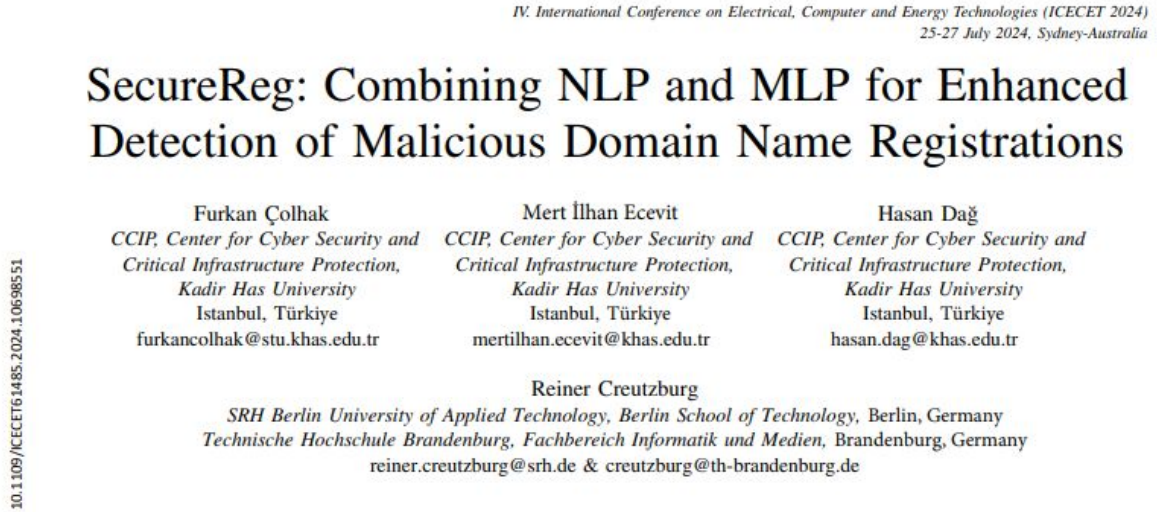
# ICANN81 Techday

81 ANNUAL GENERAL MEETING

## •AI techniques in DNS Abuse Mitigation


- Furkan Çolhak*[1], Mert İlhan Ecevit[1], Hasan Dağ[1] ,and Reiner Creutzburg[2,3]
- Affiliation:
  - [1] Kadir Has University , CCIP, Center for Cyber Security and Critical Infrastructure Protection
  - [2] SRH Berlin University of Technology,Berlin School of Technology, Berlin, Germany
  - [3] Technische Hochschule Brandenburg, Department of Informatics and Media, Brandenburg, Germany

# Presentation Background



IV. International Conference on Electrical, Computer and Energy Technologies (ICECET 2024)
25-27 July 2024, Sydney-Australia

SecureReg: Combining NLP and MLP for Enhanced Detection of Malicious Domain Name Registrations

Furkan Çolhak
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Türkiye
furkancolhak@stu.khas.edu.tr

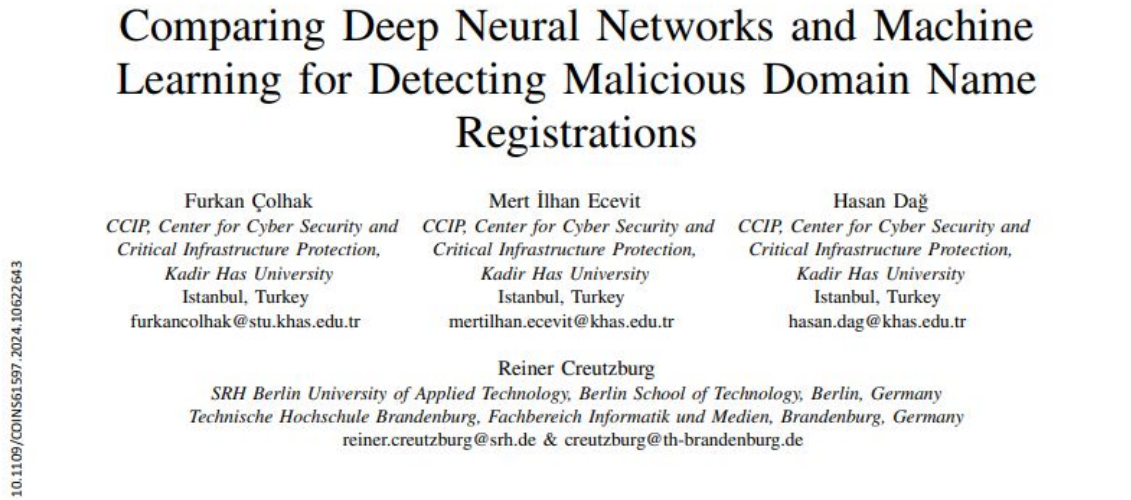
Mert İlhan Ecevit
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Türkiye
mertilhan.ecevit@khas.edu.tr

