International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2020.3612

E-ISSN : 2454-6135

Volume.6, Issue 5
May -2020

Artificial Intelligence in Cyber Security

Matthew N. O. Sadiku, Omobayode I. Fagbohungbe, and Sarhan M. Musa

Roy G. Perry College of Engineering,

Prairie View A&M University,

Prairie View, TX, USA.

ABSTRACT

Cybersecurity is the process of protecting computer networks from cyber attacks or unintended unauthorized access. It is the need of the hour. Organizations, businesses, and governments need cybersecurity solutions because cyber criminals pose a threat to everyone. Artificial intelligence promises to be a great solution for this. By combining the strength of artificial intelligence with cybersecurity, security experts are more capable to defend vulnerable networks and data from cyber attackers. This paper provides an introduction to the use of artificial intelligence in cybersecurity.

Key Words: Cyber security, Cyber-attacks, Artificial Intelligence.

1. INTRODUCTION

Today, we live in cyber world where everything is digital and data is king. Data security (especially sensitive or personal data) is now more important than ever. Hackers are becoming smarter day by day and they are more innovative in exploiting the vulnerable data of individuals, organizations, and governments. With new cyberattacks, data bridges, and data breaches, data poisoning, hackers attacks, and crashes come to light almost every day. Cyber criminals pose a threat to organizations, businesses, governments, and consumers who use computer networks. Cyber-attacks have been ranked as one of the top five most likely sources of severe, global-scale risk. Attacks to networks are becoming more complex and cybercriminals are becoming more sophisticated every day. This compels organizations and others users of computer networks to pay close attention to their network security.

Cybersecurity refers to technology and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. Cybersecurity takes different forms including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, and information systems. The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. As shown in Figure 1, involves multiple issues related to people, process, and technology [1].

Cyber attacks are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). Cyber attacks or threats include malware, phishing, denial-of-service attacks, social engineering attacks, and man-in-the-middle attack. Cybersecurity involves reducing the risk of cyber-attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [2].

Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the Department of Homeland Security (DHS). The DHS has a dedicated division responsible for risk management program and requirements for cybersecurity called the National Cyber Security Division. The Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical computer networks and networked infrastructure. The Computer Fraud and Abuse Act (CFAA) remains the most relevant applicable law expressing the US proactive cybersecurity effort [3].

2. OVERVIEW ON ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is one of the most important global issues of the 21st century.

The term "artificial intelligence" (AI) was coined in 1956 by John McCarthy during a conference held on this subject. AI is the branch of computer science that deals with designing intelligent computer systems that mimic human intelligence. The ability of machines to process natural language, to learn, to plan makes it possible for new tasks to be performed by intelligent systems. The main purpose of AI is to mimic the cognitive function of human beings and perform activities that would typically be performed by a human being. AI is stand-alone independent electronic entity that functions much like human healthcare expert. Today, AI is integrated into our daily lives in several forms, such as personal assistants, automated mass transportation, aviation, computer gaming, facial recognition at passport control, voice recognition on virtual assistants, driverless cars, companion robots, etc. AI technologies are performing better and better at analyzing data [4-5].

An important feature of AI technology is that is can be added to existing technologies. AI has benefited many areas such chemistry and medicine, where routine diagnoses are initiated by AI-aided computers. It embraces a wide range of disciplines such as computer science, engineering, chemistry, biology, physics, astronomy, neuroscience, and social sciences.

