

Analysis of Different Machine Learning Models to Detect Phishing Websites

Tavin Thompson, Computer Science

Mentor: Professor Adwith Malpe, Assistant Professor
School of Computing and Augmented Intelligence



Background

Phishing scams are responsible for the greatest monetary and reputational losses, with over five million reports of phishing in 2023 alone. Limiting the success of these evolving scams is critical for national and economic security.

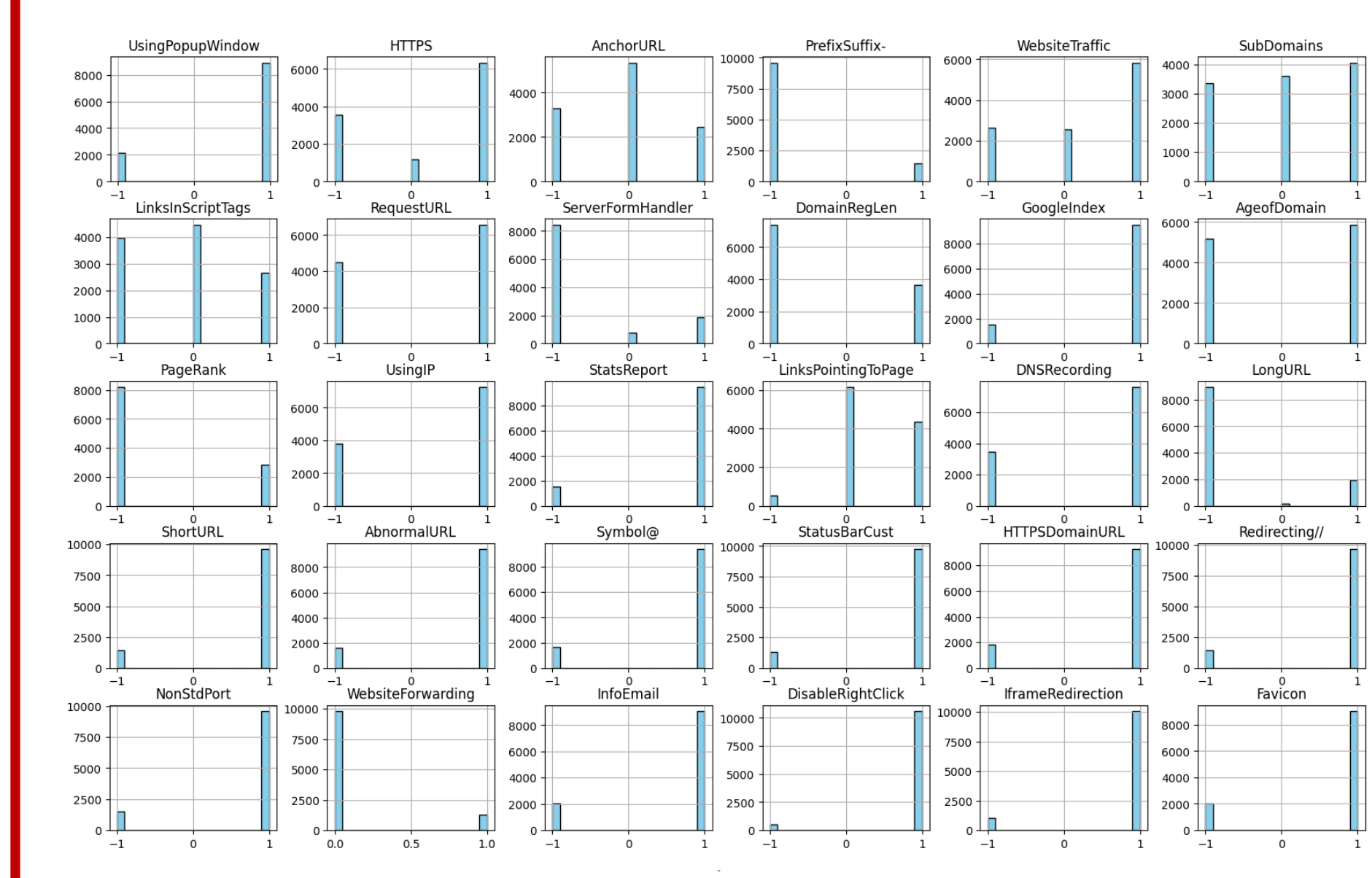
Findings

Deep Q-Networks are not great for classification as it relies on a reward structure that guides the learning process. In classification, there is no natural reward signal.

