Sri Lanka Institute of Information Technology

Artificial Intelligence(AI) will play an increasing role in both cyber-attacks and defense

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT19122410	W.P.T. Pamalka

Date of submission

Table of Contents

Abstract

Cyber-attacks happen every day. Every day more than 100 of systems gets hacked and thousands of data gets compromised. Such attacks are due to data being invaluable with today's world. Without data, no industry can function properly. However, it is not easy to preform a all in all successful cyber-attack. The hacker must have a good knowledge regarding cyber security, programing and other subject matters and must have a great patience, time and money in order preform a completely successful attack. This is where artificial intelligence plays an increasing role. Artificial intelligence is becoming more influenced in cyber-attacks and defense strategies at present in order to make attacks and defense strategies more accurate, timely and overall, less/more damaging.

In this research:

- What is Artificial Intelligence?
- A brief history of AI
- Cybersecurity and its key objectives
- Cyber attacks and its features including most common types of attacks
- AI influenced cyber attacks
- AI influenced cyber defense strategies, will be discussed

Introduction

In the community of computer science, the first ever founders dreamed of creating a machine that would be able to perform rationally in parallel with the human brain. Although, inventors tried to create a human like machine who could behave and preform like humans, they have not yet achieved the full capacity of this almost impossible creation as of 2020. However, regarding artificial intelligence many beyond amazing millstones have been achieved within these years and step by step they are getting closer to create an almost human machine.

Cyber security, has been one of the most important topics starting from the 20th century. Most of our information is shared within sites and apps that are connected with the internet and they can be hacked anytime, anywhere. It is speculated that hackers, now use AI influence hacking tools in order preform their attack more accurate, successful and overall, more damaging than ever. Therefore, AI must also be used in cyber defense mechanisms in order to minimize the risk of overall damages and to make hacking attacks or cyber-attacks unsuccessful.

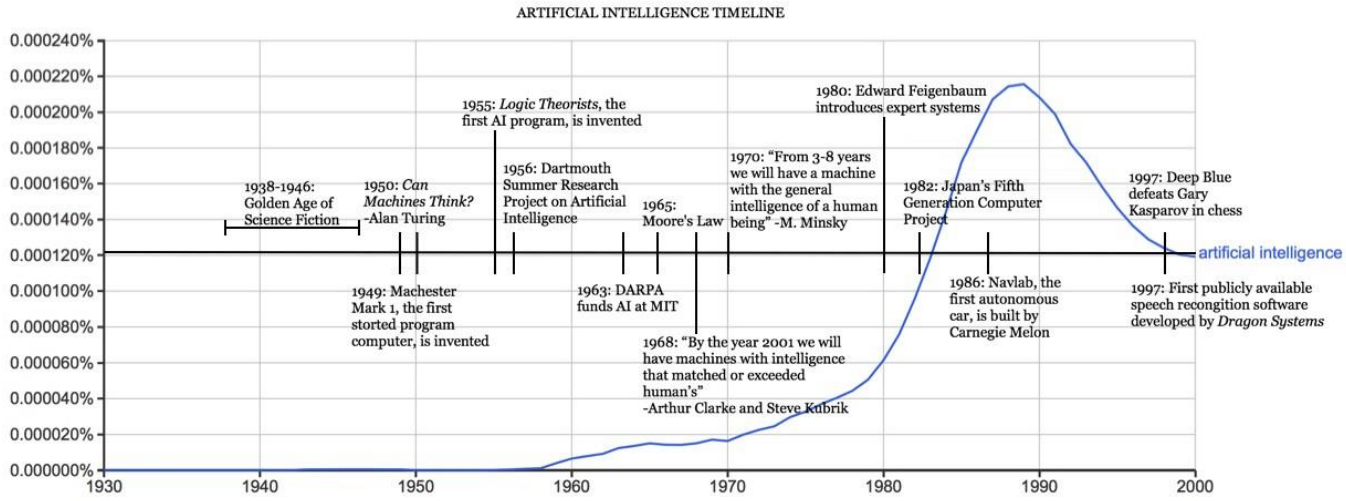
What is Artificial Intelligence (AI)

By definition artificial intelligence is the ability of a computing device to mimic the human intelligence and thought process in order to perform tasks and solve problems successfully. AI systems are made to adapt to the environment and situation it is in, so that it could deliver better results of the activity it is employed in. These tasks can be common day to day life activities such as shopping, or special tasks such as military tasks. Whatever the task maybe, it is no doubt that artificial intelligence will give humans an easy and more error free life style. One of the best examples for AI so far is self-driving cars that happened in 2018 and chess playing computing devices. Although this is not yet advanced as we have seen in sci-fi movies, we are surely and slowly getting there.