AI is not a single technology but a range of computational models and algorithms. The major disciplines in AI include expert systems, fuzzy logic, and artificial neural networks (ANNs), machine learning, deep learning, natural language processing, computer vision, and robotics. The various computer-based tools or technologies that have been used to achieve AI's goals are the following [6,7]:

- *Expert Systems*: An expert system (ES) (or knowledge-based system) enables computers to make decisions by interpreting data and selecting between alternatives just as a human expert would do. It uses a technique known as rule-based inference in which rules are used to process data.
- *Neural Networks*: These computer programs identify objects or recognize patterns after having been trained. Artificial neural networks (ANNs) are parallel distributed systems consisting of processing units (neurons) that calculate some mathematical functions. The ANN model represents nonlinear relationships which are directly learned from the data being modeled. Neural networks are being explored for healthcare applications in imaging and diagnoses, risk analysis, lifestyle management and monitoring, health information management, and virtual health assistance.
- *Natural Language Processors*: Computer programs that translate or interpret language as it is spoken by normal people. NLP techniques extract information from unstructured data such as clinical notes to supplement and enrich structured medical data. NLP includes applications such as speech recognition, text analysis, translation and other goals related to language. There are two basic approaches to NLP: statistical and semantic. Healthcare is the biggest user of the NLP tools [8].
- *Robots*: Computer-based programmable machines that have physical manipulators and sensors. The introduction of intelligent robots in the healthcare domain enhances patients' satisfaction, accuracy of diagnosis, and operational efficiency of hospitals. Medical robots can help with surgical operations, rehabilitation, social interaction, assisted living, etc. Robotic-guidance is becoming common in spine surgery [9].
- *Fuzzy Logic*: Reasoning based on imprecise or incomplete information in terms of a range of values rather than point estimates. Fuzzy logic deals with uncertainty in knowledge that simulates human reasoning in incomplete or fuzzy data. The fuzzy model is robust to parameter changes and tolerant to impression.
- *Machine Learning:* Algorithms to make predictions and interpret data and "learn", without static program instructions. ML is a statistical technique for fitting models to data and training models with data. ML extracts features from input data by constructing analytical data algorithms and examines the features to create predictive models. The most common ML algorithms are supervised learning, unsupervised learning, reinforcement learning, and deep learning. The most common application of ML is precision medicine. ML algorithms are a good fit for anti-malware solutions because machine learning is well suited to solve 'fuzzy' problems.
- *Deep Learning*: A subset of machine learning built on a deep hierarchy of layers, with each layer solving different pieces of a complex problem. It aims at increasing the capacity of supervised and unsupervised learning algorithms for solving complex real-world problems by adding multiple processing layers. An illustration of deep learning with two hidden layers is in Figure 2 [10]. The relationship between artificial intelligence, machine learning, and deep learning is shown in Figure 3 [11].
- *Data Mining:* This deals with the discovery of hidden patterns and new knowledge from large databases. Data mining exhibits a variety of algorithmic tools such as statistics, regression models, neural networks, fuzzy sets, and evolutionary models.

Each AI tool has its own advantages. Using a combination of these models, rather than a single model, is recommended. AI technologies are drastically influencing the retail industry and customer experience. Applications of AI technologies for

DOI : 10.31695/IJERAT.2020.33612

cybersecurity tasks are attracting greater attention from the private and the public sectors due to the rate at which threats are developing.

3. APPLICATIONS OF AI IN CYBERSECURITY

There is a wide range of interdisciplinary intersections between AI and cyber security. AI tools (such as expert systems, computational intelligence, neural networks, intelligent agents, artificial immune systems, machine learning, data mining, pattern recognition, fuzzy logic, heuristics, etc.) have been increasingly applied for cyber crime detection and prevention [12]. They can be used to learn how to enable security experts to understand the cyber environment in order to detect abnormalities. The use of artificial intelligence can help broaden the horizons of existing cyber security solutions. To enhance existing cybersecurity systems, companies can apply AI in the following four areas: automated defense, cognitive security, adversarial training, parallel and dynamic monitoring.

