УДК 004.056.5
DOI: 10.31673/2409-7292.2025.031949

Chepel D. O., Malakhov S. V.

MULTIBASED CLOUD MONITORING OF DNS TRAFFIC FOR OPERATIVE CORRECTION OF CURRENT RPZ PARAMETERS

The paper presents the results of test studies of a software tool (ST) for monitoring the current state of a defined group of DNS servers. To improve the informative content and timeliness of test measurement data analysis, artificial intelligence (AI) capabilities are integrated, enabling flexible adjustment of test structures and profiles. The improved ST increases situational awareness regarding security threats in DNS traffic. The experimental version implements cloud-based multi-source measurements using spatially distributed cloud sensors, centrally controlled via an administrator console. This architecture allows monitoring DNS query processing parameters from simulated clients located in different domain zones. Within the framework of simulation modeling for various DNS query encryption protocols, the parameters of the daily availability of servers were evaluated. The results confirmed the system's ability to automatically adapt measurement parameters and structure based on real-time AI analytics of previous observations. The generalization of the obtained information has made it possible to identify promising directions for further improvement of the implemented concept, including: enhancing the administrative procedures of the cloud bot-testers system; refining the specifics inherent to different AI systems in accordance with the monitoring tasks performed; formalizing criteria for assessing the current state of DNS traffic; improving precedent-based analysis mechanisms for detecting anomalous traffic; enhancing the procedures for synthesizing new scenarios to detect previously unknown threats exploiting DNS traffic (services and applications) vulnerabilities.

Keywords: DNS, RPZ, AI, information security, traffic filtering.

Problem Statement

Scientific and technological progress, along with new developments in the field of high technology, give rise to a new spectrum of threats to existing information and communication systems (ICS). This dialectic of processes necessitates continuous attention to cybersecurity and information protection issues. The present work continues a series of studies dedicated to enhancing the protection capabilities of modern ICS by improving tools for monitoring and analyzing DNS (*Domain Name System*) traffic. Addressing these issues enhances the adaptability of adjustments to the current parameters of Response Policy Zones (RPZ) and enables the early detection of DNS traffic anomalies that pose potential security threats to modern ICS [1-3].

Within the framework of this research, the structure of the test algorithm for a decentralized cloud-based DNS query monitoring system has been revised, and certain software (SW) modules previously presented in [2] have been improved. The updated version of the algorithm ensures greater flexibility, scalability, and the capability for automated analysis of monitored parameters. A key distinction lies in the integration of artificial intelligence (AI) capabilities through *Gemini API* solutions [4]. Incorporating AI enhances the audit of the collected measurement statistics and creates the necessary conditions for promptly adjusting the parameters of the active RPZ. As part of the overall research concept, it was hypothesized that the implementation of AI execution modules within the algorithm's structure could improve the administration parameters of the employed cloud sensor subsystem. The conducted modeling confirmed the validity of the implemented architectural changes to the test monitoring system and demonstrated increased variability of test measurements (*in both the composition and structure of queries*).

Analysis of Recent Studies and Publications

The presented results constitute another step in research aimed at improving the protection of modern ICS through the enhancement of the DNS traffic monitoring subsystem, enabling prompt adjustment of current RPZ parameters and the early detection of dangerous traffic anomalies [1–3]. Filtering DNS traffic is an integral part of information security (IS) measures for the vast majority of modern ICS. Monitoring DNS queries allows for the control of the circulation of the corresponding traffic and enables the implementation of adequate corporate information security policies [1].

Based on the analysis of issues related to DNS traffic monitoring and filtering, the following main vectors of effort can be identified [1–3, 5–18]:

1. Threat Intelligence Feeds**.** These serve as an important source of information on the current state and list of cyber threats. Consolidation of such information facilitates the early detection of and rapid response to emerging IS threats. The main challenge in this area lies in assessing the authenticity and adequacy of the relevant feeds. In addition, IS specialists emphasize the high redundancy of false positives in various intelligence feeds [1, 5-7].

2. Means for Detecting Botnet Command-and-Control Servers**.** Research in this area is primarily focused on the specifics of detecting botnet command-and-control channels. It involves improving behavioral analysis methods through comprehensive monitoring of DNS traffic (including encrypted traffic). The authors of relevant works [1, 8–10] report a fairly high detection accuracy for already known types of botnets, but note certain limitations of these approaches.

3. DNS Traffic Encryption**.** Conceptually, it provides a more secure channel for DNS query circulation, preventing spoofing and/or interference by malicious actors. However, on the other hand, the introduction of DNS encryption complicates the process of detecting malicious traffic [3], particularly traffic originating from botnet command-and-control centers. Moreover, there are documented cases of "successful" attacks against DNS encryption, which call into question its effectiveness as a universal tool for ensuring the confidentiality of users' network activity [1, 11-13].

4. Implementation of Response Policy Zones (RPZ). RPZ is an effective tool for managing the security of modern ICS at the DNS service level, enabling the proactive detection and blocking of dangerous domains [1, 14-15].

