

Advanced Persistent Threat (APT) Detection and Mitigation Framework

Delivery Vector Analysis through Phishing Email Detection

R25-037

Project Proposal Report

D.L.K.L.Gangaboda - IT21812330

Supervisor - Dr. Harinda Fernando

Department of Information Technology

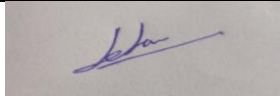
Sri Lanka Institute of Information Technology

Sri Lanka

January 2025

Declaration

I hereby declare that this document contains original research conducted as part of a project proposal for the fulfillment of academic requirements. All sources have been appropriately cited and referenced. This work has not been submitted for any other academic award.

Name	Student ID	Signature
D.L.K.L. Gangaboda	IT21812330	

Supervisor Declaration:

I confirm that I have reviewed this project proposal and approve it for submission.

.....

Signature of the Supervisor

.....

Date

.....

Signature of the Co – Supervisor

.....

Date

Acknowledgment

I would like to express my sincere gratitude to my supervisor, Mr. Harinda Fernando and my co-supervisor Mr. Amila Senarathne for their invaluable guidance, expertise, and continuous support throughout the development of this research proposal. I would also like to thank my peers for their helpful discussions and insights. Finally, I acknowledge Sri Lanka Institute of Information Technology for providing the necessary resources and infrastructure to conduct this research.

Abstract

This study proposes research work that aims to boost APT protection through better phishing email detection practices because phishing acts as a key pathway for such attacks. The main research goal consists of developing an advanced phishing detection model through Transformer-based architecture implementation and BERT model fine-tuning. The proposed model performs phishing classification by examining both content text and metadata alongside file attachments. The research process includes acquiring various phishing and legitimate mail datasets for preprocessing and designing a specific data workflow before tuning a BERT model featuring attention components for feature-weighting followed by comprehensive evaluation using precision, recall and F1-score metrics. The model will be enhanced with a continuous learning method that helps it adjust to changing phishing technique patterns. A improved detection system will emerge from this work to provide active defense against advanced phishing attacks within the APT environment. Early-stage threat detection stands as the key importance of this research because it strengthens the framework protecting against APT attacks.

Keywords: APT, Phishing Detection, Transformers, BERT, Cybersecurity, Natural Language Processing (NLP), Machine Learning, Attention Mechanisms

Table of Contents

1. Introduction
2. Background & Literature Review
 - 2.1 Overview of Phishing as an APT Delivery Vector
 - 2.2 Role of Transformers in Phishing Detection
 - 2.3 Related Work
3. Research Gap
4. Objectives
 - 4.1 Main Objective
 - 4.2 Specific Objectives
5. Methodology
 - 5.1 Dataset Collection
 - 5.2 Preprocessing Pipeline Design
 - 5.3 Model Fine-Tuning
 - 5.4 Model Evaluation
 - 5.5 Continuous Learning Mechanism
6. System Architecture
7. Requirements
8. Anticipated Benefits
9. Research Constraints
10. Project Plan
11. Budget and Justification
12. Gantt Chart
13. Work breakdown Structure
14. Conclusion
15. References

1. Introduction

A significant and evolving cybersecurity issue is the emergence and vulnerability of Advanced Persistent Threats (APTs). Attacks by APT actors tend to be more complex and targeted, utilizing a multi-stage strategy that often starts with exploiting human vulnerability through phishing emails. Attackers are first allowed to access targeted systems through the use of these emails, which act as a primary delivery mechanism for malicious payloads. The advanced techniques used by APT groups are more challenging than those that have been traditionally employed in phishing detection, which often involves static rule-based approaches and basic machine learning models. To overcome this limitation, more sophisticated and versatile detection methods must be developed. By utilizing Natural Language Processing (NLP) and BERT, the project seeks to develop a robust and intelligent phishing detection mechanism. The ability to capture contextual relationships within text data has made BERT models a valuable tool for analyzing the intricate details of phishing emails, as evidenced by recent research. This research seeks to combine this NLP expertise with meticulous feature extraction and robust evaluation to greatly improve the accuracy and adaptability of phishing detection as part of an overall APT detection framework. The proposed research explores how improving the performance of a Transformer/BERT model and utilizing attention mechanisms to prioritize important features in email text, metadata (including attachments), can enhance protection from potential phishing attempts within an APT scenario [1].

