ISSN 2710–3056

ARTICLE

DOI 10.36074/grail-of-science.20.02.2026.112

MULTIBASE CLOUD MONITORING OF DNS TRAFFIC BASED ON PRECEDENT ANALYSIS OF DNS PROTOCOL ANOMALIES

Danylo Chepel
Postgraduate student of the Department of Cybersecurity of Information Systems, Networks and Technologies
V. N. Karazin Kharkiv National University, Ukraine, Ukraine

Serhiy Malakhov
Ph.D., Senior Researcher, Associate Professor of the Department of Cybersecurity of Information Systems, Networks and Technologies
V. N. Karazin Kharkiv National University, Ukraine

Summary. *The paper presents the results of an experimental study of a software tool for DNS traffic data analysis with the involvement of artificial intelligence based on a case-based reasoning (CBR) approach. In order to increase the transparency, reliability, and traceability of AI-assisted analysis of test measurement results, case-based reasoning methods were integrated. The experimental prototype was implemented as a Python client integrated with the Gemini API and operates on a dataset obtained from previous studies, thereby ensuring continuity and comparability of results. The system utilizes a manually defined initial set of cases and autonomously expands it by adding new anomalous cases accompanied by explanatory comments. The experimental results demonstrate that the proposed mechanism supports both targeted anomaly detection and the identification of general deviations in the data. The obtained results confirm the feasibility of using a case-based approach to enhance the transparency and traceability of AI-assisted DNS traffic analysis. At the same time, the experiments revealed clustering effects that may lead to false positive results and incorrect data interpretation, which necessitated a revision of the analysis constraints. Further evaluation confirmed that the introduced changes reduced the identified effect and increased the reliability of anomaly interpretation.*

Keywords: *DNS; RPZ; AI; CBR; cybersecurity; traffic filtering; network anomalies; precedent analysis; cloud monitoring; multibase monitoring; data analysis.*

Introduction. Scientific and technological progress brings new developments in the field of information and communication systems, but also gives rise to a new set of threats, such as the ones that use DNS-based attack vectors. Under these conditions, traditional approaches to DNS traffic analysis may show limitations, particularly when faced with encrypted or obfuscated traffic, dynamic domain changes by adversaries or irregular traffic flow patterns. The presented work extends previous research on improving the monitoring capabilities of a multibased cloud DNS monitoring system and focuses specifically on testing the applicability of the

precedent-based analysis paradigm in AI-assisted traffic analysis. The use of this approach may lead to the increase in validity, timeliness and interpretability of adjustments to the parameters of Response Policy Zones (RPZ) and ensure the early detection of DNS traffic anomalies that can be related to potential threats [2,3,5].

The core idea of a precedent analysis paradigm lies in forming and maintaining structured precedent data of characteristic DNS activity patterns that can be used to interpret current traffic in relation to historically observed behaviors. Introducing such a mechanism requires revising the structure of the previously proposed test algorithm, as well as modifying data gathering and preprocessing modules to ensure the adequate generation, storage, and retrieval of precedents. The performed simulation has demonstrated the feasibility of integrating precedent-based mechanisms into the cloud monitoring system and has confirmed the system's ability to handle a broader spectrum of DNS traffic anomaly types.

The purpose of this article is to present results obtained from experiments in precedent-based analysis of DNS traffic data. The implemented system enhances the interpretability of network event analysis and improves accuracy in detecting DNS traffic anomalies.

Analysis of recent studies and publications. DNS traffic filtering is an essential part of security of modern information and communication systems. Timely and accurate detection of DNS traffic anomalies can help mitigate damage from DNS-based threats and strengthen the overall effectiveness of policy enforcement [2].

An analysis of threat intelligence feeds, RPZ mechanisms, combating botnet activity, and DNS traffic encryption was previously presented in [5].