History of Artificial Intelligence (AI)

One of the very firsts theories that brought artificial intelligence to the world was by Alan Turing. In his paper, “Computing Machinery and Intelligence” he explained the fundamentals of in-built machine intelligence. However, these theories never got the rightful place it deserved as computers were not easily accessible to the public as it was expensive. Also, during the time this paper was published computers could not store commands, it could only execute them. Therefore, many people thought the concept of machine intelligence was just fictitious.

In 1956, Allen Newell, Cliff Shaw and Herbert Simon introduced the Logic theorist program that was developed to imitate human's problem-solving skills. This is considered as one of the first AI programs that were created. During the stage of 3rd generation of computers AI started to take another step as computers become more accessible to people and faster. Even the institutes started showing an interest in this concept and start to fund research programs in order to create a perfect human like machines.



Another expansion of AI was created by the discovery of expert systems that imitate the process of decision making of a human expert. At present we have medical expert systems, financial forecast systems and more on the internet. A major milestone of AI was met when Gary Kasparov, the world chess champion at 1997 was defeated by a chess playing computer program created by IBM. Then another landmark goal was met when speech recognition software and "Kismet" a robot that could understand and display human emotions were created.

Features of Artificial Intelligence

Authors Stuart Russell and Peter Norvig of "Artificial Intelligence: A Modern Approach" discuss the features of AI as:

1. Thinking humanly
2. Thinking rationally
3. Acting humanly
4. Acting rationally

The first set of features deal with though and reasoning process whereas the second set of features deal with how the AI should behave correctly.

- **Evolution of the topic**

What is Cyber Security

"Protection that is given to an information system in order to preserve its integrity, availability and confidentiality of information system resources" is the definition of cyber security given in the NIST Computer Security handbook.

There are three main key objectives that needed to be maintained in order to uphold security. They are:

1. Integrity
2. Availability
3. Confidentiality

Preserving integrity is to make sure that the system is running without unauthorized manipulations or system errors. Loss of integrity means data can be modified or destroyed. Secondly, persevering availability is to make sure that the data is only available for authorized users at all times and if this is violated, the data could be disclosed to unauthorized users. Thirdly, confidentiality ensures that unauthorized users can not gain access to data. If this objective is violated, that would mean the data is disclosed to unauthorized people. Therefore, it could be seen that in order to preserve cyber security, one must ensure that these key objectives are not violated.

What is a Cyber-Attack?

A cyber-attack is a threat in action. It is where either one hacker or a group of hackers maliciously tries to breach its security so that the hackers could steal or modify the system with a negative effect. If this attack is successful, it leads to a violation of system's security.

There are two types of attacks:

1. Active attack
2. Passive attack

An active attack is an attack where the attacker tries to modify the system to affects its operations and a passive attack is where the attacker tries to copy/steal information off of the system without affection the system nor its operations.

An attack can also be classified according to its origin. Therefore, there are two types of attacks depending on the origin of the attack:

1. Inside attack
2. Outside attack

An inside attack preformed by an attacker inside the security perimeters. The attacker is authorized to access the system but then uses the authorization in a malicious way. An outside attack is preformed by someone outside the security perimeters and the attacker is an unauthorized user.

Most common types of cyber-attacks are:

1. Malware – Malware is a malicious software that is used to breach a network by exploiting a vulnerability within the network. Spyware, ransomware, viruses and worms. belongs to malware.

2. Phishing – Phishing is a technique of sending malicious communications such as emails text messages, that looks like reliable and legitimate and use it to lure victims to giving their sensitive information or to install a malware on machines.

3. Man-in-the-middle attack– This attack is also known as eavesdropping attack. Here an attacker or attackers position themselves in a transaction between 2 or more people in order to steal data.

4. Denial of service attacks– This attack floods the severs with traffic. As a result, the severs become exhausted and the system is unable to fulfil legitimate user requests. When an attacker used many devices to launch a DoS attack it is known as a distributed denial of services attack (DDoS).

5. SQL injections– In this attack, the attacker injects malicious SQL codes inside to force the server to disclose information.

6. Zero-day exploit– This attack is occurred, when a system's vulnerability is published and before they could fix the vulnerability.