Hasan Dağ
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Türkiye
hasan.dag@khas.edu.tr

Reiner Creutzburg
*SRH Berlin University of Applied Technology, Berlin School of Technology,* Berlin, Germany
*Technische Hochschule Brandenburg, Fachbereich Informatik und Medien,* Brandenburg, Germany
reiner.creutzburg@srh.de & creutzburg@th-brandenburg.de

10.1109/ICECET61485.2024.10698551

[1] F. Çolhak, M. İ. Ecevit, H. Dağ and R. Creutzburg, "SecureReg: Combining NLP and MLP for Enhanced Detection of Malicious Domain Name Registrations," *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*, Sydney, Australia, 2024, pp. 1-6, doi: 10.1109/ICECET61485.2024.10698551.



Comparing Deep Neural Networks and Machine Learning for Detecting Malicious Domain Name Registrations

Furkan Çolhak
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Turkey
furkancolhak@stu.khas.edu.tr

Mert İlhan Ecevit
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Turkey
mertilhan.ecevit@khas.edu.tr

Hasan Dağ
*CCIP, Center for Cyber Security and Critical Infrastructure Protection, Kadir Has University*
Istanbul, Turkey
hasan.dag@khas.edu.tr

Reiner Creutzburg
*SRH Berlin University of Applied Technology, Berlin School of Technology, Berlin, Germany*
*Technische Hochschule Brandenburg, Fachbereich Informatik und Medien, Brandenburg, Germany*
reiner.creutzburg@srh.de & creutzburg@th-brandenburg.de

10.1109/COINS61597.2024.10622643

[2] F. Çolhak, M. İ. Ecevit, H. Dağ and R. Creutzburg, "Comparing Deep Neural Networks and Machine Learning for Detecting Malicious Domain Name Registrations," *2024 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, London, United Kingdom, 2024, pp. 1-4, doi: 10.1109/COINS61597.2024.10622643.

# Agenda

- Introduction: Domain Abuse
- Existing Solutions
- Requirements and Research Objective
- Proposed Approach
- Methodology
- Results and Discussion
- Conclusions and Future Works

# Introduction

The Domain Name System (DNS) is essential for converting human-readable domain names into IP addresses, making it a **vital part of internet infrastructure**[3].

However, its significance also makes it a **prime target** for cyberattacks [4]**. AI-driven applications** in **DNS security** play a crucial role in protecting this infrastructure from various threats, including:

- Cache poisoning
- Distributed Denial of Service (DDoS) attacks
- DNS hijacking
- DNS tunneling
- **Domain Abuse**

# Introduction (Cont'd)

**Domain Abuse** occurs when domain names are **registered for malicious activities** like **phishing**, **scams**, and **malware** distribution [5].

ICANN's **Domain Abuse Activity Reporting (DAAR) System** tracks various types of domain abuse, identifying security threats like financial losses, scams, and data breaches, particularly affecting generic Top-Level Domains (gTLDs) and highlighting the severe impact of DNS abuse on internet security [6].

**AI in DNS Security: Domain Abuse**

- **Domain Analysis:** AI algorithms analyze domain registration data to detect potential threats.
- **Pattern Recognition:** Natural Language Processing (NLP) and Machine Learning (ML) are employed to identify suspicious patterns.
- **Prevention Measures:** These technologies help prevent domains from being used for phishing, malware distribution, and botnet operations.

