Enhancing Network Security Through Router-Based Firewalls: An Investigation into Design, Effectiveness, and Human Factors

Jingqing Liu *

College of Engineering, University of Delaware, Newark, 19716, United States of America

* Corresponding Author Email: jingqing@udel.edu

Abstract. A firewall serves as a crucial computer program designed to block malicious software, thereby safeguarding the user's system. It helps prevent the unauthorized dissemination of personal information and the incursion of harmful viruses. Taking inspiration from China's "Great Firewall"—a sophisticated system utilizing advanced software and hardware to automatically filter, censor, and monitor internet content—this research aims to devise a router-based firewall system capable of autonomously shielding users' computers from viruses and unauthorized websites. A comprehensive questionnaire was deployed to unearth the predominant sources of information leakage among computer users and ascertain the role of firewalls within computer systems. The analytical findings underscore that the majority of information leakage security risks stem from a significant lack of personal privacy awareness and a deficient understanding of firewall security systems. The proposed firewall system harnesses router-based control to address the limitations inherent in PC software-based firmware systems. This innovation enhances the control of viral threats and the prevention of user privacy leaks. Serving as a tangible barrier, the router-based firewall obstructs the route of viruses or malevolent programs before reaching the user's computer. This strategic design substantially reduces user intervention, ensuring the continuous operation of the firewall to steadfastly protect the user's computing environment.

Keywords: Firewalls, Router-based Firewalls, Firewalls, Information Leakage, Virus Control, Network Security.

1. Introduction

In the era of the internet, ensuring security is of utmost importance. With the ever-evolving landscape of cyber threats, the necessity for robust security measures has become glaringly evident. Serving as the initial barrier against malicious intrusions, firewalls assume a pivotal role in safeguarding information. This report delves into the intricacies of firewall design, with a particular emphasis on a router-centric approach complemented by cloud-integrated capabilities. A deeper comprehension of the feasibility of router-centric cloud firewalls for network security can be attained by examining the diverse components and policies integrated into firewall design.

2. Relevant Theories

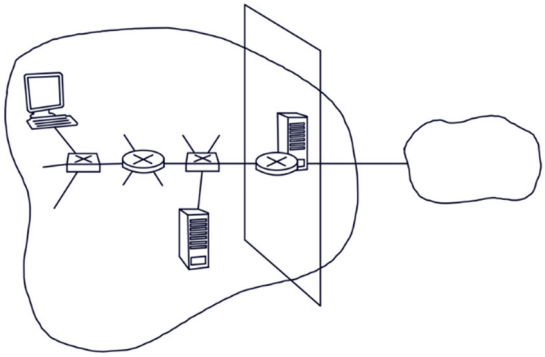


Figure 1. Firewall Placement between the Administered Network and the Outside World (Photo/Picture credit: Original).

From Computer Networking: A top-down approach: “A firewall is a combination of hardware and software that isolates an organization ‘s internal network from the entire Internet, allowing some packets to pass and blocking others.” (Kurose & Ross, 2022) A firewall is the first gate to network security. It is vital to keep it researched and updated [1]. As shown in Figure 1.

3. Design Reference

3.1. A tool for countries to block information or maintain politics

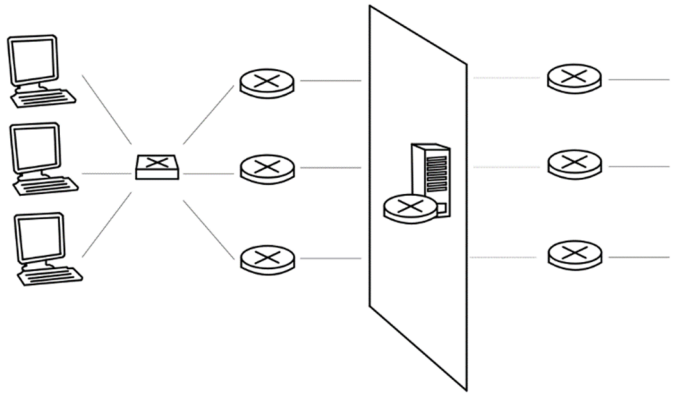


Figure 2. The Great Firewall Placement (Photo/Picture credit: Original).