7. Social Engineering attacks– This is an attack that is based on manipulating people into avoiding security protocols so that attackers could gain access to the systems.

What are botnets?

Botnets are a collection of devices that are contaminated with a malware such a trojan horse, attackers have the control of a botnet, making the entire network of computers a slave system. It is used to increase the accuracy of the attack. Botnets are used when preforming a DDoS attack.

Why Cyber Security is important and Cyber Attacks happens frequently at present?

As humans, in the 21st century people spend most of their time on none another place than the internet. People allow companies to take more data through apps and other subscription services. People share most of their personal and sensitive information on the internet with a hope that no one would rob them from their privacy. The truth however, is the total opposite. Over thousand to hundred thousand attacks can happen per day. According to a study at the University of Maryland [1] average of every 39 seconds, one hacker attacks occurs and per every 39 seconds at latest 3 user's privacy gets affected.

No industry is safe from cyber-attacks. If it is connected to the internet, it can definitely be hacked. Personal and sensitive information or data is invaluable and at wrong hands, it can cost our privacy, money and also security at some point. According Juniper Research [2], the average cost of data breaches in 2020 will exceed by 150 million dollars. Therefore, one should protect themselves when they are on the internet from security/privacy breaches and hackings.

"Why such attacks happen?" one might ask. Well there are several reasons to why cyber-attacks happen. It is due to data being one of the most valuable assets in today's world. Without data industries can't function properly. They need customers insight in order to deliver a better service and to understand and achieve their targets says USA Today [3] and personal sensitive data can be held against its rightful owner. Many attacks happen around stealing customer data from large companies then selling it on the black or grey markets for financial gains. In 2015 in around 10 healthcare facilities, data was breached in the US and approximately 29.3 million

patient records were compromised from the attack and they were been sold on the black market for 500 dollars per patient record depending on the buyer [4].

Another reason is customers pay hackers to hack into company systems in order to obtain sensitive documents to sabotage the cooperation. One of the major damages after a hacker attacks occurs is the victim company's reputation plunges, which may lead to stock prices and sells lower that ultimately leave the company forced to shut down. However, not all cyber-attacks are wrongful. The hacker group "Anonymous" has deleted around 8,000 child pornography sites on the dark web according to Forbes website [5]. There is also ethical hacking (white collar) where a security expert tries hacking in to a system in order ensure the security of a system.

Cyber attacks are becoming more sophisticated than ever. Using different types of algorithms and technologies cyber attacks are becoming more damaging to its victim. AI is a new technology that is being used in cyber attacks to be more successful, damaging and harder to detect.

why Artificial Intelligence is an important influence when launching a Cyber Attack today?

To conduct an attack is not an easy task. One must have very deep knowledge of programming languages, logic and mathematics in order conduct a successful attack. The attacker must have a great patience, as it can take from 1 hour to a whole day or even more than that to conduct a single attack and it might not be even successful. This is where artificial intelligence could play an intense role. According to the website InfoQ [6] it is extremely easy for an attacker to program an algorithm with hacking techniques in an AI program or use botnets to their full capacity to launch an attack. If the first time fails, the system gets better with each time it tries as they adapt to the problem very quickly.

It is said that hackers are "weaponizing" AI in order to meet a better success rate of their malicious activities [7]. With advance AI systems could analyze system code and used its intelligence to identify potential loop holes within the system then inject AI influenced malware to the system in order to hack into the system. At the moment cyber-attacks do not happen very frequently, but we can see the fledgling steps of cyber-attacks happening around the world.

In April 2018, an online market place for freelance known as TaskRabbit was attacked. The attack was lunched using a large botnet controlled by an AI which was then used to perform a massive DDoS attack on the website's servers. The attack was so deadly, the site has to be disabled until the security was restored again. Personal information including Social Security numbers, banking details of 3.75 million users were compromised during the attack. Additionally, more 141 million users were affected from the shutdown of the site [8].

As a more recent attack, in 2019 starting from August to November, Instagram has to endure two cyber-attacks. Although Instagram have not yet released an official statement, it is suspected that this attack was launched using AI technologies. [9]

AI influenced cyber-attacks have been on the rise in recent years. The reason why is that with time, data keeps on being more valuable to hackers and companies and sites use more secured solutions nowadays to protect data. Therefore, hackers must too, have to up their game in order to successfully obtain more data with less time and effort. AI technology has the ability to adapt according the environment or the situation, which make the attack more successful and efficient with each time it is launched. AI attacks are faster, overall, less expensive, works 24/7 without breaks and more adaptable and more accurate comparing with human hackers. Therefore, AI cyber-attacks are becoming more reliable than human based cyber-attacks.

