Global Scientific JOURNALS

GSJ: Volume 10, Issue 3, March 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

REVIEW ARTICLE RELATED TO THE ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Yashaf Zain, Maaz Ahmed

INTRODUCTION:

This article will give an insight on the application, benefits along with its disadvantages, dangers, and future of Artificial Intelligence in terms of Cybersecurity.Mohammed, I.A., 2020. ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE. *ARTIFICIAL INTELLIGENCE*, *7*(9).

The discipline that could be beneficial for humans globally related to Cyber security by introducing Artificial Intelligence (AI). The term related to Cyber security, information technology (IT) security, computer security that any computer system and networks remain protected from any leakage of information, data robbery, leakage or disclosure of data, hardware or software damage, or data disruption.[3] Moreover, it refers to the protection or security of any computer system from software changes or damage, misdirection of the services provided by any source or organization. Artificial Intelligence can be applied based on human insights and knowledge. AI application is essential for helping in reducing the increasing number of threats concerning computer systems. [3]

These cyber-threats are very critical to handle for it appears to damage the system and information in form of data worldwide. Artificial Intelligence is not able to perform its functions without the involvement of human effort and intelligence. Considering the fact that AI needs a proper environment where human intelligence and Artificial Intelligence combine and performs their functions efficiently. [1] Different organizations have been working on providing suitable approaches where Artificial Intelligence meets Human Intelligence to give remarkable services to achieve great successes in the future. Recent truth is that where Artificial Intelligence is developing new reforms in the technology globally at the same time it has its challenges to be faced. Reduction of increasing various possibilities of danger and risks related to Artificial Intelligence is one of the foremost concerns of the organizations. [2]

The number of cyber attacks and their severity is increasing frequently. Tremendous progression in cyber attacks and their powerful and more targeted nature is becoming a challenging concern for cyber security. On account of encountering these attacks, it is essential for making great cyber security measures to minimize these attacks. Since 1988, when the first cyberattack

Denial-of-service (DoS) was launched, the culture, the number, and impacts of cyberattacks increases notably. Formerly, the cyber security tool was limited relates to the identification of viruses and their prevention from accomplishment afterward a lot of approaches are designed to provide a wide range of protection. Numerous researches happening to maximize the range of implementation of tackling the cyber issues and development of newer issues by increasing practical implementation of Artificial Intelligence in a cyber security system. This is an alarming situation of implementation of Artificial Intelligence (AI) in cyberspace give rise to the upcoming future of decreasing human efforts and more reliability over Artificial Intelligence (AI). [7]

Researchers associated with the information and communication sector are agreed to perform relevant research to secure data containing information (InfoSec). Information security is one of the primary concerns of Artificial Intelligence (AI). Therefore, a lot of technological methods or technologies are adopted to complete the research. Examples include the use of Malware detectors, intrusion detectors and prevention systems (IDPs), Data encryption, algorithms, and sophisticated firewall setups. There are a lot of arguments are going on between the researchers like that data security only related to human behavior while others thought that data security is not fully dependent on human behavior alone instead organizations recognized there is a need to apply reforms in between human behavior, technology and policy management. There is a necessity to improve the quantum of information handling and the organization's data security activities. [7]

Fix algorithms and physical devices for example sensors and detectors were used as conventional cyber security tools used for preventing the data and information by the application of these technologies. [3] These tools are found ineffective compared to the new cyberspace threats. Occasionally, the methods of identification of viruses for the first generation of antivirus system by scanning bit signature provide the concepts of viruses by studying the pattern of bit in all occurrences. Although, the systemic approach for the modernization of signature and algorithms on daily basis. Whenever the devices come in contact with the internet connection the conventional technology called Vast Malware becomes ineffective by just altering the sophistication and due to irregular release of data, this makes the program ineffective. The capabilities of Vast Malware alters by attacking methods like behavioral identifications. Therefore, AI has gained the interest of researchers and become effective. [2]

This demonstrates the importance of improving in implementation of Artificial Intelligence in the cyber security domain. Undoubtedly, the application of AI has made it possible to develop a relatively efficient and effective system that can recognize any evil activities related to cyberspace automatically. [6] AI applications are also being used for the enhancement of already existing technology and cyber operating systems. They are also responsible to introduce various effective mechanisms and standards to control the cyber attack in a better way. It also helps to prevent the recurrence of these malicious attacks in cyberspace. These rapid advancements happening within cyberspace specifically in Artificial Intelligence have made the work of researchers more challenging to hold that rapid evolution most beneficially. These approaches have made rapid changes in the world of technology and introduced new challenges for the researchers to make this technology sustainable in the means of cyber security or information security. [4]

Organizations, researchers, and practitioners associated with cyber security suggest that Artificial Intelligence has proven most of the expectations related to information security and cyber security. Moreover, the application of Artificial Intelligence has improved many of the domains of cyberspace but there is a lot of necessary knowledge is needed to get innovative and speculative results. There are many researchers and experimentation are being involved to improve the conventional methods used to secure data and information. Those technologies and mechanisms are being followed to improve cyberspace and enhance the security of data from getting any damage or deterioration. Consequently, it is necessary to explore the ways which summarize the challenges, issues, and future research relates the Artificial Intelligence in the field of cyber security or information security.