Based on the analysis of trends related to AI-driven DNS traffic monitoring and filtering, several research directions emerge that are relevant to this study: [4, 6-12]:

1. AI in data analysis. In the reviewed literature it is noted that intelligent systems enable automated extraction of structured knowledge from large and diverse datasets, outperforming traditional statistical approaches in scalability and adaptability. A recurring trend in recent publications is the integration of machine learning, knowledge-based reasoning, and optimization techniques as main elements of modern analytical methods. Deep learning is identified as the most prominent analytical paradigm. Studies also report significant advances in image recognition, signal interpretation and anomaly detection achieved through neural network architectures. However, despite high predictive accuracy, deep learning remains associated with several limitations, including substantial data requirements, computational cost, and reduced interpretability. This motivates the exploration of methods that incorporate explicit domain knowledge, symbolic reasoning and transfer learning mechanisms with the goal of improving applicability and transparency of AI. Also, the authors note the reliability challenges of AI, emphasizing the need for validation of AI-generated results.

Overall, the studies demonstrate that AI not only enhances the efficiency and accuracy of data analysis but also reshapes data analysis practices, shifting the focus towards integrated, intelligent systems capable of processing complex, multimodal data in real time. Despite rapid progress, the challenges of using AI in data analysis remain, such as interpretability, need for result validation and computational cost [7,10,11].

2. AI in DNS traffic analysis. Recent literature notes an increase in use of AI for DNS traffic analysis. The primary reason being the decline in the effectiveness of

traditional signature-based approaches, which may struggle with obfuscated channels, rapidly changing domains, and sophisticated evasion strategies. Studies show that machine learning models are capable of detecting anomalies even when informative features are obscured by encryption or masked by attackers.

It is emphasized that AI-based methods provide not only higher classification accuracy but also the ability to adapt to new types of attacks. On the other hand, the issue of interpretability still remains. There is a notion that integrating AI into security systems is impossible without explainable mechanisms that allow analysts to understand why a particular query or flow is flagged as suspicious. This need is directly linked to trust, auditability of decisions, and the practical applicability of such systems in real-world environments, where automation must be balanced with oversight.

Research highlights that modern architectures can operate in real time and remain resilient to evasion attempts by adversaries, making them a promising direction for enhancing protection in DNS domain. Overall, the studies indicate that there is a use case for applying AI in DNS monitoring that combines detection, adaptation, explanation, and scalability [4,12].

3. Case-based reasoning. Case-Based Reasoning (CBR) is gaining interest as a foundation for building more transparent, adaptable, and user-interpretable AI systems. As modern AI models increasingly exhibit “black-box” behavior, CBR is viewed as a natural counterbalance because it relies on explicit precedents and analogical reasoning. Studies emphasize that the core CBR cycle of retrieval, reuse, revision, and retention provides an interpretable structure through which AI decisions can be grounded in past experiences rather than unclear statistical correlations. This makes CBR especially attractive in areas where trust, auditability, and explainability are critical. The literature consistently concludes that case-based explanations improve user trust and comprehension, particularly in expert-driven fields such as healthcare or security analytics.

Another direction explored in studies is the integration of CBR with advanced AI models, including large language models (LLM). CBR helps LLM-based agents to mitigate hallucinations, handle domain-specific tasks more reliably, and provide precedent-based justifications for their outputs.

Overall, the common conclusion is that CBR offers both methodological and conceptual benefits for AI systems. It enhances transparency, consistency, adaptability and makes AI systems more aligned with human reasoning patterns [6,8,9].

Main content. In this study, an evaluation of the integration of a precedent-based analysis paradigm into the AI-driven DNS-monitoring workflow was conducted, with the goal of automatically augmenting a precedent table with newly detected anomalies. The dataset used in the experiment was sourced from the previous work [5], ensuring continuity of measurement conditions and comparability of results. The experimental program is implemented using a Python client with querying done through Gemini API.

The current prototype relies on a manually prepared initial precedent table that defines several baseline cases and their corresponding interpretations. Once the initial (seed) precedent table (table 1) is provided, the system autonomously extends the table by inserting new precedents with explanatory comments

describing the reason of their inclusion. This mechanism enables the prototype to draw conclusions from earlier records when interpreting new observations, improving the accuracy, interpretability and traceability of analytical outcomes.

