# A Hybrid Deep Learning Framework For Detecting Phishing Websites

Yash V Nadkarni
H00410472 | yvn2000@hw.ac.uk
BSc (Hons) Computer Science (Cyber Security)
Heriot-Watt Univeristy, Dubai

Supervisor: Dr. Md Azher Uddin
18th November 2025

# Presentation Structure

1. **Introduction**
    - Background
    - Motivation
2. **Existing Studies**
    - List-Based
    - Heuristics-Based
    - Visual Similarity-Based
    - Machine Learning-Based
    - Deep Learning-Based
3. **Proposed Framework**
4. **Evaluation**
5. **Project Plan**

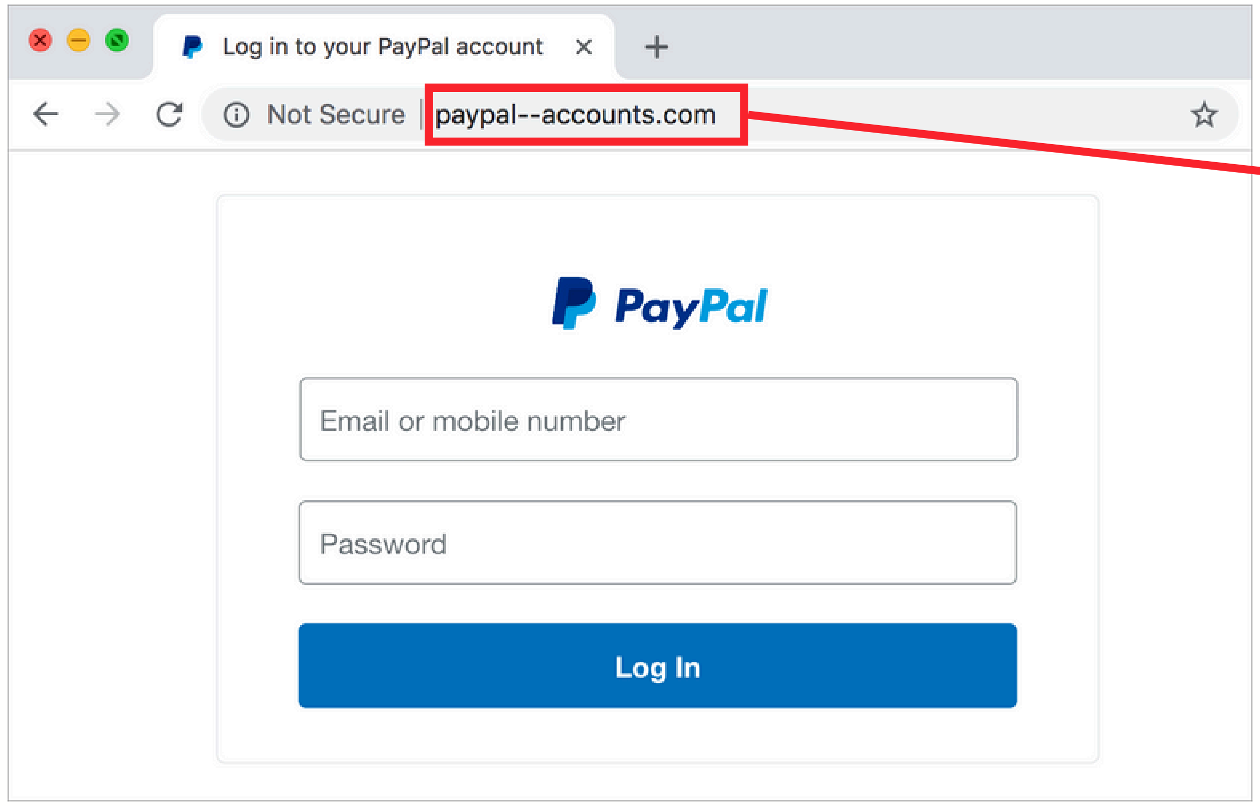
Introduction

# Background

1
2
3
4
5

Phishing is the practice of masquerading malicious websites as legitimate.