2. Background & Literature Review

2.1 Overview of Phishing as an APT Delivery Vector

Phishing has emerged as one of the most potent tools in Advanced Persistent Threat (APT) campaigns, often serving as the first step in compromising a target. Unlike traditional cyberattacks that usually exploit technical flaws, phishing primarily takes advantage of human psychology and social engineering, tricking users into actions that jeopardize system security. By using deception instead of directly targeting software or network weaknesses, phishing helps cybercriminals breach highly secure environments.

One of the most alarming types of phishing seen in APT attacks is spear-phishing. This method is highly focused and tailors communications to particular individuals or organizations. In contrast to broad phishing attempts that target many people at once, spear-phishing emails feature personal information collected through research, such as a person's job title, work connections, recent projects, or even personal interests. This customization drastically boosts the chances that a recipient will trust the email, which lowers their guard and makes them more inclined to interact with harmful content [2] [3].

APT attackers devote considerable resources to crafting phishing emails that look legitimate and match an organization's usual communication style. They might impersonate colleagues, business associates, IT teams, or executives to gain trust. By using tactics like domain spoofing, similar-looking domains, and compromised email accounts, they can make their messages seem credible. When a message appears to come from a trusted source, it reduces the target's defenses and boosts the chances of a successful infiltration [4].

Phishing Payloads and Attack Execution

In a phishing email, the "payload" refers to how attackers carry out their malicious intentions. These payloads are often designed to bypass standard security measures like antivirus software, spam filters, and endpoint protection programs. There are three main avenues through which phishing emails facilitate APT infiltration:

- **Malicious Links** – Attackers embed URLs in emails that lead to sites they control, often mimicking legitimate platforms like corporate login pages or cloud storage services to trick users into entering their login info. Once they have these credentials, attackers can gain unauthorized access to internal systems. Some phishing links also initiate drive-by downloads, which install malware automatically as soon as the victim visits the site.
- **Weaponized Attachments** – Many phishing emails include harmful document attachments like PDFs, Microsoft Word or Excel files, or ZIP files. These documents often carry macro-based malware, embedded scripts, or exploits meant to trigger malicious payloads when opened. Sophisticated phishing attacks may utilize zero-day vulnerabilities, allowing the malware to go undetected and execute without triggering security alerts.
- **Credential Harvesting via Fake Forms** – Certain phishing emails direct victims to fake login pages that closely resemble real services. These counterfeit forms are designed to capture usernames, passwords, and multi-factor authentication (MFA) codes. Cybercriminals can then leverage these stolen credentials to infiltrate corporate networks, enabling further movement throughout the organization.

The Role of Phishing in APT Attack Chains

Phishing is particularly effective in APT campaigns because it serves as a gateway for gaining persistent access to a target's infrastructure. Once the phishing payload is activated, attackers establish an initial foothold and begin to progress through the cyber kill chain. Here's a look at how phishing plays a role in the overall execution of an APT attack:

- **Initial Access** – The phishing email tricks a user into clicking on a malicious link or opening a weaponized attachment. This move grants the attacker a foothold in the system, often without raising any alarms.
- **Execution of Exploits** – If the phishing email contains an exploit targeting a software vulnerability, it executes upon user interaction. Attackers may deploy remote access trojans (RATs), keyloggers, or backdoors to retain control over the compromised system.
- **Privilege Escalation** – The malware might attempt to gain higher privileges by exploiting local system vulnerabilities or stealing admin credentials, allowing attackers to access more than just the initially compromised account.
- **Lateral Movement** – Once inside the network, attackers use methods like pass-the-hash, credential dumping, or living-off-the-land (LOTL) techniques to navigate through the organization's systems without being detected.
- **Persistence & Cleanup** – To evade detection, attackers build backdoors and persistence methods, enabling them to return to the system even if the original phishing attempt is identified. Some APT groups use fileless malware that runs entirely in memory to avoid being caught by endpoint security tools.