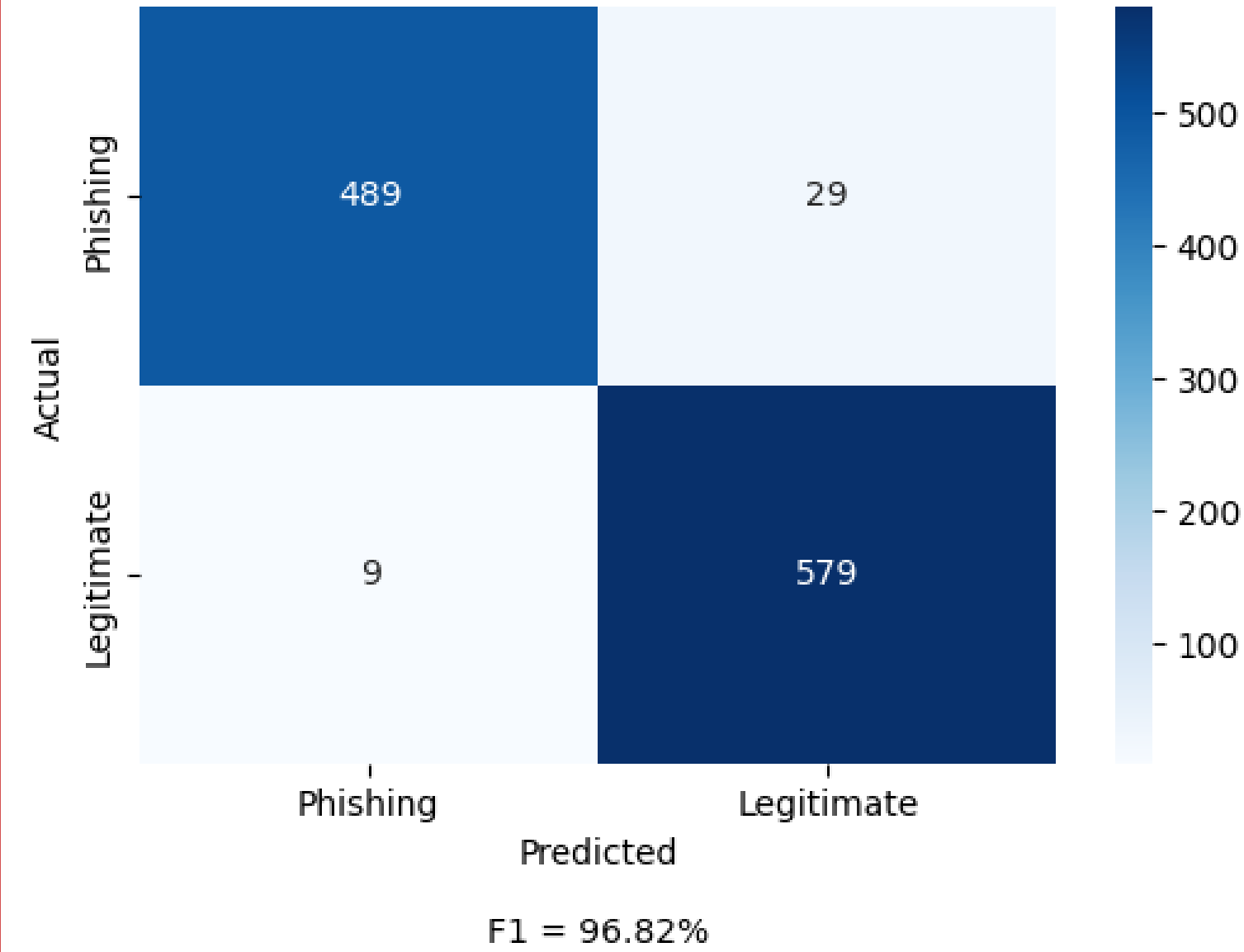
Other methods such as KNN, SVM and Liner Regression had varying levels of success, with KNN being consistently higher.

