**Literature Review**

**2.1 Introduction**

Phishing attacks continue to be one of the most common and dangerous threats on the internet. These attacks aim to trick people into sharing personal details like passwords, banking information, or login credentials. As phishing methods have become more advanced, researchers and developers have looked for smarter ways to detect and stop these attacks. This chapter reviews the existing methods used for phishing detection, especially focusing on how machine learning (ML) has improved security. It also discusses how this project builds on those ideas and adds something new.

**2.2 Traditional Phishing Detection Techniques**

In the past, phishing was mostly detected using simple methods like blacklists or rule-based systems.

**2.2.1 Blacklists**

Blacklists are lists of websites known to be dangerous. Browsers like Chrome or Firefox will block these sites if they’re reported and confirmed as phishing. However, they only work after a site has already been found to be harmful. Many phishing sites go live and disappear before they’re ever reported, making blacklists less effective (Liu et al., 2018).

**2.2.2 Rule-Based Detection**

Some systems use fixed rules to spot suspicious behavior; checking if a URL has too many redirects, or if it uses numbers or symbols in odd ways. These rules can catch some obvious attacks, but they can’t easily adapt when attackers change their tactics.

Because phishing techniques change quickly, these static approaches are often too slow to react. That’s where more adaptive methods like machine learning come in.

**2.3 Machine Learning Approaches**

Machine learning allows computers to learn from data and find patterns, making it a great tool for detecting phishing websites or emails.

**2.3.1 Supervised Learning Methods**

Supervised ML models are trained on labeled data which i lists of phishing and legitimate websites; so they can predict if a new website is safe or not.

Usman-Hamza and Ajiboye (2024) compared different ML models for phishing detection and found that Random Forest achieved the best accuracy (96.7%). Other commonly used models include Support Vector Machines (SVM) and Decision Trees, which are still popular because they perform well without needing a lot of resources.

**2.3.2 Deep Learning Techniques**

Deep learning models, like Convolutional Neural Networks (CNNs), can detect phishing by automatically learning useful features from data without needing manual feature engineering. A study by Yerima and Alzaylaee (2020) developed a CNN model that achieved 98.2% accuracy, showing how powerful deep learning can be, although it usually requires more computing power and time.

**2.3.3 Natural Language Processing (NLP)**

NLP techniques are used to detect phishing in emails or suspicious URLs by analyzing how words are used. Bharuka et al. (2024) applied NLP with ML algorithms and achieved 98% accuracy in spotting phishing emails. This combination of language understanding and ML is especially useful for filtering scam messages.

**2.4 Browser-Based Phishing Detection Tools**

Many phishing attacks happen inside web browsers, so some developers have created browser extensions that can detect them in real-time.

Arun and Abosata (2024) built a browser extension that uses a Random Forest model to check URLs instantly. Their system had a 98.32% accuracy rate, showing that it's possible to protect users right when they’re browsing, without needing to wait for server responses or blacklist updates.

This type of tool inspired this project, as the goal is to make something simple, effective, and fast enough to run in the browser.

**2.5 Phishing in the African Context**

Phishing is a growing issue in Africa. Interpol’s Operation Serengeti in 2024 showed just how serious the problem has become, with over 1,000 people arrested for cybercrime across the continent (AP News, 2024). Unfortunately, there aren’t many phishing tools built specifically for African users or environments.

Many existing tools are designed for areas with fast internet and lots of computing power. But this project is built with the African context in mind; it works offline when needed, runs directly in the browser, and helps users learn how to report phishing websites too.

**2.6 Challenges and Future Directions**

Even though machine learning and deep learning have improved phishing detection, there are still challenges; changing phishing tactics mean that models need to be updated often to stay effective, lack of localized data makes it harder to train models that understand phishing behavior in specific regions like Africa and resource constraints in developing areas mean that tools must be lightweight and fast, without requiring powerful servers or expensive infrastructure.

Future work should focus on improving regional datasets, using more efficient ML models, and making tools that are easy to install and use, even on older computers or slow internet connections.

**2.7 Conclusion**

In summary, phishing continues to be a major cybersecurity problem. Traditional detection methods like blacklists and rule-based systems are still useful but limited. Machine learning offers a smarter and more adaptable way to detect phishing, and studies show that both classic ML models and newer deep learning techniques can work very well.

This project builds on that research by creating a browser extension that uses ML to detect phishing websites in real-time. It’s designed to be lightweight, practical, and especially useful in regions like Africa — where phishing is on the rise but not enough localized tools exist.

**References**

AP News, 2024. Interpol clamps down on cybercrime and arrests over 1,000 suspects in Africa. [online] Available at: https://apnews.com/article/208111329edd3a1a64faf85cc7c0d2c0 [Accessed 15 Apr. 2025].

Arun, A. and Abosata, N., 2024. Next Generation of Phishing Attacks using AI powered Browsers. arXiv preprint arXiv:2406.12547.

Bharuka, V., Almeida, A. and Patil, S., 2024. Phishing Detection Using Machine Learning Algorithm. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. [online] Available at: https://ijsrcseit.com/index.php/home/article/view/CSEIT2410228 [Accessed 15 Apr. 2025].

Liu, W. et al., 2018. Online phishing detection: An extreme learning machine based approach. Computers & Security, 38, pp.55-63.

Usman-Hamza, F.E. and Ajiboye, A.R., 2024. Performance Analysis of Selected Machine Learning Algorithms in the Detection of Phishing Attacks on Vulnerable Websites. International Journal of Software Engineering and Computer Systems, 10(1), pp.1-12.

Yerima, S.Y. and Alzaylaee, M.K., 2020. High Accuracy Phishing Detection Based on Convolutional Neural Networks. arXiv preprint arXiv:2004.03960.