Bypassing Traditional Security Measures

Today's phishing campaigns are crafted to dodge conventional security defenses. Some advanced evasion methods used in APT phishing attacks include:

- **Obfuscation** – Cybercriminals alter email headers, subject lines, and content encodings to slip past detection systems.
- **Encryption & Steganography** – Malicious payloads are concealed within encrypted files or hidden inside images and legitimate documents to escape antivirus detection.
- **Compromised Accounts** – Instead of sending phishing emails from external sources, attackers may take over real email accounts within an organization, making the phishing emails look more credible.
- **AI and Automation** – Some APT groups utilize AI tools to dynamically generate phishing emails, making them tougher to catch with static filters.

2.2 Role of Transformers in Phishing Detection

The field of NLP has been revolutionized by the use of BERT (Bidirectional Encoder Representations from Transformers), which capture complex relationships within text data using models. By analyzing the bidirectional context of words in a sentence, BERT can process them relative to their preceding and subsequent text. This is different from previous unidirectional models of machine learning that only consider one word at occurrence. This implies that the model is better equipped to detect subtle alterations in language, such as urgency signals and deceptive requests, used by phishing actors. In addition, BERT can process and understand sequence data, which is why it is used to manage the structure of emails (headers, body text, subject lines etc.) By producing contextualized embeddings with high quality, the model can also be utilized for text classification, enabling it to distinguish between benign and malicious emails more accurately. Unlike manual feature engineering, which relied heavily on keyword lists, BERT can learn relevant features from the data and adapt to new phishing techniques and language patterns. In addition, BERT can efficiently handle both text and metadata, including sender addresses, time stamps, and email headers. This combination enables enhanced accuracy through the inclusion of rich representation.

2.3 Related Work

Phishing detection has been extensively studied, using a variety of techniques from rule-based systems and traditional machine learning techniques to more recently developed deep learning-backed approaches. Early attempts at phishing detection were often based on system matching by pattern and keyword. Despite their simplicity, these early systems were not very versatile and could be easily bypassed by attackers through the use of common tricks or subtle modifications in attack patterns. Among the most popular machine learning algorithms for detecting phishing are Support Vector Machines (SVM), Naive Bayes, and Random Forests. These models often require manual feature engineering and fail to account for the intricate contextual cues found in phishing emails. However, they are still useful tools for this purpose. The use of deep learning models like Recurrent Neural Networks (RNNs), Convolutional Neural Network (CNNs) and Transformers has been a recent area of research that deals with detecting

phishing. RNNs, particularly LSTMs (long-range persistent networks) demonstrate promising results for extracting sequence information within the text of the emails, but their sequential nature means they are computational burdens and can only capture short distances. CNNs have demonstrated their ability to detect local patterns. While it is beneficial, it does not aid in comprehending larger contextual dependencies. BERT and other Transformer-based models have achieved remarkable improvements in accuracy, as they incorporate self-attention mechanisms to model global relationships within text data. More investigations reveal the utilization of attention mechanisms to prioritize crucial aspects and boost model efficiency..

3. Research Gap

Research on phishing detection currently offers meaningful findings but additional examination becomes required because of various remaining gaps. The current models designed to find phishing attacks fail to demonstrate the required adaptability needed to match the continual modifications made by APT actors. The rules used in static detection systems get easily bypassed since traditional machine learning models exhibit limited adaptability towards new phishing method variations. Research of phishing focuses mainly on email message content while disregarding important metadata findings and attached-file characteristics. This narrow view of examination results in decreased capabilities to detect complex attacks because those incidents depend strongly on contextual signals. Strategies to effectively run and enhance these implementations at scale in operational environments encounter resistance. Production environments characterized by high-speed processing requirements have limitations with many deployed models which cannot process data in real time. The critical requirement at present involves implementing ongoing learning processes. These systems need to show their capability in adapting to new emerging phishing techniques because this ability keeps them effective. The models degrade in effectiveness since they require ongoing training and development for staying relevant. APT detection frameworks show an existing limitation when integrating approaches that use sentiment analysis in their infrastructure. This research merges three elements by developing a model which analyzes textual and metadata content alongside attachments and enables dynamic learning capabilities to modify itself according to shifting attack patterns.

