a cybercriminal from accessing the data through credentials alone. AI systems would probably end the control of each hacker completely.

- Keystroke Dynamics
  The practice of defining and authenticating individuals based on their typing habits is known as keystroke dynamics. With the aid of tempo, flight time, time to stay. keystroke dynamics can distinguish individuals. The time between release of a key and pressing another key is the time interval of the time you push a key. The time required to locate the correct button and the time taken to press the key can be calculated together to verify persons. To classify individuals, AI systems may monitor details about how people type and the time period between two keys for the most used keys.

- Facial recognition
  Multiple smartphones and on social media networks like Facebook are popular with facial recognition. Facial recognition, on the other hand, is easily fooled. For example, a video or picture of the owner can be used to fool the Smart phone’s face unlock. In certain instances, the owner's sibling's face will fool the face unlock feature. Such accidents have occurred in the past as a result of 2D facial recognition inaccuracies. Machine learning can be used to make facial recognition more accurate. To accurately validate a person's face, AI learns through billions of photographs and employs 3D biometrics. Predictive analytics may be used also by AI systems for evaluation of the influence on human faces of ageing. To this end, AI evaluates photographs of the elderly to reconstruct younger ones. AI and biometrics can jointly construct more precise authentication models by using vast quantities of accessible facial data.

- Gait Detection
  Gait identification is a tool that authenticates people according to their course. This authentication method has been studied for decades, but it has never been widely used. Gait detection can however, by means of AI, be a viable authentication solution. The accuracy of 99.3 percent in AI gas detection was achieved by the researchers at the University of Manchester. With the aid of floor sensors, the AI-powered detection analyses the steps of a human. Gait identification and diagnosis of many medical conditions can be used with AI for protection in airports.

- Voice Recognition
  Voice and speech recognition is used by a number of smart home devices, including Google Home and Amazon Alexa, to perform tasks such as answering questions, ordering items, and playing music. Nevertheless, before performing any of the operations, these devices cannot authenticate users. Google has also included voice recognition-based ‘Smart Lock' in a number of Android devices. However, it can be unlocked because it cannot work in a noisy situation, while defining a user's voice. The AI transformation will prepare the biometric systems using millions of different users' voice samples. Analyzing a voices pattern like pace, accent, tone and pitch can help AI and biometrics like voice recognition assess the biometric signature of an individual. Biometrics of this kind can be fast and accurate in identifying people. The identification and presence of certain AI-powered voice recognition in environments is used.

Learning with natural language processing

The promise of Natural Language Processing, which comes into play when using AI for cybersecurity, is one of the most compelling reasons to do so. By scanning papers, reports, and news on cyber threats, AI-powered systems will automatically collect data for reference. Natural Language Processing is used by AI systems to extract valuable information from scanned data. Cyber threats, anomalies, mitigation, and prevention techniques would all benefit from this knowledge. Cybersecurity companies may use the analyzed data to determine timeframes, quantify risks, extract data, and draw conclusions.

Cybersecurity companies will also remain up to date with emerging cyber threats and plan efficient plans to protect organizations from various cyber-attacks.

Remote workforce raises cybersecurity risks, and AI comes to the rescue.

48 percent of US experts reported having encountered phishing emails, callings or texts in work context within the first six months of the pandemic. According to the company, AI implemented to user authentication could allow the identification of many more unsafe users, patterns, and anomalies in access requests, as well as a decrease in time-consuming re-certification processes. Expert decision-making will start making policymakers satisfied by recognizing that machines produce smarter and quicker outcomes versus frustrated human beings who could control how and what.

Data centers

Power consumption, backup power, internal temperatures, bandwidth utilization, and cooling filters are only a few of the important data center processes that AI can track and optimize. AI offers insight into the principles that can enhance data center technology safety and effectiveness. AI will help you save money on repairs. AI will trigger warnings that notify you when hardware failures need to be addressed. AI-based warnings allow you to repair your equipment before it suffers more damage.

Threat Detection

On the market, there are hundreds of devices and techniques for identifying attacks. Companies, in enforcing these, have cybersecurity teams that constantly track and examine risks to their processes, networks, and architecture. There are a growing number of cybersecurity professionals worldwide, but not enough researchers and specialists willing to help develop cyber-attacks and threats.