# Existing Solutions

| Registry | System | Method | Focus | Limitations |
|---|---|---|---|---|
| ***EURid (.eu)*** | Premadoma [7] | Machine Learning | Large-scale malicious campaigns | Limited detection for single suspect domains |
| ***DNS Belgium (.be) & SWITCH (.ch, .li)*** | - [8] | Static Rules-Based | Potentially malicious registrations | Limited customization; exploring machine learning |
| ***Nominet (.uk)*** | Domain Watch [9] | Not Disclosed | Phishing scams; suspends suspicious domains post-registration | Limited public information available |
| ***SIDN (.nl)*** | RegCheck [8] | Logistic Regression | Assigns weights to risk factors for risk scoring | Performance limitation 47.8% recall and 22.08% precision. |

Table I: Existing Solutions Summary

# Requirements and Objective of Study

**System Requirements for DNS Abuse Detection:**

1. **Accuracy:** The system must prioritize accuracy to minimize risks, effectively identifying malicious registrations while avoiding excessive false alarms.
2. **Simplicity:** Favor straightforward methods over complex models to ensure resource efficiency and ease of interpretation.
3. **Sustainability:** Models must be sustainable, adaptable to large, evolving TLD databases, with frequent, efficient retraining.

**Objective of Study:**

- Determine if Natural Language Processing (NLP) and pre-trained models can enhance DNS abuse detection.
- Compare deep neural network (DNN) models with simpler machine learning (ML) models.

# Proposed Approach

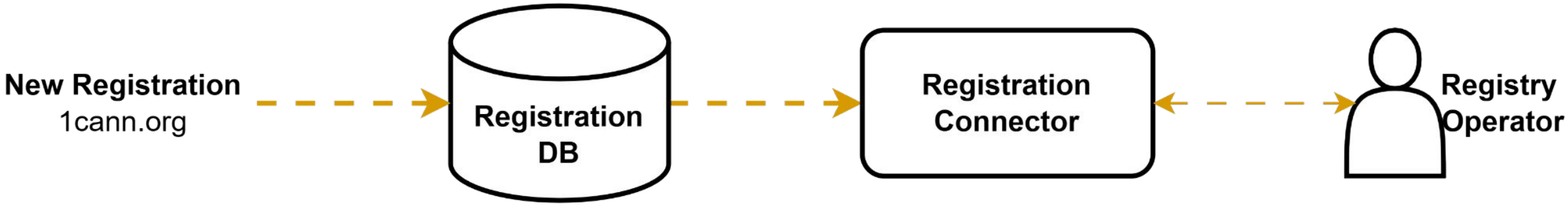



Figure 1: Registration System Overview [8]