- Purpose is to exploit user trust to steal personal information. [1]




Phished Website URL!

- Similar layout, color schemes, etc BUT different URL! [2]
- Modern attacks create more dynamic and sophisticated phishing URLs. [3]

1

2

3

4

5

Introduction

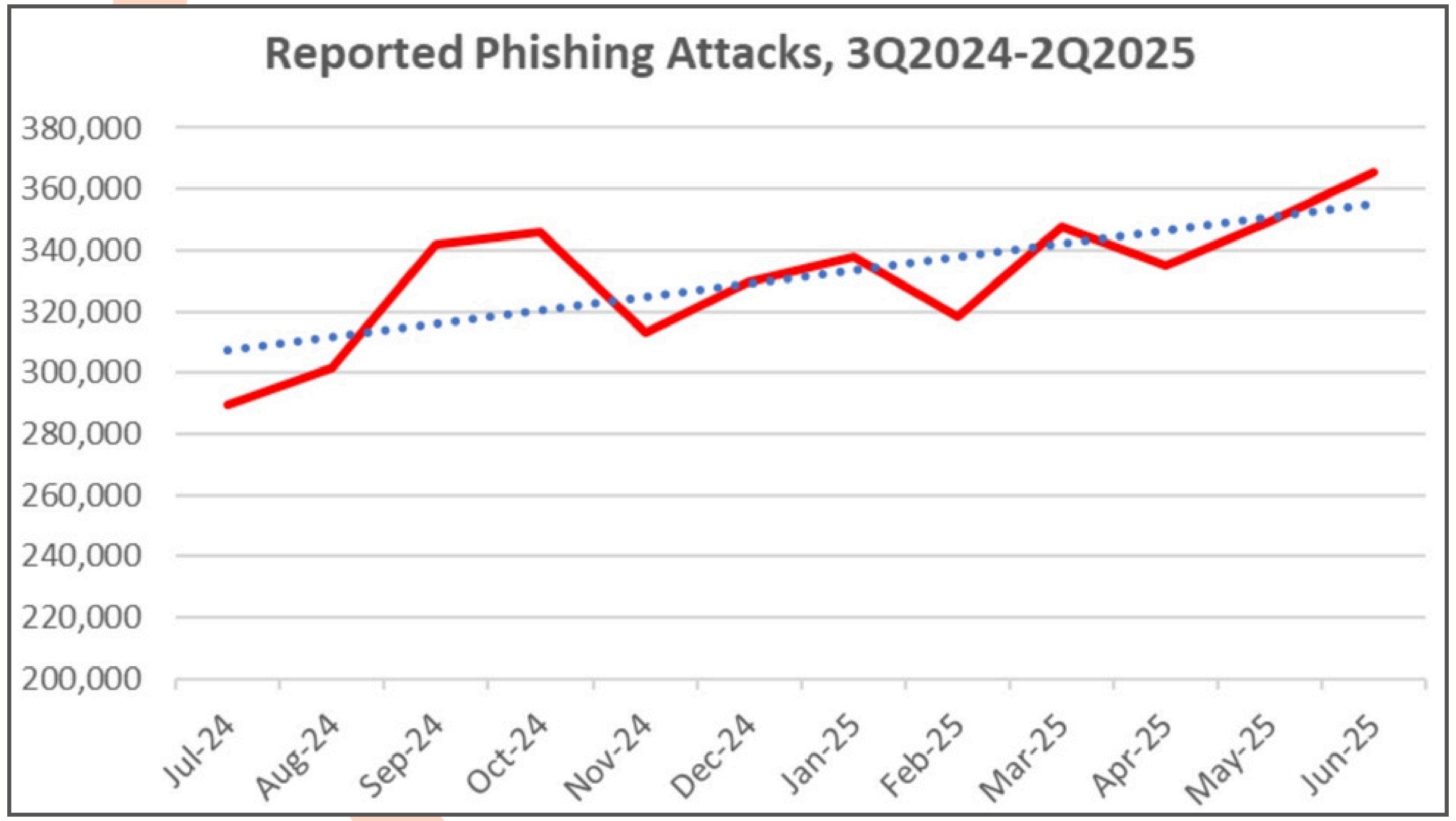
# Motivation

### Phishing Activity Trends Report 2025 [4]

- 2 Million attacks in first half of 2025.
- Finance, Healthcare, Education and several more sectors targeted.