The Great Firewall generally refers to the combined use of hardware devices such as routers and software applications to monitor, filter, and restrict Internet content within China [2]. As shown in Figure 2.

3.2. Software and Hardware of GFW

Software: China's Great Firewall (GFW) uses a multifaceted software approach to monitor Internet traffic. One of its main tools is Deep Packet Inspection (DPI), which detects and blocks specific keywords, websites, and services by scrutinizing the content of Internet traffic. In addition, GFW has a DNS blocking and redirection mechanism that enables it to block DNS lookup requests and block or redirect access to selected foreign websites [3]. GFW maintains a blacklisting system that prevents access to specific IP addresses and URLs to further extend its reach. If a user attempts to access restricted content, GFW can passively detect and block fully encrypted traffic in real time [4].

Hardware: The infrastructure behind China's Great Firewall (GFW) is large and complex, equipped with powerful hardware to manage China's massive Internet traffic [5]. Behind the GFW, some high-capacity routers and switches are essential for managing and directing large data traffic in large-scale networks to ensure efficient, uninterrupted data flow. (Kurose & Ross, 2022) Deploy probes at strategic points within the network to collect traffic pattern data and monitor traffic in real-time to help analyze and optimize the network [6].

3.2.1. Comparison with firewalls in other countries

The GFW is one of the best-known national firewalls, but many countries implement similar systems. For example, Russia aims to create a national Internet infrastructure that gives the government control over Internet exchange points. Like GFW, Russia has been making a concerted effort to create a sovereign Internet, taking steps to control Internet exchange points and introducing Deep Packet Inspection (DPI) for monitoring. Russia's DNS system and Internet traffic should be routed domestically to minimize reliance on foreign infrastructure [7].

3.3. Challenges in Design

Designing a firewall system, especially one on the scale of GFW, presents several challenges, including the need for the system to handle large volumes of traffic while causing minimal latency, adapting to evolving users and technologies, and instantly updating in a way that bypasses censorship.

4. Data Analysis

4.1. Data Breach Investigations Report 2022 (DBIR)



Figure 3. Percentage of Human Factors (Photo/Picture credit: Original).

The Data Breach Investigations Report (DBIR) for 2022 provides valuable insights into the factors contributing to security breaches. A standout observation from this year's report is the predominant role of human actions in these breaches. Specifically, 82% of the reported breaches were found to have a human element involved [8], underscoring the critical role of human behavior in cybersecurity. As shown in Figure 3.

Despite all the advanced security tools and policies, misconfiguration is still a major security risk, causing 13% of all breaches, as shown in DBIR 2022 [9]. Misconfiguration is usually caused by negligence, lack of expertise, or over-reliance on default settings, representing the human factor as an important factor in cybersecurity pitfalls. As shown in Figure 4.