Emotet trojan is a prototype AI malware. Its main mechanism is phishing that tricks users on clicking malicious email to steal data. It is able to insert itself to a pre-existing email, asking the victims to click on the link which then turns out to be the malicious email. Since the malware is inside a pre-existing email, it doesn't raise much suspicious.

In a demonstration by the researches of IBM infected a video conference application with WannaCry ransomware, and it could be seen that it remains undetected by anti-malware software and other detecting tools. Deeplocker is a newly built AI influenced malware that can stay hidden until it has reached its target. It uses AI technologies such as face and voice recognition to identify its targets. This malware can easily hide in applications such as video conferencing software and stay undetected until it has reached its target.

Since AI cyber-attacks are now in rapid development, cyber security is also becoming unreliable and less trustworthy. In present day, devices are being interconnected and Internet of things platforms are being more popularized, if a full capacity AI cyber-attacks is launched, the damaged that may occur is so deadly that billions of systems and its data might be compromised at once including life threatening systems such as peacemakers and many other essential systems such as home security systems. A whole stream of services can be affected at once that it can affect day to day life of peoples.

Another deadly circumstance might be that, since AI systems are adapting and getting better with each time it attacks, it could be used by a terrorist group to hack into nuclear systems in countries and manipulate the system into lunching nuclear weapons into other countries which can bring much destruction and a possible world war. As a result, it can be seen that, it is impossible that one must be able to detect and defense themselves from an AI cyber-attack in order to protect their sensitive data and privacy when on the internet.

Why AI influenced cyber-attacks will be deadlier than human attacker based cyber-attacks?

The main reason why new opportunities have been open toward AI influenced cyber attacks is because it has a more success rate, accuracy than hacker based cyber-attacks. However, there are many more reasons to why AI cyber attacks are deadlier than hacker based cyber-attacks. One reason is that AI cyber attacks will be harder to detect when comparing with hacker-based attacks. AI will learn how to blend into a system, disguising itself in order to spread around the system more successfully than ever. Another reason is that AI will have the intelligence to choose which data is more valuable at rapid speed which will save time and effort. Thirdly, AI will be able to impersonate as trusted source. As mention above, AI is supposed to act like a human with a superior intelligence. Therefore, the AI malware will be able to imitate a user's behavior in order to replicate messages and emails that looks reliable. Lastly, the attacks will be faster with more damaging results. AI cyber-attacks can target valuable and vulnerable targets and do millions of dollars in damages.

Therefore, AI based cyber attacks can be given as one of the reasons to why it is important to influence AI with cyber defense.

What is cyber defense?

Cyber defense is the ability to prevent or to protect itself from a cyber-attack. This defense mechanism should be a concern for everyone from a large cooperation to a smart phone user since this age, most of our private, sensitive data are on the internet. It is also to identify weak spots within your system in order to act effectively to fix up the patches to minimized the risk of damage and to detect a threat on real time in order to respond to the attack fast.

To uphold one's cyber defense system one must:

- Maintain hardware and software that are able to deter attackers
- Analyze the system regularly for vulnerabilities and fix them quickly as possible.
- Act on real time to stop the spread of the attacks.
- Recover fully from cyber-attacks fast.

Computer security strategies

Computer security strategy has 3 main aspects to it. They are specification/policy which describes what the security system supposed to do. Secondly, Implementation/mechanism that explains how the security system does it and thirdly, correctness/assurance that describes how it really works. When implementing a computer security strategy, one must take in to consideration about the value of the data that has to be protected, the system's vulnerabilities and potential threats and possible attacks and overall cost of security failure and recovery

Computer security strategies focuses four main actions. They are:

- Prevention
- Detection
- Response
- Recovery

Prevention of an attack is the best option out there, but it is not always possible as one cannot maintain absolutely protected system yet. There is no network, system or a site that is truly un-hackable, it is just a matter of time with technology and skills that a site, system or a network is hacked. The best possible option is to detect a cyber-attack using software such as anti-virus, anti-malware software and maintaining a detection log to identify such attack. Thirdly, when an attack is detected, a respond must be launched in order to stop the attack or to minimize the damages. Lastly, the system has to recover from the attack using backup copies of data and other methods.