### Limitations of Traditional Systems

- Struggle to keep up with evolving techniques
- Zero-Day Attacks [5]
- Existing models do not capture lexical patterns and temporal dependencies
    - Proposed Hybrid Framework




Phishing Activity Trends Report for 2025 from Anti-Phishing Working Group [4]

1

2

3

4

5

Existing Works

# List-Based Systems

## Whitelists [6]

- Stores and grants access only to proven legitimate websites
- Limitation: Needs to be constantly updated

## Blacklists [5]

- Denies access to stored proven malicious websites
- Limitation: Vulnerable against Zero-Day Attacks

Existing Works

# Heuristics-Based Systems

- Analyzes technical features and attributes to make predictions [7]
- Works against Zero-Day attacks [8]
- Limitation: Relies on pre-determined algorithms, no learning involved to increase adaptability

Existing Works

# Visual Similarity-Based Systems

- Analyzes screenshots to form predictions
- Extracts layouts and color schemes [9]
- Limitation: Requires significant computation power
- Limitation: Bad layouts can cause large rate of false negatives

Existing Works

# Machine Learning-Based Systems

- Adaptive detection systems that identify patterns and relations from data through different learning techniques to form distinctions.

| Study | Model | Accuracy |
|---|---|---|
| [10] | J48 Decision Tree | 93% |
| [11] | Random Forest | 98.40% |
| [12] | Random Forest | 97.30% |
| [13] | Random Forest | 99.06% |
| [14] | Multilayered Stacked Ensemble Model | 98.90% |
| [15] | GA-based XGBoost | 98.57% |

- **Observations**
  - Strong baseline accuracies
  - Limitation: Relies heavily on strong feature quality. Cannot discover deep hidden patterns from raw data.