- *Automated Defense:* There are two types of cybersecurity systems: expert (analyst-driven) and automated (machine-driven). Expert systems are developed and operated by people, while automated systems use AI intelligent tools. AI-based systems are autonomous, self-learning agents. A good example of automated system is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). The speed and amount of data necessary to defend the cyber space cannot be handled by humans without automation. As networks become larger and more complex, artificial intelligence can be a huge boon to an organization's cyber protections. An ideal cyber-defense aims at fully protecting users, while preserving all the functionalities. AI automated systems can be integrated into existing cyber security functions. Some of these functions include [13-14]:
- Creating more accurate, biometric-based login techniques
- Detecting threats and malicious activities using predictive analytics
- Enhancing learning and analysis through natural language processing
- Securing conditional authentication and access
- Improving human analysis – from malicious attack detection to endpoint protection
- Using in automating mundane security tasks
- Having no zero-day vulnerabilities

There are many advantages to integrating artificial intelligence in cyber security. AI-based cybersecurity solutions are designed to work around the clock to protect you.

- *Cognitive Security:* Cognitive security combines the strengths of artificial intelligence and human intelligence. Cognitive computing (CC), an advanced type of artificial intelligences, leverages various forms of AI. It refers to hardware and/or software that mimics the way the human brain works. AI and CC remain closely similar in the intent, but they differ in their tendencies to interact naturally with humans. Artificial intelligence (AI) has been described as technologies capable of performing tasks normally requiring human intelligence. Cognitive computing seeks to overcome the boundaries of conventional programmable (von Neumann) computers. Watson for cybersecurity, IBM's first cognitive system, demonstrated through a Jeopardy exhibition match that it was capable of answering complex questions as effectively as the world's human champions. Watson learns with each interaction to connect the dots between threats and provide actionable insights. This allows an analyst to respond to threats with greater confidence and speed [15].
- *Adversarial Training:* This term is often used to refer to the development and use of AI for malicious purposes. Cybersecurity engineers are creating pre-emptive adversarial attack models to probe AI vulnerabilities. An adversarial learning attack can cause the algorithms to misbehave or reveal information about their inner workings. Adversarial training between AI systems can help to improve their robustness as well as facilitate the identification of vulnerabilities of the system. The more we adopt an "adversarial" and "always-on" strategy, the safer the AI applications become [16].
- *Parallel and dynamic monitoring:* The learning abilities of the targeted systems require some form of constant monitoring during deployment. Monitoring is necessary to ensure that divergence between the expected and actual behavior of a system is captured and addressed adequately. To do so, providers of AI systems should maintain a clone system as a control system, which serves as the benchmark against which the behavior of the original system is assessed [16].

DOI : 10.31695/IJERAT.2020.33612

4. BENEFITS

Artificial intelligence is well suited to solve some of the most difficult problems including cybersecurity. It is an enabling technology that transforms our lives. Embedded in our homes, cars, and devices, it will make everything "smarter" and more efficient [17]. AI can detect a software whether is a malware or a normal software. New AI capabilities can make the world safer, just, and environmentally friendly. Due to their flexibility and adaptive behavior, AI-based techniques can help us overcome of the deficiencies of conventional cybersecurity tools.

Businesses now depend on AI technologies, like machine learning, deep learning, and natural language processing, to help security analysts to respond to threat with speed and accuracy. They also help protect networks and sensitive data. AI can be used to detect threats and other malicious activities. It can analyze user behaviors, deduce a pattern, and identify all sorts of abnormalities in a computer network. It is capable of adapting and responding to a constantly changing world. It improves how cybersecurity experts analyze, study, and understand cybercrimes. A key benefit of machine learning in cybersecurity is that it identifies and promptly reacts to suspected problems.

5. CHALLENGES

Although artificial intelligence tools could help fight cybercrime, the tools are not a silver bullet and could be exploited by malicious hackers. There are limitations which prevent AI from becoming a mainstream tool. The downsides of AI in cyber security include cost, intensive resources, and training. AI in cybersecurity requires more resources and finances than traditional non-AI cyber security solutions and may not be practical in some applications. Cybersecurity is a domain where absolute security is impossible.

