The Future of the “Metaverse”: Artificial Intelligence and Cybersecurity

Keke Yang

School of Literature & Journalism, Sichuan University, Chengdu, 610207, China
yangkeke1007@163.com

Abstract

The “Metaverse” has been determined as the future form of cyberspace, and how to ensure the safety of people in cyberspace has become the first issue to be considered before the arrival of the “Metaverse”, in which Artificial Intelligence plays a vital role. On the one hand, the development of AI has ensured the security of information in cyberspace, including ANN, Agent, Map/Reduce, IDS, AIFW, and other technologies are important tools to maintain cybersecurity, and compared with traditional computer means, AI has the advantages of low cost, high efficiency, and learnability; but on the other hand, AI has its hidden risks in terms of framework security, algorithm security, and data security. Therefore, to build secure cyberspace and realize the vision of a “Metaverse”, we need to make good use of the double-edged sword of AI.

Keywords: *Metaverse; Artificial Intelligence; Cybersecurity; advantages; pitfalls*

1 INTRODUCTION

In the first half of 2021, the “Metaverse”, a 30-year-old “old concept”, was reborn and became increasingly popular in the capital market, the industrial ecosystem, and the public opinion arena. In particular, after Facebook changed its name to “Meta”, the public’s attention to the “Metaverse” was pushed to a climax. The “Metaverse” is the future of cyberspace, cybersecurity is the core concern of the “Metaverse”, and AI is the key technology to ensure cybersecurity.

There are a large number of papers on the relationship between AI and cybersecurity, and these papers address various aspects of the relationship between AI and cybersecurity, for example, Praveen Kumar Donepudi discusses the crossing point of AI in cybersecurity [1]; Ricardo Calderon elaborates on the benefits of AI in cybersecurity [2]; Murat Kuzlu, Corinne Fair, and Ozgur Guler comprehensively discuss the role of AI in cybersecurity [3]. All three of these papers praise the important role of AI for cybersecurity in a positive light, but there are also many academics who have expressed concerns, for example, Vishal Dineshkumar Soni states the challenges of AI in cybersecurity in the US [4]; Roman V. Yampolskiy and M. S. Spellchecker demonstrate the timeline of AI failures in cybersecurity [5]. Thus, Mariarosaria Taddeo, Tom McCutcheon, and Luciano Floridi conclude: “trusting artificial intelligence in cybersecurity is a double-edged sword. [6]” However, all these papers discuss the security advantages or security pitfalls of AI from one aspect and do not look at the two together in a general dialectical way. Moreover, most of the papers discussing AI and cybersecurity do not involve a specific analysis of the key technologies of AI. Therefore, the purpose of this paper is to let readers understand the advantages and pitfalls of AI in cybersecurity through the analysis of specific technologies, which is a double-edged sword so that it will provide a reference for people to use AI to secure their networks in the future.

2 ANALYSIS OF CONCEPTS

What is the “Metaverse”? In terms of semantic structure, Metaverse is a combination of Meta + Verse, with Meta originally meaning “beyond” and Verse being a shortened version of Universe, the literal meaning of Metaverse is “the universe beyond the physical world”. MDPI describes the “Metaverse” as: “The Metaverse is the post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital virtuality. It is based on the convergence of technologies that enable multisensory interactions with virtual environments, digital objects, and people such as virtual reality (VR) and augmented reality (AR). Hence,

B. Fox et al. (Eds.): IC-ICAIE 2022, AHCS 9, pp. 1627-1632, 2023.
https://doi.org/10.2991/978-94-6463-040-4_246

the Metaverse is an interconnected web of social, networked immersive environments in persistent multiuser platforms. [7]" This is a generally accepted definition at present.

Artificial Intelligence is a field of computer research that encompasses a wide range of aspects, mainly through the full analysis and extraction of human thinking and cognitive activities, the establishment of models, and then through computer simulation, so that the computer can have the ability to self-learn and intelligent operation under human control so that the computer can respond in a way similar to human intelligence. Figure 1 illustrates the stages in the development of AI, despite the global economic slowdown due to the epidemic, as South Korean scholar Lee Byong-kwon put it, "Currently, the metaverse is rapidly emerging in a situation where human encounters are decreasing as non-face-to-face status continues due to COVID-19" [8]. AI, an important component of the "Metaverse", is also developing rapidly.