1

2

3

4

5



# Deep Learning-Based Systems

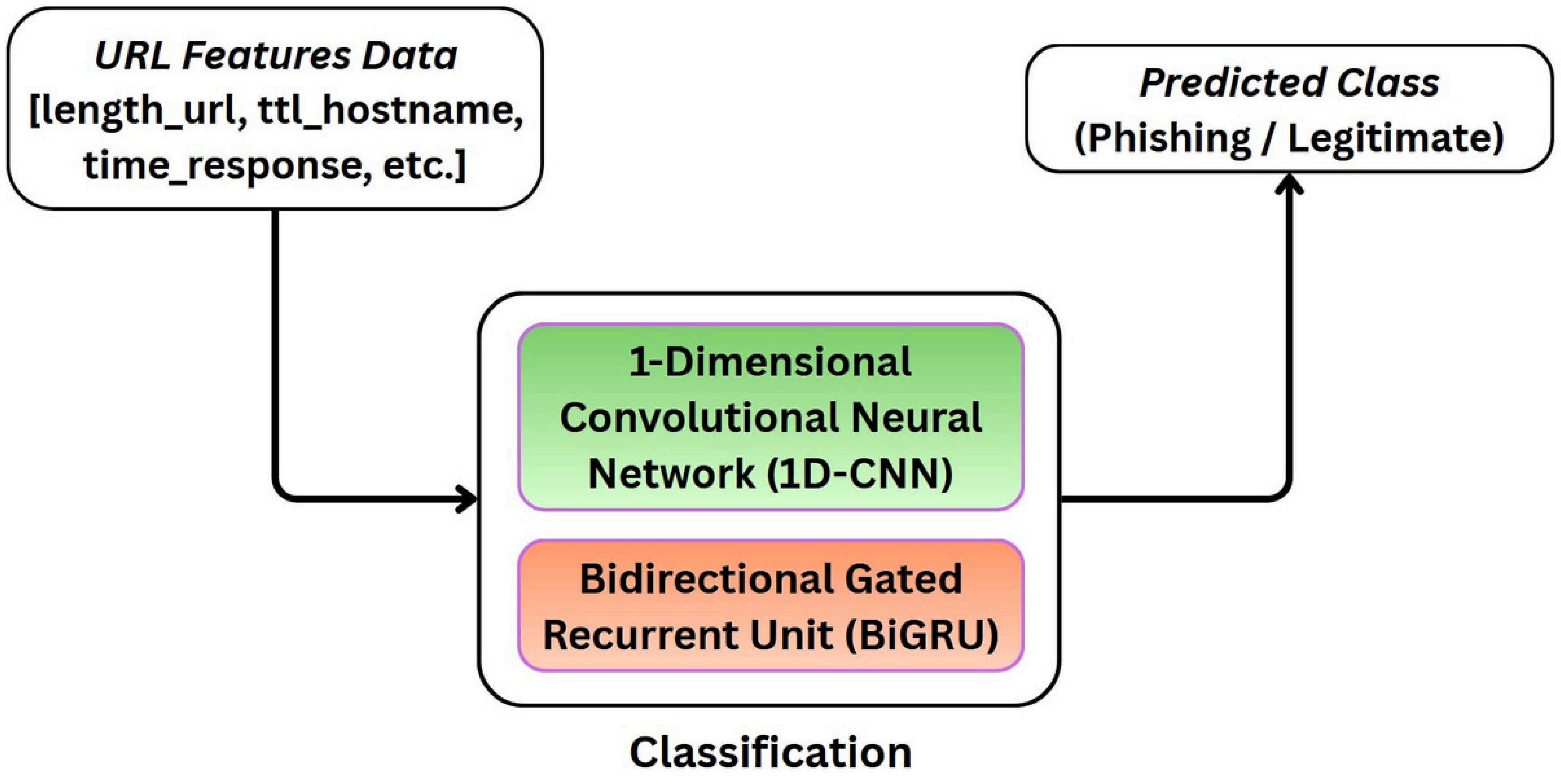
- Form of machine learning that automatically learns hierarchical representations from data to capture complex relationships.

| Study | Model | Accuracy |
|---|---|---|
| [16] | CNN | 99% |
| [17] | CNN | 99.20% |
| [18] | RNN-GRU | 99.18% |

- **Observations**
  - CNNs outperform ML models and other DL models
  - CNNs capture lexical and spatial patterns only.
  - GRU captures temporal dependencies.
  - Employment of GRU increased performance of RNN from 74% to 99.18%.
  - **Gap**: Need for hybrid model that captures both spatial patterns and temporal dependencies.

1
2
3
4
5

# Proposed Hybrid Framework




- 1D-CNN captures spatial patterns from URL's local lexical features
- BiGRU models the sequential relations, learning dependencies from both directions of the URL.

# Evaluation

- **Datasets**
  - UCI 2015 Dataset [19]
    - 11,055 Websites (4,898 Phishing, 6,157 Legitimate)
    - 31 handcrafted features
  - Mendeley 2020 Dataset [20]
    - 88,647 Websites (30,647 Phishing, 58,000 Legitimate)
    - 111 lexical features