The purpose of this report is to give an insight into the flaws of conventional cyber security systems as well as the progress that has been made in cyberspace after the implementation of Artificial Intelligence (AI). This report summarizes the concerns, future, dangers and also explores dimensions of Artificial Intelligence in cyberspace. [3]

For the purpose to complete this research report two methods had been adopted the first one is qualitative and the other one is quantitative. The qualitative includes data for this research report is taken out from the introduction includes the definition of Artificial Intelligence and its applications in cyberspace specifically in what manner Artificial Intelligence improves the Cyber attacks and including various types of cyber attacks and their method of prevention.

The study has been conducted in three different phases consisting of *Planning*, where we identify the cause of research, identify the possible questions that can be related to research, find out about the relevant terminologies that describe the definition. Once the purpose of the research has been fully identified and got approval then the second phase has started called *Conducting*, this phase of the study includes the relevant searching of online databases, designing the databases according to our framework, designing the questions to be asked according to the studies. The third phase is called *Documenting,* where the actual analytical procedure has been started. Analyze the report matches the actual purpose of report writing according to the literature review through various researches. The discipline that could be beneficial for humans globally related to Cyber security by introducing Artificial Intelligence (AI). [7]

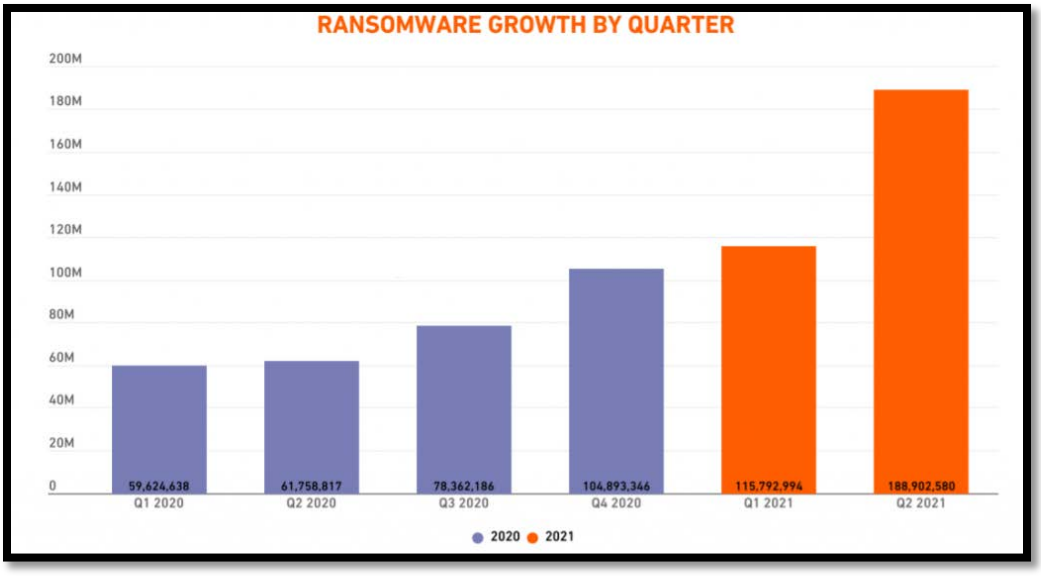
The term related to Cyber security, information technology (IT) security, computer security that any computer system and networks remain protected from any leakage of information, data robbery, leakage or disclosure of data, hardware or software damage, or data disruption. Adopting the qualitative method describes, Types of Cyber security by getting to know about cyber security firstly, Cyber security refers to the term that describes the protection of the network from being attacked by unauthorized intruders. Internet protocol i.e. IP is considered as the most transmitting traffic flow nowadays. It is a matter of fact that networks are designed in many forms of layers and all of those layers are vulnerable to attacks. [7]