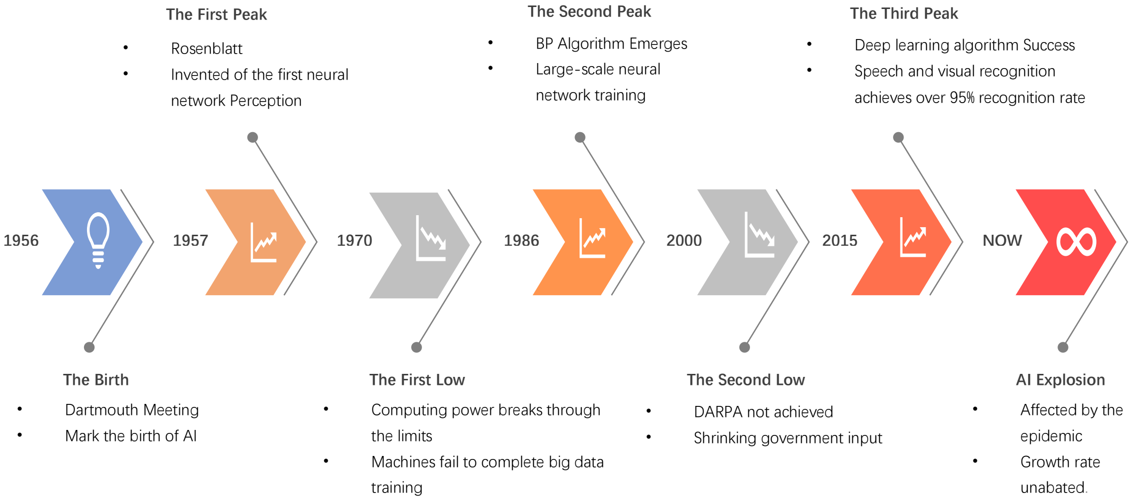

The First Peak
Rosenblatt
Invented of the first neural network Perception
The Second Peak
BP Algorithm Emerges
Large-scale neural network training
The Third Peak
Deep learning algorithm Success
Speech and visual recognition achieves over 95% recognition rate
1956
1957
1970
1986
2000
2015
NOW
The Birth
Dartmouth Meeting
Mark the birth of AI
The First Low
Computing power breaks through the limits
Machines fail to complete big data training
The Second Low
DARPA not achieved
Shrinking government input
AI Explosion
Affected by the epidemic
Growth rate unabated.

Fig.1 The stages in the development of AI

Baidu's definition of cybersecurity is: "Cybersecurity means that the hardware and software of a network system and the data in the system are protected from damage, alteration, and leakage due to accidental or malicious reasons and that the system operates continuously, reliably, and normally without interruption of network services. [9]" Specifically, cybersecurity includes several aspects such as system security, information security, communication security, and content security.

3 THE KEY TECHNOLOGIES OF ARTIFICIAL INTELLIGENCE

ANN. Artificial Neural Network, which can also be called neural networks, are models that simulate biological neural networks for information processing. Information processing is achieved by simulating the mechanisms and mechanisms of the animal brain while incorporating the behavioral characteristics of animal neural networks. Artificial neural networks have a very wide range of research content and are an important manifestation of the intersection of multidisciplinary fields. They are widely used in many fields because of their highly parallel structure, parallel implementation capability, non-linear processing capability, self-learning capability, self-organization, and self-adaptability.

Agent. Agent technology refers to computing entities that play a continuous autonomous role in distributed systems, with a certain level of interactivity and autonomy. This technology has evolved in distributed computing from people finding information to information finding people, allowing some parallel engineering and distributed interactive simulation problems to be handled effectively and allowing the original distributed computing model of only receiving user requests in order to provide services to be broken. Figure 2 shows the flow of the Agent model, (specific description) and we can see that with the application of the Agent technology's hub-and-spoke capability, the information points of the information publisher can be registered, so that the Agent can combine relevant information, through the relevant users who can provide the corresponding information, and can take the initiative to inform the information provider of the current need for the information it can provide, to achieve the continuous improvement of the network application.