4. Objectives

4.1 Main Objective

The key aim of this research is to create an advanced model for detecting phishing that smoothly integrates into a system designed for detecting and mitigating threats during the delivery phase of Advanced Persistent Threats (APTs). This model will use a BERT-based Transformer architecture to effectively identify phishing emails, which often serve as the first point of attack in APT campaigns. By harnessing natural language processing (NLP) and deep

learning techniques, we aim to boost the efficiency of phishing detection, make it more adaptable to new threats, and reduce false positives. Ultimately, this will strengthen cybersecurity measures by adopting a proactive stance on identifying and addressing phishing-related APT intrusions.

4.2 Specific Objectives

Dataset Acquisition & Preprocessing

- Gather a large dataset that includes both legitimate and phishing emails from reliable sources like public cybersecurity repositories, Kaggle datasets, and organizational threat intelligence feeds.
- Clean and structure the data to ensure a top-notch dataset for training and validation.
- Preprocess email texts, metadata, and attachments to create a well-organized input format suitable for machine learning.

Data Pipeline Design

- Set up a data preprocessing pipeline that efficiently manages text cleaning, tokenization, and feature extraction.
- Make sure this pipeline extracts key elements such as header data, embedded URLs, file attachments, and relevant email context.
- Convert raw text into numerical vector representations that are compatible with Transformer-based models.

Transformer/BERT Model Fine-Tuning

- Fine-tune a BERT-based Transformer model to distinguish between phishing and legitimate emails with high accuracy.
- Add attention mechanisms to focus on crucial phishing indicators such as suspicious links, urgency-driven language, and references to malicious attachments.
- Optimize the model through hyperparameter tuning to enhance its learning efficiency.

Model Evaluation & Performance Testing

- Assess the model's accuracy using established industry metrics, including:
 - Precision (the accuracy of phishing email predictions).
 - Recall (how effectively it detects phishing attempts).
 - F1-score (a balance between precision and recall).

- Conduct comparative tests against existing machine learning and heuristic-based phishing detection systems to measure performance improvements.
- Test the model's effectiveness on real-world phishing datasets to ensure its practical usability.

Continuous Learning & Model Adaptation

- Create a continuous learning system that adjusts to emerging phishing techniques.
- Implement real-time updates to the model to stay current with new phishing attack patterns.
- Ensure the model keeps improving over time through automated updates, enabling it to recognize new threats and maintain efficacy in a constantly evolving cybersecurity environment.

5. Methodology

5.1 Dataset Collection

This research collects its data from public Kaggle datasets which include phishing and genuine email examples. Data sets include,

The Phishing Emails Dataset acts as a training resource through its collection of original emails received from the wild. This set of phishing emails consists of multiple samples that show different features as well as several text content types. The data collection method will acquire both email textual content together with metadata components including sender fields alongside timestamp and header data alongside file characteristics. The data team will prepare the dataset by selecting realistic phishing attack samples that undergo thorough labeling procedures.

5.2 Preprocessing Pipeline Design

Python along with its libraries Pandas and Matplotlib will process the obtained email dataset. The text normalization during data cleaning involves stripping away HTML tags that produce inappropriate characters. After text separation into words through tokenization the words will undergo root reduction through stemming. Term frequencies along with extracted n-grams through TF-IDF method will be obtained from the text bodies. The tool will extract domain names from senders and infrastructure information as well as timestamp and time stamps from metadata. The detection of attachments includes a combination of file extensions with their hash values and their file sizes as well as all attachment metadata. The analysis of this research does not include attachment execution because static assessment will suffice for attachment examination [5].

5.3 Model Fine-Tuning

The transformers library enables text tokenization through AutoTokenizer while RoBERTa operates as the embedder for text vector creation. AutoModel will undergo fine-tuning for sequence classification before the next stage of development. Attention mechanisms function as an addition to BERT with the purpose of pinpointing essential features that detect phishing attacks. The BERT model starts from pre-trained weights before undergoing training with the phishing email data that contains labels [6]. The model becomes capable of understanding distinctive phishing attack features through this process

5.4 Model Evaluation

The model will reach evaluation using precision-recall-F1-score metrics according to industry standards. The generated metrics will combine model predictions with the physical labels found in the dataset in order to calculate precision, recall and F1-score values. The evaluation will use sklearn as its operation tool. The evaluation will incorporate Area Under the Curve as well as specific metrics to acquire a detailed evaluation of the model performance. TensorFlow alongside Scikit-learn and Keras and PyTorch will aid in deep learning model building and both training and evaluation tasks during the evaluation phase.