5. Enhancing the Detection of Domain Generation Algorithm (DGA) Activity. The prompt identification and blocking of further proliferation of "synthetically created" malicious domains is a priority focus area for many groups of specialized experts [1, *16-18*].

6. Monitoring the Current State of DNS Servers**.** The work in [2] presents the results of simulation modeling of specialized measurements for assessing the availability of a target group of DNS servers under conditions involving the use of different types of protocols (*including DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH)*). The conducted research helped refine the general structure and composition of the corresponding system and improve data collection and analysis procedures. Based on the simulation results, it was concluded that this direction could be further developed as a tool for proactive detection of DNS traffic anomalies.

Purpose of the Article – is to present new modeling results obtained after improvements to previously proposed mechanisms for monitoring the current state of DNS traffic. The implemented modifications enhanced the informative content of network event analysis and improved the responsiveness in adjusting the settings of corporate Response Policy Zones (RPZ). Collectively, these improvements have strengthened the ability to proactively respond to potential collisions and/or anomalies in DNS traffic behavior.

Main Content

In the updated release of the experimental program, the processes of collecting and analyzing source information are carried out through extensive implementation of cloud services and AI-based tools. Overall management of all processes is performed from the main administrator console. In essence, the updated tool is a decentralized cloud-based system for monitoring the current state of DNS traffic, consisting of the following components:

1. Cloud Testing Bots (Google Cloud Run): implemented as code modules that accept input testing parameters, perform the corresponding measurements, and store the obtained data in the cloud. These modules are deployed in *Google* data centers located in various geographic regions worldwide. The required configuration and location of the testing bots are determined from the administrator console and adjusted in real time based on the progress of the measurements.

2. Java Client: **–** responsible for managing the operation of the cloud bots, maintaining feedback with them, and formalizing the obtained measurement results.

3. Cloud Storage: **–** used to store the raw results of test measurements within the supported bot cloud infrastructure.

© Chepel D. O., Malakhov S. V. (2025) Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Сучасний захист інформації, 3(63), 176–185.
https://doi.org/10.31673/2409-7292.2025.031949

4. Python Client: – responsible for sending the accumulated measurement data and formalized tasks (prompts) to the Gemini 2.0 Flash model for further analysis of the obtained information via the Gemini API.

The choice of Gemini is driven by a combination of characteristics that make it particularly effective for data analysis tasks. The Gemini API offers seamless integration with the Python environment, enabling rapid configuration of data exchange between the data collection subsystem and the AI module. Another key advantage is its long-context capability, with a baseline limit of up to 1,048,576 tokens per request. This allows the processing of large datasets that require in-depth analysis and consideration of cause-and-effect relationships [19–20].

As noted above, the enhanced version of the program has been augmented with the capability to dynamically adjust current measurement parameters. This primarily concerns the list of domain names used when sending test queries to the target group of DNS servers. The corresponding algorithm is implemented through a mechanism of synchronous-cyclic data collection and analysis, with adjustments to the structure of test queries in subsequent measurement rounds. Within this operational concept, the testing process involves the group transmission of artificially synthesized DNS queries, with subsequent recording of the servers' responses.

In the current version of the software, the parameters of all test queries within a single measurement round are identical. A set of test queries with the same structure constitute one measurement round. A round may contain either a single test query or a set of individual queries with the same structure. In the first case, this represents a one-time measurement; in the second, the process operates in a cyclic measurement mode, with repetitions occurring at specified time intervals. Thus, different measurement rounds are characterized by different configuration parameters. Possible configurations for various measurement rounds are stored in a dedicated scenario file. The use of testing scenarios enables rapid adjustment or selection of the desired monitoring behavioral profile. The scenario for any measurement round contains the following information: - a list of target servers; - a list of cloud sensors in use (i.e., sensor locations); - the measurement start time; - the structure of the query used; - the total number of queries; - the timeout values between all test queries within the same round.

A simplified modeling scheme is presented in Figure 1. The sequence and essence of the main procedures can be summarized as follows.

1. From the administrator's console, a control message is sent to a pre-configured set of sensor bots operating in Multi Base mode [21]. This message contains information on the configuration parameters for the scheduled measurement round, as well as the setup of the cloud-based testing sensors involved in the measurements ("Cloud Functions," Fig. 1). The configuration parameters ("Testing Parameters") for a measurement round include [1, 3]:

- a list of monitored DNS servers;
- domain names — the use of different domains allows the assessment of DNS traffic characteristics for various combinations of "sensor–server" pairs;
- the start time of the measurement round (logical "Start");
- a description of the structure of the test query, including:

a) the sequence in which the servers are queried;

b) the type of protocol used (DoT, DoH) (may be identical for all servers or specified individually for each server. In the present case, the DNS query protocol within a single measurement **round** remained unchanged);

c) the number of test query repetitions (i.e., number of cycles);

d) the timeout between measurement cycles within the same round (timeouts between different **cycles** may be uniform or vary (for refining the detection of conditional "peak times"). In the conducted modeling, all cycle timeouts remained unchanged).

