Journal of Computing and Electronic Information Management

ISSN: 2413-1660

On Application of Artificial Intelligence in Information Security

Yukun Li

Guangdong University of Science and Technology, 523083, Dongguan, Guangdong, China

Abstract: With the rapid development of global economy and science and technology, with artificial intelligence, cloud computing, big data, the Internet, the Internet, mobile Internet represented by advanced technology plays a more and more important role in various fields, followed by the frequent Internet security problems, therefore, in the background of the new technology era, how to use artificial intelligence technology to effectively guarantee information security, become a topic must focus on in computer security work. Overall, in 2020, the COVID-19 epidemic hindered the economic development and social operation of countries around the world, and also brought new threats and challenges to global cyberspace security. Security problems such as cyber attacks, data leaks, security vulnerabilities, and video conferencing software risks have undergone new changes under the impact of the epidemic. To this end, countries around the world have strengthened the top-level design of cyberspace, improved policies and regulations, speed up the construction of cyber security institutions and professional forces, promoted data security governance, and taken multiple measures to maintain cyber security.

Keywords: AI; big data; information security.

1. Introduction

According to statistics, the current domestic artificial intelligence has made breakthroughs in many aspects. From iFlytek focusing on a specific task, such as voice recognition and translation, and IFlytek, Baidu, which have been dedicated to artificial intelligence, artificial intelligence has entered a period of high growth from basic research, technology to industry. According to the statistics of the China Society of Electronics, in 2018, the global market size of AI core industries exceeded US $58.03 billion, up 52.3% year on year compared with 2017[1]. Data show that the development of global artificial intelligence presents a tripartite state of China, the United States and Europe. The Chinese government has elevated AI to a national

strategy. In July 2017, The State Council issued the Development Plan for the New Generation of Artificial Intelligence, which clearly pointed out the strategic goal of the new generation of artificial intelligence being divided into three steps. By 2030, China's AI theory, technology and application will generally reach the world's leading level and become the world's main AI innovation center.

China has initially established a national information security organization and security system. The Information Office of the State Council has set up a special leading group for network and information security, and all provinces, cities and autonomous prefectures have also set up corresponding administrative organs. In July 2003, the State Council information leading group passed the opinions on strengthening information security work, in September of the same year, the central general office, the State Council forwarded the national information leading group on strengthening information security opinions, mentioned the information security to promote economic development, maintain social security, ensure national security, strengthen the construction of spiritual civilization, and put forward the "active defense, comprehensive prevention" information security management policy[2]. In July 2003, the National Computer Network Emergency Response Technology Processing and Coordination Center was established, which is specially responsible for collecting, summarizing, verifying and releasing authoritative emergency processing information. International information security management has entered the era of standardization and systematic management. In 1995, the UK pioneered the BS7799 Information Security Management Standard, which was recognized by the International Organization as an International Standard for Standardization ISO /IEC 17799. in 2000 Now the standard has attracted the attention of many countries and regions, and has been popularized and applied in some countries. Organizational implementation of the standard can manage the security system of information security risks, so as to realize organizational information security. Other countries and organizations have also put forward many standards related to information security management. The United States and Europe are at the world's leading level in the research and development and application of artificial intelligence technology. The United States has fully realized the strategic significance of artificial intelligence, has always paid attention to technology research and development in this field, and has stepped up its layout from the national strategic level. Excellent technology research and development institutions and various laboratories in cognitive disciplines have laid a solid technical foundation for the development of artificial intelligence and achieved a large number of remarkable research and development achievements. The United States has released a number of AI plans since 2013, and in 2016, the development of AI has released a number of strategic plans. At an air, sky and online conference held by the