If a machine learning-based security tool misses a particular kind of cyberattack because it is not coded into it, that may to lead to problems. Hackers themselves can use AI to test and develop their malware and make it to potentially become AI-proof. Some critics have warned that AI could make cyberattacks more dangerous and more difficult to spot than ever before [18]. Some regard AI in cybersecurity as posing both a blessing and a curse, although the good outweighs the bad. Just as AI technologies can be used to identify and stop cyberattacks, cybercriminals can also use the AI systems to launch attacks. Besides, shortage of cybersecurity experts is another problem. These challenges prevent AI from becoming the only cybersecurity solution.

6. CONCLUSION

Artificial intelligence has become a growing area of interest and investment within the cybersecurity community. Some early AI adopters include Google, IBM, Juniper Networks, Apple, Amazon, and Balbix. An increasing number of companies and organizations are jumping on the AI bandwagon. As cyberattacks grow, artificial intelligence is helping security operations analysts stay ahead of threats. AI automated systems will soon become an integral part of cybersecurity solutions, but it will also be used by cybercriminals to do harm. The future of AI-enabled cybersecurity is very promising. More information on artificial intelligence in cybersecurity can be found in the books in [19-23] and the following related journals:

- *Journal of Computer Security*
- *International Journal of Artificial Intelligence & Applications*
- *International Journal of Computer and Internet Security*

REFERENCES

[1] "Eliminating the complexity in cybersecurity with artificial intelligence,"
https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/

[2] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," Doctoral *Dissertation*, University of Toledo, 2015.

[3] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi," A primer on cybersecurity," International *Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[4] M. N. O. Sadiku, T. J. Ashaolu, and S. M. Musa," Artificial Intelligence in medicine: A primer," International *Journal of Trend in Research and Development*, vol. 6, no. 1, Jan.-Feb. 2019, pp. 270-272.

[5] Y. Mintz and R. Brodie, "Introduction to artificial intelligence in medicine," *Minimally Invasive Therapy & Allied Technologies*, vol. 28, no. 2, 2019, pp. 73-81.

[6] R. O. Mason, "Ethical issues in artificial intelligence," *Encyclopedia of Information Systems*, vol 2, 2003, pp. 239-258.

[7] A. N. Rames et al., "Artificial intelligence in medicine," *Annals of the Royal College of Surgeons of England*, vol. 86, 2004, pp. 334–338.

DOI : 10.31695/IJERAT.2020.33612

[8] M. N. O. Sadiku, Y. Zhou, and S. M. Musa, "Natural language processing in healthcare," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 5, May 2018, pp. 39-42.

[9] "No longer science fiction, AI and robotics are transforming healthcare,"
https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html

[10] F. Jiang et al., "Artificial intelligence in healthcare: Past, present and future," *Stroke and Vascular Neurology*, 2017.

[11] "Quantum computing,"
https://quantumcomputingtech.blogspot.com/2019/05/ai-machine-learning-venn-diagram.html

[12] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," *International Journal of Artificial Intelligence & Applications*, vol. 6, no. 1, January 2015, pp. 21-39.

[13] C. Crane, "Artificial intelligence in cyber security: The savior or enemy of your business?" July 2019,
https://www.thesslstore.com/blog/artificial-intelligence-in-cyber-security-the-savior-or-enemy-of-your-business/

[14] "The role of AI in cyber security," https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/

[15] "Artificial intelligence for a smarter kind of cyber security," https://www.ibm.com/security/artificial-intelligence

[16] M. Taddeo, T. McCutcheon, and L. Floridi , "Trusting artificial intelligence in cybersecurity is a double-edged sword," *Nature Machine Intelligence*, vol. 1, November 2019, pp. 557–560.

[17] Unknown source.

[18] D. Palmer, "AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know," March 2020,
https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/

[19] N. J. Daras and M. T. Rassias (eds.), *Computation, Cryptography, and Network Security.* Springer, 2015.