© Chepel D. O., Malakhov S. V. (2025) Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Сучасний захист інформації, 3(63), 176–185.
https://doi.org/10.31673/2409-7292.2025.031949

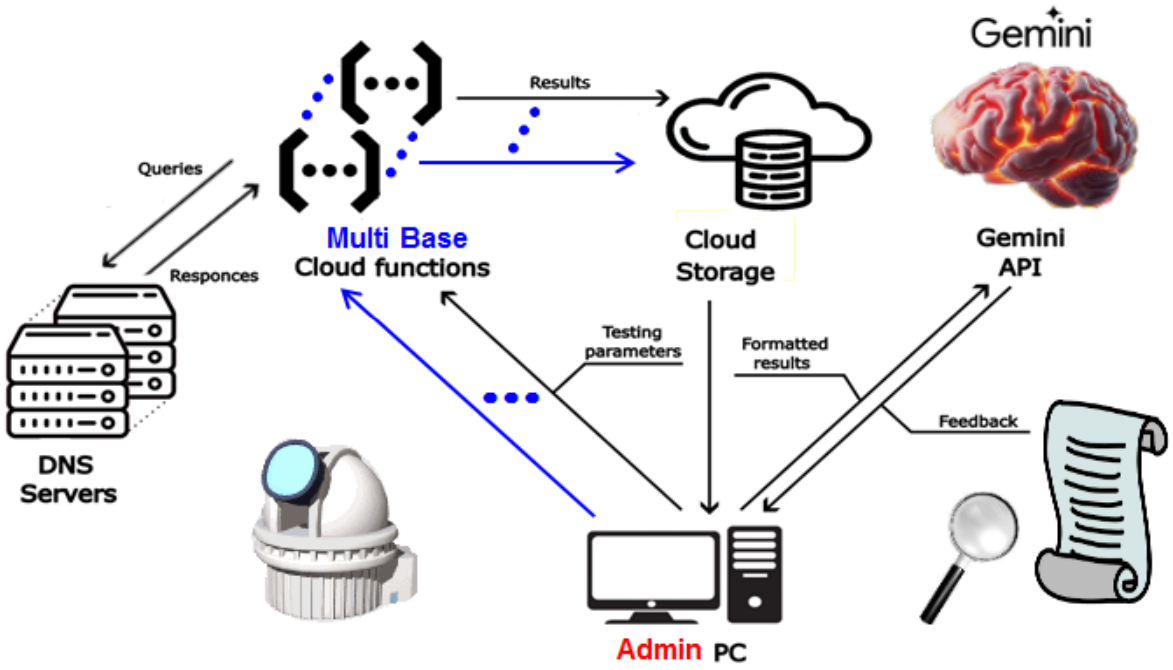

Fig. 1. Simplified modeling scheme in Multi Base mode

2. Upon receiving the initialization data from the administrator's console, the cloud sensors perform round-based measurements according to the combinations: time – server – domain – protocol – number of cycles. The results of each measurement round are stored in the cloud storage ("Cloud Storage" in Fig. 1);

3. The aggregated results are downloaded to the console, where they are appropriately formalized and transferred for analysis to the AI module ("Gemini" in Fig. 1);

4. Based on the AI model's analysis, a new list of domain names is generated, which is then used in the next monitoring round.

Data analysis using AI capabilities makes it possible to automate and accelerate the detection of abnormal delays in the processing of DNS queries from monitored servers. However, during the modeling process, ambiguity was observed in the AI's responses to identical procedural scenarios ("prompts"). For example, in earlier stages, the responses obtained from the AI were converted into instructions for subsequent test rounds, with the list of domain names specified as the first line of the AI's output. Despite repeated clarifications of this requirement in the procedural instructions for the AI module, after six "successful" measurement rounds, the first lines of its responses began to contain non-specific messages such as "OK, here is the updated list of domains and data analysis from the table", "OK, understood," or special symbols such as "```". These "universal" responses from the AI lead to incorrect interpretation of measurements. As a result, the next two measurement rounds were based on deviant input data, necessitating their exclusion from the overall observation statistics.

This interaction issue with the AI was resolved by enforcing formalization of the output instructions to eliminate verbal reactions. To address these difficulties, the following measures can be implemented: 1 - limiting the depth of analysis of test cycles, which removed the prerequisites for AI self-optimization (effectively enforcing discretization of cycle measurements); 2 - performing additional validation of input data by generating a repeated request to the AI model with an explicit requirement to isolate the target output line. Both approaches result in some time overhead and essentially implement a "re-query" logic. In the first case, the procedure is carried out in two steps: segmentation and analysis of local datasets, followed by integration of observation analytics across all measurement rounds. In the second case, an additional verification request is used.