5.5 Continuous Learning Mechanism

To support continuous learning, we'll set up an automated pipeline that gathers new samples of identified phishing emails from various sources. These incoming samples will be processed through the same data pipeline we outlined earlier. The model will then incorporate incremental updates using this new labeled data, allowing it to adjust to fresh phishing techniques. Updates will be made using online learning methods, which guarantees that the model stays adaptive and updates itself with the latest tactics used by malicious actors [7]. This whole cycle of continuous learning will run in the background, ensuring the model is constantly adapting without interfering with its performance [8].

6. System Architecture

Our proposed system architecture revolves around a modular pipeline that ties together data collection, processing, model training, evaluation, and continuous learning into a unified framework.

Data Collection Module: Gathers data from chosen public sources, ensuring that emails are clearly labeled as phishing or legitimate, and includes newly found phishing emails as well.

Preprocessing Module: Handles data cleaning, tokenization, and feature extraction on the raw email data, transforming it into a format that's ideal for our machine learning model.

Model Training Module: Adjusts the BERT model using the preprocessed data and incorporates attention mechanisms to highlight key features within the dataset.

Model Evaluation Module: Evaluates the model's performance through metrics like precision, recall, F1-score, and Area Under the Curve (AUC).

Continuous Learning Module: Incorporates automated pipelines for integrating newly discovered phishing emails into the model's training data, allowing it to stay updated with changing phishing techniques [9].

7. Requirements

Functional Requirements

These outline what the system needs to achieve for effective phishing detection using BERT-based transformers.

Data Collection & Preprocessing

The system should gather both phishing and legitimate emails, which involves

- Capturing email text (body and subject)
- Collecting metadata (sender details, headers, timestamps, and email authentication info)
- Including attachments (like file type and hash values)

Emails should be preprocessed by

- Cleaning up the text (removing HTML tags and special characters)
- Tokenizing the emails with AutoTokenizer and RoBERTa
- Extracting relevant features from metadata and attachments

Model Development & Training

- The system needs to fine-tune a Transformer/BERT-based model to categorize emails as phishing or legitimate.
- The model should be capable of sequence classification to examine email patterns.
- It ought to feature attention mechanisms for highlighting critical phishing attributes.
- The system should enable hyperparameter tuning for better optimization.

Phishing Email Detection & Evaluation

- The system must effectively identify phishing emails using Transformer models.
- It should provide a confidence score that reflects the likelihood of an email being phishing.

Evaluation of detection performance must include

- Precision (how accurately phishing emails are detected)
- Recall (the system's ability to discover all phishing emails)
- F1-score (the balance between precision and recall)

Continuous Learning & Model Updates

- The system should support continuous learning by incorporating new phishing data.
- It must allow for incremental model training without needing a complete retrain.
- The detection pipeline should automatically adapt to new phishing techniques.

Integration & Deployment

The phishing detection model should work seamlessly with:

- Email security gateways (like Proofpoint and Mimecast)
- SIEM platforms (such as Splunk and Elasticsearch)
- Incident response systems to provide real-time alerts

Detected phishing emails need to be stored for future analysis.

- The system must be capable of generating alerts and reports for any identified phishing emails.
- It should allow for real-time scanning of incoming emails.

Non-Functional Requirements

These details how the system is intended to perform rather than specifying the tasks it completes.

Performance & Scalability

- The system must identify phishing emails in real-time with minimal delay.
- The model should be scalable enough to manage large volumes of email traffic (like that of corporations).
- The system should be able to process at least 100,000 emails per hour without losing performance.

Accuracy & Reliability

The model must reach at least:

- 90% precision (keeping false positives to a minimum)
- 85% recall (detecting the majority of phishing emails)
- 88% F1-score (maintaining a good balance between precision and recall)

Additionally, the system should minimize false positives to avoid disrupting legitimate communications.

It should work reliably with various email providers (like Gmail, Outlook, and Yahoo).

Security & Compliance

- User email data needs to be securely handled using encryption (such as AES-256).
- The system must adhere to GDPR and other data privacy regulations.
- Access to email classification results should be limited to authorized personnel.
- It must be capable of identifying evasion techniques, including obfuscation and hidden payloads.