Various malicious activities are occurring frequently out of which two are Network Intrusion and Distribution denial of service (DDoS) attacks. *Network Intrusion* is defined as the Introduction of an unauthorized or unwanted exploiter into the network. The intrusion purpose will be to consume resources of that particular network grab the information provided and gain knowledge about the Cyber system which can be used for later attacks with more severity. The main

objective for applying any security towards the information is to secure the network functionalities and keep prevented from any sort of cyber attacks, in purpose to prevent the application from any sort of cyber attack. *Testing* is one of the key elements to preserve the data throughout the lifespan of the application. It is very essential to secure the *Clouds* as the vast amount of data is being stored in the Clouds. The protection of clouds is necessary utilizing protecting any physical storage. Since Cloud services are based on Virtual Machines solutions it is very crucial to secure these sorts of platforms as they get to attack easily. Virtual machines are very much prone to get attacked by the Denial of the system (DoS) and Data Breaches. [7]

A service Injection Attack is a type of attack which attacks the Cloud in which the attacker inserts a malicious input to the system and alters the function of the command. The other Cyber security aspects can be described as End Points. *End Point Security* is considered as the practice of preventing the data entry point meaning the point where all the information comes from any exploitation or any other cyber attack. Various devices in the same manner including mobile phones, desktops, printers, laptops, smartwatches functions through a network. Standard Antivirus software is not enough to direct the complexity of today's malicious attacks. The End Point Protection (EPP) is considered as the future of Cyberspace. [7]

Furthermore, the qualitative analysis includes a detailed study of the different types of threats. European Network and Information Security Agency ENISA reported some of the kinds of threats that have been threatening the cyber system repeatedly. ENISA has provided a landscape through which threats can be reproduced to damage any cyber system including *Malware*, Web-based attacks, Phishing, Web application attack, Distributed denial of service (DDoS), and data breach. Among them, Malware is one of the leading methods to threaten any cyber system. Malware comprises the viruses such as Ransomware and Trojan horses. It has the ability to theft identity, disruption, and cyber espionage in the cyber system, designed as a bug that destroys the software lately. According to the statistics, 50% of Malware steals personal information while 71% targets business. Malware-as-a-service (MAAS) and Software-as-a-service (SAAS) is alarming trend that hits the business market. [6]



The quantitative and qualitative analysis includes the designing of questions in the planning stage which identifies the goal of the study which becomes the foundation of the study. For that purpose Goal-Question-Metric approach was adopted. [7]

Purpose: to analyze the study
Issues: Future direction, publication domain, trends of publication, methods of study
Object: Application of Artificial Intelligence AI in Cyber security
Viewpoint: between 2011 and 2021

The Questions that are included for the research purpose are mentioned below:

Sno#	Research Question	Incentive	Method
01	Artificial Intelligence its methods in cyber security along with its publication trends?	To determine the ways of identification of various domains working in the field of AI its value in the recent era depends on the number of studies conducted over a period.	Quantitative
02	What are the issues on which Artificial Intelligence can be applied for including its methods used in cyber security?	To objectify various methods through which AI can be fruitful in terms of cyber security along with identification of lack ness observed by the researchers on concentrating the potentials over the information provided.	Qualitative
03	What are the impacts of AI on the methods identified in cyber security?	To determine the current impact of AI on cyber security.	Qualitative
04	What is the future research direction of AI on Cyber security?	This question arises the need to glorify the future of artificial intelligence in terms of cyber security	Qualitative

All the data, research, and studies that have been mentioned in this research paper are based on this methodology followed. [7]

DISCUSSION:

Employing preparing this report is to highlight the point through which we can enhance the knowledge regarding Artificial Intelligence particularly in terms of Cyber security. This report generally sectioned first gives an insight over the introduction about the Artificial Intelligence that Artificial intelligence helps in making computers to learn from experience, adjust to new data and perform some complex tasks which require human intelligence...Research interest in AI includes ways to make computers simulate intelligent human behavior such as thinking, learning,

reasoning, planning, etc. [5] Examples of AI applications include self-driving cars, recommendation systems, advanced search engines, face recognition, etc. Artificial Intelligence has various domains of working where it produces its optimum functionality such as helping in implementing AI against cyber attacks to achieve trustable security. To assist in using new machine learning models to reduce human dependability and produce faster results, to make use of Data Science, gather and feed enough data to the system to increase efficiency and accuracy to avoid cyber attacks. Various stakeholders are being involved in the betterment of its application, for example, Artificial Intelligence Engineer, Cyber Security Experts, Software Developers, Client Product Customers. [6]