AI will help a lot in this area by "helping out" and supplementing human efforts. They are capable in real time of detecting threats. The algorithms understand various types of attacks and how each type can be handled in various circumstances. Best of all, by analyzing each case, behavior and design every day they constantly learn. If the algorithm becomes better at identifying actual threats, the occurrence of false positives decreases.

Fraud Detection

The capabilities of the fraud sensing strategy of a company can be greatly improved by AI and the results are increasingly reliable without equivalent increase in resources or costs. The precise identification of potential fraud is thus increased and cases of false positive and negative are decreased significantly. AI is currently the only tool that can help detect fraud in real time and prevent an unusual-looking transaction from proceeding. They raise the lengthy task of analyzing vast quantities of data and only tag things that analysts need to analyze or decide.

Data overload

Since the security monitoring provided by the third-wave AI identifies and surfaces threats in real time, there is no need to store and store large quantities of data until they can compromise your network. Even in rapidly evolving environments, best-in-class AI can recognize patterns and gain a human-like understanding of what regular traffic looks like.

The Baseline Network Activity Expected Approach.

Self-supervised third wave AI learns over time how to define and address problems that conventional solutions cannot. Predictive AI easily detects deviations from expected baseline behavior and notifies protection.

Cyber criminals who had been waiting for a time like this for years swooped in as the world's workforce suddenly moved to work-from-home. Bad actors not only sought out network vulnerabilities exposed by these SIEM and related problems, but they also wasted no time launching phishing schemes when security teams were busy fixing urgent network issues. Organizations who had invested in third-wave AI solutions, on the other hand, had far less problems. These mechanisms are the basis for normal network behavior. These organizations' third-wave AI solutions were able to adapt on the fly as a "new standard" set in.

AI integration in Cybersecurity: Real Life Examples

Security screening

Immigration officers can identify people who are lying about their intentions by security screening. A device called AVATAR, which displays human body movements and facial expressions, has been developed by the United States Homeland Security Department. In order to collect minor changes in face and body expressions that can increase skepticism, AVATAR relies on AI and big dates. A screen with a simulated face that asks questions is part of the scheme. It detects changes in one's responses and variations in speech. The information gathered is contrasted to factors that may mean that someone is lying. If a passenger is suspected of being a terrorist, they are flagged for further investigation.

Examine endpoints on mobile devices.

To monitor mobile endpoint risks, Google uses AI. This research can be used by businesses to safeguard the increasing range of individual smart phones.

Zimperium and MobileIron announced a cooperation to help companies implement artificial intelligence mobile counter malware solutions. Network, system, and application threats can be tackled by combining Zimperium's AI-based threat detection with MobileIron's enforcement and protection engine. Skycure, Lookout, and Wandera are some of the other mobile security providers. To detect possible threats, each provider employs its own AI algorithm.

Lastly, With the all-pervasiveness of Artificial Intelligence (AI), a recent study has predicted that technology could overtake people from around the world of cybersecurity by 2031, since attackers are using more advanced equipment. According to a new study from cloud security firm 'Trend Micro,' more than two-fifths (41%) of IT leaders believe AI will replace their position by 2030.

AI did not substitute its job in the next decade just 9% of the respondents said. Almost a third (32 percent) said that AI will ultimately aim to automate all cybersecurity completely. By 2025, nearly one-fifth (19%) of respondents agree that attackers using AI to improve their capabilities might be widespread.

4. Conclusion

Suddenly, the analysis indicates a number of positive advances in the implementation of AI in cyber. AI made it possible for computer complexity to be reduced and models to be trained. The domain has also been found to be significantly distorted. In addition, scientists have concentrated on fewer algorithms and are not mainstream as these new algorithms are. For researchers, this represents both a threat and an opportunity. AI apps are believed to continue offering cyber security opportunities. Study must never remain, nevertheless, and researchers must begin to embrace new methods and adapt them and publish them more widely. People, however, may also be the weakest player in the cybersecurity chain. While Artificial Intelligence can use machine-to-machine information learning to significantly assist in cyber-attacks, a sole irresponsible individual can produce severe damage to the entire system, and there is no way to predict this.

Professionals in the field of cybersecurity have embraced AI as the industry's future, but AI cybersecurity is not yet fully designed to fix all of the issues. While AI and machine learning boost cyber security, hackers also support cybercrimes by creating tools without human involvement. For adequate security, AI-based technologies and traditional security approaches must be used and combined together.