© Chepel D. O., Malakhov S. V. (2025) Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Сучасний захист інформації, 3(63), 176–185.
https://doi.org/10.31673/2409-7292.2025.031949

Based on the results of the conducted simulation, an assessment was performed regarding the availability of the target DNS servers under the condition of simultaneous generation of test queries from multiple domains (representing different configurations of cloud sensors). Figures 2–5 present histograms illustrating the average query latency (excluding the influence of daily load fluctuations) for the selected set of test servers. A synthesis of the obtained data permits the following conclusions:

- irrespective of the place where the test queries were generated (i.e., the location of the cloud sensors) and the type of DNS query protocol employed, Google servers demonstrated consistently good latency performance;
- backup DNS servers generally exhibited slightly better performance compared to primary servers. This phenomenon is likely attributable to the conventional routing of the majority of users to the primary servers within existing cluster groups;

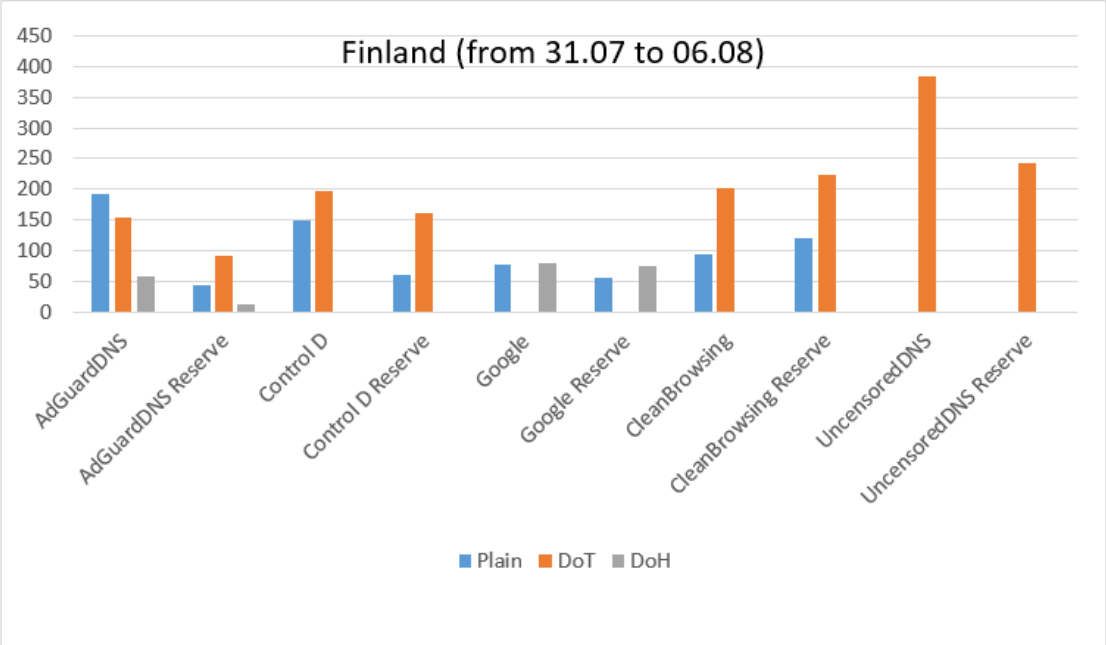

Fig. 2. Average DNS query latency (Finland)

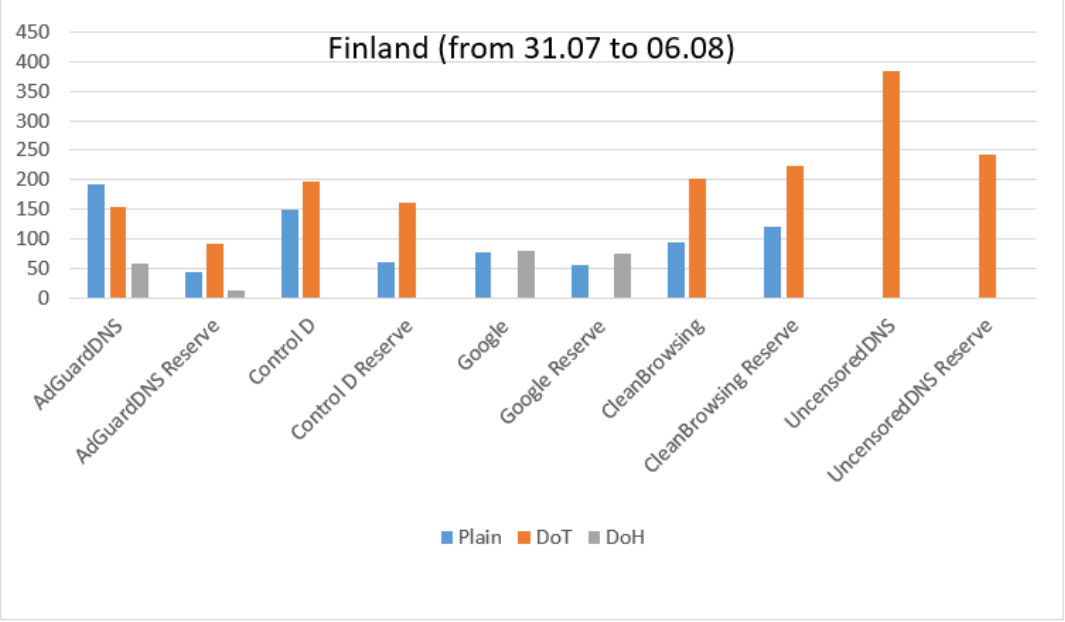

Fig. 3. Average DNS query latency (USA)