# Proposed Approach (Cont'd)

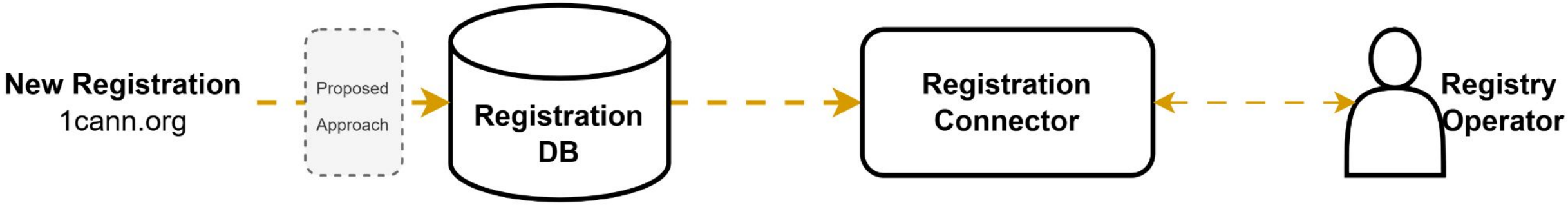



Figure 2: Registration System Overview [8] and Proposed Approach Location

# Proposed Approach (Cont'd)

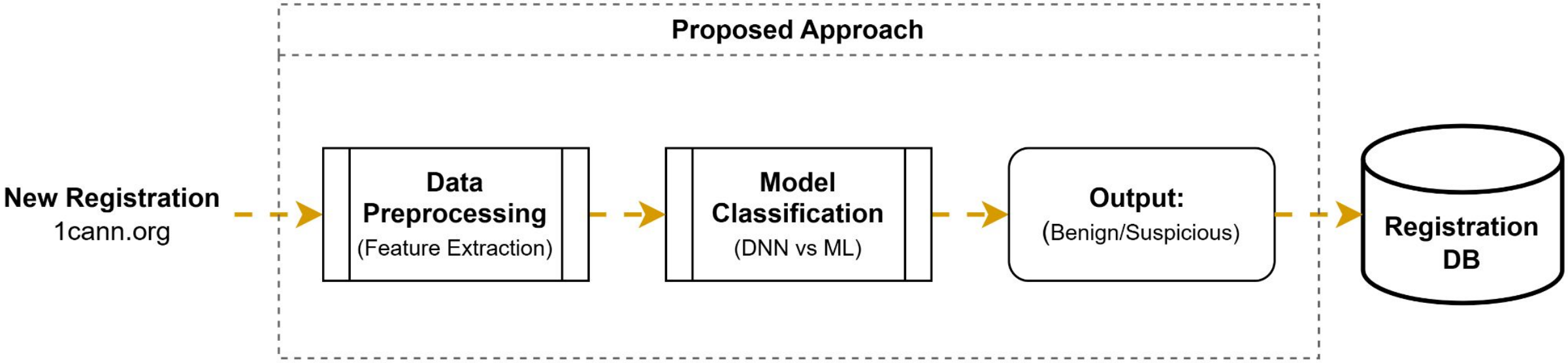



Figure 3: Proposed Approach Overview [1,2]

# Methodology: Dataset

**Dataset Overview:**

- **Sources:** Benign URLs from Alexa (top 2000 + random) and malicious URLs from OpenPhish.
- **Composition:** 50,000 benign and 50,000 malicious URLs (MTLP Dataset on Google Drive [9]).

**Preprocessing Steps:**

1. Parse URLs to isolate domain names.
2. Exclude TLDs, subdomains, protocols, file paths.
3. Ensure unique domain names (drop duplicates).

- **Final Dataset Size:** 36,848 benign and 28,747 malicious domain names.
- **Visualization:** Fig. 2 shows domain name feature extraction.


Figure 2: Domain name extraction

**Feature Extraction:**

- **Textual Feature:** Domain name (F1) serves as the primary feature (see Fig. 1).
- **Numeric Features:** Derived from domain names, including:
  - Total length (F2), Special character count (F3), Digit count (F4)
  - Entropy (F5), Vowel-to-consonant ratio (F6)
  - Digit-to-character ratio (F7), Special character-to-character ratio (F8)

# Model Methodology

Figure. 4 illustrating the methodologies of Machine Learning and Deep Neural Networks which applied in this study.