US Defense Department, the US Defense Minister pointed out that the "third offsetting" strategic elements should use the progress of artificial intelligence and independent technology to enable the US military to regain operational advantages and strengthen conventional deterrence[3]. In October 2016, the US National Science and Technology Commission issued two important strategic documents, "Preparing for the Future of Artificial Intelligence" and "National AI Research and Development Strategy Plan", which elevated artificial intelligence to the national strategic level and formulated a grand plan and development blueprint for the development of AI in the United States. The United States, Russia, Japan and other countries have already, or are, working out their own development strategies and plans for information security to ensure that information security develops in the right direction. The highest authority of information security management in the United States is the Homeland Security Bureau. The institutions that share information security management and implementation include the NSA, the FBI, the US Department of Defense, etc. They mainly implement information security work according to the corresponding policies and policies combined with the situation of their own departments. In early 2000, the United States introduced a computer space security program designed to strengthen the defense capabilities of key infrastructure and computer systems networks from threats.In July 2000, the Japan Information Technology Strategy Headquarters and the Information Security Conference formulated the Information Security guidelines. In September 2000, Russia approved the National Information Security Concept, clarifying the measures to protect information security.

2. Impact of Artificial Intelligence on Information Security

1. AI technology can effectively improve the efficiency of information security work. One of the biggest problems security teams today is the fatigue of security alerts. North American businesses receive up to 1,000 security alerts a day. Large ts of malicious attacks drowned in the alarm were not taken seriously. Artificial intelligence uses big data, parallel computing and other technologies to integrate multiple information sources, can quickly comb and process millions of data streams, and generate analysis reports, which helps enterprises and network security companies to obtain accurate security risk assessment reports, and effectively improve the efficiency of network security work.

2. AI technology provides new convenience for hacking. Advances in artificial intelligence technology have also provided new convenience for hackers' cyber attacks. On the one hand, AI technology has uncovered many new vulnerabilities in computer systems that enabling attacks. On the other hand, new applications generated by artificial intelligence technology have become new targets of hacking attacks. At the

Geek Pwn2017 International Security Geek Competition, the White Hat hackers staged a summit showdown with modern technology, including the most popular face recognition, voice print recognition, and the use of bank cards in smart POS machine consumption. The amazing project crack show revealed the security problems of the new applications.

3. AI applications themselves can create new security problems. Take the field of intelligent transportation as an example, with the popularization of driverless cars and intelligent transportation systems, the efficiency of traffic operation is effectively improved, and the probability of traffic accidents is greatly reduced. However, while the existing risks are eliminated, new risks are introduced: hackers can invade the smart car terminals from wireless channels and the background information control system from wired channels, so as to take over the control of driverless cars and even intelligent traffic systems. In fact, driverless cars or intelligent traffic system is composed of complex automatic machines and information systems. Its information collection, transmission and processing are facing security risks. At present, there have been cases of hackers controlling self-driving cars by stealing the mobile App account password.

4. Artificial intelligence brings new challenges to national information security. Artificial intelligence is the "double-edged sword". The development of new technologies and business forms, such as big data, memory computing, blockchain and parallel computing etc. On the one hand, it has improved the level of informatization, and on the other hand, it has also blurred the boundary of national security. Artificial intelligence technology itself has no moral attributes, and the identity, thoughts and motivation of users can not be effectively screened and judged. From the perspective of users, it is completely possible to use artificial intelligence technology to carry out crimes, network fraud, or even terrorist activities. Western countries can integrate global information through Google, Facebook and other network applications, bringing all-round challenges to national information security.

3. Main Advantages of Artificial Intelligence in Field of Information Security

1. Guarantees the data security

Big data analysis and threat identification, to provide security guarantee for big data. The use of artificial intelligence to screen the original fuzzy and non-linear massive data, effectively improve the security detection efficiency and accuracy of big data, and can carry out automated detection.

2. Analyzes the internal and external hidden dangers

Carry out a comprehensive analysis of the internal and external safety risks. Artificial

intelligence can be used to comprehensively analyze the internal and external security risks. The function that can discover, analyze, evaluate and predict various factors that have an impact on information security is an effective way and method to conduct information security analysis, and can provide more accurate security measures. Through the induction, analysis and processing of the corresponding elements, so as to carry out the analysis and prediction of related security situation, and finally the comprehensive analysis of information security elements and situation, but also can make its development momentum effectively predicted, and then build a perfect information security threat situation awareness system.