- the impact of encryption (in the present experiments, DoT and DoH) on query processing time is present. This effect is predominantly localized within each individual cluster group of servers. In other words, DNS query latency depends to a greater extent on the current performance characteristics of a particular server (even within the same DNS cluster) than on the type of protocol utilized;

- the factor of the current time of day across different time zones has a significant impact on the load characteristics of DNS servers located within those zones. In other words, the influence of regional specifics, particularly the duration of the "local" working hours, on the temporal parameters of query processing is substantial;

- the level of development of regional IT infrastructures affects query processing times. Indirectly, it creates conditions for an increase in the volume of cached data queues at network "bottlenecks." At the same time, in regions with well-developed infrastructure, increased variability in traffic routing compensates for the time losses caused by longer routing paths.

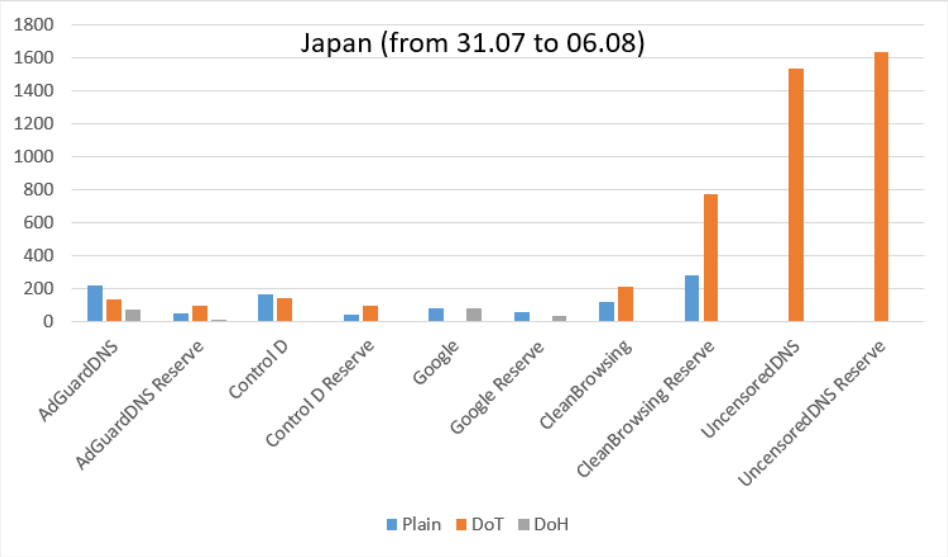

Fig. 4. Average DNS query latency (Japan)

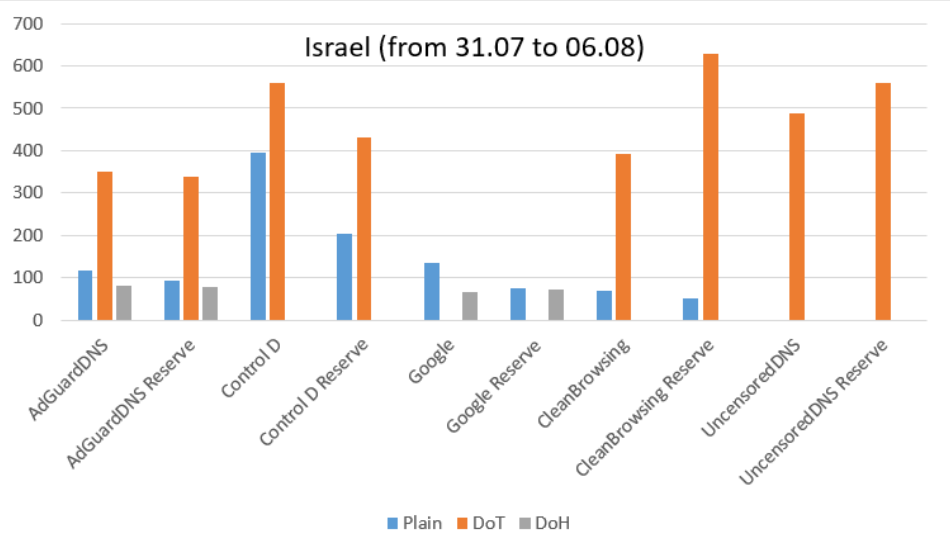

Fig. 5. Average DNS query latency (Israel)

Overall, the results of the conducted simulation are consistent with previously obtained findings [2]. That is, the real-time adjustment of ongoing round measurement parameters (an AI function) improves the quality of DNS traffic monitoring. This opens new opportunities for reducing response

© Chepel D. O., Malakhov S. V. (2025) Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Сучасний захист інформації, 3(63), 176–185. https://doi.org/10.31673/2409-7292.2025.031949

times to potential security threats inherent in the operational environment of DNS services and infrastructure.

