Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-6, Issue-8, August 2024
DOI: 10.53469/jrse.2024.06(08).11

Analysis of the Current Status of Patent for AI in Network Security Protection

Xiaoyi Xiao

Patent Examination Cooperation Sichuan Center of the Patent Office, Chengdu, Sichuan, 610213, China

Abstract: ***With the rapid development of information technology, the forms of cyber attacks have changed, making network security problems increasingly prominent. Artificial intelligence can better respond to threats by continuously learning from large amounts of data and making predictions and judgments. Applying artificial intelligence to network security protection is currently a hot research topic. This paper analyzes the application of artificial intelligence in network security protection from the perspective of patents. Based on the patent data retrieved, it analyzes the situation from multiple dimensions such as the overall situation of patents, the ranking of applicants, and the distribution of technologies, and provides corresponding suggestions based on the results to provide reference for innovative entities in related fields.***

Keywords: AI, Machine learning, Network security, Network attacks, Patent analysis**.**

1. Introduction

In recent years, the Internet has become increasingly popular, and computer networks have become an indispensable part of people's work and life. However, with the rapid development of network technology, network security issues have become increasingly severe. Artificial intelligence technology has been a research hotspot in recent years, with powerful data processing, self-learning, and predictive capabilities [1]. It can dynamically provide corresponding defense strategies for the emerging new network security issues. Based on artificial intelligence, efficient network defense tools can be implemented to identify malicious software attacks, network intrusions, phishing and spam emails, data breaches, etc. The patent map analyzes the bibliographic items and technical solutions in a large number of retrieved patent documents, extracts, screens, organizes, and summarizes relevant information to obtain patent information, and uses visual charts to describe patent information [3]. This paper uses the patent map to analyze the patent status of artificial intelligence applied to network security protection from a patent perspective.

2. Data Source

The paper data comes from the commercial database incoPat Global Patent Comprehensive Literature Database, which specially collects and processes patent data from commonly used countries, and provides corresponding translated texts. The data information is complete and easy to read and retrieve. The paper searched for patents in the field of artificial intelligence network security in the incoPat database using classification numbers and keywords, and obtained 8842 patents on June 27, 2024. To ensure the accuracy and effectiveness of the data, preliminary denoising was performed on the retrieved data using classification numbers, followed by further cleaning through manual screening. After merging with the same family, 5829 valid patents were finally obtained. This paper analyzes the data as the research object.

3. Analysis of the Overall Situation of Patents

3.1 Analysis of Application Trends

Firstly, an analysis of the application volume of artificial intelligence network security over the years will be conducted. As patent applications in this field have only been filed in China since 2005, and prior to this, relevant patents in other countries were only in single digits, only the global and Chinese patent application situation from 2005 to 2024 will be presented here, as shown in Figure 1. From Figure 1, it can be seen that the development of artificial intelligence network security can be divided into three periods. The period from 2005 to 2012 was the embryonic stage of technology, with a small number of patent applications per year. The period from 2012 to 2018 was a slow growth period, with the number of patent applications gradually increasing each year. From 2018 to present, it is a rapid growth period, with an explosive increase in the number of patent applications per year. The decrease in the number of patent applications in 2024 is due to the fact that only over half of the year was searched and some patents were not made public, and they are still in a period of rapid growth. In addition, although China started relatively late compared to foreign countries, its development speed is significantly faster. Since 2019, China's application volume has exceeded half of the global application volume, and by 2023, it has accounted for nearly 70% of the global application volume, and this proportion is still increasing year by year. It can be seen that China is developing rapidly in the field of artificial intelligence network security, accounting for the majority of the global market.

Figure 1: Trends in Artificial Intelligence Network Security Applications

3.2 Regional Layout Analysis

In the regional layout distribution, the main analysis is the global regional ranking, which can display the distribution of the number of patents for artificial intelligence network security in various countries or regions. Through this analysis, the activity level of technological innovation in artificial intelligence network security in different regions can be understood, as well as the main sources and markets of technological innovation. The distribution of AI network security patents in various countries is shown in Figure 2. From the graph, it can be seen that the number of patent applications published in China is far ahead, reaching 3236, more than twice that of the second ranked United States and nearly six times that of the third ranked India. This shows that artificial intelligence network security technology is very active in China. As the country of origin of artificial intelligence, the United States also has a considerable number of patents, reaching 1285. The essence of artificial intelligence is computer programs, so India, a software powerhouse in history, also has a considerable number of patents in this area, reaching 541. In addition, South Korea and the European Patent Office also have a certain number of patents, while the number of patents in other countries is relatively small.