There is also a need for assurance. Assurance by definition is "Confidence that one has that the security measures will work as intended to protect the system and data it has" according to NIST text book.

Why a cyber defense system is important?

The reason why cyber defense is an important matter is because it focuses on preventing, detecting and protecting a system in real time from attacks so that there are no damages to the system or to the information stored. No matter who the user may be, it is essential that user have a cyber defense system in order to protect itself from a cyber-attack that might occur to steal data or to corrupt a system.

There are two types of cybersecurity systems:

1. Expert systems – Expert systems are based on recognizing threat signs to prevent an attack
2. Automated systems – it is software that identifies harmful or dangerous activities based on previous analysis data of the systems.

Today, there is a large threat to cyber security more than ever. That is due to global connectivity through the internet and now online services are being used and promoted. These online services are really helpful to human's daily life as it has become ubiquitous. These services have people's personal sensitive data in online servers which an attacker could preform a very sophisticated attack in order to gain access to these servers to either corrupt the server or to steal data completely.

What are the common mechanisms used in cyber defense or security?

1. Use of strong passwords.

   This is one of the basic and easiest way to protect oneself from a cyber-attack, however people are still use weak passwords to protect one of their most valuable assets, personal and sensitive data. One of the most common cyber-attacks are done by automatic password generating software. The worst, yet most commonly used for 2020 has been [10]:

   - 12345
   - 123456789
   - Qwerty

   When creating a password, it should be hard to guess. The use of both lower and upper-case letters, numbers, symbols and making the password at least 12 characters long is advised by experts. The password should also be change regularly and should only be used once. Use of two factor authentication is also advised.

2. Control access.

   Access control is another way security strategy that should be maintained. It is about maintaining the access to data. The access should only be given to authorized people. This can be done physically and also digitally. Control access method now could be easily done with modern operating software.

   Controlling physical access to server room and computer rooms so that only authorized users can use these services, controlling access to data and services though application controls, restricting what information could be copied and saved into other storage devices can be seen as common methods use when controlling access.

3. Firewall

   Firewall is like a gate between the computer and the internet. It acts as a barrier to protect computing devices from common cyber threats such as viruses.

4. Use security software.

   Security software help to detect and remove malwares and viruses that might get in contact with the computing device. Anti-virus, anti-spyware and malware programs are the most commonly used security software.

5. Updating software and systems on a regular basis.

   Software and system updates usually hold newly added features plus fixed up vulnerabilities that are within the previous update. Therefore, by updating systems and software regularly, one can minimized the risk security threats.

6. Awareness about cyber security in general.

   Although this is the 21st century, still there are people who have zero awareness about how to secure one's privacy when on the internet. 99% of people never read a software policy or guidelines before pressing "accept" button, when downloading an app or software. This may seem harmless but they may be allowing these app to track their search histories and other details, which then if this software gets hacked, all of their private data is in the hands of complete strangers who can take an advantage of it.

   Therefore, people should have an awareness about the value of their privacy and their sensitive data. Awareness can be raised using YouTube videos, lectures blogs and other methods.

- **Future development in the area**

Why AI influenced cyber defense mechanisms are on the rise?

Cyber security analysts are overwhelmed from the task of detecting a large number of structures and data in order to protect a system from a possible attack. Also, to minimize the damage scale cyber attacks should be met with fast and quick intervention which requires round the clock attention from an expert, which can be an exhausting task. Majority believes that AI will be the solution for this constant problem that rises. AI influenced security software will be able to respond to attacks without any support from humans once this technology becomes fully developed.

There is an expert shortage within the cybersecurity industry. More than 3.5 million vacancies are left unfilled due to lack of skill, experienced, knowledge and other reason. AI can be the solution for this rising problem. AI security systems does not need full time supervision of experts. It is designed to identify malicious files from clean set of data. AI is fast learning and respond faster more than a human ever could. With AI's abilities, the shortage of cyber expertise could be filed in matter of months, maybe years.

Currently Microsoft uses monotonic models to run on top of traditional models to catch malicious software. AI security systems are fast when detecting malicious activities and files and it is less costly comparing with regular security software. It is also efficient when analyzing problems and give accurate results.AI would also be used to examine a software or a system and to identify its vulnerabilities and to create a solution that is far more advance that what we have today.