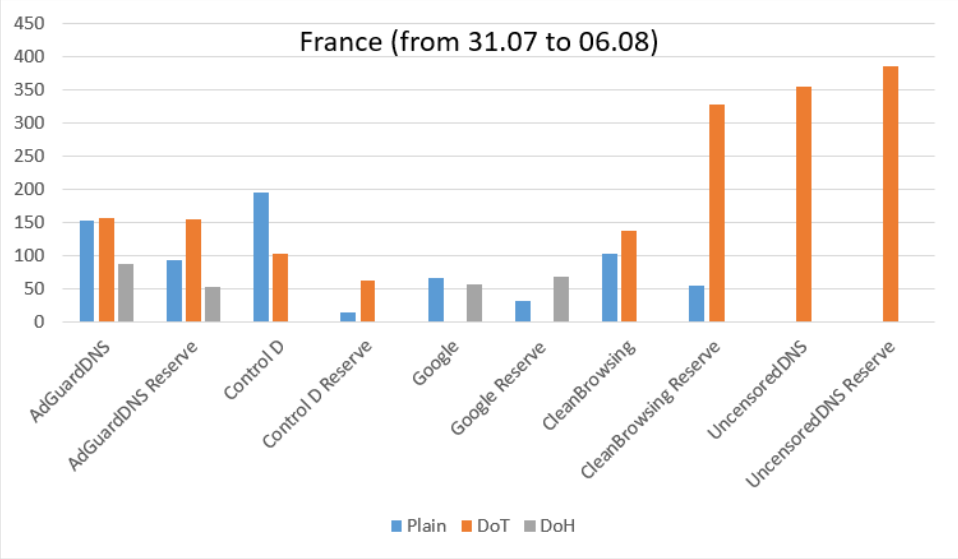

Fig. 6. Average DNS query latency (France)

Table 1

Example of the test domain name registry

Date	Domain names
Input data ***(Start)***	bbc.co.uk gov.za rozetka.com.ua post.japanpost.jp lemonde.fr taiwannews.com.tw usa.gov
↓ 31.07 day	**bbc.co.uk taiwannews.com.tw gov.za post.japanpost.jp lemonde.fr usa.gov** work.ua ca.gov bbc.com
↓ 01.08 night	**bbc.co.uk taiwannews.com.tw gov.za post.japanpost.jp lemonde.fr usa.gov work.ua** ca.gov **bbc.com**
↓ 01.08 day	**bbc.com ca.gov work.ua** theguardian.com xinhuanet.com.cn marca.com mercadolivre.com.br naver.com aljazeera.com
↓ 02.08 night	taiwannews.com.tw **mercadolivre.com.br xinhuanet.com.cn aljazeera.com theguardian.com bbc.com ca.gov work.ua marca.com** news.yahoo.com
↓ 02.08 day	**taiwannews.com.tw** rozetka.com.ua **xinhuanet.com.cn aljazeera.com bbc.com** gov.za **marca.com mercadolivre.com.br** lemonde.fr **aljazeera.com**
↓ 03.08 night	**taiwannews.com.tw rozetka.com.ua xinhuanet.com.cn aljazeera.com bbc.com** ca.gov **lemonde.fr marca.com** work.ua edition.cnn.com
↓ 03.08 day	**bbc.com lemonde.fr** universite-paris-saclay.fr **marca.com aljazeera.com** mercadolivre.com.br **xinhuanet.com.cn** gov.za **ca.gov rozetka.com.ua**
↓ 05.08 night	**bbc.com lemonde.fr xinhuanet.com.cn marca.com** edition.cnn.com **gov.za aljazeera.com** bbc.co.uk yahoo.com **mercadolivre.com.br**
↓ 05.08 day	**bbc.co.uk** taiwannews.com.tw **gov.za** post.japanpost.jp **lemonde.fr** usa.gov work.ua ca.gov **bbc.com aljazeera.com**
↓ 06.08 night	**bbc.com** marca.com xinhuanet.com **gov.za aljazeera.com** lequipe.fr mercadolivre.com.br naver.com edition.cnn.com **ca.gov**
06.08 day ***(Stop)***	bbc.co.uk taiwannews.com.tw **gov.za** post.japanpost.jp lemonde.fr usa.gov work.ua **ca.gov bbc.com** npr.org

Note: in Table 2, entries highlighted in bold represent "old" records that were present in the previous monitoring round; the time of day is given in Kyiv time.

Table 1 reflects the daily dynamics of changes in the domain name registry, the positions of which were adjusted by the AI module. The following requirements were set for the registry update process: - prioritization of domain zones with unstable and/or excessively long query response times; - prevention of excessive concentration of measurements on a single domain zone; - ensuring geographical diversity (proportional coverage of different time zones); - inclusion of a portion of stable domains, whose queries yield temporally consistent results.

