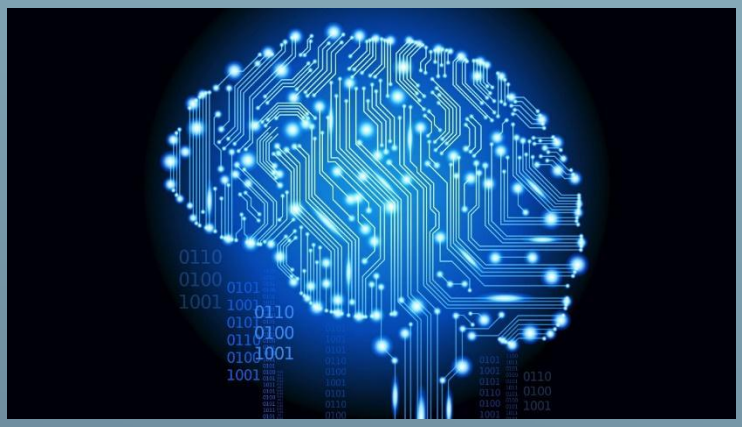


Sri Lanka Institute of Information Technology

Security Challenges Presented By Artificial Intelligence

Individual Assignment

IE2022 - Introduction to Cyber Security

By Weerasiri H.A.K.D
IT19154640

Table of Contents

Abstract

In certain places, there are significant dangers to humanity about the high degree of computer knowledge and innovative AI in over a decade.

In this report, it addresses the Security Challenges posed by Artificial Intelligence and includes, with the introduction of the subject, the evolution of those security challenges, the potential development of the problem and, finally, its conclusion.

In the "Introduction to the topic" section, explain what is meant by AI, Most AI Security Threats, Facts of Trusted Artificial Intelligence, Some AI Security Challenges and other key aspects of AI Security Challenges.

When it comes to the 'evolution of the Artificial Intelligence,' so far with its 'philosophies,' how does AI develop it, the present state of AI and its' safety with AI failures of all time, the major AI failures of the journey, and finally the present situation of AI.

In the chapter "Future Development of the AI and its Security" on the security risks of AI-Enabled Systems and the necessary development aspects of AI and the future of privacy and human rights, the most common facts are the danger of Artificial Intelligence and finally use cases for AI in defense organizations.

Then summarize the key point of this report in great order in a succinct manner with the conclusion portion. Relooking the study with relevant details is rather consequential. Finally, the reference component is protected and it includes the entire toolbox of the study.

1.

2. Introduction

The prolonged progress of AI is progressive, and mistakes, for example image recognition, regulation, regular language processing, and examination of information are now exceeding the level of productivity at the human level. Money can be thought of as accepting new AI innovations that are large and poorly impacted by efforts in almost every region. Misuse of simulated intelligence for significant security measures can be misused, sidelined, and deceived by application, for example, provision control equipment, money frames, or automated vehicles. Powerful and powerful techniques and best practices are very influential. [1]

Similarly as AI-systems require advanced cybersecurity apparatuses and strategies to upgrade their proficiency and strength. Cybersecurity should utilize AI to build perceivability, react to, and help its general viability. Also with ongoing attacks shifting the current attackers against the protecteur asymmetry, this involves flexibility and adaptation. A system that detects the vulnerabilities of a rival, uses perception procedures and learns exercises, can use AI to control various types of assaults and tell versatile reactions (e.g., quickly recognize errors and realize how to deal with them) on a scale. A small team of cyber defenders is conscious that applications that are used by a large number of people will successfully be accredited. Using AI would extend a similar degree of frame security, all-inclusive, and provide the field required to deal with different perspectives, such as institutional boundaries and frame revoking practices. [1]

What is Artificial Intelligence,

"*Artificial intelligence (AI) is a copy of the human understanding of PCs intended for people and their behavior, and the term can be extended to any computer that displays a person's mood, for example learning and Critical Thinking."* [2]

IEEE definition of AI,

***"Artificial. Intelligence** is that activity devoted to making machines **intelligent**, and **intelligence** is. that quality that enables an entity to function appropriately and with foresight in its."* [3]

Artificial intelligence's philosophy is the ability to support and take actions which have the clearest chance of achieving a distinct objective.

With the SIRI via autonomous control systems, computing (AI) is progressing quickly. Though fantasy has always been willing, from Google Quest Calculation to Watson's IBM, to independent arms, to portray AI as humanoid robots.

Greatest security threat to artificial intelligence

The Artificial Intelligence may pose three kinds of security danger.

• AI has spread rumors and disinformation.

For all these references to fake news, and subsequently to the latest elections, lots of play in the media can be done at once. Bot's planting of sham social media information networks like Twitter and Facebook is not the only way to use AI to render audios and videos of political figures that appear like people in the real world in an attempt to influence public opinion. [4]

- **Hacking should be more advanced by AI.**

Latest analyzes have shown that bugs in computer systems are more rapid than humans are – and hackers may use this AI technology to search machine software to find vulnerabilities, so that machines may exploit them for ransomware-like attacks. [4]

• Cyber weapons can be rendered using AI.