Of course, all this is good news, but not so good news. While the modern business is foolish not to take all of the above into account, those considerations are also sober. There are significant resources needed for cybersecurity. Much of the above is expensive, resource-intensive and ongoing. Higher management must be prepared to commit itself permanently. In the future, companies or enterprises operating in various countries will depend largely on AI concepts to ensure secure online, given that artificial intelligence (AI) is of great importance in cybersafety. Because of Artificial Intelligence, both of the above forecasts mean that the future of cybersecurity is in good hands (AI). But how they use AI notions to boost their cybersecurity in the coming years depends largely on businesses and other stakeholders.

5. References

[1]*https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf*. 2021.

[2]*https://www.coursehero.com/file/79983963/Artificial-Intelligence-in-Cybersecurity-Jan2017pdf/*. 2021.

[3]*https://www.nitrd.gov/pubs/AI-CS-Detailed-Technical-Workshop-Report-2020.pdf*. 2021.

[4]*https://ieeexplore.ieee.org/document/9152956*. 2021.

[5]*https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security?enrichId=rgreq-3d52991dcc114d8789ac3c89a8f08bce-XXX&enrichSource=Y292ZXJQYWdlOzMzMDU2OTM3NjtBUzo5MjY2MDYwNzU5MTYyOTBAMTU5NzkzMTUxMjI1Mg%3D%3D&el=1_x_3&_esc=publicationCoverPdf*. 2021.

[6]L. Columbus, "Top 20 Predictions Of How AI Is Going To Improve Cybersecurity In 2021", *Forbes*, 2021. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2020/12/05/top-20-predictions-of-how-ai-is-going-to-improve-cybersecurity-in-2021/?sh=2a6e23eb19c1. [Accessed: 23- May- 2021].

[7]N. Joshi, "Cybersecurity in 2021: How Artificial Intelligence Powered Biometrics is Providing More Security", *Bbntimes.com*, 2021. [Online]. Available: https://www.bbntimes.com/technology/cybersecurity-in-2021-how-artificial-intelligence-powered-biometrics-is-providing-more-security. [Accessed: 23- May- 2021].

[8]A. Sinha, "Key Cybersecurity Trends You Need To Keep An Eye On In 2021", *BW Businessworld*, 2021. [Online]. Available: http://www.businessworld.in/article/Key-Cybersecurity-Trends-You-Need-To-Keep-An-Eye-On-In-2021/09-04-2021-386174/. [Accessed: 23- May- 2021].

[9]A. Sinha, "Key Cybersecurity Trends You Need To Keep An Eye On In 2021", *BW Businessworld*, 2021. [Online]. Available: http://www.businessworld.in/article/Key-Cybersecurity-Trends-You-Need-To-Keep-An-Eye-On-In-2021/09-04-2021-386174/. [Accessed: 23- May- 2021].

[10]"https://www.g2.com/articles/history-of-artificial-intelligence#ai-1", *https://www.g2.com/articles/history-of-artificial-intelligence#ai-1*, 2021. [Online]. Available: https://www.g2.com/articles/history-of-artificial-intelligence#ai-1. [Accessed: 23- May- 2021].

[11]T. Scott, "Cybersecurity Trends in 2020: Artificial Intelligence | TechnologyAdvice", *TechnologyAdvice*, 2021. [Online]. Available: https://technologyadvice.com/blog/information-technology/cybersecurity-trends-2020-ai/. [Accessed: 23- May- 2021].

[12]"https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-how-predictive-ai-will-change-cybersecurity-in-2021/", *https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-how-predictive-ai-will-change-cybersecurity-in-2021/*, 2021. [Online]. Available: https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-how-predictive-ai-will-change-cybersecurity-in-2021/. [Accessed: 23- May- 2021].

[13]"AI Cyber Security: An Easy Guide For 2021", *Jigsaw Academy*, 2021. [Online]. Available: https://www.jigsawacademy.com/blogs/cyber-security/ai-cyber-security/#Artificial-Intelligence-and-Cyber-security. [Accessed: 23- May- 2021].

[14]"https://securetriad.io/ai-and-the-changing-cyber-security-landscape-in-2021/", *https://securetriad.io/ai-and-the-changing-cyber-security-landscape-in-2021/*, 2021. [Online]. Available: https://securetriad.io/ai-and-the-changing-cyber-security-landscape-in-2021/. [Accessed: 23- May- 2021].