A synthesis of the results of the domain registry update confirms the validity of the chosen strategy regarding the utilization of AI capabilities for the operational adjustment of the domain name list. For example, according to the data in Table 1, the daily updated domain list systematically includes domain names absent from the initial set (such as ca.gov, xinhuanet.com.cn, theguardian.com, marca.com, edition.cnn.com, aljazeera.net, among others), which enhances the representativeness of the obtained test measurement data. As an example, Table 2 presents a fragment of the corresponding "Anomaly Report" generated by the experimental system based on measurements conducted on 06.08.25 for the "USA" region:

- UncensoredDNS: Persistent lack of support for Plain DNS and DoH protocols.
- AdGuardDNS: Significant delays observed for the DoT protocol across multiple domains, indicating potential issues with the DNS over TLS configuration or performance.
- CleanBrowsing: Exhibits high latency for the domain gov.za, especially under the Plain DNS protocol, which may indicate routing problems or server issues in Japan.

Evaluating the data in Table 2, it can be noted that even this very limited excerpt of the report generally corresponds to factual reality. At the same time, despite clarifications in the prompt wording, the AI model classifies the absence of support for one or more protocols as an anomaly.

Table 2

Test system report on delays in the region «USA»

Time stamp	DNS server	DNS server IP	Test domain	Plain time (ms)	DoH time (ms)	DoT time (ms)
06.08.2025 13:46:03	CleanBrowsing	185.228.168.9	xinhuanet.com	212	0	1322
…	CleanBrowsing	185.228.168.9	gov.za	588	0	424
…	CleanBrowsing	185.228.168.9	aljazeera.com	19	0	163
…	CleanBrowsing	185.228.168.9	lequipe.fr	20	0	163
…	AdGuardDNS	94.140.14.14	xinhuanet.com	3243	39	2242
…	AdGuardDNS	94.140.14.14	gov.za	280	39	238
…	AdGuardDNS	94.140.14.14	aljazeera.com	43	42	245
…	AdGuardDNS	94.140.14.14	lequipe.fr	40	41	245
…	UncensoredDNS	91.239.100.100	xinhuanet.com	0	0	1637
…	UncensoredDNS	91.239.100.100	gov.za	0	0	743
…	UncensoredDNS	91.239.100.100	aljazeera.com	0	0	748
06.08.2025 13:46:03	UncensoredDNS	91.239.100.100	lequipe.fr	0	0	774

Conclusions

1. Testing of the software tool for monitoring the current state of target DNS servers have been conducted. The algorithm structure integrates AI capabilities, which has enhanced the responsiveness and informative content of DNS traffic monitoring. The program provides analysis and visualization

© Chepel D. O., Malakhov S. V. (2025) Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Сучасний захист інформації, 3(63), 176–185. https://doi.org/10.31673/2409-7292.2025.031949

of monitoring results and supports dynamic modification of measurement input parameters through extensive implementation of cloud solutions and AI functions.

2. Based on the simulation results, a comparison of the availability indicators of DNS servers across different regions of the world and the characteristics of DNS query processing under various generation conditions was performed. It was established that at the time of the simulation, for the chosen configuration of interacting nodes (within the "bot-tester – target server" system), Google servers consistently demonstrated the lowest latency. It was also determined that backup servers, in some cases, exhibited slightly better performance than primary servers. The analysis of latency when processing queries using encryption technologies (DoT and DoH protocols) indicates a noticeable difference for certain server cluster groups. The main trend observed is a loss of performance when using encrypted DNS traffic (in this case, DoT and DoH).

3. The simulation confirmed the capability of the experimental system to automatically adapt the parameters of test measurements through real-time analytics (an AI function) of previous observation results. For instance, the data in Table 1 demonstrate a dynamic change in the list of domain names, with the inclusion of elements absent from the initial dataset (such as ca.gov, xinhuanet.com.cn, theguardian.com, marca.com, edition.cnn.com, aljazeera.net, among others).

4. Verification of network anomaly reports generated by the experimental system was conducted. The analysis of these reports was performed by comparison with measurement results presented in Table 2. A synthesis of all the obtained information allows concluding that the artificially generated reports correspond to actual conditions. This confirms the validity of the chosen strategy regarding the utilization of AI for automating analytics and detecting anomalies in DNS traffic.

5. Within the scope of this research, the concept of multi-basis measurements was implemented. The operational parameters forming a specific scenario for round measurements include: - the system of cloud sensors; - the set of target servers; - the structure of the test queries; - the duration of observations.

6. Prospects for further research include: - formalization of criteria for assessing the current state of DNS traffic; - refinement of the precedent analysis paradigm for detecting hazardous DNS traffic anomalies; - expansion of the monitoring system's capabilities regarding the variability of supported test measurement scenarios.

References

1. Chepel, D., & Malakhov, S. (2024). Uzahalnennia napriamiv filtratsii DNS trafiku yak skladovoi bezpeky suchasnykh informatsiinykh system [Summary of DNS traffic filtering trends as a component of modern information systems security]. Computer Science and Cybersecurity, (1), 6–21. https://doi.org/10.26565/2519-2310-2024-1-01 [in Ukrainian].

