# **CHAPTER ONE: INTRODUCTION**

# **1.1 INTRODUCTION AND BACKROUND OF STUDY**

Information security is a significant aspect of communication, which involves safeguarding data and information from unauthorized access and tampering. The protection of sensitive information ensures that it remains confidential and that it cannot be altered by unauthorized users. The secure transmission of data from one entity to another is crucial, and the rise in the number of information attacks over the last few decades highlights the importance of implementing effective information security measures [1]. Cybercriminals attempt to capture valuable information for their own purposes. The security of an organization's information depends on various types of data that the organization possesses. As the world increasingly becomes connected through the internet, it has become necessary for businesses to migrate onto the internet. This has increase the number of buying and selling on the internet. The introduction of covid-19 led to an increase in online transactions due to the fact that countries all over the world went into quarantine. This made businesses and jobs operate remotely through the internet, therefore, there was a drastic increase in the number of phishing attacks on organizations and individuals [2].

Phishing attacks have become a major threat to online security, causing significant financial loss and reputational damage. These attacks typically involve the use of fraudulent emails, websites, or other forms of electronic communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or social security numbers. The consequences of phishing attacks can be severe, ranging from identity theft to financial loss and reputational damage. To address the growing problem of phishing attacks, researchers and security professionals have developed a range of methods for detecting and preventing these attacks. Machine learning algorithms have emerged as a promising approach to phishing detection, as they can analyze large volumes of data to identify patterns and anomalies that may be indicative of phishing activity (Alshehri et al., 2020; Khan et al., 2021).

In this thesis, we propose an enhanced random forest model for detecting phishing attacks. Random forest is a popular machine learning algorithm that is well-suited for classification tasks (Breiman, 2001). We extend the basic random forest model by incorporating additional features and techniques that are specifically tailored for phishing detection. The enhanced random forest model leverages a combination of supervised and unsupervised learning techniques to identify common features and characteristics of phishing attacks. These include features related to the structure and content of emails and websites, as well as network-level features that can provide insight into the behavior of phishing attacks (Zhang et al., 2020). We also incorporate several techniques for feature selection and hyperparameter tuning to optimize the performance of our model. These techniques enable us to identify the most important features for phishing detection and tune the parameters of our model to achieve the best possible performance (Bartlett et al., 2017). To evaluate the effectiveness of our enhanced random forest model, we train and test our model using several datasets of both legitimate and phishing electronic communications. We use a range of performance metrics to assess the accuracy, precision, and recall of our model, and compare its performance to other state-of-the-art phishing detection methods (Alzahrani et al., 2019; Singh et al., 2021).

Our research aims to contribute to the ongoing efforts to improve online security by proposing an enhanced random forest model for phishing attack detection. By leveraging machine learning techniques and incorporating additional features and techniques, we hope to improve the accuracy and effectiveness of phishing detection and help protect users from the harmful effects of phishing attacks. In summary, this thesis proposes an enhanced random forest model for phishing attack detection. By extending the basic random forest model and incorporating additional features and techniques, we aim to improve the accuracy and effectiveness of phishing detection and contribute to the ongoing efforts to improve online security.

## 

# **1.2 PROBLEM STATEMENT**

## Phishing attacks are a serious threat to online security and traditional approaches to detection may not be effective against new and evolving techniques. Machine learning algorithms, such as random forest, have shown promise in detecting phishing attacks. However, the performance of traditional random forest models can be limited by their inability to handle imbalanced data and to capture complex relationships between features. Therefore, this research aims to propose an enhanced random forest model for phishing attack detection that addresses these limitations and improves the accuracy and effectiveness of phishing detection.

# **1.3 SIGNIFICANCE AND SCOPE OF STUDY**

Phishing attacks are one of the most prevalent and devastating threats to online security, with individuals and businesses suffering significant financial and reputational damage as a result of successful attacks. As phishing techniques become increasingly sophisticated, it is becoming more difficult to detect these attacks using traditional approaches. Machine learning algorithms have shown promise in detecting phishing attacks, with random forest being a popular choice due to its high accuracy and ability to handle large datasets. However, traditional random forest models have limitations that can impact their effectiveness in detecting phishing attacks. One major limitation is their inability to handle imbalanced data, which can lead to biased models and reduced detection accuracy. Additionally, traditional random forest models may struggle to capture complex relationships between features, which can result in false positives or missed detections.

The proposed enhanced random forest model for phishing attack detection aims to address these limitations and improve the accuracy and effectiveness of phishing detection. By incorporating techniques such as oversampling, under sampling, and feature selection, the enhanced model is designed to handle imbalanced data and capture complex relationships between features. This will lead to more accurate and reliable detection of phishing attacks, reducing the likelihood of successful attacks and the resulting financial and reputational damage. The significance of this study lies in its potential to improve online security for individuals and businesses by providing an effective method for detecting phishing attacks. By improving the accuracy and effectiveness of phishing detection, the proposed enhanced random forest model can help prevent financial losses, data breaches, and other negative consequences of successful phishing attacks.

The scope of this study is to evaluate the performance of the proposed enhanced random forest model for phishing attack detection. The study will use a dataset of phishing and legitimate websites to train and test the model, and will compare the performance of the enhanced model to that of traditional random forest models. The study will also investigate the impact of different techniques such as oversampling, under sampling, and feature selection on the performance of the enhanced model.