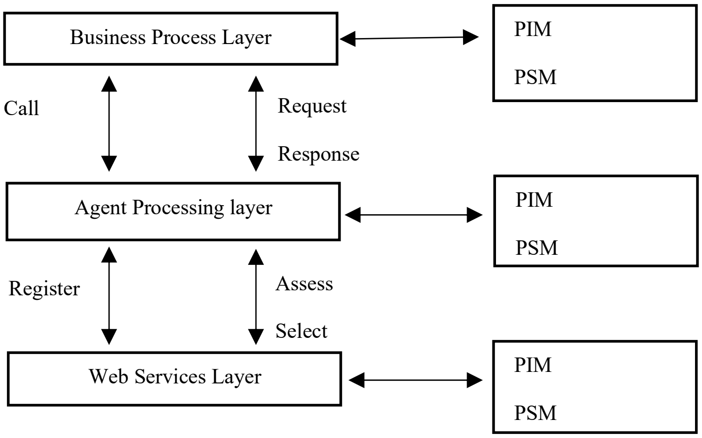
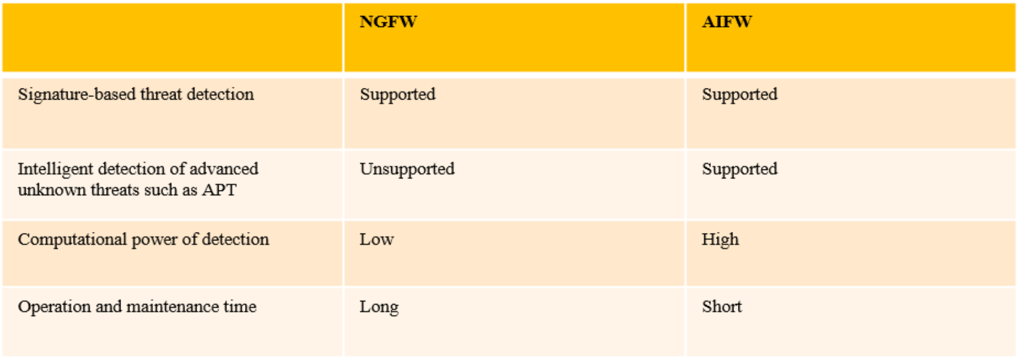


Fig.2 The flow of the Agent model

Map/Reduce. Map/Reduce technology is a model in computing that has an important role to play in the implementation of the Internet Plus and AI. The “Internet+” and artificial intelligence both have extremely strong information processing needs, so a reliable model should be chosen to enhance the efficiency of computer algorithm use and prevent computer systems from falling behind by choosing a reliable applications model. Applying the Map/Reduce model to the computer’s computing program can perform a hierarchical and independent computing function, improving the computer’s efficiency and effectively solving the problem of large-scale data application.

IDS. As a network protection technology, Intrusion Detection System is able to prevent risks and dangerous factors from both inside and outside, effectively intercepting all kinds of external viruses and hackers on the one hand, and reducing the adverse effects caused by various wrong operations on the user’s operation level, on the other hand, ensuring the safety of users in computer network operations. At the same time, its specific application does not cause any adverse impact on the computer network, which is one of the most important security barriers to monitoring the protection of computer networks, in addition to the firewall.

AIFW. The AI Firewall is a program that accurately determines viruses and requests assistance from the user when there is network access by an uncertain process, without normally asking the user. The intelligent firewall uses statistical, probabilistic, memory, and decision-making methods in the field of AI to identify relevant data based on which access control is achieved, and intelligence is the most prominent feature of this firewall. On computer networks, the use of intelligent firewalls can effectively solve the following problems: DDOS (denial of service attacks), virus propagation, advanced application intrusion, etc. It is much more secure than traditional firewalls. As shown in Figure 3, the advantages of AIFW compared to NGFW (Next Generation Firewall) are still very obvious.



	NGFW	AIFW
Signature-based threat detection	Supported	Supported
Intelligent detection of advanced unknown threats such as APT	Unsupported	Supported
Computational power of detection	Low	High
Operation and maintenance time	Long	Short

Fig.3 NGFW versus AIFW

4 THE SECURITY BENEFITS OF ARTIFICIAL INTELLIGENCE

AI holds huge advantages over people in many ways, such as fast computing, huge memory, sleeplessness, and independence from emotions. Intelligent machines can perform many tasks at the behest of people, which both reduces the pressure on people to work and will reduce errors in their work. The advantages of AI technology are mainly reflected in the innovation of ideas and technical means.

Low cost. AI is able to introduce Internet algorithms into the mix, which to a large extent can effectively increase the speed of network information when it is calculated, improve the efficiency of the use of resources and enable network security defense systems to be optimized in the analysis and calculation of information. The increase in efficiency and the reduction in resource consumption will reduce the pressure on workers and increase the speed of network operations.