Table 1

Extract from seed precedent table

Location	Server	Domain	Plain time (ms)	DoH time (ms)	DoT time (ms)	Comment
JAPAN	Cloudflare	gov.za	750	747	101	PQ and DHQ latency spike
FINLAND	Quad9-Reserve	nic.ar	11	10	1105	DTQ latency spike
FRANCE	Google	sina.com.cn	300	348	-	PQ and DHQ latency spike
ISRAEL	OpenDNS-Reserve	paris.fr	279	1185	1742	PQ, DTQ and DHQ latency spike
USA	OpenDNS-Reserve	gov.za	261	11	1255	PQ and DTQ latency spike

[author's development]
Note: in Tables 1 and 2, "PQ"," DTQ" and "DHQ" stand for plain, DoT and DoH query respectively.

Analysis of the precedents generated by the system (table 2) demonstrates that because the model is instructed not only to identify anomalies corresponding to those included in the initial seed set but also to detect additional irregularities, new types of anomalies appear in the table, such as missing responses or failed DNS queries. This indicates that the experimental program supports not only targeted anomaly detection, but also may catch general data anomalies, not included in the seed set. Moreover, the use of precedent structures facilitates the mitigation of false positives, as analysts can explicitly flag incorrect or inappropriate entries, refining the system's decision-making over time.

Table 2

Examples of generated precedents

Location	Server	Domain	Plain time (ms)	DoH time (ms)	DoT time (ms)	Comment
FRANCE	Quad9-Reserve	post.japanpost.jp	1425	0	1284	DHQ latency is zero, PQ and DTQ latency spike.
JAPAN	Quad9	bbc.co.uk	249	35	155	High PQ latency relative to DHQ and DTQ
ISRAEL	OpenDNS	nic.ar	2034	2719	2865	Extreme PQ, DHQ and DTQ latency.
FRANCE	Cloudflare	nic.ar	920	228	290	High PQ latency relative to DHQ and DTQ
ISRAEL	ControlD	sina.com.cn	279	-	1106	DTQ latency spike
ISRAEL	ControlD	nic.ar	1102	-	764	Plain query result is null

[author's development]

However, during the testing of the first iteration of the system, the model exhibited hyperfocusing behavior, which was particularly evident in cases where clusters of anomalies of a similar type were present. Specifically, across multiple entries corresponding to different geographic locations and DNS servers, the occurrence of an extreme latency value for a single protocol in consecutive records frequently led the model to classify all such entries as a "latency spike in singular protocol", without sufficiently accounting for the behavior of other latency metrics within the entries. In other cases, the system classified "no response" events as anomalies even when it is specified that the queried server does not support the corresponding protocol. This behavior was present when such entries were located adjacent to records representing genuine request failures. These observations indicate that local contextual similarity and perceived continuity of patterns may override rule-based distinctions, causing the model to generalize its interpretation across neighboring cases, even when such generalization contradicts explicit domain constraints or results in the neglect of other relevant data attributes.

Additional evidence of this behavior includes anomaly comments such as "DTQ = 0" in cases where other latency metrics were also outside of normal ranges. Similarly, a substantial number of comments focused exclusively on a single metric, despite the presence of multiple anomalous indicators within the same record, suggesting an excessive emphasis on isolated extreme parameters.

To address this issue, a new set of implicit instructions was introduced, encouraging the model to pay closer attention and to slow its judgment when processing clusters of similar anomalies. The goal of this modification was to prompt the model to consider the broader context of latency metrics within each observation, rather than fixating on a single extreme value, thereby reducing the risk of hyperfocusing on one aspect of an entry and potentially overlooking other relevant data or producing false positives.

Following the introduction of these instructions, a notable change in the structure and content of comments for anomalous entries was observed. Instead of concise, single-factor classifications such as "Plain query latency spike" or "DoH query time is 0", the model began producing more comprehensive and comparative descriptions. For instance, entries previously labeled solely as "Plain query latency spike" were subsequently described using more nuanced formulations, such as "Plain query latency spike, DoH query latency within norms". Likewise, cases involving zero or extreme values began to incorporate explicit comparisons with other latency metrics, for example, "Zero DoT query latency with high plain query latency".