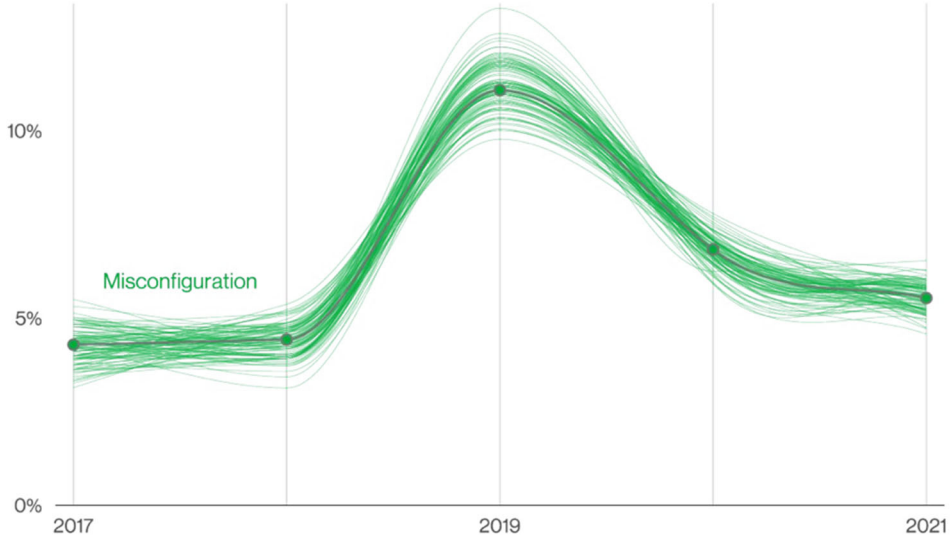


Figure 4. Misconfiguration over time in breaches from DBIR 2022 (Photo/Picture credit: Original).

4.2. Results from the Questionnaire

4.2.1. Questionnaire. Q1 What computer operating system are you using?

Q2 Which of the following methods do you usually use to download computer applications?

Q3 What do you think is the main reason for the leakage of personal information in the network?

Q4 Do you read the User Information Protection and Liability Policy before registering on an unfamiliar website or downloading software?

Q5 When using the computer, have you ever done the following?

Q6 Can you identify phishing websites?

Q7 Do you have a Firewall on your computer?

Q8 Do you keep your computer's firewall open?

Q9 Do you know the brand of your computer firewall?

Q10 What is the brand of your computer's firewall?

4.2.2. Analysis of the Questionnaire

1) When using the computer, have you ever done the following?

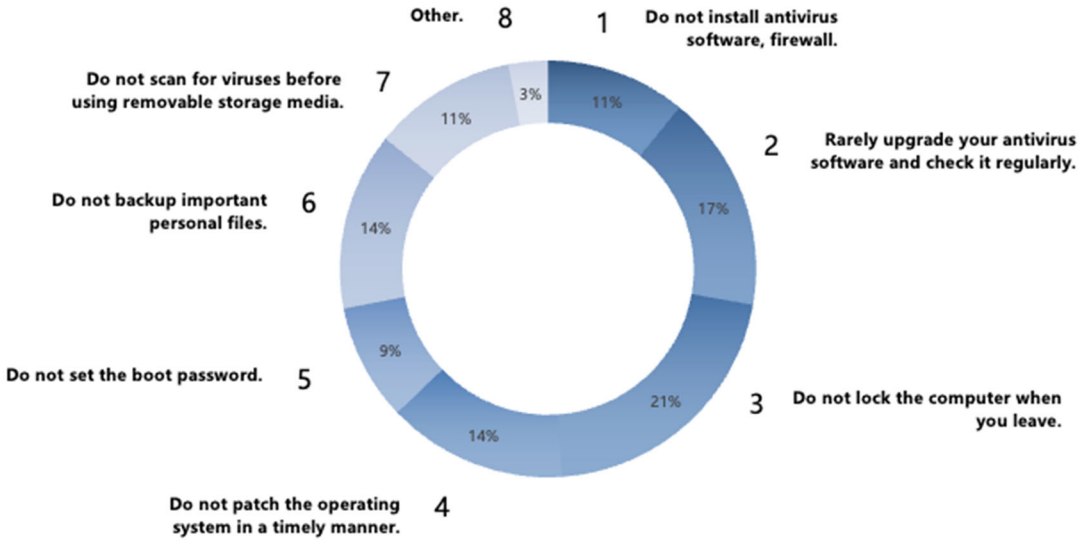


Figure 5. Percentage of Question "When using the computer, have you ever done the following?" (Photo/Picture credit: Original).

A survey was conducted to investigate the factors contributing to potential data breaches. The sample consisted of 300 individuals. Alarmingly, all respondents, representing 100% of the sample, admitted to actions or initiatives that could potentially lead to a data breach. This unanimous response further emphasizes the human factor's significance in data security. As shown in Figure 5.