- **Evaluation Metrics**

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

1

2

3

4

5



# PLES Considerations

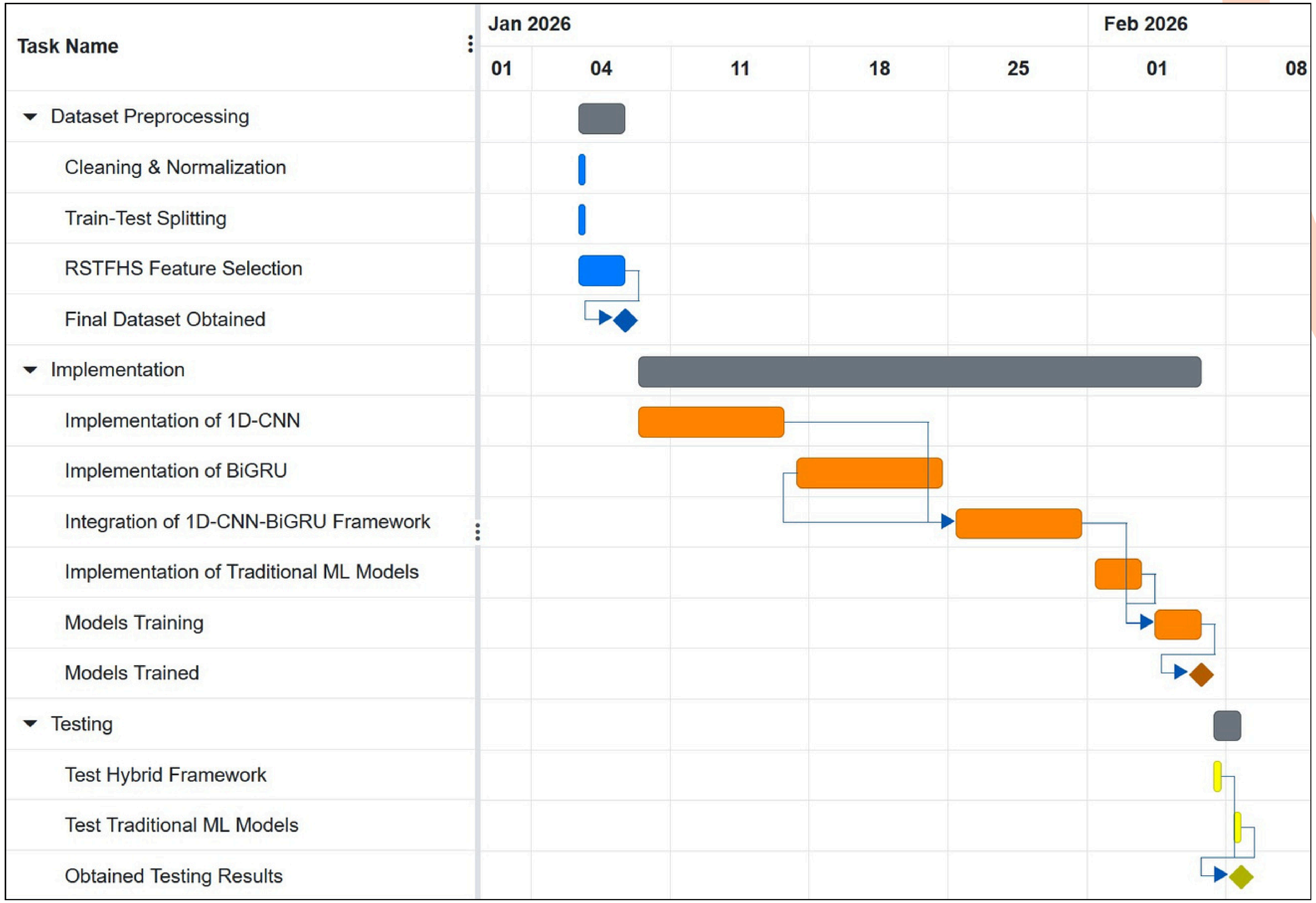
- **Professional**
  - Project adheres to recognized professional standards and principles.
- **Legal**
  - Project complies with relevant data protection regulation.
- **Ethical**
  - Project only uses public technical data, with no user-specific participation or information.
- **Social**
  - Project contributes positively to societal efforts against phishing without pertaining to any other broader social issue.

## Implementation Environment

- Windows 11
- AMD Ryzen 9 5900HX
- NVIDIA GeForce RTX 3050 Ti (4 GB VRAM)
- 32 GB RAM
- 100 GB SSD