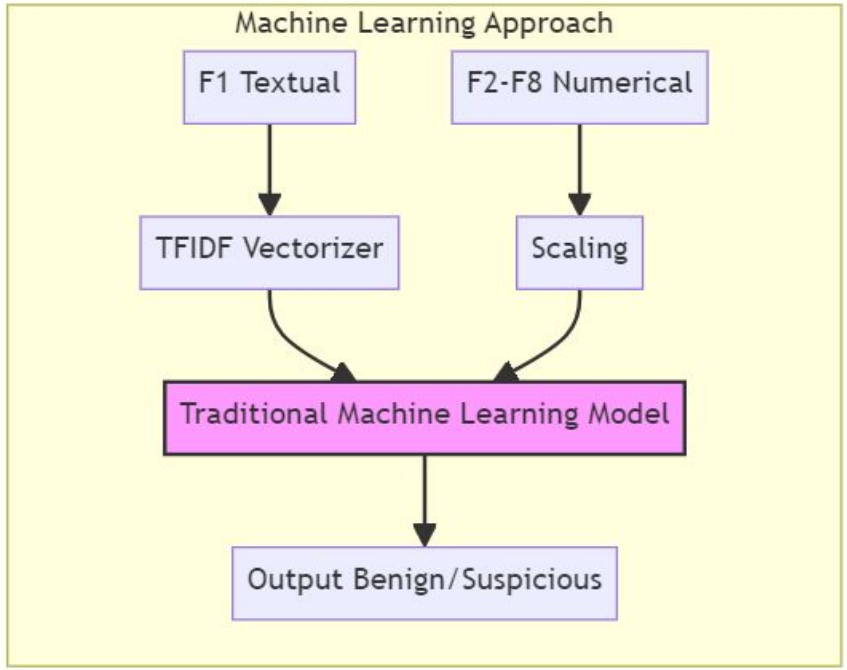
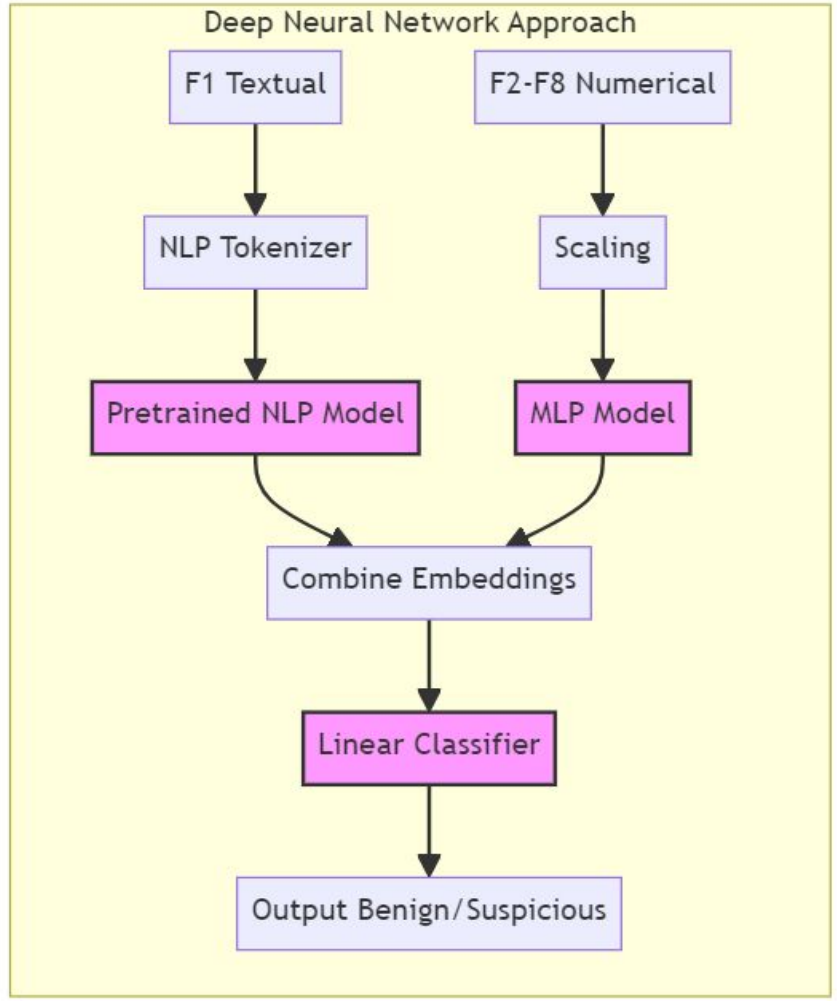



Figure 4: Model Methodology [2] for DNN vs ML



# Model Results

| | Models | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) | Training Time | Model Size (mb) |
|---|---|---|---|---|---|---|---|
| DNN | **Canine + MLP** | **85.81** | **91.14** | 82.31 | **86.46** | **9m 51s** | 1428.76 |
| | BERT + MLP | 83.61 | 86.19 | 83.72 | 84.85 | 20m 22s | 1259.44 |
| | RoBERTa + MLP | 84.37 | 87.08 | **84.24** | 85.55 | 27m 55s | 1433.30 |
| | ALBERT + MLP | 84.90 | 88.04 | 84.16 | 85.95 | 29m 44s | **140.02** |
| | MobileBERT + MLP | 84.42 | 88.73 | 82.27 | 85.32 | 24m 1s | 288.79 |
| ML | RF + (TFIDF) | 82.77 | 84.48 | 82.77 | 82.77 | 0m 6s | 13.74 |
| | **SVM + (TFIDF)** | **83.84** | **86.12** | **83.84** | **83.82** | 4m 6s | 715.43 |
| | KNN + (TFIDF) | 80.83 | 82.89 | 80.83 | 80.81 | **0m 2s** | 944.71 |
| | XGB + (TFIDF) | 83.04 | 84.78 | 83.04 | 83.04 | 0m 15s | 0.59 |
| | LR + (TFIDF) | 83.74 | 85.90 | 83.74 | 83.72 | 0m 8s | **0.05** |