2) Do you have a Firewall on your computer?

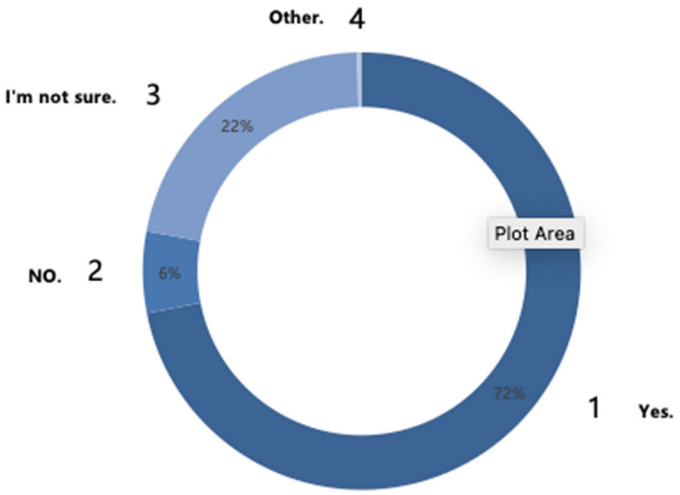


Figure 6. Percentage of Question "Do you have a Firewall on your computer?" (Photo/Picture credit: Original).

As shown in Figure 6. The survey revealed the current attitude of Internet users towards Internet security, with 72% of respondents having a firewall installed on their computers, indicating a strong awareness of Internet security. However, 6% of respondents confirmed that they do not have a firewall installed, indicating potential vulnerabilities. Alarmingly, 22% of respondents needed clarification on the status of their firewall, highlighting a significant knowledge gap. This uncertainty highlights the need for increased cybersecurity education and at the same time demonstrates that the human factor is one of the causes of cybersecurity risks.

3) Do you keep your computer's firewall open?

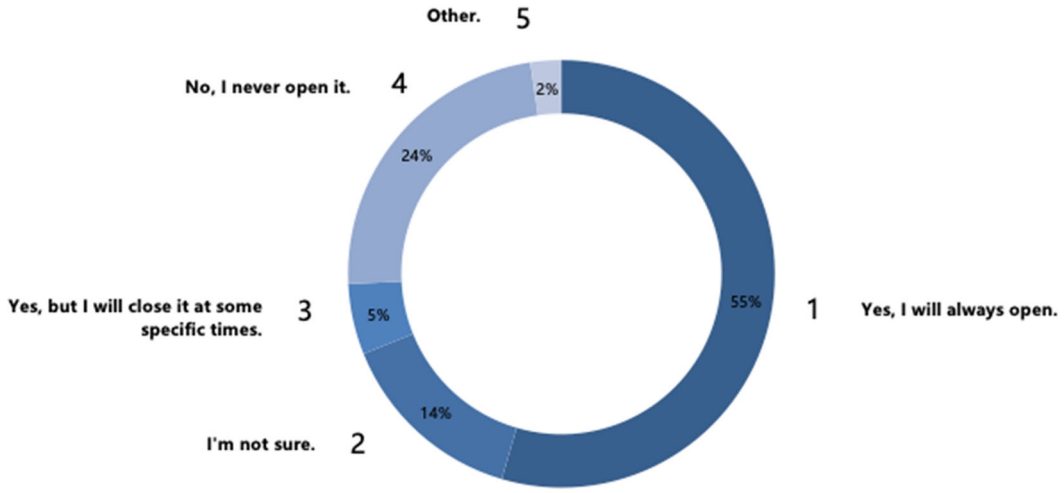


Figure 7. Percentage of Question "Do you keep your computer's firewall open?" (Photo/Picture credit: Original).