The purpose of this study is to provide acknowledgment over the crime-related activities especially on cyber crimes and to provide possible knowledge to identify the ways through which we can secure the data and information related to the cyber system. The Crimes targets the system that has informative data typically bank accounts, personal data, websites, computer servers, digital records, computers, servers, and of public and private organizations. Every day we are faced with an increasing number and variety of cybercrimes since this technology presents an easy way for criminals to achieve their goals.[6]

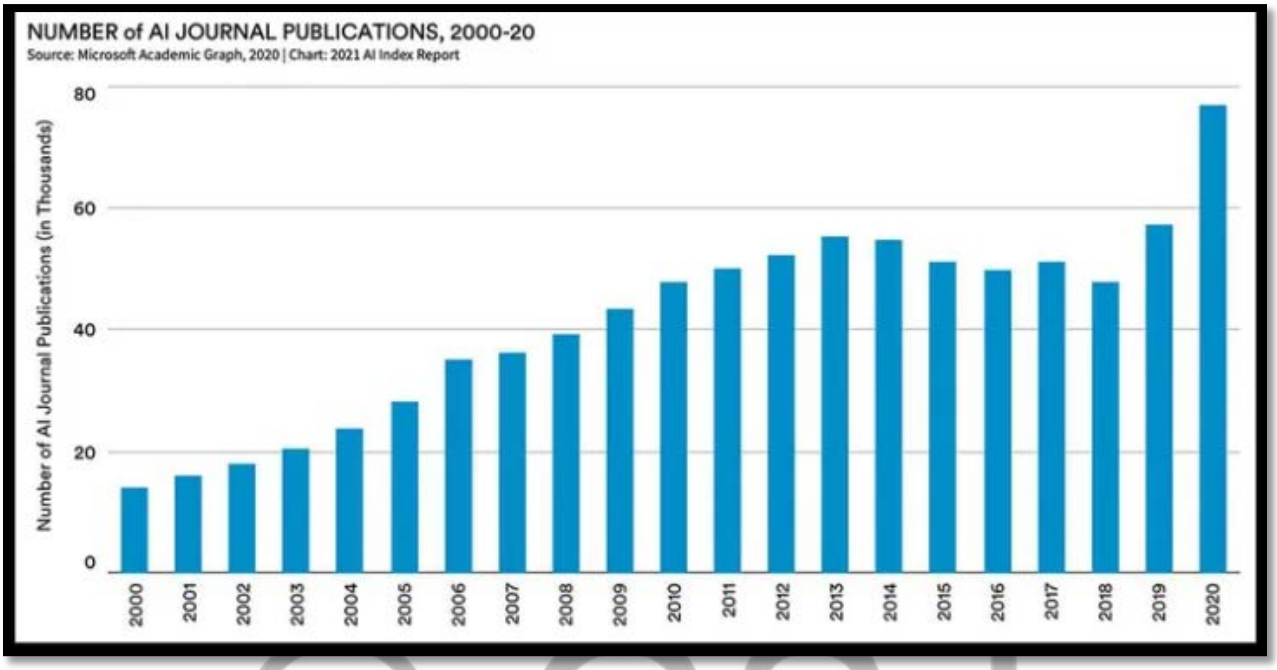
The *application* of Artificial Intelligence in cyber security has started a long ago as *Gmail* has already been introduced as an email section specified for unrecognized email senders and presented as spam email this is all done by AI. *Frauds* can be detected utilizing AI, such algorithms have already been designed for early detection of any fraudulent activity from an intruder through expected consumer habit, transactions made by MasterCard can be used to identify the consumer buying patterns, the algorithm used for increasing transaction, tracing the location of the transaction, can apply to determine the algorithm to trace any unusual purchasing or selling. [8]