Overall, this shift in the model's commentary indicates that the implemented measures were effective in mitigating hyperfocusing behavior. The revised system demonstrates a more coherent interpretation of anomalous DNS latency cases, reducing the likelihood of single-metric bias and contributing to more accurate, context-aware, and analytically informative anomaly detection outcomes.

Conclusions. 1. Experimental modeling of a software tool for comprehensive DNS traffic monitoring was conducted using the concept of case-based reasoning (CBR) as the foundation of the procedural AI paradigm. Its suitability for increasing the transparency of behavioral traffic anomaly detection was confirmed. The

modeling results indicate that the CBR approach improves the correlation of new observations with the existing knowledge base, thereby expanding the capabilities for reverse auditing of AI decision logic and increasing the degree of validation of the decisions (AI system responses) made.

2. The implementation of CBR enhances the transparency, consistency, and adaptability of artificially synthesized decisions and makes the behavioral logic of AI systems more aligned with the traditional logic of human reasoning.

3. The experimental system successfully augmented the initial precedent table with new information on anomalies. The ability to detect both predefined categories of anomalies and additional (previously unspecified) irregularities in the monitored data was confirmed. The applied data processing algorithm enables interpretation of monitoring results beyond explicitly defined examples, while preserving and considering the logic of causal relationships among observed events, based on information from formalized case pattern templates.

4. During the modeling process, limitations of the applied approach were identified. The experimental AI system exhibited a property of "clustering of its own interpretations". This may lead to incorrect interpretation of processes and, consequently, to false positive detections. The effect manifests in cases where similar anomalous records are located in close proximity to one another (record clusters). In such situations, the logic of contextual similarity dominates over explicit protocol constraints. As a compensatory measure, a new set of constraints (direct-action instructions) was introduced. Subsequent testing confirmed that these changes reduced the manifestation of the identified effect, thereby increasing the reliability of anomaly interpretation.

5. The obtained modeling results allow the conclusion that "the logic of AI systems is not something uniquely inherent and unconditionally axiomatic". In this context, it is necessary to consider the intrinsic tendency of AI systems toward self-optimization in the process of solving assigned tasks. This specific "tendency" requires the introduction of additional instructions and explicit prohibitions. A key prerequisite for the proper implementation of such restrictive and controlling measures is the ability to perform inverse auditing of the logic behind AI decision-making.

6. Further research directions should include: - improvement of mechanisms for moderating the precedent registry; - scaling the CBR paradigm to all components of the cloud-based DNS traffic monitoring system; - expansion of system capabilities with respect to the variability of monitoring scenarios and the structure of test queries in order to improve the detection of new anomalies.

References:

[1] Коробейнікова, Т., & Федчук, Т. (2024). Огляд протоколів DNS, DoT та DoT. Débats scientifiques et orientations prospectives du développement scientifique. European Scientific Platform. https://doi.org/10.36074/logos-01.03.2024.056.

[2] Чепель, Д., & Малахов, С. (2024). Узагальнення напрямів фільтрації DNS трафіку як складової безпеки сучасних інформаційних систем. Computer Science and Cybersecurity, (1), 6–21. https://doi.org/10.26565/2519-2310-2024-1-01.