As shown in Figure 7. The results of the survey reveal users' habits regarding the use of computer firewalls. 55% of respondents always keep their firewalls turned on, indicating they place a high value on cybersecurity. However, 24% of users never enable their firewalls, which is a worrying percentage as they may be exposed to various cyber threats. Additionally, 5% of users turn off their firewalls in specific contexts, possibly because it is required for certain operations, but this could pose a security risk. It is concerning that 14% of the respondent's needed clarification about the status of their firewalls. This indicates that the basics of cyber security still need to be improved among some users. It can be seen that the human factor is one of the main causes of network security risks.

4.2.3. Analysis Conclusion

The human element has a significant impact on the security of computers.

Compared to software firewalls, Hardware Firewall minimizes user involvement and keeps the firewall running to protect the user's computer and prevent personal information leakage.

5. Proposed Firewall Design

5.1. Overview

A firewall connected to the cloud database filters and monitors data transmitted through the router, and synchronized updates between the router and the cloud database prevent new viruses from appearing and block them promptly. As shown in Figure 8.

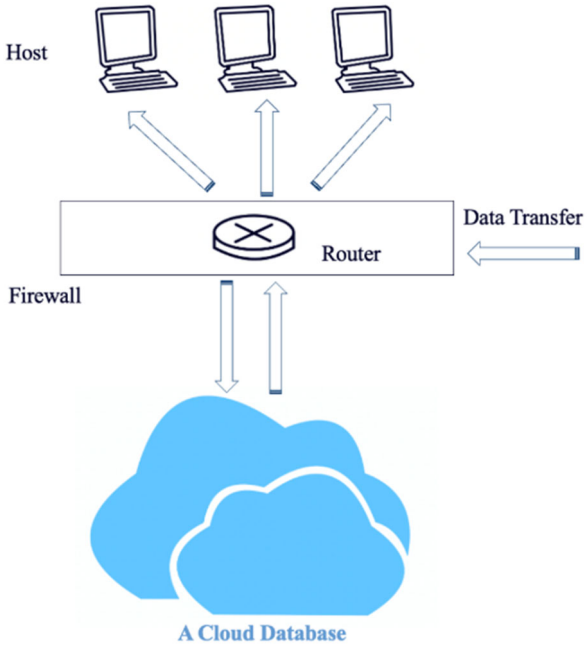


Figure 8. Firewall design placement for connecting to cloud databases (Photo/Picture credit: Original).

5.2. Cloud Integration

5.2.1. Real-time monitoring and advanced filtering

Cloud computing capabilities allow algorithms to process large amounts of data almost instantaneously [10]. This fast processing ensures that any malicious packets are identified and dealt with before they can cause harm. In the case of a large influx of data, the power ensures that latency is minimized, thus guaranteeing that data is processed in real time. Secondly, cloud computing allows for sophisticated algorithms that are also very responsive in the cloud, identifying even the most insidious packet threats and ensuring that data is processed accurately.

5.2.2. Advanced data learning and analytics

As described in the previous section, the cloud's ability to process data Through advanced data learning and analytics, the cloud can dig deeper into the data and identify potential vulnerabilities or hidden threats. In addition, by analyzing current data patterns, predictive analytics can anticipate upcoming threats, paving the way for anticipated security measures [11].

5.2.3. Adaptive Threat Intelligence

Traditional databases are static, dependent on manual updates, and often need to catch up in providing real-time threat intelligence. Unlike traditional databases that require manual updates, cloud databases evolve in real time to absorb new threat intelligence from countless global sources [12]. This ensures that comprehensive, up-to-date defense mechanisms are learned from global cyber events, not just local data and that defenses are in place before potential threats arrive.

5.2.4. Adaptive Threat Intelligence

Cloud computing has the adaptability of resource allocation [13]. Resource allocation is a technique that distributes the available resources in a cloud data center among users. Unlike the local fixed data processing model, cloud computing can automatically allocate more resources during high-risk periods, ensuring that the cloud is always available, and performance is not affected. Conversely, it automatically scales down resources during calmer periods to prevent resource wastage. This type of resource allocation not only ensures the stability of firewall effectiveness but also saves costs.