A community of experts from the USA and the United Kingdom reported in a study by Cambridge in February this year. Advanced of the machine victimization technology's capacity for discrediting the targets or 'superhuman hacking' of robots, clever vehicles, or guns — with catastrophic effects. These tips have light emitting diode (LED) viewers like Elon Musk, CEO of Tesla, who need to be strictly monitored to avoid the victimization of AI and it falls into wrong hands. [4]

Cyberspace Strikes AI-based security systems

Scientists recently proposed some technologies that uses AI techniques to identify or categorize malware, to preview network device, to phish and spam emails.; Domain detection algorithms (DGAs) and APT response (Advanced Persistent Threat).

Network intrusion detection; phishing and spam recognition malware; Identification; and other problems which undermine APT and DGAs' control. [5]

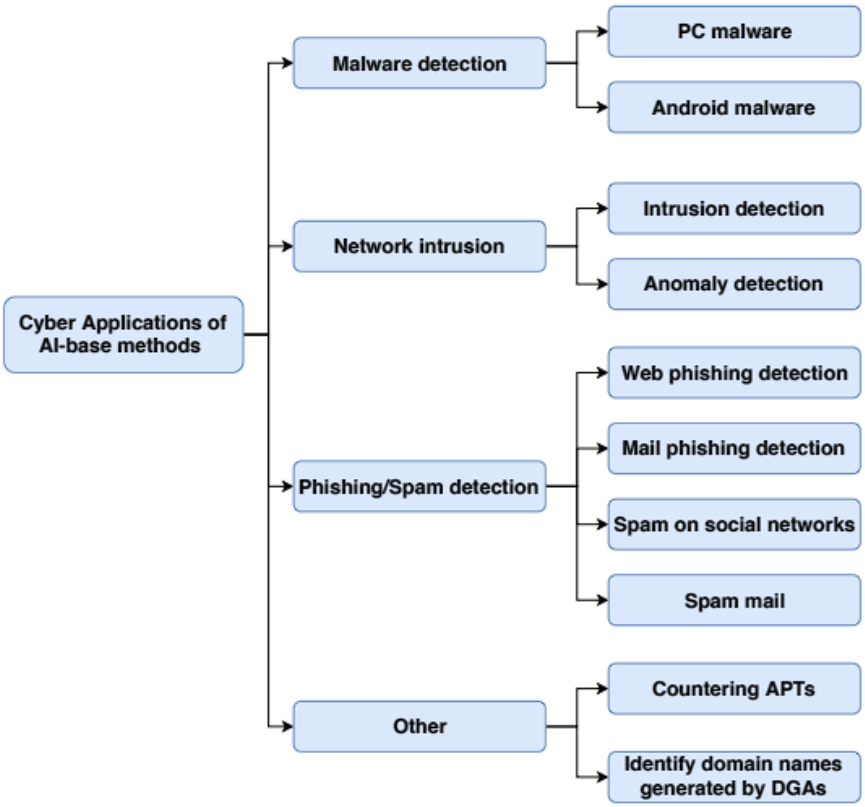


Figure 1. Main branches of cybersecurity applications adopting AI techniques.

Intrusion Detection.

The Intrusion Detection Device (IDS) is a device to defend the network against future accidents, infringements, or immediate threats. The AI techniques are adaptable in order to improve the IDS. Also suitable for the development of other techniques are their simplicity, adaptability, simple calculations, and fast learning. Consequently, many researchers researched intelligent methodologies for the efficiency of IDS. The aim was to boost classification in order to remove falsehood. It was intended that design should be simplified. [5]

SPAM and Phishing Identification

An assault by phishing is a cyber-attack that hugs attempting to bargain with the customer's personality or financial service. Such threats are now one of the web's most important risks. Specific enormous new methodologies were used to evaluate these problems. [5]

Malware Detection

Completely malware is a common term for a number of malware programs, which nowadays include botnets, viruses, worms, retroviral, hacks, Trojan horses, and malware. The consequences of malware on advanced societies are enormous, and extensive work has been carried out to keep malware away and restrict it through AI procedures. [5]

Others

Any of the new works use AI approaches to reduce certain other forms of cyber threats Some of the new studies are being carried out using AI technologies to reduce other cyber threats. More accurately., the combat measures against the threat of APT exist, and DGAs do. [5]

Used threats of AI in Social Engineering.

In order to gather individually similar information in the interests of user accounts, AI is able to hack vast databases containing social network information. In addition, malicious players may use AI to generate custom malicious links or create custom phishing e-mails automatically based on user details. Artificial intelligence can be difficult. [5]

AI-Powered Malware

Increased malware performance, and autonomy, complexity, speed and detection difficulty may be assisted by AI technology. The new generation of malware is more sophisticated, and can function independently with AI. Intelligent parameters, based on device parameters or Automated malware decision taking strategies, can be automatically propagated through a network or a computer system, allowing the target network to be fully compromised. [5]

Intelligent Threats to AI and Autonomy

The dangers of AI-powered hazards are increased with a view to the mechanization of human ability and forms and overcoming current human abilities. The AI Innovation Guide will grow your weapons by committing on-screen characters in order to make them better, more believable, and easier to understand. Within this area, designers of severe, independent hazards are explored to remove dangerous on-screen characters from the barrier system. [5]

There are few main challenges of Artificial Intelligence Security.