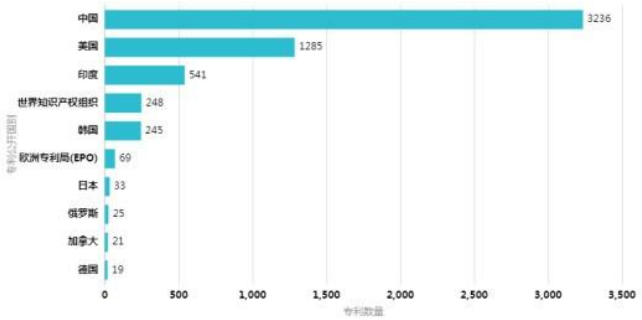

Figure 2: Distribution of AI network security patents in various countries

4. Applicant Analysis

4.1 Analysis of Applicant Ranking

The paper summarizes the top ten applicants in terms of application volume, as shown in Figure 3. From the graph, it can be seen that China accounts for 6 out of the top ten applicants, while foreign countries account for 4. Among them, CHITKARA University and BLUEST METTLE SOLUTIONS PRIMATE LIMITED, ranked first and second respectively, are Indian companies, while CISCO TECHNOLOGY INC, ranked third, and CYLANCE INC, ranked seventh, are American companies. The top three applicants belong to the first tier, with significantly higher application volumes than other applicants, while the number of other applicants is not significantly different. Based on Figure 2, it can be concluded that although China has a large total number of applications, there is not much difference among the applicants, and no applicant has entered the first tier, lacking super large leading enterprises. In addition, five out of the six seats in China are held by universities, indicating that universities are the main force in this field and have invested a lot of research in this area.

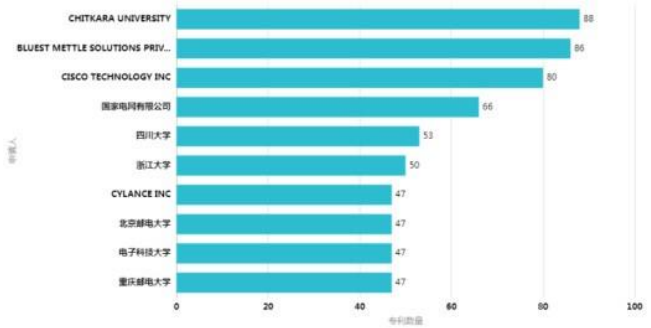

Figure 3: Top Ten Patent Applications for Artificial Intelligence Network Security

4.2 Analysis of Applicant Types

The paper also specifically counted the types of applicants for Chinese patent applications in the field of artificial intelligence network security, as shown in Figure 4. From the graph, it can be seen that universities and enterprises are the main innovative entities in this field. According to the number of applications, universities account for more than half, enterprises account for 46.76%, while the remaining types account for only 9.28% in total. It should be noted that since an application may involve multiple applicants, it may correspond to multiple applicant types. Therefore, the total proportion of each type may exceed 100%, and a similar situation may also occur in the technical distribution section 5 of the paper. The high proportion of universities indicates that this field tends to focus on basic research, possibly because artificial intelligence mainly uses computers to implement complex training algorithms with strong theoretical basis and low cost, mainly in terms of computing equipment cost. These aspects are the advantages of universities and facilitate scientific research.

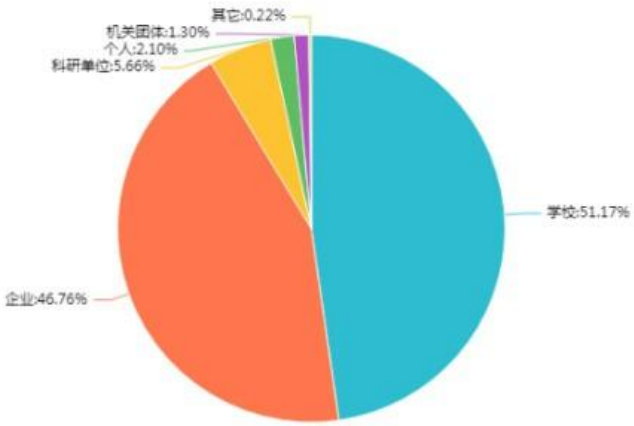

Figure 4: Types of Chinese Patent Applicants for Artificial Intelligence Network Security

5. Technical Analysis

5.1 Technical Distribution Analysis

Analyzing the distribution of patents in the field of artificial intelligence network security across various technological directions can provide insights into the types of technologies involved and the level of innovation in each branch of technology. Due to the imprecise classification of subcategories, we have chosen to study the distribution of patent technologies in the field of artificial intelligence network security through a large group classification, as

shown in Figure 5.