5.3. Router-Centric Defense: The First Line of Resistance

5.3.1. Immediate Threat Neutralization

The router is the gateway for all incoming and outgoing traffic, and by placing the firewall at the router level, it ensures that malicious entities are intercepted before they can reach and potentially harm devices in the link, protecting the integrity of local devices and also greatly reducing the impact of the human factor. A router's tight integration with the cloud enhances its defenses, and real-time updates from the cloud allow the router to instantly identify and eliminate threats, making it a strong first line of defense for the network.

5.3.2. Efficient Traffic Segmentation

Traffic management is an art, and the router is the master artist. Every piece of data flowing through a network pass through a router, which is an ideal place for traffic segmentation [14]. Routers can effectively classify and prioritize packets by analyzing various parameters, including the source of traffic and the nature of its content. This approach to traffic management ensures that secure requests are handled quickly, and the network is continuously available. This ensures optimal network performance and user experience.

5.3.3. Unified Protection Across Devices

The variety of devices a router can connect to a network is vast, including many IoT devices ranging from traditional desktop computers to smartphones. This diversity can create unimaginable challenges for security systems that need to cater to different device specifications and operating systems. A router-centric firewall defense that focuses security at the router level ensures that all devices benefit from consistent security protocols regardless of device type or operating system. This approach not only simplifies security management and greatly reduces the impact of the human factor but also ensures that all devices are protected.

5.3.4. Intrusion Prevention System (IPS)

Traditional firewalls excel at filtering known threats based on pre-existing rules. However, the dynamic nature of network threats requires a more proactive approach, namely an integrated intrusion detection system (IDS). The foundation of an IDS is a monitoring system that collects evidence to facilitate detection and support forensic analysis. As soon as an anomaly is detected, the IDS triggers an alert that alerts the user to a potential security breach. However, an Intrusion Prevention System (IPS) can be used in a router-centric firewall to ensure that the human factor is minimized. Intrusion Prevention Systems (IPS) include proactive responses and passive monitoring, such as blocking ongoing breaches or changing network configurations. An IPS that enhances a firewall can alter packets, remove malware, or send a TCP reset to terminate a connection; an in-host IPS can terminate a process. (Oorschot & Nugent, 2020)

5.4. Proactive and Predictive Measures

5.4.1. Behavioral analytics

In the field of cybersecurity, "normal" behavior is critical. The system's behavioral analysis methodology is based on this understanding. By continuously monitoring network traffic, it captures and establishes a baseline of regular activity and interactions and has identified a reference point for subsequent network activity. (Padilla et al., 2021) When activity deviates from this established standard, it immediately issues an alert. By recognizing these deviations in real-time, the system ensures that potential threats are identified and dealt with promptly, in terms of detecting threats that may not necessarily be overtly malicious but may have subtle patterns of anomalies.

5.4.2. Machine Learning Integration

Integrating machine learning into a system's defense mechanisms can greatly boost active cybersecurity. Traditional defenses are static; they typically rely on known threat signatures, and while they can be effective against recognized threats, they can be ineffective in dealing with

unknown challenges. Machine learning algorithms, on the other hand, are dynamic. They learn from every piece of data they process, and over time, as more and more data are processed, they become more adept at recognizing patterns, even those of threats that have never been seen before. Furthermore, these algorithms apply to understanding past and present threat patterns. Machine learning can use historical data to predict future threats, allowing systems to pre-emptively adjust their defenses and cast a net over threats before they appear and arrive. (Jordan & Mitchell, 2015)

5.4.3. Ongoing Vulnerability Assessments

Proactive network security identifies and corrects potential vulnerabilities before they can be exploited. The system's ongoing vulnerability assessment involves regular network scanning, scrutinizing every node, connection, and data point from which any potential weak points that malicious entities could exploit are identified. Once vulnerabilities are identified, proactive cybersecurity immediately deploys remedies to strengthen these weak points. This continuous vulnerability assessment ensures that network defenses are always in top shape, minimizing the risk of vulnerabilities. One good example is IPS. (Oorschot & Nugent, 2020)

5.5. Future-proof and scalable

5.5.1. Modular design

Adaptability is critical in the ever-changing network security environment. A router-centric cloud firewall is a flexible framework that can easily accommodate new features, technologies or updates. As network threats evolve and new defense mechanisms emerge, the firewall can seamlessly integrate these advanced technologies without needing a complete overhaul, making it a truly future-proof solution.