- Building Trust
- AI Human Interface
- Software Malfunction
- Higher Expectation

Human Interface of AI

For people to engage in data science, the most important way are the most artificial intelligence challenges. In industry, there is a shortage of talent. Enterprise owners had to prepare their experts.

Building Trust

Technological research and algorithms are all about AI. Many who are not completely aware of the algorithms and technologies behind the AI implementation may be hard to understand.

Malfunction of Software

No technology is available, and people are fine. If hardware fails, it is obviously difficult to point the wrong direction. Alternatively, behaviors powered by human beings are copied.
Anyway, it is difficult for anyone to be responsible for or explain the product / equipment crash with the machines and the inherent equations in the picture. A repeated event may be a lifelong driving passenger

Biggest Expectation

Made brainpower (MBP) may have serious problems with people's perceptions. Individuals, above all, have no top-to-bottom understanding of how AI operates, and they need excessively high standards along these lines; some of this is not feasible. People have a bow to anticipate high from something that is slanting, and in turn, along these lines the yields from it will be great. In either case, AI is similar to other elective innovation with distinct impediments. Experts with different companies differ however from the fact that AI can operate over the next century, but there are some difficulties that interfere with AI.

AI can transform fire into hackers' hands

In fact, speed is a major downside of AI. Programmers understand the AI equations behind innovation's success to reside subtle attacks on specific men. Since AI is routinely "instructed" with knowledge sets, hacker can either produce their own projects or monitor existing malicious capability frameworks. In general, AI assaults should be more successful, possibly because ingenuity simplifies the production of malware, adaptive to avoid even discovery of unrestrained risks. For instance, mixing polymorphic malware with AI makes updating their code simple, ensuring the existing cybersecurity framework.

Hackers can also change the calculation of venture AI by modifying inputs to adjust the methods that the device recognizes as different components. This strategy is often known to the network in order to disregard threats and to allow hackers to have side characteristics and access to controls by management. **[6]**

3. Evolution of the AI and its' Security Aspects Challenges

In this chapter, the report provides a rapid overview of controls that have contributed to concepts, viewpoints, and procedures to AI. As for other literature, this one is compelled to think of a limited number of things, times, and emotions, and to ignore those that were of shared significance. Mankind is writing the history of a series of inquiries. They really wouldn't want to maintain the impression that these inquiries are the only ones to answer the requests, or that the controls have all worked towards AI as their final fulfillment.