[20] A. Parisi, *Hands-On Artificial Intelligence for Cybersecurity: Implement Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies.*
Packt Publishing, 2019.

[21] S. Halder and S. Ozdemir, *Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem.* Packt Publishing, 2018.

[22] M. Gilbert (ed.), *Artificial Intelligence for Autonomous Networks.* Boca Raton, FL: CRC Press, 2018.

[23] B. B. Gupta and Q. Z. Sheng, *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices.* Boca Raton, FL: CRC Press, 2019.

ABOUT THE AUTHORS

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interests include computational electromagnetics and computer networks. He is a fellow of IEEE.

Omobayode I. Fagbohungbe is a doctoral student at Prairie View A&M University, Prairie View Texas. He holds a masters of science degree in control engineering from The University of Manchester, UK and a bachelor degree in electrical and electronics engineering from Obafemi Awolowo University, Nigeria. He is a graduate member of the IEEE. His current research interests are in data science, machine learning, and deep learning.

Sarhan M. Musa is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His research interests include computer networks and computational electromagnetics.

DOI : 10.31695/IJERAT.2020.33612

Figure 1: Cybersecurity involves multiple issues related to people, process, and technology [1].

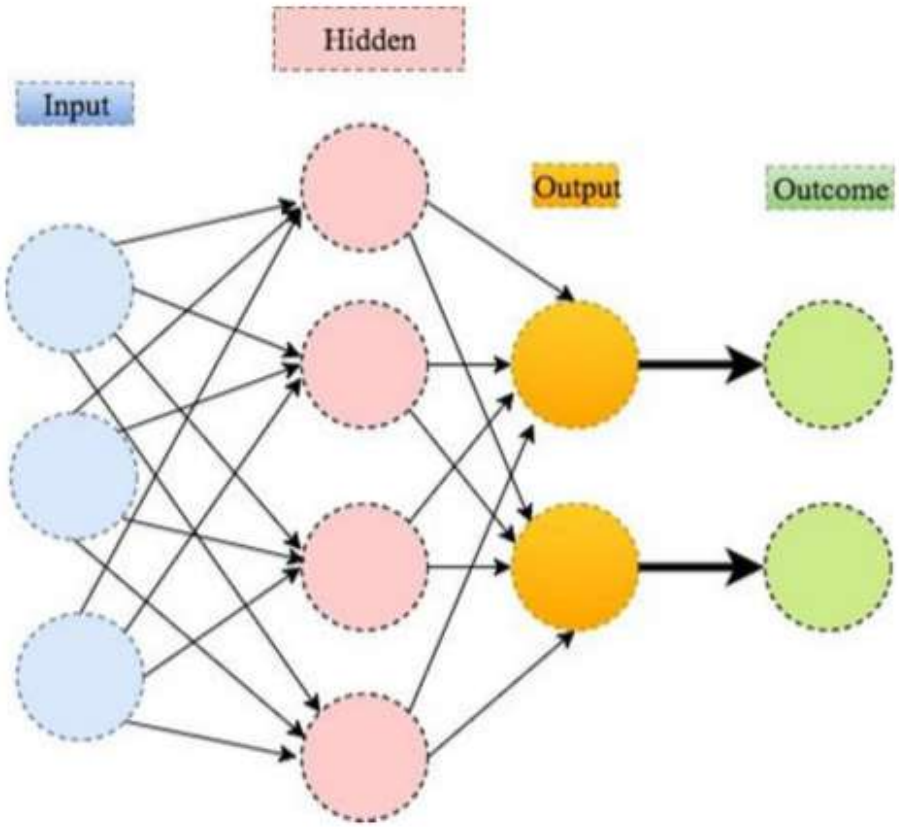

Figure 2: An illustration of deep learning with two hidden layers [10].