# Project Plan

- **Implementation Gantt Chart**



1

2

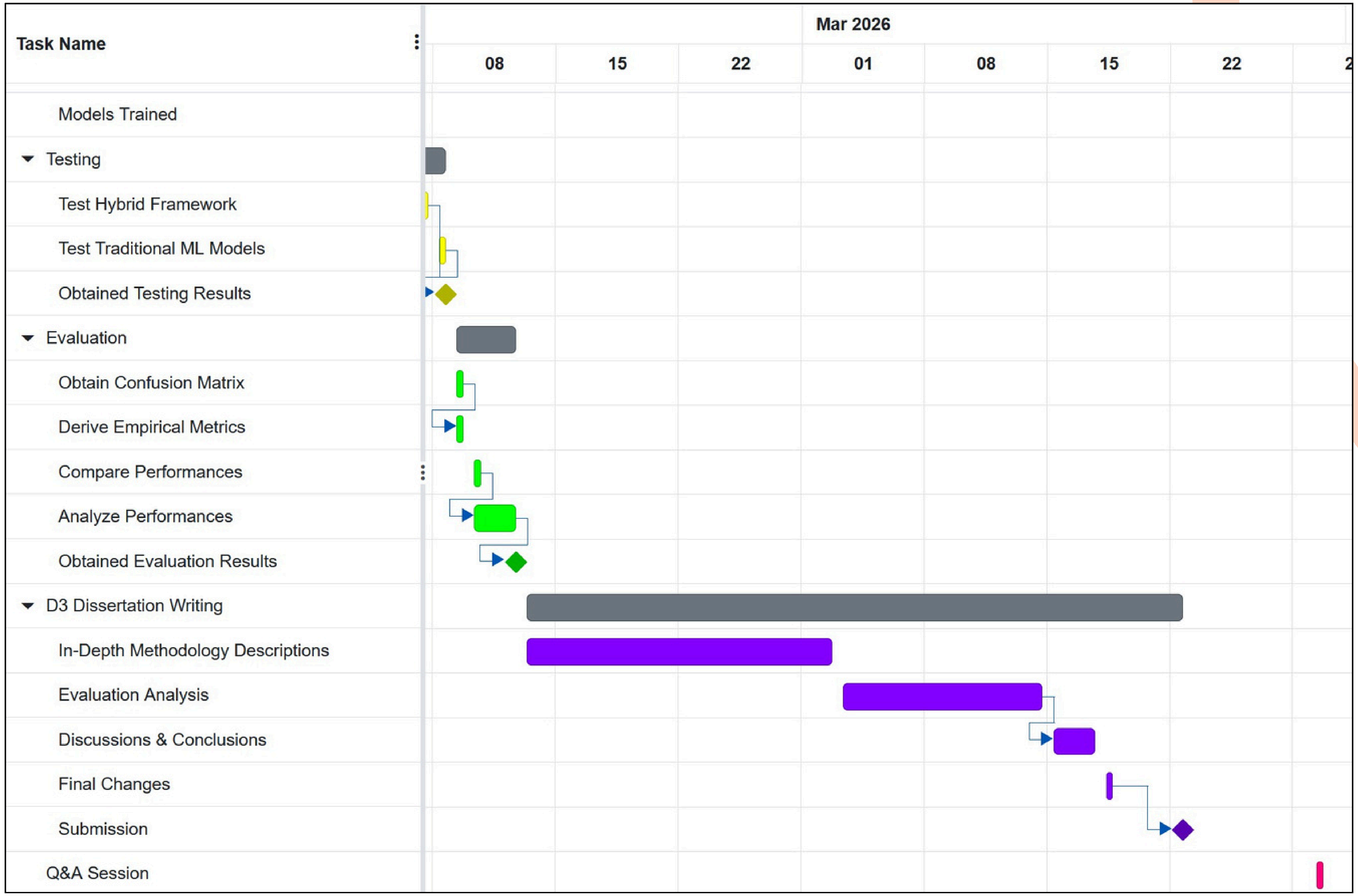
3

4

5

# Project Plan

- **Evaluation & Documentation Gantt Chart**



# Project Plan

- **Major Risks**

1
2
3
4
5

| Risk | Likelihood | Mitigation |
|---|---|---|
| System Failure | Unlikely | Make cloud based backup saves |
| Data Corruption | Unlikely | Make regular local backups |
| Low Performance of Hybrid Framework | Likely | Extensive hyper-parameter tuning |
| Inconsistent Evaluation Results | Possible | Conduct multiple test runs |

# References


[1] A. Fedele, M. Tonin, and M. Valerio. 2024. Phishing attacks: An analysis of the victims' characteristics based on administrative data. Economics Letters 237 (2024), p.111663.