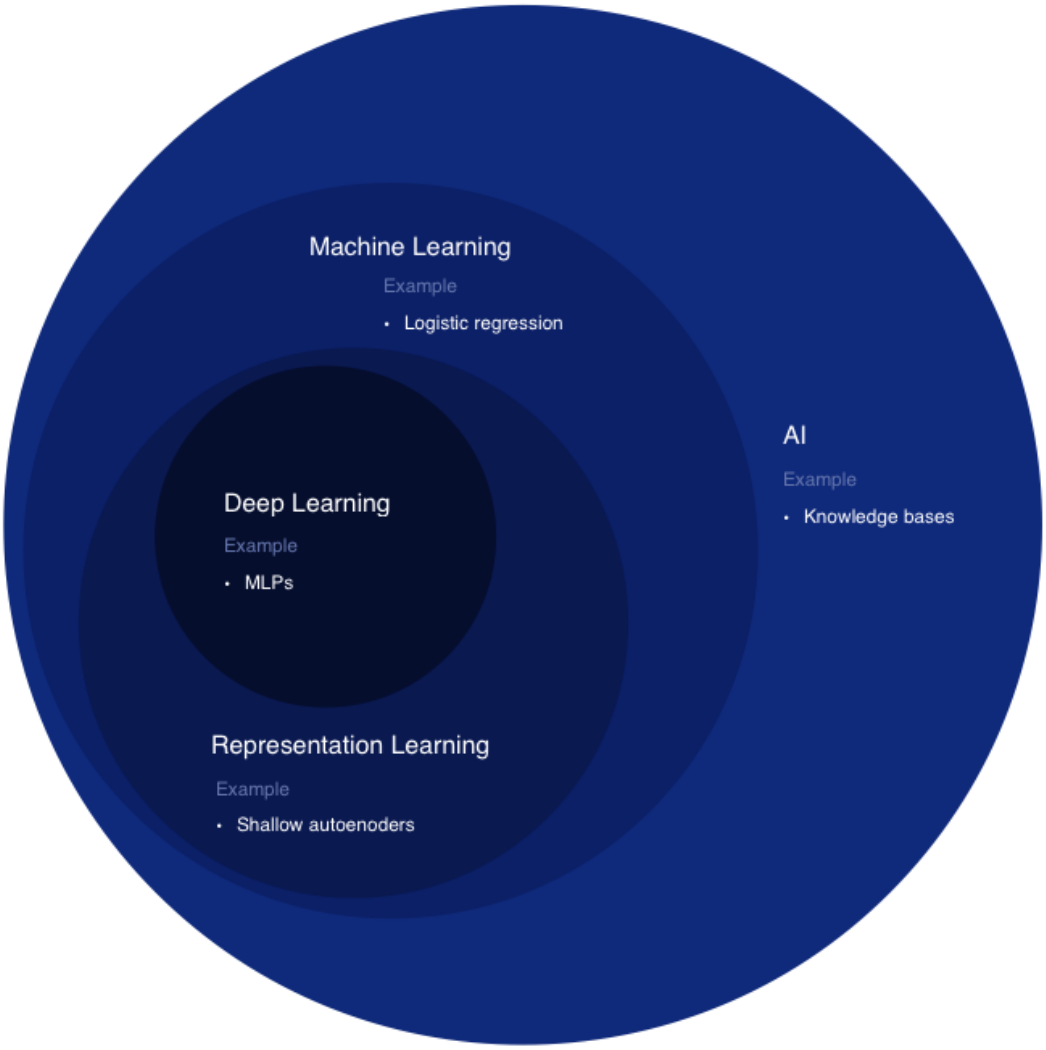
The AI Philosophy

- Is it possible to use specific rules to draw relevant conclusions?
- How is the consequence of knowledge?
- Where is the information coming from?
- How can a real brain render mind appear?

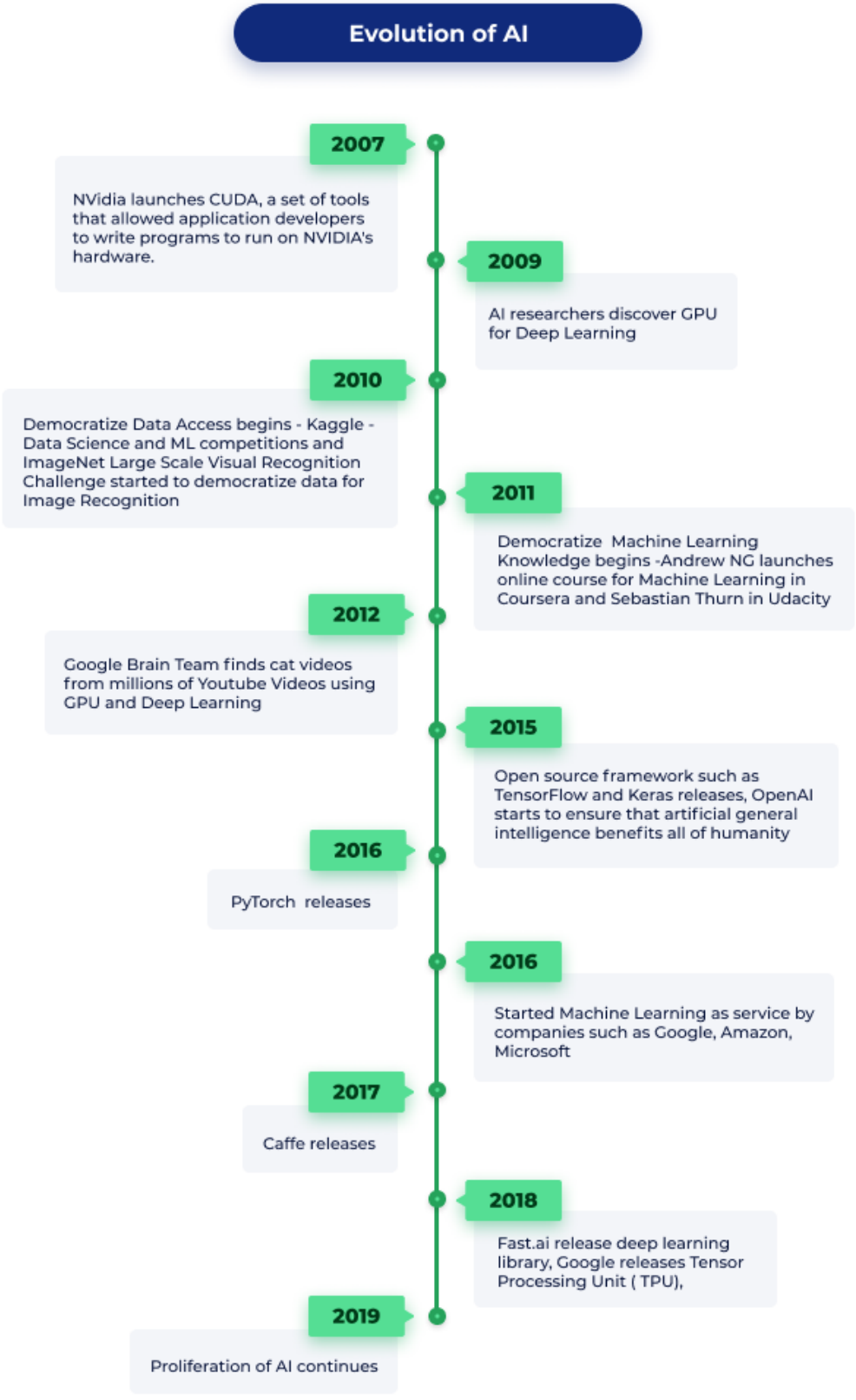
Over the last few years, AI has progressed to a solid platform that empowers computers to believe and acts like human beings. It has also gained concentration from tech organizations across the globe and is ranked as the following outstanding next notable movement after development in cloud platforms and mobile. Some also found this to be the fourth mechanical upset.