2. Chepel, D., & Malakhov, S. (2025). Multyprotokolnyi monitorynh trafiku DNS, yak osnova dlia koryhuvannia potochnykh parametriv RPZ [Multiprotocol monitoring of DNS traffic as a basis for adjusting current RPZ parameters]. ΛΌГОΣ. Collection of Scientific Papers, 242–246. https://doi.org/10.36074/logos-24.01.2025.049 [in Ukrainian].

3. Korobeinykova, T., & Fedchuk, T. (2024). Ohliad protokoliv DNS, DoH ta DoT [Overview of DNS, DoH and DoT protocols]. ΛΌГОΣ. Collection of Scientific Papers, 253–256. https://doi.org/10.36074/logos-01.03.2024.056 [in Ukrainian].

4. Google. (n.d.). Gemini Developer API. https://ai.google.dev/gemini-api/docs

5. Haneef, A. (n.d.). On the scalable generation of cyber threat intelligence from passive DNS streams. http://surl.li/phbham

6. Korte, K. (n.d.). Measuring the quality of open source cyber threat intelligence feeds. http://surl.li/yhiqoe

7. Li, V. G., Dunn, M., Pearce, P., McCoy, D., Voelker, G. M., Savage, S., & Levchenko, K. (2019). Reading the tea leaves: A comparative analysis of threat intelligence. USENIX Security Symposium, 851–867. https://atc.usenix.org/system/files/sec19fall-li_prepub.pdf

8. Alieyan, K., ALmomani, A., Manasrah, A., & Kadhum, M. M. (2015). A survey of botnet detection based on DNS. Neural Computing and Applications, 28(7), 1541–1558. https://doi.org/10.1007/s00521-015-2128-0

9. Choi, H., Lee, H., Lee, H., & Kim, H. (2007). Botnet detection by monitoring group activities in DNS traffic. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 715–720. https://doi.org/10.1109/CIT.2007.90

10. Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A., & Garant, D. (2013). Botnet detection based on traffic behavior analysis and flow intervals. Computers & Security, 39, 2–16. https://doi.org/10.1016/j.cose.2013.04.007

11. Lyu, M., Gharakheili, H. H., & Sivaraman, V. (2022). A survey on DNS encryption: Current development, malware misuse, and inference techniques. ACM Computing Surveys, 55(8), 1–28. https://doi.org/10.1145/35473

12. Lu, C., Liu, B., Li, Z., Hao, S., Duan, H., Zhang, M., Leng, C., Liu, Y., Zhang, Z., & Wu, J. (2019). An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come? Proceedings of the ACM Internet Measurement Conference (IMC '19), 22–35. https://doi.org/10.1145/3355369.3355580

13. Siby, S., Juarez, M., Diaz, C., Vallina-Rodriguez, N., & Troncoso, C. (2020). Encrypted DNS – Privacy? A traffic analysis perspective. Proceedings of the 27th Network and Distributed System Security Symposium (NDSS). https://arxiv.org/abs/1906.09682

14. Connery, H. M. (n.d.). DNS response policy zones history, overview, usage and research. https://www.dnsrpz.info/RPZ-History-Usage-Research.pdf

15. Ichise, H., Jin, Y., & Iida, K. (2023). Policy-based detection and blocking system for abnormal direct outbound DNS queries using RPZ. Proceedings of the 22nd International Symposium on Communications and Information Technologies (ISCIT) ,1–6. https://ieeexplore.ieee.org/document/10376042

16. Patsakis, C., & Casino, F. (2019). Exploiting statistical and structural features for the detection of domain generation algorithms. Journal of Information Security and Applications, (Preprint). https://arxiv.org/pdf/1912.05849

17. Koh, J. J., & Rhodes, B. (2018). Inline detection of domain generation algorithms with context-sensitive word embeddings. In Proceedings of the 2018 IEEE International Conference on Big Data, 2966–2971. https://ieeexplore.ieee.org/document/8622066

18. Kumar, A. D., Thodupunoori, H., Vinayakumar, R., Soman, K. P., Poornachandran, P., Alazab, M., & Venkatraman, S. (2019). Enhanced domain generating algorithm detection based on deep neural networks. Companion Proceedings of The 2019 World Wide Web Conference, 189–196. https://doi.org/10.1145/3308558.3316498

19. Google Cloud. (n.d.). Gemini 2.0 Flash. https://cloud.google.com/vertex-ai/generative-ai/docs/models/gemini/2-0-flash#2.0-flash

20. Relevance AI. (n.d.). Explore the capabilities of Gemini 2.0 Flash. https://relevanceai.com/llm-models/explore-gemini-2-0-flash-capabilities

21. Chepel, D. O. (2024). Analiz suchasnykh metodiv i tekhnolohii DNS filtratsii trafiku, yak skladovoi bezpeky suchasnykh informatsiinykh system [Analysis of modern DNS traffic filtering methods and technologies as part of the security of modern information systems] (Master's thesis, V. N. Karazin Kharkiv National University). [in Ukrainian].

Надійшла 17.08.2025