[2] O.K. Sahingoz, E. Buber, O. Demir, and B. Diri. 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications 117 (2019), pp.345–357.

[3] R. Zieni, L. Massari, and M.C. Calzarossa. 2023. Phishing or not phishing? A survey on the detection of phishing websites. IEEE Access 11 (2023), pp.18499–18519.

[4] Anti-Phishing Working Group. 2025. Phishing Activity Trends Report – 2nd Quarter 2025. Available at: https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf. (Accessed: 2025-10-16).

[5] M. Guo, G. Wang, H. Hata, and M.A. Babar. 2021. Revenue maximizing markets for zero-day exploits. Autonomous Agents and Multi-Agent Systems 35(2) (2021), p.36.

[6] Y. Cao, W. Han, and Y. Le. 2008. Anti-phishing based on automated individual white-list. In Proceedings of the 4th ACM workshop on Digital identity management. pp.51–60.

[7] Y. Zhang, J.I. Hong, and L.F. Cranor. 2007. Cantina: a content-based approach to detecting phishing web sites. In Proceedings of the 16th international conference on World Wide Web. pp.639–648.

[8] Kumar M. Kompella R.R. Prakash, P. and M. Gupta. 2010. Phishnet: predictive blacklisting to detect phishing attacks. In 2010 Proceedings IEEE INFOCOM. pp.1–5.

[9] A.K. Jain and B.B. Gupta. 2017. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks 2017(1) (2017), p.5421046.

[10] J. James, L. Sandhya, and C. Thomas. 2013. Detection of phishing URLs using machine learning techniques. In 2013 international conference on control communication and computing (ICCC). pp.304–309.

# References

[11] I. Tyagi, J. Shad, S. Sharma, S. Gaur, and G. Kaur. 2018. A novel machine learning approach to detect phishing websites. In 2018 5th International conference on signal processing and integrated networks (SPIN). pp.425–430.
[12] S. Alnemari and M. Alshammari. 2023. Detecting phishing domains using machine learning. Applied Sciences 13(8) (2023), p.4649.
[13] A. Almomani, M. Alauthman, M.T. Shatnawi, M. Alweshah, A. Alrosan, W. Alomoush, and B.B. Gupta. 2022. Phishing website detection with semantic features based on machine learning classifiers: a comparative study. International Journal on Semantic Web and Information Systems (IJSWIS) 18(1) (2022), pp.1–24.
[14] L.R. Kalabarige, R.S. Rao, A. Abraham, and L.A. Gabralla. 2022. Multilayer stacked ensemble learning model to detect phishing websites. IEEE Access 10 (2022), pp.79543–79552.
[15] M. Al-Sarem, F. Saeed, Z.G. Al-Mekhlafi, B.A. Mohammed, T. Al-Hadhrami, M.T. Alshammari, A. Alreshidi, and T.S. Alshammari. 2021. An optimized stacking ensemble model for phishing websites detection. Electronics 10(11) (2021), p.1285.
[16] N.F. Almujahid, M.A. Haq, and M. Alshehri. 2024. Comparative evaluation of machine learning algorithms for phishing site detection. PeerJ Computer Science 10 (2024), p.2131.
[17] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q.E.U. Haq, K. Saleem, and M.H. Faheem. 2023. A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Electronics 12(1) (2023), p.232.
[18] L. Tang and Q.H. Mahmoud. 2021. A deep learning-based framework for phishing website detection. IEEE Access 10 (2021), pp.1509–1521.
[19] R. Mohammad and L. McCluskey. 2015. Phishing Websites. UCI Machine Learning Repository. Available at: https://doi.org/10.24432/C51W2X. (Accessed: 2025-10-19).
[20] G. Vrbančič. 2020. Phishing Websites Dataset. Mendeley Data, V1. Available at: https://doi.org/10.17632/72ptz43s9v.1. (Accessed: 2025-10-19).

# Thank You