The Merriam Websters dictionary says "Artificial Intelligence is an IT division that deals with the simulation of smart behavior on computers". It can be brought into being artificially when a system can intelligently select. Many users can be seen using Machine Learning, AI synonymously and Deep Learning. Machine Learning is a subset of AI and deep learning is a component of Machine Learning.

The Venn diagram shows how profound learning is a sort of representational learning, which is a kind of master learning used by many IA approaches but not all. An example of AI is given in each section of the Venn diagram.



In the 1800s the theories, fantasy and speculation were limited to AI. Included in human beings were classic philosophers' devices. Nevertheless, they were only portrayed in literature as Mary Schelly's "Frankenstein". In 1956 the actual start in AI began. In Darthmod University, participants who were named as AI pioneers for decades returning to the laboratory were the seed leading towards a future of the AI.


Evolution of AI
2007
NVidia launches CUDA, a set of tools that allowed application developers to write programs to run on NVIDIA's hardware.
2009
AI researchers discover GPU for Deep Learning
2010
Democratize Data Access begins - Kaggle - Data Science and ML competitions and ImageNet Large Scale Visual Recognition Challenge started to democratize data for Image Recognition
2011
Democratize Machine Learning Knowledge begins -Andrew NG launches online course for Machine Learning in Coursera and Sebastian Thurn in Udacity
2012
Google Brain Team finds cat videos from millions of Youtube Videos using GPU and Deep Learning
2015
Open source framework such as TensorFlow and Keras releases, OpenAI starts to ensure that artificial general intelligence benefits all of humanity
2016
PyTorch releases
2016
Started Machine Learning as service by companies such as Google, Amazon, Microsoft
2017
Caffe releases
2018
Fast.ai release deep learning library, Google releases Tensor Processing Unit (TPU),
2019
Proliferation of AI continues

AI vulnerabilities and faults in the current of nowadays and AI Failures of all time

Various organizations have turned to Artificial Intelligence to reinforce the cornerstones of their cybersecurity solutions as cyber threats continue to grow by the minute. AI has been recognized as a path for cyber defense and has been integrated into a variety of products for cybersecurity in order to introduce the maximum safeguard against certain cyber threats-a standard immunity against all diseases. Researchers suggest AI by evaluating historical attack behavior using algorithms dominated by neural networks. They could be required to practice themselves and hence develop malware detection. [7]

- Increased frequency of detections.
  AI protection mechanisms, as other cyber methods, seem to be classifiers; they classify continuous activity by calculating how similar such patterns are to malware behavior. Classification is highly vulnerable to both false positive and false negatively and it requires a potential high extent of company-by-company fine-tuning. Restraint should also be exercised to prevent false positives; one may unintentionally slack heavily in the implementation, which can lead to additional vulnerabilities and a false sense of protection. This can lead to a time-consuming, challenging, and frustrating effort to manage and develop them properly. [7]

- Restricted protection from zero-day exploits and revolutionary new threats.
  AI's fundamental concept is the ability to learn from previous trends of data and operation, which assumes omnipresent surveillance is necessary to ensure the needles are in the haystack. These same concepts are followed by AI-driven cyber defenses; they need to be qualified to know how malware looks and also how it behaves. The reliance on historical, i.e., documented and recognizable, malware behavior makes AI-based security significantly less successful in identifying zero-day vulnerabilities and modern malware variants that do not meet past malware characteristics over which the AI was educated. [7]

- Being vocal by attacks focused on AI

The Twenty-six scientists and industry professionals participating in this research collectively agreed that AI has become an important foundation block of complex malware. It's due mainly to the increased automation that AI brings and its ability to determine the actions of AI protection systems. [7]

The section below is restricted to reporting alleged breaches of the intelligence. In addition, the following instances represent only the primary instance of a specific problem, but similar problems can also be found again in later years. Third, hacking or other intentional reasons for AI failures do not appear on the list. Nevertheless, the timeline for inadequate artificial intelligence is rising. [8]