3. Has built its own defense system

Realize the self-learning emergency response defense system, and build and improve a set of active safety defense system. Today's information security defense needs faster and more accurate capabilities, for upcoming or unknown attacks, with the help of artificial intelligence, and the organic combination of security strategies and threat intelligence, and finally realize intelligent and active security defense measures and strategies. At present, at this stage, the excellent performance of AI in the field of network security defense, such as network intrusion detection, predictive malware defense, network security dynamic perception and other aspects has been demonstrated.

4. Specific Applications of Artificial Antelligence in Field of Information Security

1. Uses artificial intelligence to detect malicious behavior and block attacks. Machine learning algorithms can quickly detect and identify malicious behavior, and block aggression in time, thus eliminating the threat in the bud. British startup Darktrace emerged in the Wannacry ransomware crisis, which infected more than 200,000 users in more than 150 countries. However, the company's machine learning algorithms quickly positioned to capture attacks and took measures to eliminate the threat, and the company's users including even unpatched users did not suffer any damage.

2. Uses AI to analyze mobile terminal security status. Machine learning technology, while already available on mobile devices, has so far largely focused on voice apps such as Google Now, Apple Siri, and Amazon Alexa. Still, Google is using machine learning to analyze threats to mobile terminals to deal with security risks in the result of using personal phones at work. In addition, several companies have also launched their own solutions[4]. MobileIron and Zimperium have announced a partnership plan to jointly provide machine learning-based anti-malware tools for mobile devices. The tool combines MobileIron's security compliance engine with Zimperium's machine learning detection method, can detect multiple threats to devices, networks, and

applications, and will automatically take countermeasures to protect data security according to their security conditions. Wandera also recently released attack detection engine MI:RIAM, that reportedly found more than 400 ransomware and its variants.

3. Uses artificial intelligence to improve information security analysis. With the help of machine learning, the technical level of all aspects of information security can be significantly improved, including malicious attack detection, network analysis, terminal protection, and vulnerability evaluation. In 2016, MIT's Computer Science and Artificial Intelligence Laboratory (CSAL) developed an AI2 system, an adaptive machine learning platform able to help security technicians conduct "seeking a needle in a haystack" -style data filtering to identify real security threats. A combined experiment with CSAL and PatternEx revealed an 85% threat detection rate for the system, along with a five-fold reduction in the false positives rate.

4. Relies on AI to automatically perform repeated security tasks. The real benefit of machine learning is completing repetitive tasks automatically, allowing security personnel to focus on more important work. Machine learning will eventually liberate security personnel from "repetitive, low-value" activities, allowing more time to do more meaningful work.

5. Uses AI to eliminate 0-day vulnerabilities. The researchers want to use machine learning technology to eliminate system vulnerabilities, especially 0-day, and the vulnerabilities that threaten the security of IoT devices. The Arizona State team tried machine learning to monitor traffic from the dark net, hoping to find data using the 0-day vulnerability. In this way, the threat of the 0-day vulnerability can be eliminated in time to prevent key data leakage.

5. Main Problems Facing Artificial Intelligence in Field of Information Security

How to abstraction the security issue. Security problem abstraction refers to the mapping of cyberspace information security problems into a category that can be solved by machine learning. Whether the appropriateness of problem mapping is directly related to the success of machine learning technology to solve cyberspace information security problems or not is [5]. For example, the detection of inferior chip or hardware Trojan, pseudo-base station detection, virtualization security, credit card fraud can be abstract as classification problems; equipment identity authentication, social network abnormal account detection, network intrusion detection can be abstract as clustering problems; user identity authentication, malicious, abnormal, intrusion detection, evidence collection analysis, network public opinion and other problems can be both abstract as classification problems and clustering problems.