5.5.2. Integration with other security solutions

A router-centric cloud firewall allows seamless integration with other security solutions, including the abovementioned Intrusion Prevention System (IPS). When the firewall works in tandem with and in conjunction with other security solutions, the effect can be greatly enhanced and create a comprehensive security ecosystem where each tool complements the other, ensuring that the network is strengthened from all possible angles and potential vulnerabilities are addressed.

5.6. Summary

The proposed firewall design supports a router-centric defense that leverages cloud integration to enhance security. The firewall sits at the router level and acts as the primary defense barrier, immediately eliminating threats. This approach ensures efficient traffic management and provides consistent protection for various devices, from PCs to IoT devices. It also combines cloud integration with proactive measures to build the firewall's adaptive analytics to predict potential threats and ensure the network's defenses remain robust. The modular design of the firewall ensures adaptability to dynamic network security environments, laying the foundation for possible future enhancements.

6. Conclusion

The field of network security is fraught with various threats. As such, firewalls play an integral role in today's connected world. The proposed firewall design emphasizes router-centric defenses and cloud integration to reduce human-induced pitfalls and comprehensively address and prevent cybersecurity threats. The design leverages the power of cloud computing, machine learning, and behavioural analytics to ensure real-time threat detection and resolution. In addition, its modular nature and integration capabilities ensure that it remains adaptable and scalable, ready to meet the changing challenges of the future. As the internet becomes more deeply integrated into human life, utilizing a router-centric cloud firewall is necessary to ensure network security's future.

References

[1] Kurose, J. F., & Ross, K. W. (2022). Computer networking: A top-down approach. Pearson Education Limited.

[2] MacKinnon, R. (2013). Consent of the networked: The worldwide struggle for internet freedom. Basic Books.

[3] Farnan, O., Darer, A., & Wright, J. (2015). Poisoning the well – exploring the great firewall's poisoned DNS responses.

[4] Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., Bock, K., Houmansadr, A., Levin, D., & Wustrow, E. (2023). How the great firewall of china detects and blocks fully encrypted TRAFFIC.

[5] Aitken, P., Claise, B., & Trammell, B. (2008). Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information.

[6] Stoja, S., Vukmirovic, S., Jelacic, B., Capko, D., & Dalcekovic, N. (2014). Architecture of real-time database in cloud environment for Distributed Systems. 2014 2nd International Conference on Artificial Intelligence, Modelling and Simulation.

[7] Verizon. (2022). 2022 data breach investigations report. Verizon Business. https: //www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations - report-dbir.pdf.

[8] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010, April 1). A view of cloud computing. Communications of the ACM.

[9] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, Perspectives, and prospects. Science, 349 (6245), 255 – 260.

[10] Fard, M. V., Sahafi, A., Rahmani, A. M., & Mashhadi, P. S. (2020). Resource allocation mechanisms in cloud computing: A systematic literature review. IET Software, 14 (6), 638 – 653.

[11] Babu, S., Subramanian, L., & Widom, J. (2004). A Data Stream Management System for Network Traffic Management.

[12] Oorschot, van, & Nugent. (2020). Computer Security and the internet. Springer International Publishing.

[13] Padilla, E., Acosta, J. C., & Kiekintveld, C. D. (2021). Cybersecurity methodology for specialized behavior analysis. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 237 – 243. https: //doi.org/10.1007/978 - 3 - 030 - 68734 - 214.

[14] Soldatov, A., & Borogan, I. (2015). The red web: The struggle between Russia's digital dictators and the new online revolutionaries. Perseus Books Group.