The study is limited to the use of a single machine learning algorithm and a specific dataset of phishing and legitimate websites. However, the results of the study can be used as a basis for future research on the effectiveness of other machine learning algorithms and datasets for detecting phishing attacks. Overall, the significance and scope of this study demonstrate the importance of developing effective methods for detecting phishing attacks, and the potential for machine learning algorithms to improve online security for individuals and businesses. The proposed enhanced random forest model for phishing attack detection has the potential to make a significant impact on the prevention of successful phishing attacks and the resulting financial and reputational damage.

# **1.4 RESEARCH GOAL.**

The primary goal of this research is to propose an enhanced random forest model for phishing attack detection that addresses the limitations of traditional random forest models and improves the accuracy and effectiveness of phishing detection. To achieve this goal, the research will focus on the following objectives:

1. To conduct a comprehensive literature review on the current state of phishing detection methods and machine learning algorithms.
2. To analyze the limitations of traditional random forest models for phishing detection, including their inability to handle imbalanced data and capture complex relationships between features.
3. To propose an enhanced random forest model for phishing attack detection that incorporates techniques such as oversampling, under sampling, and feature selection to address the limitations of traditional models.
4. To evaluate the performance of the proposed enhanced random forest model using a dataset of phishing and legitimate websites.
5. To compare the performance of the enhanced model to that of traditional random forest models, and investigate the impact of different techniques on the performance of the enhanced model.

The first objective is to conduct a comprehensive literature review on the current state of phishing detection methods and machine learning algorithms. This will involve a thorough analysis of existing research and studies on phishing detection, with a focus on machine learning algorithms such as random forest. The literature review will provide a foundation for the research and inform the development of the proposed enhanced random forest model.

The second objective is to analyze the limitations of traditional random forest models for phishing detection. This will involve a detailed investigation of the challenges faced by traditional models, including their inability to handle imbalanced data and capture complex relationships between features. This analysis will help to identify the specific areas where improvements can be made in the proposed enhanced random forest model.

The third objective is to propose an enhanced random forest model for phishing attack detection that incorporates techniques such as oversampling, under sampling, and feature selection. These techniques are designed to address the limitations of traditional models and improve the accuracy and effectiveness of phishing detection. The proposed model will be designed to handle imbalanced data and capture complex relationships between features, resulting in more accurate and reliable detection of phishing attacks.

The fourth objective is to evaluate the performance of the proposed enhanced random forest model using a dataset of phishing and legitimate websites. This will involve training the model on a dataset of known phishing and legitimate websites and testing its accuracy and effectiveness in detecting phishing attacks. The evaluation will provide quantitative data on the performance of the enhanced model and its ability to detect phishing attacks.

The fifth objective is to compare the performance of the enhanced model to that of traditional random forest models, and investigate the impact of different techniques on the performance of the enhanced model. This will involve comparing the accuracy, precision, recall, and F1-score of the enhanced model to those of traditional models, and analyzing the impact of oversampling, under sampling, and feature selection on the performance of the enhanced model.

Overall, the goals of this research are to develop an enhanced random forest model for phishing attack detection that addresses the limitations of traditional models, and to evaluate its performance using a dataset of phishing and legitimate websites. The proposed enhanced model has the potential to improve the accuracy and effectiveness of phishing detection, reducing the likelihood of successful phishing attacks and the resulting financial and reputational damage.

## .

# 

# **REFERENCES**

1. Li, M., Nazir, S., Khan, H. U., Shahzad, S., & Amin, R. (2020). Modelling features-based birthmarks for security of end-to-end communication system. *Security and Communication Networks*, *2020*, 1-9.
2. Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T. J. (2017, November). Intelligent phishing website detection using random forest classifier. In 2017 International conference on electrical and computing technologies and applications (ICECTA) (pp. 1-5). IEEE.
3. Muppavarapu, V., Rajendran, A., & Vasudevan, S. K. (2018). Phishing detection using RDF and random forests. Int. Arab J. Inf. Technol., 15(5), 817-824.
4. Alshehri, A., Traore, I., & Woungang, I. (2020). Machine learning techniques for phishing detection: A comprehensive review. Journal of Network and Computer Applications, 154, 102470.
5. Alzahrani, A. I., AlGhamdi, F. S., Almulhim, M. A., & Zaidan, B. B. (2019). Phishing detection techniques: A review. IEEE Access, 7, 20491-20512.
6. Bartlett, M. S., et al. (2017). Simple, interpretable models for high-accuracy phishing detection. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1857-1866).
7. Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.
8. Khan, N., et al. (2021). A comparative study of machine learning-based phishing detection techniques. Journal
9. Alzahrani, A., & Alfaresi, E. (2019). A survey of phishing detection techniques. Journal of Cybersecurity, 5(1), tyz002. <https://doi.org/10.1093/cybsec/tyz002>
10. Balasubramanian, A., & Baskaran, R. (2019). A random forest-based approach for phishing detection. In 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 138-142). IEEE. <https://doi.org/10.1109/INCOS.2019.8916895>
11. Bharti, S., Kumar, A., & Goyal, L. M. (2019). A review of machine learning techniques for phishing detection. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE. <https://doi.org/10.1109/ICCCNT45670.2019.8945139>
12. Chandrasekhar, V., & Swarup, V. (2018). Phishing websites detection using random forest algorithm. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 34-39). IEEE. https://doi.org/10.1109/CONFLUENCE.2018.8442872