[3] Чепель, Д., & Малахов, С. (2025). Мультипротокольний моніторинг трафіку DNS, як основа для коригування поточних параметрів RPZ. Theoretical and practical aspects of modern scientific research. European Scientific Platform. https://doi.org/10.36074/logos-24.01.2025.049.
[4] Ali, B., & Chen, G. (2025). Next-generation AI for advanced threat detection and security enhancement in DNS over HTTPS. Journal of Network and Computer Applications, 244, 104326. https://doi.org/10.1016/j.jnca.2025.104326.
[5] Chepel, D., & Malakhov, S. (2025). Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. Modern Information Security, 63(3), 176–187. https://doi.org/10.31673/2409-7292.2025.031949.
[6] Hatalis, K., Kondapalli, V., & Christou, D. (2025). Review of case-based reasoning for LLM agents: Theoretical foundations, architectural components, and cognitive integration. arXiv. https://doi.org/10.48550/arXiv.2504.06943.
[7] Inala, J. P., Wang, C., Drucker, S., Ramos, G., Dibia, V., Riche, N., Brown, D., Marshall, D., & Gao, J. (2024). Data analysis in the era of generative AI. arXiv. https://doi.org/10.48550/arXiv.2409.18475.
[8] Pradeep, P., Caro-Martínez, M., & Wijekoon, A. (2024). A practical exploration of the convergence of Case-Based Reasoning and Explainable Artificial Intelligence. Expert Systems With Applications, 124733. https://doi.org/10.1016/j.eswa.2024.124733.
[9] Pradeep, P., Caro-Martínez, M., & Wijekoon, A. (2025). Empowering explainable artificial intelligence through case-based reasoning: A comprehensive exploration. IEEE Transactions on Knowledge and Data Engineering, 1–20. https://doi.org/10.1109/tkde.2025.3609825.
[10] Rahmani, A. M., Azhir, E., Ali, S., Mohammadi, M., Ahmed, O. H., Yassin Ghafour, M., Hasan Ahmed, S., & Hosseinzadeh, M. (2021). Artificial intelligence approaches and mechanisms for big data analytics: A systematic study. PeerJ Computer Science, 7, Article e488. https://doi.org/10.7717/peerj-cs.488.
[11] Safitra, M. F., Lubis, M., Kusumasari, T. F., & Putri, D. P. (2024). Advancements in artificial intelligence and data science: Models, applications, and challenges. Procedia Computer Science, 234, 381–388. https://doi.org/10.1016/j.procs.2024.03.018.
[12] Zebin, T., Rezvy, S., & Luo, Y. (2022). An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks. IEEE Transactions on Information Forensics and Security, 1. https://doi.org/10.1109/tifs.2022.3183390.

МУЛЬТИБАЗОВИЙ ХМАРНИЙ МОНІТОРИНГ DNS-ТРАФІКУ НА ОСНОВІ ПРЕЦЕДЕНТНОГО АНАЛІЗУ АНОМАЛІЙ DNS ПРОТОКОЛІВ

Чепель Данило Олександрович
аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В.Н. Каразіна, Україна
Малахов Сергій Віталійович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

Анотація. *У статті наведено результати експериментального дослідження програмного інструменту для аналізу даних DNS-трафіку із залученням ШІ на основі підходу прецедентного аналізу. З метою підвищення прозорості, надійності та простежуваності результатів аналізу тестових вимірювань із використанням ШІ було*

інтегровано методи прецедентного аналізу. Експериментальний прототип реалізовано у вигляді Python-клієнта, інтегрованого з Gemini API, який працює з набором даних, отриманим із попередніх досліджень, що забезпечує безперервність і порівнянність результатів. Система використовує визначений вручну початковий набір прецедентів і автономно розширює його шляхом додавання нових аномальних випадків із пояснювальними коментарями. Результати експериментів демонструють, що запропонований механізм підтримує як цільове виявлення аномалій, так і виявлення загальних відхилень у даних. Отримані результати підтверджують доцільність використання прецедентного підходу для підвищення прозорості та простежуваності аналізу DNS-трафіку із залученням ШІ. Водночас експерименти виявили ефекти кластеризації, які можуть призводити до хибних позитивних результатів та неправильного трактування даних, що зумовило перегляд обмежень аналізу. Подальша оцінка підтвердила, що внесені зміни зменшили виявлений ефект і підвищили надійність інтерпретації аномалій.

Ключові слова: *DNS; RPZ; ШІ; CBR; кібербезпека; фільтрація трафіку; мережеві аномалії; прецедентний аналіз; хмарний моніторинг; мультибазовий моніторинг; аналіз даних.*