How to carry out data pretreatment and feature extraction. In a real network

environment, the data collected may have a large number of missing values, and the noise may also produce anomalous points due to manual input errors, so the data needs to be cleaned and normalized. If a feature has more missing values, the feature is usually discarded, otherwise large noise may affect the effect of the machine learning model. If the missing values are small, you can use fixed value filling, mean filling, median filling, interpolation method, or random number filling methods. Remove the directly if outliers exist. In some security issues, sometimes anomalous or malicious data samples are far less than normal samples, and for such non-equilibrium datasets, oversampled or undersampled methods are often used to construct balanced datasets. After that, the dataset was split and divided into three sets: training set, validation set, and testset. The validation set is mainly used to validate the model and parameter tuning. Commonused dataset segmentation methods have random sampling and cross-validation. Feature extraction refers to the extraction of the most essential characteristics of security problems from data, such as the identification of malicious web pages, web content features, static connection and dynamic web behavior relations. It is difficult to extract features, and deep learning technology is needed.

3. How to conduct model building, model verification, and model effect evaluation. In the machine learning field, datasets are classified into supervised and unsupervised learning based on whether they are tagged, such as marking each piece of data in spam detection as "spam" or "non-spam messages. "In the unsupervised learning, the data does not contain the label information, but the internal association of the data can be inferred through the unsupervised learning algorithms, such as the clustering of friends and thumb up behavior in the detection of social network accounts, so as to find the internal association of the account. In recent years, deep learning has been used to solve anomaly protocol detection, malware detection, and network intrusion detection. In addition, the deep enhancement learning algorithm combining deep learning and enhanced learning can also be applied to the malicious detection [6] of mobile terminals. Selected algorithms and training datasets often face tuning challenges when using selected datasets for model training. Model validation mainly adopts K x cross-validation method, which divides the data preprocessing into k similar sized and mutually exclusive subsets, each subset keeps the data distribution as consistent as possible, and then uses the subset as the training set to obtain the k training and validation test, the final result is the mean of the k validation test results. In the security field, there are accuracy rate, accuracy rate and recall rate, which is the proportion of correctly classified normal samples and the number of malicious samples to the total number of samples. Warrant (accuracy) is the proportion of the number of correctly identified normal samples identified as normal, and recall (recall)

is the proportion of the sum of the correctly identified and the correctly identified and misidentified malicious samples (simply the correctly identified normal samples).

6. Conclusion

With the development of science and technology, artificial intelligence has been gradually applied to people's life and production, and people also pay more and more attention to the security of information, which will not only affect the national ideology, financial environment and political atmosphere, but also affect people's lives. Artificial intelligence era, the national level should vigorously support and develop the application of artificial intelligence in the field of security, at the same time, we must realize the importance of computing information security and protection, and according to the actual situation and need to take timely measures to prevent and solve, actively use artificial intelligence for security, improve the security of all walks of life, but also realize the rapid development of our society, promote the progress of human society.

Acknowledgements

Fund project: This paper is the phased outcome of 2021 Guangdong University of Science and Technology in China: The Application Research of Artificial Intelligence in Information Security (GKY-2021KYYBK-30).

References

[1] Zheng Jianhua. On artificial intelligence [J]. China Information Security, 2018,101 (05): 62-63.

[2] Xingcong. Network Information Security and Prevention Analysis -- thinking on Facebook information leakage events [J]. Modern Information Technology, 2018,2 (07): 172-173.

[3], Deng Wenbing. Challenges and Countermeasures of Information Security Supervision in the era of Artificial Intelligence [J]. Information Security in China, 2018,106 (10): 108-110.

[4] Marx Cheung. Information security in the era of AI [J]. Electronic Technology and Software Engineering, 2019 (02).

[5] Xu Tao, Chen Yuling. Research on Computer Network Security and Protection in the Background of Big Data [J]. Information and Computer (theoretical version), 2020,32 (3): 182-184.

[6] Qin Cheng, Bin He Yu. Computer network information security prevention in the era of artificial intelligence [J]. Electronic Technology and Software Engineering, 2020 (3): 255-256.