ISSN 2181-3187

DYNAMIC FILTERING METHODS IN INFORMATION COMMUNICATION SYSTEMS

Raxmanqulova Mashhura Ruziboyevna
Assistant teacher of "Information security"department, Urganch branch of Tashkent University ofInformation Technologies named after Al-Kharazmi Khorezm, Urgench, mraxmanqulova@mail.ru

Annotation. In the context of Information Communication Systems (ICS), dynamic filtering rules represent a flexible and flexible approach to filtering incoming and outgoing data. In this article, you can get answers to questions about dynamic filtering methods, their configuration and development, the main features of dynamic filtering rules, what role dynamic filtering plays as an important protector of efficiency and security. Information has also been cited on current examples of dynamic filtering.

Keywords: Encryption, decryption, cyber attacks, vulnerabilities, hackers, dynamic filtering, filtering methods.

ICSda offers a strong and flexible approach to data filtering that provides more efficient and flexible security, content management, and personalization solutions.Controlling the flow of information and striving to protect systems from damage has long been the impetus for the development of filtering methods. While the filtering concept itself has existed for centuries, dynamic filtering rules represent a relatively recent section of this interesting story with the ability to adapt and learn.Early filters relied on static, hand-coded rules to offer limited flexibility and struggled to adapt to evolving threats and user needs. With the growth of email and web content, the main focus has shifted to the analysis of real data on packages. Keyword-based rules and pattern matching methods have become commonplace, allowing content-based filtering of spam, malware, and inappropriate content. While offering more subtle control, these static rules did not have the dynamism to control the ever-changing digital landscape.

The era of artificial intelligence (AI) further enhanced the capabilities of dynamic filtering rules. Deep learning algorithms, big data analysis and self-learning mechanisms have opened up new paths for:

1.High precision threat detection: AI models can analyze complex data structures and detect subtle anomalies, leading to more accurate and efficient filtering.

2. Large-scale personalized experiences: Advanced recommendation systems can take into account a wide range of user information that offers personalized content and services with an unprecedented delicacy.

ISSN 2181-3187

3. Flexible security solutions:Security systems can improve protection against constantly evolving cyberattacks, ahead of even the most complex threats.

Unlike static rules, which remain expressed and predetermined, dynamic rules can be adjusted and developed depending on various factors, including:

Real-time data analysis: they are in real-time

they can analyze incoming data flows, identify patterns, anomalies, and potential threats based on changing criteria.

Machine learning algorithms: machine learning algorithms

integration with dynamic rules allows you to learn and adapt over time, they become more accurate and more efficient when processing more data.

External sources of information: they update and filter the criteria

it can use external sources such as Threat Intelligence, Security databases, and user feedback to improve its decisions.

Key features of dynamic filtering rules:

Flexibility: they give new threats, developing can adapt to trends and changes in user behavior.

Granularity: they are certain types of data based on different parameters or it can be fine-tuned to target content .

Accuracy: they learn from flexible nature and data due to their ability, they can achieve higher accuracy than static rules.

Complexity: implementation and management of dynamic rules / static it can be more complicated than rules, which require experience in data analysis, machine learning and system management.

Application of dynamic filtering rules in ICS:

Spam detection: identify and filter spam letters and other unwanted messages in real time.

Malware and attack detection: detection and blocking of malware and network attacks based on behavioral analysis and threat data.

Content filtering: implementing organizational policies and user preferences by filtering unwanted content such as pornography, violence, or hate speech.

Personalization: providing personalized content and recommendations based on personal preferences and activities of users.

Examples of dynamic filtering rules:

Electronic identified by threat intelligence as spam sources

a rule that blocks postal addresses.The network traffic, which shows the behavior characteristic of the Botnet activity of the clock

determining rule. News based on the user's reading history and interests

rule recommending their articles. Now let's think about the future of dynamic filtering. The evolution of dynamic filtering rules is not over yet . Continued advances

ISSN 2181-3187

in artificial intelligence, data science and distributed computing offer excellent opportunities for the future:

Context-aware filtering: taking into account factors such as user location, time of day, and social context for more specific and relevant filtering decisions.

Explanatory AI: strengthening trust and transparency by allowing users to understand how dynamic filtering rules make decisions.

Federal Education: joint improvement of filtering models across different systems without compromising user privacy or security.

In general, the rules of dynamic filtering have gone a long way, from simple static walls to flexible solutions based on artificial intelligence. This journey reflects our constant search for control and security in the ever-evolving digital world. One thing remains clear as technology progresses: the dynamic dance between filtering and evolving information continues to shape the future of our online experiences. In the rapidly developing world of Information Communication Systems (ICS), where information flows continuously and threats are hidden in every corner, dynamic filtering occupies a central place as an important defender of efficiency and security.

References:

1.“Dynamic Packet Filter: An Efficient Mechanism for Network Security”/H. Adrichem, J. Jansen, and H. Sips.//International Conference on Computational Science and Its Applications (ICCSA), 2005.

2.“Dynamic Filter Chains for Flexible Network Security Policies”/A. Belenky and N. Ansari//IEEE Transactions on Dependable and Secure Computing, 2010.

3.”Dynamic Spectrum Access in Cognitive Radio Networks: A Survey”/Authors: I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty//IEEE Communications Magazine, 2011.

4.”Dynamic Filter Banks for Adaptive Time-Frequency Analysis”/L. Cohen, R. A. Gopinath, and S. Zahorian// IEEE Transactions on Signal Processing, 1995.

5.Dynamic Spectrum Management in Cognitive Radio Networks: A Comprehensive Survey"/ I. F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty//IEEE Communications Surveys & Tutorials, 2011.

6.”Dynamic Filters for Cooperative Spectrum Sensing in Cognitive Radio Networks”/Y. Zeng, Y.-C. Liang, and B. Li//IEEE Transactions on Wireless Communications, 2010.

7.”Dynamic Spectrum Access in Wireless Networks: A Survey”/Q. Zhao, L. Tong, A. Swami, and Y. Chen//IEEE Signal Processing Magazine, 2007.

8. “Dynamic Packet Filter: A Simple and Efficient Firewall”/B. Yener and K. Anwar//IEEE Transactions on Computers, 2003.