- AI was a general problem solver in 1959, and it struggled to explain problems in the real world. [8]
- Program developed to make discoveries in 1982, figured out how to cheat. [8]
- In 1983, the early warning system for nuclear attack misrepresented that the attack occurred. [8]
- Advanced AI inventory tools triggered a flash crash of a trillion dollars in 2010. [8]
- E-Assistant said that in 2011 the individual was referred to as "Calling me an ambulance." Ambulance. [8]
- 2013 Neural recognition networks saw fantastic objects especially noise images. [8]
- In 2015 Insufficient responses were given by the Automated email answer generator. [8]
- A robot took a man and killed him in 2015 for car parts. [8]
- In 2015, the black people identified as gorillas for Image tagging apps. [8]
- Failed to remove offensive material for adult content filtering applications in 2015. [8]
- AI built for 2016 to project discriminatory acts of recurrence. [8]
- In 2016, unlicensed superweapons. [8]
- Again in 2016, the patrol robot hit a boy. [8]
- Go-playing AI lost a game at the 2016 world champion point. [8]
- Self-driving vehicles sustained a fatal crash in 2016. [8]
- AI was verbally aggressive in 2016, intending to speak with Twitter users. [8]

Study on AI today

AI work continues today, and continues to expand. According to many development analysts, AI research has risen entirely annually around the world by 12.9 per cent over the past five years.

After that China is expected to be the world's most important artificial intelligence supply for the next four years and will take the second lead over 2004 in the United States — and is increasingly being closed down on the most attractive position in Europe.

Europe is one of the largest and the many of diverse region in the artificial intelligence research sector with a high degree of international cooperation. As far as AI, China and even the United States are concerned, India is the third largest research country.

The AI ethics evaluation includes seven separate fields where details are covered.

- Deciding and planning
- Neural Networks
- Computer Vision
- Check and Optimization
- Fuzzy Systems
- Understanding human language and facts
- Machine Learning and Probabilistic Reasoning

In neural networks, machine learning, probabilistic thinking and computer vision, the vast amount of research has increased.

AI Security's existing positions.

Through the use of modern technologies focused on Artificial Intelligence, hackers have imitated and thus made transactions, such as money transfers, with the voices of many top corporate officials worldwide. In just 20 minutes, the app can learn to imitate an entire speech and then talk to the voice and tell the hacker type on your computer.
Using advanced artificial intelligence systems, hackers have imitated the voices of some of the world's largest corporations and provided transaction orders, such as money transfers. After only 20 minutes listening, the program will learn how to mimic a speech in its entirety, speak with the voice and say things that the hacker types in the app.
Some of those attempts have been failing, but other hackers have managed to get the money into their pockets. [9]

Improving Applications Trustworthiness

The AI developments will capture and process huge quantities of data generated inside the existing innovation frameworks. This skill produces the planning knowledge which is required to guide growth and creation of the AI system. Computer-based intelligence-based thought steady with data protection objectives may offer increased confidence to both completely computed and human-based frameworks. The development and deployment of more safe operating systems and identity management are two possible fields. Promising work includes the use of AIs to track program failure, control good practice, identify network bugs, and make security in their systems simpler for software engineers. [1]

Spear-phishing on the rise

Standard phishing attempts use links or notifications to make individuals click on a taint association or to get individuals to do specific things. Today, clients are typically prepared to

rapidly assess and keep away from reacting to innovations such as phishing sends contain comparable or inadmissible substances from obscure individuals or addresses. [6]

Yet today's current AI systems allow "highly advanced lance phishing activities" against individuals of "high value," including CEOs and ranking executives, and send messages directly from individuals they know by and large and with odd things, like continued money for the job they're going to apply for. [6]

A propelled AI system would enable an aggressor to "conduct most of these measures very quickly for any reason," with the intention of targeting 'thousands or even a large number of targets.' [6]

Semiautonomous and Autonomous

Cyber protection will certainly be used by both attackers and cyber-precautionary measures as well as other effective AI applications (e.g. spam sifting). The traditional technique for evacuating vulnerabilities or through the expense of attack changes with the introduction of AI. Every self-sufficient and semi-self-governing system will need to be set up for the most catastrophic scenarios, with a view to forecasting, reacting and investigating possible and actual risk events. There are a few partners that bypass AI-based options, including information owners, professional co-ops, and gadget administrators. The consultation and awareness of stakeholders on autonomous operations and the assignment and constraint of decision-making are important considerations. Cybersecurity personnel are most likely to face autonomous attacks at several levels: attacks could use classical deterministic planning in a secure cyber climate; attacks in an unstable setting could lead to uncertainty in design; attackers who are not aware of the setting could use AI to obtain information and learn how to strike, identify, and find ways to attack. This requires methods and techniques to ensure that the systems deployed are immune to autonomous analysis and attack. Promising approaches include automated separation, supporters, and unique mission strategies. [1]

Interfaces between Humans and AI

When threats become more complex and serious, coordination between AI-cybersecurity systems is not only necessary, but coordination and trust between human-AI interfaces is also crucial. From corporate IT to self-driving cars, problems arise when individual system components accomplish their own objectives without taking system-level objectives into account. Attackers can induce the module to behave in a manner that is locally optimal but globally pathological. In addition, integrated strategies, using and integrating the diverse capacities and experiences of people and the IC, are required at a time when information can be misinformed, misdirected or exploited by smart decision-making. Three key areas of research need to be considered: human-machine teaming, building trust in systems and individuals, and providing decision-making assistance. [1]

4. Future developments in the area

There is hardly any big modern AI industry – a lot of "narrow AI" in particular, which performs target functions that victimize data models and often fall into deep-seed research categories or machine learning – that is not already affected. This is particularly true in recent years, as data collection and analysis have increased dramatically due to the powerful Internet of Things networks, the proliferation of smart devices and computer processing.