Efficiency. Artificial intelligence can analyze uncertain information and manage network resources in a timely manner, so it has a unique advantage in the processing of information. It can help users to filter and summarise some information that cannot be determined in the process of using the network, and help technicians deal with and solve problems while helping users to avoid harmful information, thus achieving the purpose of improving the effectiveness of users' work.

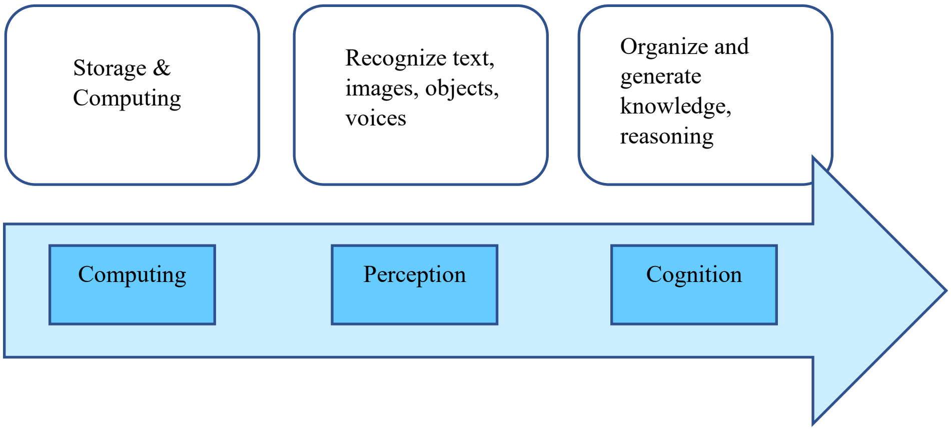

Storage & Computing
Recognize text, images, objects, voices
Organize and generate knowledge, reasoning
Computing
Perception
Cognition

Fig.4 AI Tendency: from perception to cognition

Learnability. AI has the same ability to learn as people, and in many cases, the ability is even better. In the reality of complex networked environmental conditions, with ample information technology resources, it is an in-depth research scientific study to analyze the data that is useful to them between complex levels of data and to integrate and discover the intrinsic connections they are most likely to produce. This requires finding the most valuable information more quickly with the superb machine learning capabilities of AI and developing AI's similar talents to those of humans for processing information. Figure 4 illustrates the development of AI from the perception stage to the cognitive stage, which shows that its efficiency and learning ability has been increasing.

5 THE SECURITY RISKS OF ARTIFICIAL INTELLIGENCE

First of all, from a macro perspective, cybersecurity includes three aspects: physical system security, network system security, and network information security. Physical system security at the physical level is the material foundation and basic guarantee of cyberspace security; network system security at the software level is the basis for ensuring the stable operation of the network environment and computer systems, and the security of user information and data; network information security at the information level is the core pursuit and important guarantee of cybersecurity. Due to the complexity and cascading effect of cyberspace, any security threat in any aspect may have a significant impact on the overall security of cyberspace, which will be more prominent in the era of AI.

Secondly, from a microscopic perspective, there are three hidden dangers in AI at present: framework security, algorithm security, and data security. In terms of framework security, the mainstream AI frameworks, such as CNTK, Torch, Caffe, etc., all have more or less the same security concerns, either heap overflow vulnerabilities or the possibility of system crashes, all of which pose hidden dangers for them to be attacked by the networks. In terms of data security, many of the sample data used for training are collected online, and it is easy for attackers to construct some illegal data and misleading data to implement interference, thus causing overfitting or complete failure of the machine learning model. Figure 5 shows the percentage of domain names tampered within mainland China in 2021, which reflects that there are still many hidden dangers in cybersecurity today.