DOI : 10.31695/IJERAT.2020.33612

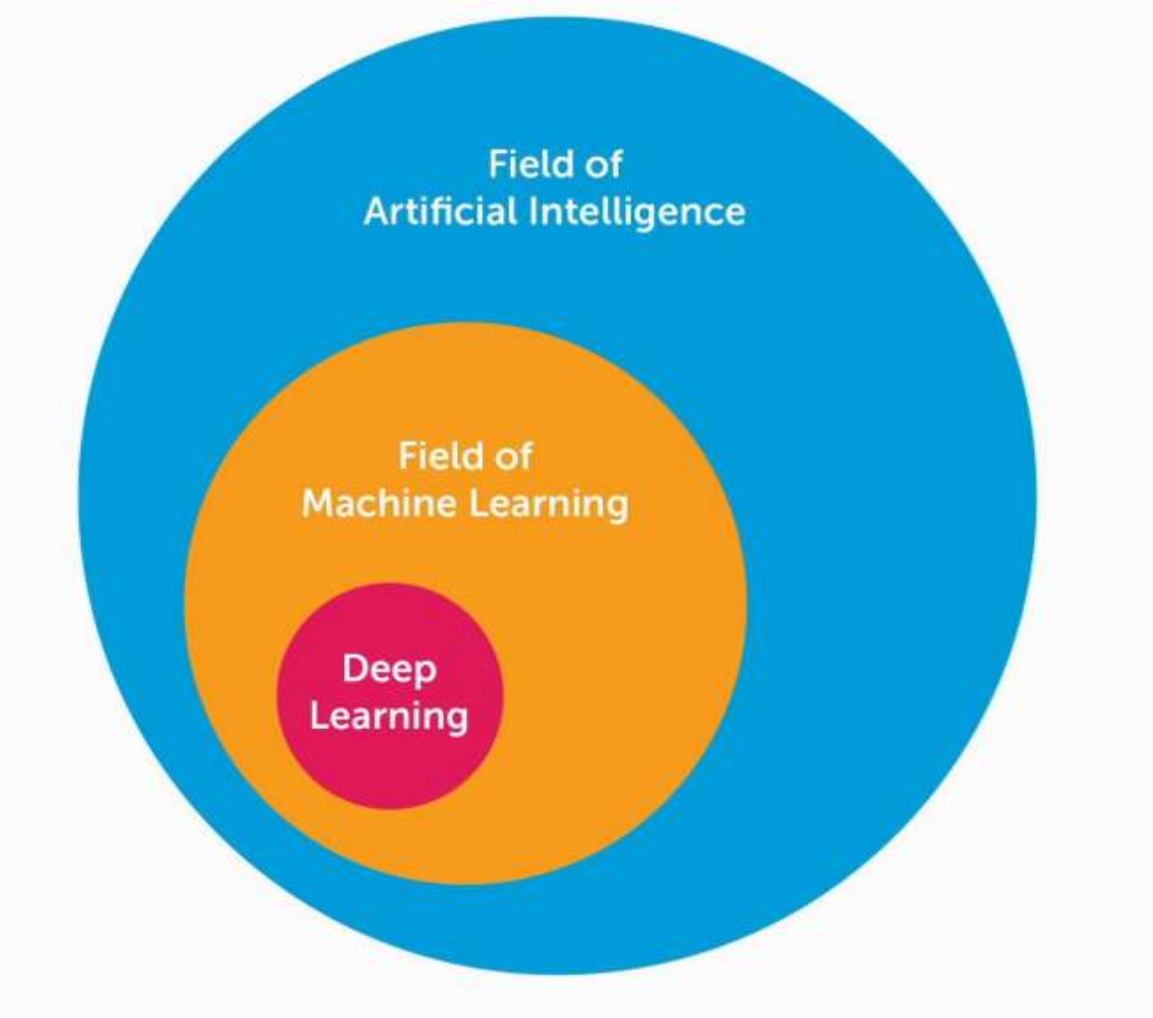

Figure 3: The relationship between AI, machine learning, and deep learning [11].

DOI : 10.31695/IJERAT.2020.33612