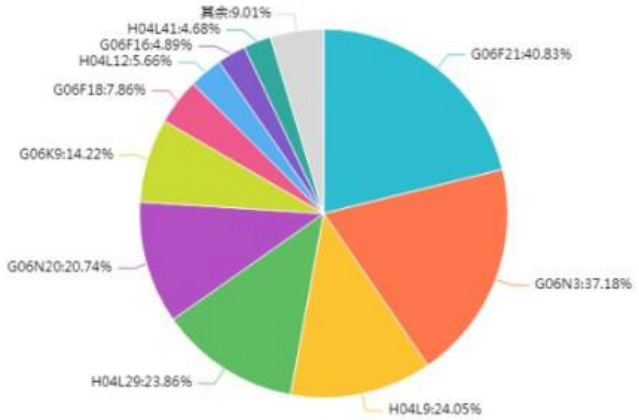

Figure 5: Distribution of Artificial Intelligence Network Security Patent Technologies

From the graph, it can be seen that G06F21 (a security device that protects computers, their components, programs, or data from unauthorized behavior) has the highest distribution. Patents in this field account for 40.83% of all patents, and it involves network security, which happens to be the focus of our research. Next is G06N3 (computational arrangement based on biological models), accounting for 37.18%. Computational arrangement based on biological models actually simulates human thinking through computer models, which is essentially artificial intelligence. In addition, artificial intelligence network security technologies are also widely distributed in H04L9 (confidential or secure communication devices; network security protocols), H04L29 (devices, circuits, and systems not included in individual groups H04L1/00 to H04L27/00), G06N20 (machine learning), and G06K9 (methods or devices for recognizing patterns), accounting for 24.05%, 23.86%, 20.74%, and 14.22%, respectively.

5.2 Key Representative Patent Analysis

The more times a patent is cited and the more it belongs to the same family, the more likely it is to be a core key patent. In addition, the shared value provided by icoPat can also serve as a reference for whether it is a key patent. The paper comprehensively considers these factors and selects some key patents to analyze their patent technology.

The patent of Sourcefire (US20120210423A1) discloses a method and apparatus for detecting malicious software through context information, class signatures, and machine learning techniques, which specifically includes extracting feature vectors from software applications; Extract metadata about the application and collect contextual information about the installation of the application in the system; Calculate the universal fingerprint of the application program; Send the data related information obtained based on the above results to the server application program; Based at least in part on the information sent above, receive information from the server application about whether the application is benign or malicious; And take actions on the application based on the information received from the server component. This technology can reduce the workload of manual analysis and the risk of false positives in the system, making it possible to achieve this through the use of automated means. Microsoft's patent (US20120158626A1) discloses a method for detecting and classifying malicious URLs, which utilizes features extracted from URLs to detect malicious URLs and classify them as phishing URLs, spam URLs, malware URLs, or one of multiple types of attack URLs. The technology uses one or more machine learning algorithms to train a classification model using a set of training data, which includes known benign URL groups and known malicious URL groups. Then use a classification model to detect and/or classify malicious URLs.

The patent of State Grid Corporation of China (CN107196910A) discloses a threat warning and monitoring system, method, and deployment architecture based on big data analysis, including a data acquisition system module for real-time data acquisition of raw network traffic; The data storage system module consolidates and cleans the data collected by the data collection system module before storing and managing it; The real-time threat intelligent analysis system module utilizes data mining, text analysis, traffic analysis, full-text search engines, and real-time processing to conduct in-depth analysis and mining of security data. It combines intrusion detection models, network abnormal behavior models, and device abnormal behavior models to identify unknown security threats in real time; The situational awareness display system module adopts a data visualization tool library to comprehensively display the security threat situation in real time and three dimensions. Used for network security threat situational awareness and in-depth analysis in various business scenarios, achieving comprehensive capabilities from attack warning, attack identification to analysis and evidence collection. The patent (CN104935600A) of the 54th Research Institute of China Electronics Technology Group Corporation discloses a mobile self-organizing network intrusion detection method and device based on deep learning. Including data collection module, data fusion module, preprocessing module, storage module, intrusion detection module, and response alarm module, the captured wireless data packets are fused and deduplicated to extract network behavior characteristics and stored; Establish a deep neural network model that expresses network behavior based on the behavioral characteristics of deep learning networks; Input the network data to be detected into a deep neural network model, complete the judgment and recognition of intrusion, and respond to alarms.