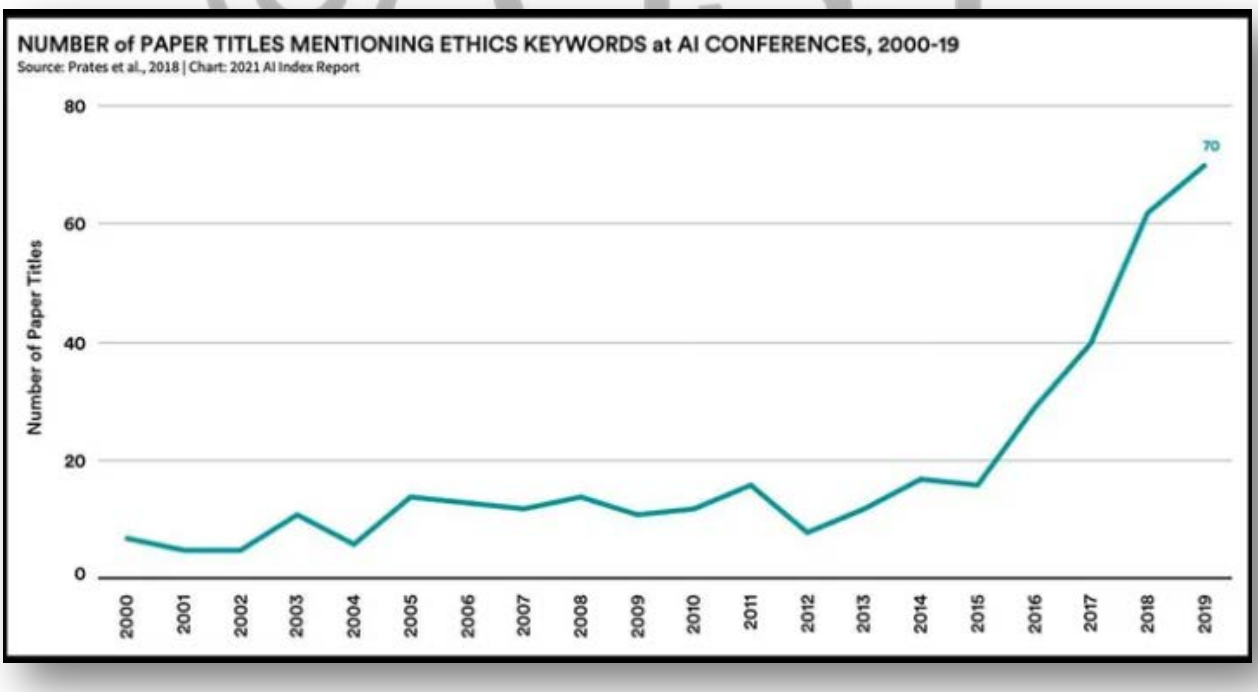
As the *future* of Artificial Intelligence is bright in terms of cyberspace, it is also beneficial to grow the business globally. Blockchain technology has the greatest potential net benefit in the US. Blockchain may assist businesses from heavy industries like mining to fashion brands to increase attention by the public and investors about sustainable and ethical procurement. Usage of digital Cryptocurrency in response to banking will have fewer chances to go through digital frauds and identity theft. [6]

In the same way, it has its drawback that needs to be addressed as the organization will need to have bigger budgets to make this technology more sustainable. There should be a properly trained system have to installed to minimize that will have the ability to act against Malware and other malicious actors. Still, AI doesn't have access to a large number of data as this technology is fully dependent upon data sets. There are a lot of chances to get the wrong information as it cannot still differentiate between the data. [5]

By adopting the mentioned qualitative and qualitative methodology following results have been found which will be further discussed in detail in the discussion while some of the facts are explained here. It has proven that the publication trends have been excessively increased in past ten years. In 2010 it is observed that approximately 45% of research have been held on AI along with its publication margin but lately, it has increased up to 80% in 2020 (the data has originated from the past 10years of data of various sources including various countries researches, from mentioned references and Google scholars authentic manuscripts such as IEEE spectrum). Practitioners' attention has become more diverted towards the research related to Artificial

Intelligence in cyber security. The qualitative analysis includes the identification, methods, and future of AI in cyber security. [7] It also determines the issues to be minimized in terms of correcting the ways through which Artificial Intelligence can be more beneficial for future needs specifically in Cyber security. Some of the publication trends are shown as graphs in the figures below:





REFERENCES:

1. C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol. 5, pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418.
2. Zhu DL, Jin H, Yang Y, et al., 2017. DeepFlow: deep learning-based malware detection by mining Android applications for abnormal usage of sensitive data. IEEE Symp on Computers and Communications, p.438-443. https://doi.org/10.1109/ISCC.2017.8024568
3. Abeshu A, Chilamkurti N, 2018. Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag, 56(2):169-175. https://doi.org/10.1109/MCOM.2018.1700332
4. Taddeo, M., McCutcheon, T., and Floridi, L., 2019. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), pp.557-560.
5. Calderon, R., 2019. The benefits of artificial intelligence in cybersecurity.
6. Soni, V.D., 2020. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *Available at SSRN 3624487*.
7. Mohammed, I.A., 2020. ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE. *ARTIFICIAL INTELLIGENCE*, *7*(9).
8. Donepudi, P.K., 2015. The crossing point of Artificial Intelligence in cybersecurity. *American journal of trade and policy*, *2*(3), pp.121-128.
9. S Nangia, M Malik, D Chahal, L KharbInternational Journal of Research In Engineering, Science and Management – 2018 researchgate.n