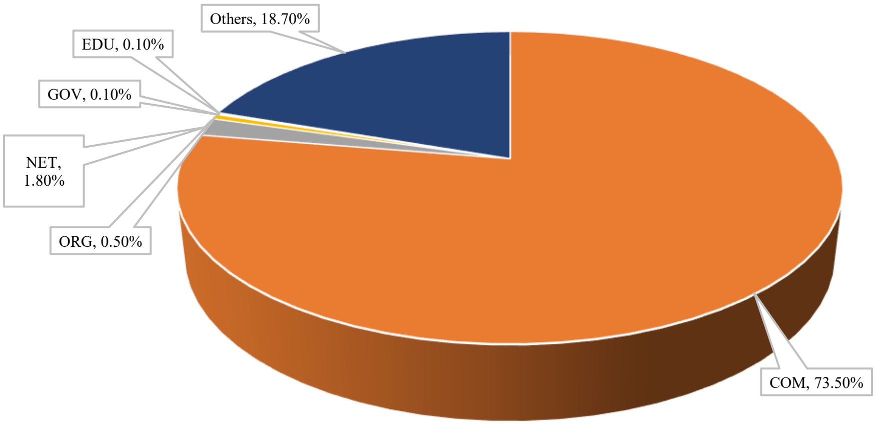


Fig.5 The percentage of domain names tampered with in mainland China in 2021

6 CONCLUSION

For cybersecurity, the application of AI technology can: firstly, rely on artificial intelligence to optimize the network structure, which can further promote the intelligence and fluency of network operation, avoid network failure caused by system factors and other problems at the same time, and provide a strong guarantee for the development of network technology; Secondly, the construction of computer network technology based on artificial intelligence can effectively realize the hierarchy of computer network management. Through the hierarchical division of computer network management modules, the computer network management system can be effectively combed and reorganized to facilitate the communication and exchange between various departments; Thirdly, relying on artificial intelligence technology can improve the efficiency of information retrieval of relevant data, and on this basis improve the fault tolerance rate of computer network data processing, while achieving non-linear network behavior, facilitating the solution of technical problems on computer networks and providing strong support for the development of computer networks. However, AI does also have three hidden risks in terms of framework security, algorithm security, and data security.

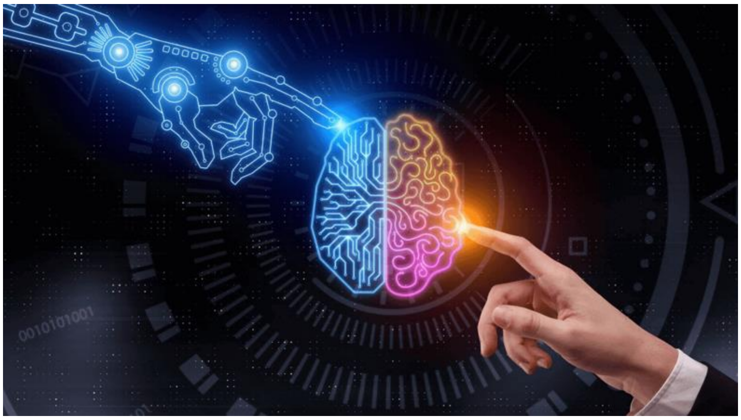


Fig.6 The future of AI is the future or “Metaverse”

M. Kaur and B. Gupta estimate that the market value of “Metaverse” will be as high as $814.2 billion by 2028 [10]. The “Metaverse” is the future of cyberspace, but the key to its realization is to deal with the issue of space security, in which AI will continue to play a vital role. This paper discusses the key role that AI plays in cybersecurity and the advantages and pitfalls of AI, this will help readers understand that AI is a double-edged sword that can bring both convenience and potential risks so that they can exploit its advantages and avoid its risks when using it to maintain cybersecurity in the future.

REFERENCES

[1] Praveen Kumar Donepudi. (2015) Crossing Point of Artificial Intelligence in Cybersecurity. In: American Journal of Trade and Policy, 2.3: 121-128.

[2] Ricardo Calderon. (2019) The Benefits of Artificial Intelligence in Cybersecurity. In: Economic Crime Forensics Capstones. p.36. https://digitalcommons.lasalle.edu/ecf_capstones/36.

[3] Murat Kuzlu, Corinne Fair, and Ozgur Guler. (2021) Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity. In: Discover Internet of things, 1.1: 1-14.

[4] Vishal Dineshkumar Soni. (2020) Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[5] Roman V. Yampolskiy, and M. S. Spellchecker. (2016) Artificial intelligence safety and cybersecurity: A timeline of AI failures. In: arXiv preprint arXiv:1610.07997.

[6] Mariarosaria Taddeo, Tom McCutcheon, and Luciano Floridi. (2019) Trusting Artificial Intelligence in Cybersecurity is a Double-edged Sword. In: Nature Machine Intelligence, 1.12: 557-560.

[7] Lee Byong-Kwon. (2021) The Metaverse World and Our Future. In: Review of Korea Contents Association, 19: 13-17.

[8] https://www.mdpi.com/2673-8392/2/1/31.

[9] https://baike.baidu.com/item/ cyber security/343664?fr=aladdin.

[10] M. Kaur, B. Gupta. (2021) Metaverse Technology and the Current Market. Insights2Techinfo, p.1.