Table 2: Model Results with metrics based on DNN vs ML [2]

# Results and Discussion

| Requirements | DNN | ML | Observation |
|---|---|---|---|
| ***Accuracy:*** **F1-Score (%)** | CANINE: 86.46%<br>ALBERT: 85.95% | SVM: 83.82%<br>LR: 83.72% | DNN models show 3% higher accuracy than ML models. |
| ***Simplicity:*** ***Model Size (mb)*** | ALBERT: 140mb<br>MobileBERT: 288mb | XGB:0.59mb<br>LR: 0.05mb | ML models is significantly lighter than any DNN. |
| ***Sustainability:*** ***Training Time (sec)*** | CANINE: 591 sec<br>BERT: 1222 sec | KNN:0.2sec<br>RF:0.6sec<br>LR:0.8sec | Logistic Regression trains ~73x faster than CANINE. |

Table 3: Results for each requirements based on DNN vs ML

# Conclusions and Future Works

This presentation builds upon our previous research [1, 2], focusing on AI techniques for mitigating DNS abuse. We have reviewed existing solutions and identified their requirements and limitations, proposing the use of NLP to address these challenges. Given the complexity of **pretrained NLP (DNN)**, it requires computational efficiency, so we compared it with **simpler machine learning** models.

The key trade-off lies between **accuracy**, **simplicity**, and **sustainability**. While DNN models offer higher accuracy, they require more resources, larger models, and longer training times. They are ideal when accuracy is critical and resources are available. In contrast, ML models are faster, more resource-efficient, and suitable for real-time detection.

Ultimately, the choice of model depends on the specific needs and resource constraints of DNS registries, balancing lightweight models with sufficient accuracy.

**Future Work:** Our future research will focus on optimizing these models for real-time detection in real DNS registries with real data. We aim to refine and enhance the models for practical application, ensuring a balance between accuracy, efficiency, and scalability.

# References


**[1]** F. Çolhak, M. İ. Ecevit, H. Dağ and R. Creutzburg, "SecureReg: Combining NLP and MLP for Enhanced Detection of Malicious Domain Name Registrations," *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*, Sydney, Australia, 2024, pp. 1-6, doi: 10.1109/ICECET61485.2024.10698551.

**[2]** F. Çolhak, M. İ. Ecevit, H. Dağ and R. Creutzburg, "Comparing Deep Neural Networks and Machine Learning for Detecting Malicious Domain Name Registrations," *2024 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, London, United Kingdom, 2024, pp. 1-4, doi: 10.1109/COINS61597.2024.10622643.

**[3]** FasterCapital. (n.d.). Domain Name System (DNS) and IPi: Understanding the Connection. Retrieved July 29, 2024, from https://fastercapital.com/content/Domain-Name-System--DNS-and-IPi--Understanding-the-Connection.html

**[4]** CSC Digital Brand Services. Domain Security Report. https://www.cscdbs.com/en/resources-news/domain-security-report/, 2024. Accessed: November, 2024.

**[5]** Hao, Shuang, et al. "PREDATOR: proactive recognition and elimination of domain abuse at time-of-registration." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

**[6]** ICANN. ICANN DAAR - domain abuse activity reporting, 2024. Accessed: November, 2024.

**[7]** L. Desmet, J. Spooren, T. Vissers, P. Janssen, and W. Joosen. Pre-madoma: An operational solution to prevent malicious domain name registrations in the .eu tld. Digital Threats: Research and Practice, 2(1):1–24, 2021.

**[8]** SIDN Labs. Assessing the Risk of New .nl Registrations Using RegCheck. https://www.sidnlabs.nl/en/news-and-blogs/ assessing-the-risk-of-new-nl-registrations-using-regcheck, 2023. Accessed: November 2024.

**[9]** Nominet. Domain Watch. https://registrars.nominet.uk/uk-namespace/ security-tools-and-protection/domain-watch/. Accessed: 9 July, 2023.

# THANK YOU FOR YOUR LISTENING.
# (Q&A)