Many businesses are on their AI route, others are seasoned travelers. It's a long way everyone's got to go. However, the implications of artificial intelligence on human lives today are hard to overlook.

Education

Early stage AI helps students to assess who is distracted or bored and to change their skills to match their individual needs with each person and face recognition test indicators. The textbooks are digitalized.

Manufacturing

Robot powered by artificial intelligence works with human beings in a number to perform a limited number of functions, such as assembly and stacking.

Media

Journalism now uses and will continue to benefit from artificial intelligence. To make the financial statements more complicated, Bloomberg uses Cyborg technology. The Associated Press employs linguistic skills in artificial intelligence and creates 3,700 articles a year, nearly four times as many as previously.

Transportation

While it could take ten or several years to perfection, self-sufficient cars could one day transport humanity.

Healthcare

Diseases are rapidly and reliably identified in the relatively modern field of health care, the development of medications is supported and efficiently handled by virtual nurses, and large-scale knowledge sharing helps build more customized know-how for patients.

There are three major ways AI can alter the essence of cyber attacks

A new category of sophisticated and stealthy attackers, recently emerging, will shape the future of cybersecurity. Their intention is not just to track users but also to exploit or modify information. There is very little chance that criminals might use artificial intelligence (AI) to accelerate the next massive upgrade of cyber weapons, and eventually pioneer the harmful misuse AI. The basic capability of AI to learn and adapt can inaugurate a new age in which highly personalized and emulating attacks can be scaled. [10]

- Fitting AI into the digital environment: Human beings are increasingly dependent on digital systems and technologies, creating an increasingly sophisticated network infrastructure that is strongly connected. Enterprises and expertise are required to ensure that tactical fights take priority – so not only the economically significant government and industry data but the integrity in digital structures that strengthen social stability and democratic institutions, are maintained [10]
- Attacks at prototype-AI (a view of the hereafter): AI-fuelled cyberattacks aren't really a theoretical principle of the future. All of the basic components needed for using offensive AI currently exist increasingly sophisticated malware, economically induced – and cynical – hackers determined to use whatever means they can to maximize their financial return, as well as open-source AI research projects that make completely useful knowledge accessible in the public domain. A great example of a prototype-AI attack is amongst the most infamous components of recent malware – the Trojan Emotet. Spam-phishing is the principal distribution method of Emotet, generally through invoice attacks that deceive consumers into tapping on harmful email attachments. [10]
- AI-Offensive(Cyber threats paradigm reform) : ‘ The WannaCry ’ ransomware attack reached entities in around 150 countries around the globe in 2017, representing the starting of the new age of sophisticated cyberattacking. Its effectiveness was in its ability

to push sideways in seconds, paralyzing hard drives, and the event spawned several copycat threats. [10]

Security risk of AI-Enabled Systems and necessary development aspects of it.

1. Security and Privacy in Machine Learning

    i. Potential Avenues for Attack.
    ii. Security Requirements and Approaches.
    iii. Putting the risk into Context.
    iv. Security Requirements and Approaches.
    v. Verifying Security.

2. Security Learning in Adversarial Physical Environments

    i. Adversarial Environments.
    ii. Realizing Physical-World Attacks.

Privacy and Human Rights Future AI

The fact that AI's reliance on big data already has a significant effect on privacy has become apparent. Look much like the Facebook shenanigans from Cambridge Analytica or the Amazon eavesdropping from Alexa, two of the most Insanity instances of Tech. Critics claim that the situation will get even worse without sufficient protections and self-imposed constraints. The 2015 Google and Facebook rivals for creepy data mining insulted Apple's CEO Tim Cook.

There are two aspects to be dangerous the AI

Many researchers agree that it is impossible that a super-intelligent AI will represent emotions of persons such as Love or hatred, and there's no reason to assume AI to be intentionally benevolent or

malevolent. Alternatively, when considering how AI may become a challenge, there are two possibilities that experts find most plausible: [11]

1. The AI is designed to make perfect, but to achieve its goal, it uses a harmful technique.

   That will happen if people crashed to dispose the AI's desires with them fully, it maybe incredibly difficult. When someone asks for law-abiding smart car to take him to the airport as soon as possible, he could be chased by helicopters and covered in blood, but he could not know what they were actually asking for. When a super-intelligent computer is charged with a complex geoengineering quest, it would cause desolation as a side-effect to the human world and look its endeavour to avoid tt is a problem to overcome. [11]