6. Conclusion

The paper analyzes the patent status of artificial intelligence applied to network security protection from the perspective of patents. From the above analysis, it can be seen that China has a significant advantage in patent applications in the field of artificial intelligence security, but has not formed a super large leading enterprise, and there is still a certain gap with foreign enterprises. Currently, research is mainly conducted in universities, and there are relatively few enterprises with large patent reserves. The following suggestions are proposed: firstly, the government should further strengthen policy guidance, cultivate and strengthen a group of world leading enterprises in the field of artificial intelligence network security, strengthen the construction of circles and chains, and form a full chain industry; Secondly, we need to seize the development opportunities of the current rapid growth period

in the industry, strengthen our overseas patent layout, and lay a solid foundation for entering foreign markets; The third is to strengthen the integration of industry, academia and research, improve the transformation and application of patents, and promote the achievements of university patents to the market.

References

[1] Pi Xun, Wu Lisheng. Design of Network Security Defense System Based on Artificial Intelligence Technology [J]. Wireless Internet Technology, 2023, 20 (18): 25-27.

[2] Wang Yueqiang, Zhang Lei, Chen Xinlei, et al. Research on the Application of Artificial Intelligence Technology in Network Security Defense [J]. Network Security Technology and Application, 2024 (6): 26-29.

[3] Jiang Yushi, Kang Yuhang. Research on Visualization of Technological Innovation Based on Patent Maps [J]. Research Management, 2013, 34 (10): 50-57.

[4] Ji, H., Xu, X., Su, G., Wang, J., & Wang, Y. (2024). Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertising. Academic Journal of Science and Technology, 9(2), 215-220.

[5] Ma, Y., Shen, Z., & Shen, J. (2024). Cloud Computing and Hyperscale Data Centers: A Comparative Study of Usage Patterns. Journal of Theory and Practice of Engineering Science, 4(06), 11-19.

[6] Ren, Z. (2024). VGCN: An Enhanced Graph Convolutional Network Model for Text Classification. Journal of Industrial Engineering and Applied Science, 2(4), 110-115.

[7] Ren, Z. (2024). Enhanced YOLOv8 Infrared Image Object Detection Method with SPD Module. Journal of Theory and Practice in Engineering and Technology, 1(2), 1 – 7. Retrieved from https://woodyinternational.com/index.php/jtpet/article/view/42

[8] Yuan, B., & Song, T. (2023, November). Structural Resilience and Connectivity of the IPv6 Internet: An AS-level Topology Examination. In Proceedings of the 4th International Conference on Artificial Intelligence and Computer Engineering (pp. 853-856).

[9] Yuan, B., Song, T., & Yao, J. (2024, January). Identification of important nodes in the information propagation network based on the artificial intelligence method. In 2024 4th International Conference on Consumer Electronics and Computer Engineering (ICCECE) (pp. 11-14). IEEE.

[10] Yuan, B. (2024). Design of an Intelligent Dialogue System Based on Natural Language Processing. Journal of Theory and Practice of Engineering Science, 4(01), 72-78.

[11] Yao, J., & Yuan, B. (2024). Research on the Application and Optimization Strategies of Deep Learning in Large Language Models. Journal of Theory and Practice of Engineering Science, 4(05), 88-94.

[12] Yao, J., & Yuan, B. (2024). Optimization Strategies for Deep Learning Models in Natural Language Processing. Journal of Theory and Practice of Engineering Science, 4(05), 80-87.

[13] Wang, Z. (2024, August). CausalBench: A Comprehensive Benchmark for Evaluating Causal Reasoning Capabilities of Large Language Models. In Proceedings of the 10th SIGHAN Workshop on Chinese Language Processing (SIGHAN-10) (pp. 143-151).

[14] Lyu, H., Wang, Z., & Babakhani, A. (2020). A UHF/UWB hybrid RFID tag with a 51-m energy-harvesting sensitivity for remote vital-sign monitoring. IEEE transactions on microwave theory and techniques, 68(11), 4886-4895.

[15] Lu, Q., Guo, X., Yang, H., Wu, Z., & Mao, C. (2024). Research on Adaptive Algorithm Recommendation System Based on Parallel Data Mining Platform. Advances in Computer, Signals and Systems, 8(5), 23-33.

[16] Wu, X., Wu, Y., Li, X., Ye, Z., Gu, X., Wu, Z., & Yang, Y. (2024). Application of adaptive machine learning systems in heterogeneous data environments. Global Academic Frontiers, 2(3), 37-50.

Author Profile

Xiaoyi Xiao (1990-), male, from Ziyang, Sichuan, China, holds a master's degree and is an assistant researcher engaged in research on network communication and wireless communication.