There are number of ways how AI could be used in cybersecurity. They are [11]:

- Monitoring user behavior – AI system will casually stay within the network, observing each and every user's behavior to identify an abnormal behavior patterns.
- AI influenced anti-virus software – AI software will be able to easily detect and respond to the attack by completely blocking the virus or the malware from system resources.
- Scanning emails – Emails has been favored technology of hackers to preform cyber-attacks, such as phishing. More than 50% of emails a person receive are spam or infected with malicious links. AI would be used to scan emails in order to identify malicious emails from safe emails

Cyber-attacks are on the rise in the 21st century due to the world being connected with internet and people use internet everyday to fulfil their need. Now, the days of using a simple antivirus software to prevent a cyber attack or the use of just a firewall are long gone. AI influence cyber attacks are very hard to detect using regular security software and tools. AI influenced security

tools and software must be used in order to detect and fight or delete malicious threats within a system.

Challenges of using AI as a security measure

AI technology is not yet developed fully. There is also lack of experts who specialized in AI technologies. Therefore, it is not an easy task to developed a fully automated AI security system just yet. Complex AI algorithms has to be developed in order to achieve this goal, although so far, the technology is still yet being developed itself. There maybe many trial and error before landing on the perfect AI security system.

Conclusion

As discussed, AI is becoming more flourish with newest advances more than ever. With no time, AI will be used in our day to day life, in order to make everything easier. It should also be noted that cyber crimes are on the rise. With data is being one of the most valuable assets, hackers try to steal data by preforming various types of attacks. These attacks are becoming more advance by day.

Attackers are now using AI influenced cyber-attacks in order to preform more accurate and damaging attacks. These attacks bring more damage to the victims comparing with regular attacks. So far, these attacks are less costly, fast, accurate and more successful that regular attacks. With AI's ability to learn and adapt, it will be able to preform on its own, creating a unique algorithm to penetrate into systems, once the AI technology is fully developed.

With AI influenced cyber-attacks, there should also be AI influenced defense system. It is a known fact that cybersecurity is having a shortage of experts. More cybersecurity job opportunities are left vacant due to lack of skills, experience and knowledge. Therefore, AI agent operating on it own can be a marvelous solution for this problem.

Also, with an AI security system it is an easy task to detect an attack and give a respond comparing with regular security software such as anti-virus and anti-malware software. With the intelligence of an AI system, there is no need for round the clock supervision. Since cyber attacks are becoming more influenced in AI, it is a safe measure to also keep cyber defense strategies influenced in AI as well. The future of cybersecurity with AI looks innovacious.

References

References

[1] "cybersoultions," 23 9 2019. [Online]. Available: https://www.forbes.com/sites/betsyatkins/2019/06/12/board-level-update-on-cyber-risk/#7182e752199c. [Accessed 20 4 2020].

[2] "forbes.com," 12 June 2019. [Online]. Available: https://www.forbes.com/sites/betsyatkins/2019/06/12/board-level-update-on-cyber-risk/#7182e752199c. [Accessed 21 4 2020].

[3] "USA TODAY," [Online]. Available: https://classifieds.usatoday.com/blog/business/5-reasons-customer-data-analysis-is-important-to-your-business/. [Accessed 23 April 2020].

[4] "Inforsec," 27 July 2015. [Online]. Available: https://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/. [Accessed 23 April 2020].

[5] "Forbes," 30 March 2020. [Online]. Available: https://www.forbes.com/sites/daveywinder/2020/03/30/hack-attack-takes-down-dark-web-7595-websites-confirmed-deleted/#474b8e514357. [Accessed 23 April 2020].

[6] S. Bocetta, "InfoQ," 10 March 2020. [Online]. Available: https://www.infoq.com/articles/ai-cyber-attacks/. [Accessed 22 April 2020].

[7] "Cisomag," November 2019. [Online]. Available: https://www.cisomag.com/hackers-using-ai/amp/. [Accessed 22 April 2020].

[8] S. Bocetta, "InfoQ," 10 March 2020. [Online]. Available: https://www.infoq.com/articles/ai-cyber-attacks/. [Accessed 23 April 2020].

[9] S. Bocetta, "InfoQ," 10 March 2020. [Online]. Available: https://www.infoq.com/articles/ai-cyber-attacks/. [Accessed 23 April 2020].

[10] "Rock IT," 23 April 2020. [Online]. Available: https://metro.co.uk/2019/12/19/10-worst-passwords-2019-revealed-nothing-changed-11932281/. [Accessed 26 April 2020].

[11] "Cisomag," 9 December 2019. [Online]. Available: https://www.cisomag.com/hackers-using-ai/. [Accessed 26 April 2020].