2. The AI is expected to do something scary.

   Autonomous vehicles are also very dangerous and artificial intelligence systems built for destruction. These weapons Might easily trigger problems Major losses in the hands of the wrongdoers. In fact, by mistake, The AI industry may lead to an AI warfare that would lead to significant casualties. These frameworks should be designed to be extremely difficult to enforce "switch off" quickly in order To stop needing to foil by the adversary in such a way that humans might credibly confuse the authority in such a circumstance. Even with limited AI, this threat is detectable, but is rising as AI knowledge and self-improvement levels. [11]

However, as such experiments clarify their features, malignancy is not a concern for advanced AI. A super-smart AI may be brilliant in achieving its goals, and if these things are incompatible with humans, they have a problem. [11]

Using cases in defense organizations for AI

A number of cases of security organizations are illustrated in this section. This List demonstrates the applications of AI the are appropriate for military purposes not only improve 'kinetic' or 'hard

force' functions, but also provide high-quality, intelligent or ongoing control, logistic and strategic applications.

1. Automating Cyber Operations
   So first, AI technologies may well perform a strong role in their "first" globe – cyberspace.

2. Automated Manpower Preparation and Distribution
   Although full-fledged 'automatic preparation' still proves to be a bottleneck in creating AI302 machine learning structures based on skill test datasets of soldiers and their past mission success (individually and in various constellations of teammates) on different types of missions, elaborate models can be formulated.

3. Targeting Algorithm
   The use of AI in the development of fast and precise auto-target recognition systems (ATR) is another major use case for AI, which is particularly important in a tactical context.

4. Awareness of the situation and comprehension
   Thus UAVs strongly support the projection of power during asymmetrical wars, they also consider a variety of operational constraints, such as flying low acceleration and air defense systems.

5. Mission Handoff
   Military operations are routinely carried out by rotating teams over longer periods of time. It may be required on a time basis (optimization of the unit operating speeds) or background (Alters in the operating environment involving special force packages).

6. Analysis of target structures / Target audiences

   Target Systems Analysis (TSA) and Target Audience Analysis (TAA) are intelligence-related approaches used to improve knowledge of future areas of action.

.

5. Conclusion

In addition to adding value to the security divisions of companies and individuals, information security intelligence also spreads power in the wrong way. In order to give AI more leverage in the future for security purposes, all human needs are to ensure that it stays solely with white hat men. If the attackers can use AI, then the defenders can also use the power of Artificial Intelligence to effectively manage today's threat landscape.

When it comes to this report, it is also regarded as an example of the security threats posed by the Artificial Intelligence Agency.

While AI technology has existed for decades, in recent years policymakers have only begun to concentrate on this technology, as the interactions between AI technologies and political, social and economic processes have increased in complexity, complexity and implications. This study outlines the specific facets of AI's safety challenges. In the paper, the evolution of AI also argues about how AI evolved with health.

According to that there are two security risk enable systems and want to development areas. Those are security of privacy in machine learning and security learning in adversarial physical environments.

Despite all these barriers and challenges, AI and ML will undoubtedly remain the best and most relevant technologies to resolve information security threats and issues of all kinds. AI and ML's position in cyber security can only be strengthened if new technical areas further enhance cyber security.

References

[1] NETWORKING & INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT SUBCOMMITTEE , "ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: OPPORTUNITIES AND CHALLENGES," NATIONAL SCIENCE & TECHNOLOGY COUNCIL , 2020. p.1. Available at: https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf

[2] Investopedia, "Artificial Intelligence (AI)," 13 March 2020. [Online]. Available: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp.

[3] IEEE, "Artificial Intelligence," 24 June 2019. [Online]. Available: https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE18029.pdf..

[4] INGRAM, 02 July 2018. [Online]. Available: https://imaginenext.ingrammicro.com/networking-and-security/the-top-3-ai-security-threats .

[5] Thanh Cong Truong , Quoc Bao Diep, Ivan Zelinka, "Artificial Intelligence in the Cyber Domain: Offense and Defense," pp. 06-17, 4 March 2020.

[6] "Artificial Intelligence Threats and Security Issues," Identity Management Institute, [Online]. Available: https://www.identitymanagementinstitute.org/artificial-intelligence-threats-and-security-issues/.

[7] G. Walter, "Vulnerabilities and Failures of Artificial Intelligence | Digital Immunity," DIGITAL IMMUNITY, 17 July 2018. [Online]. Available: https://www.digitalimmunity.com/vulnerabilities-and-failures-of-artificial-intelligence/.

[8] R. Yampolskiy, "Predicting future AI failures from historic examples," pp. 03-06, 18 October 2018.

[9] S. SOLOMON, "AI a new and 'frightening' battlefield in cyber war, experts warn," 16 February 2020. [Online]. Available: https://www.timesofisrael.com/ai-a-new-and-frightening-battlefield-in-cyber-war-experts-warn/.

[10] William Dixon, Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, 19 June 2019. [Online]. Available: https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.

[11] M. Tegmark, "Benefits & Risks of Artificial Intelligence - Future of Life Institute," Future of Life Institute, 2016. [Online]. Available: https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/.

25th April 2020