Due to the constant evolution of phishing tactics, it is impossible to represent all methods of phishing within training data, resulting in a degree of uncertainty when exposed to new data. Likewise, there is a high degree of noise and variability between how phishing webpages are crafted.

Feature Distribution



KNN Confusion Matrix



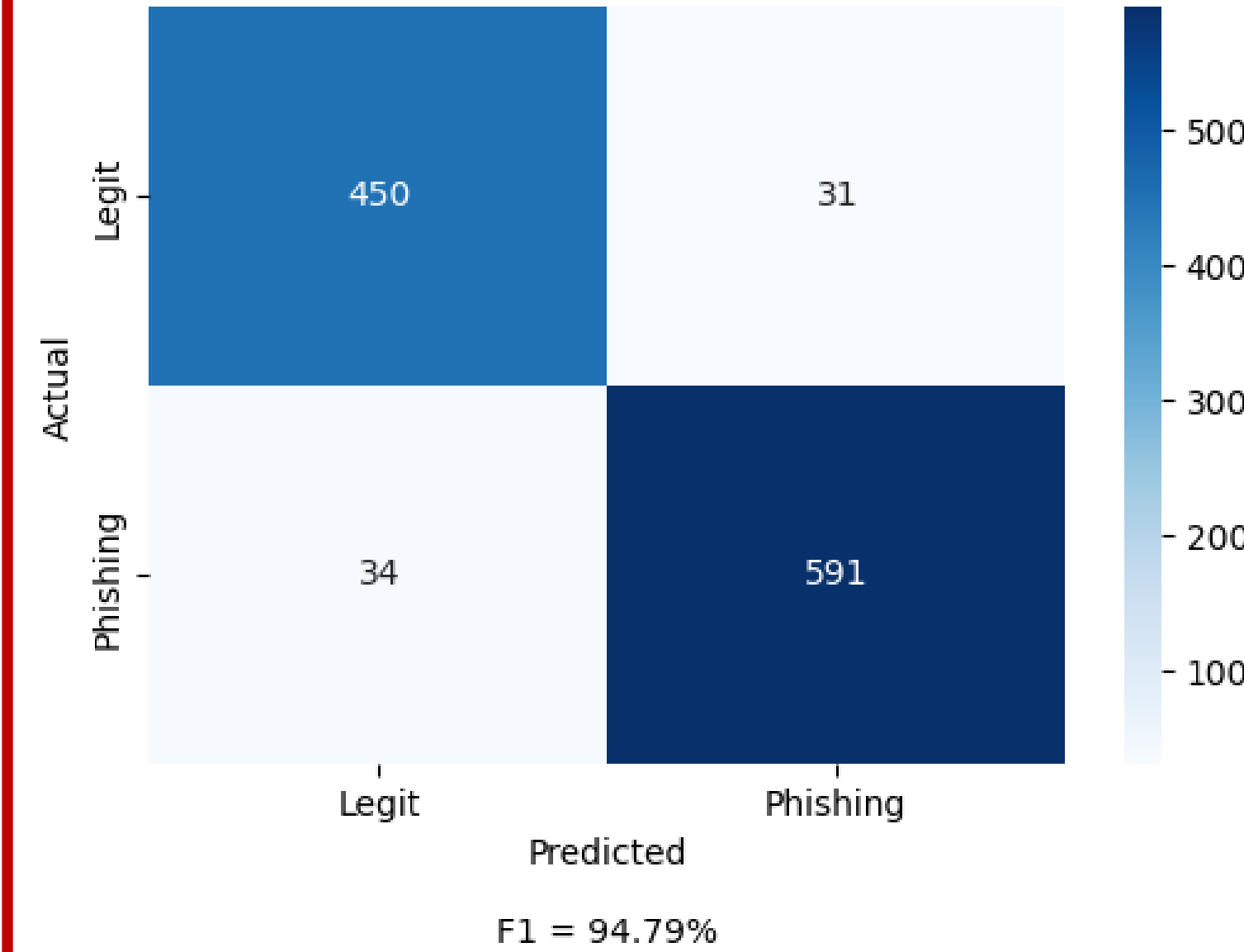
Pros:

- Handles categorical data well, fitting the dataset.
- Simple logic allows fast real-time phishing detection.

Cons:

- May not scale well on very large datasets.
- Sensitive to noisy data and irrelevant features.

Linear Regression Confusion Matrix



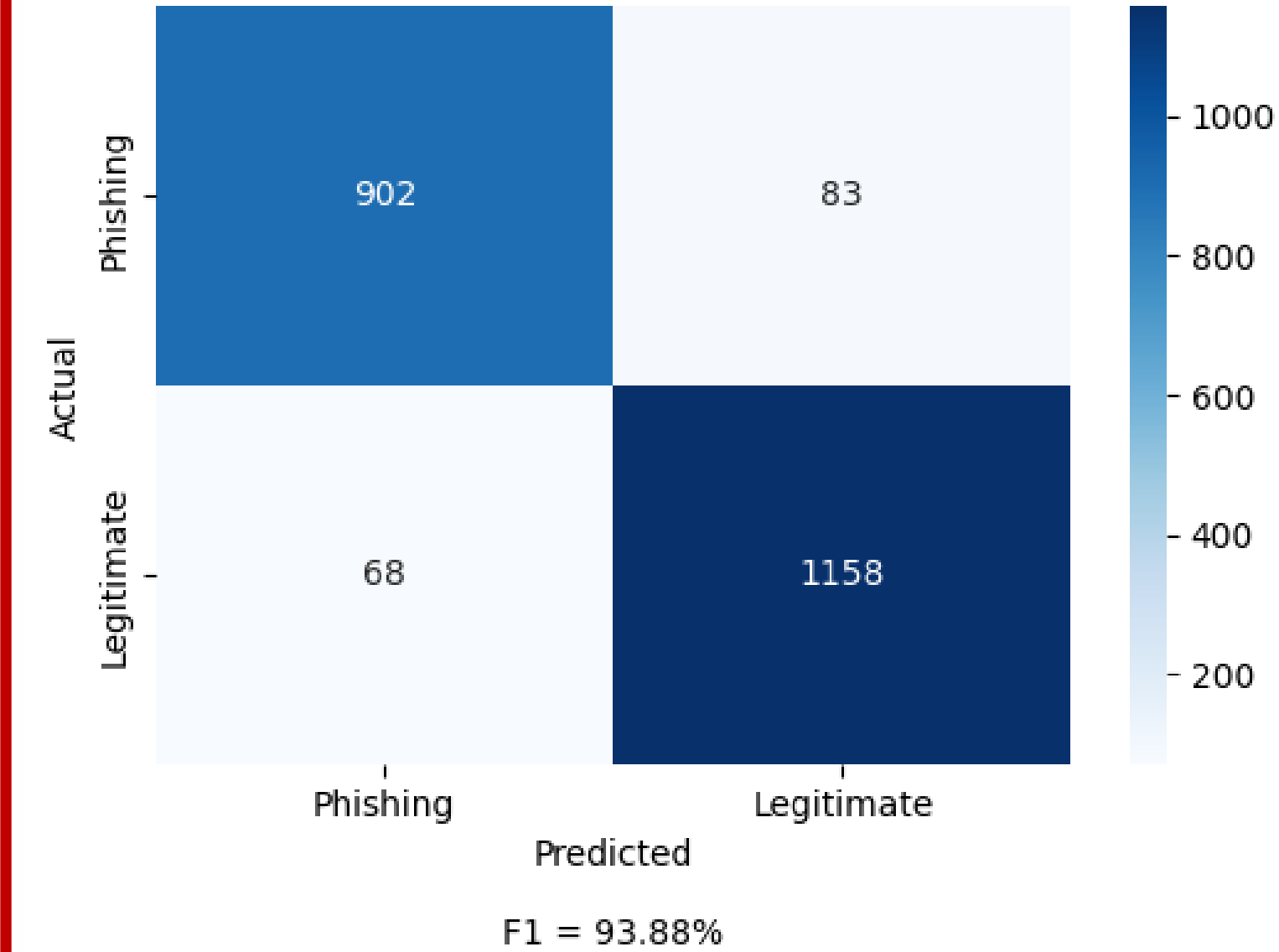
Pros:

- Efficient for large datasets with fast training.
- Highlights which features affect phishing risk.

Cons:

- Best for regression, not classification tasks.
- Assumes linearity, which may not reflect reality.

SVM Confusion Matrix



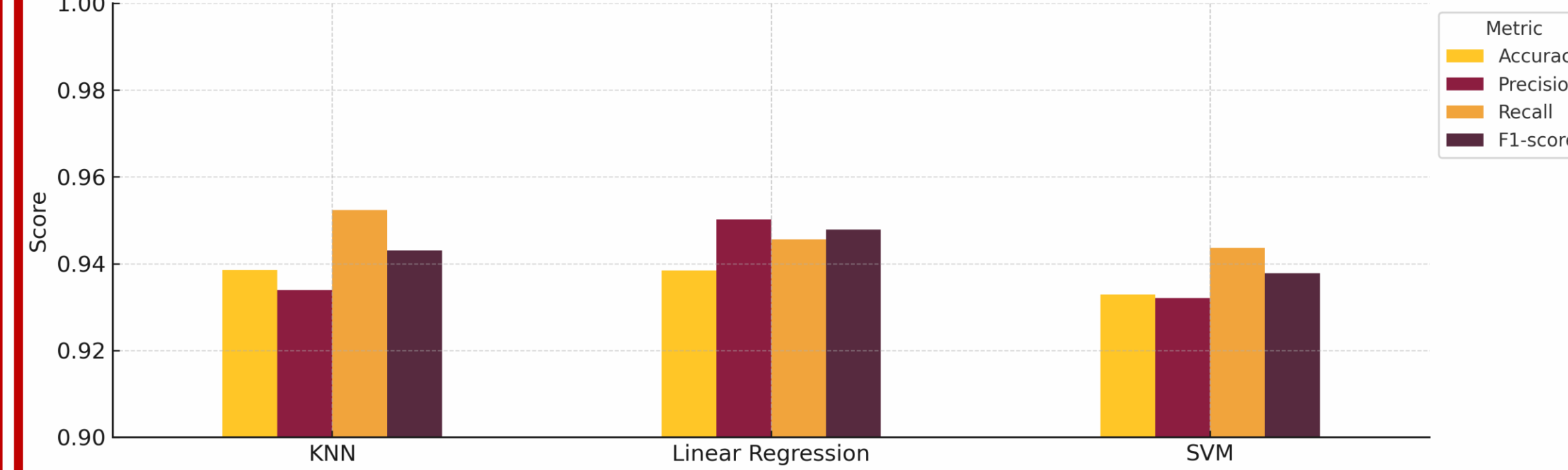
Pros:

- Works well in complex, high-dimensional data.
- Maintains accuracy even with some noisy input.

Cons:

- Can overfit without regularization techniques.
- Computational cost is high with non-linear kernels.

Performance Metrics of ML Models for Phishing Detection



Future Work:

- Explore ensemble methods for improved detection.
- Evaluate real-time performance in deployed systems.
- Integrate phishing detection into email/web filters.

Applications:

- Browser plugins
- Email security tools
- Enterprise phishing firewalls