Maintainability & Extensibility

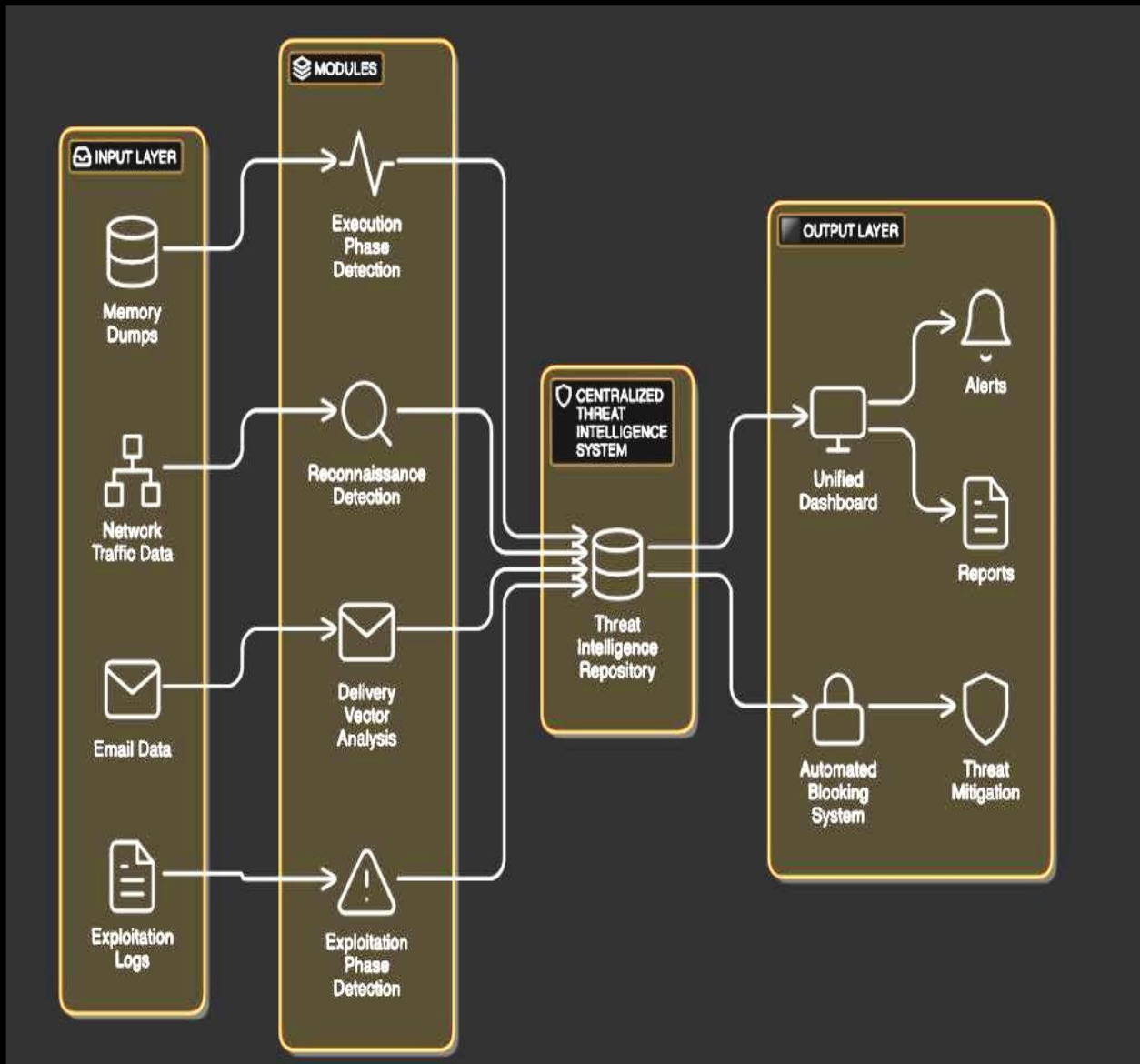
- The system should facilitate easy updates when new phishing tactics arise.
- The framework should accommodate plug-and-play model upgrades (like switching from BERT to RoBERTa).
- API access must be provided for straightforward integration with other security tools.

Usability & Visualization

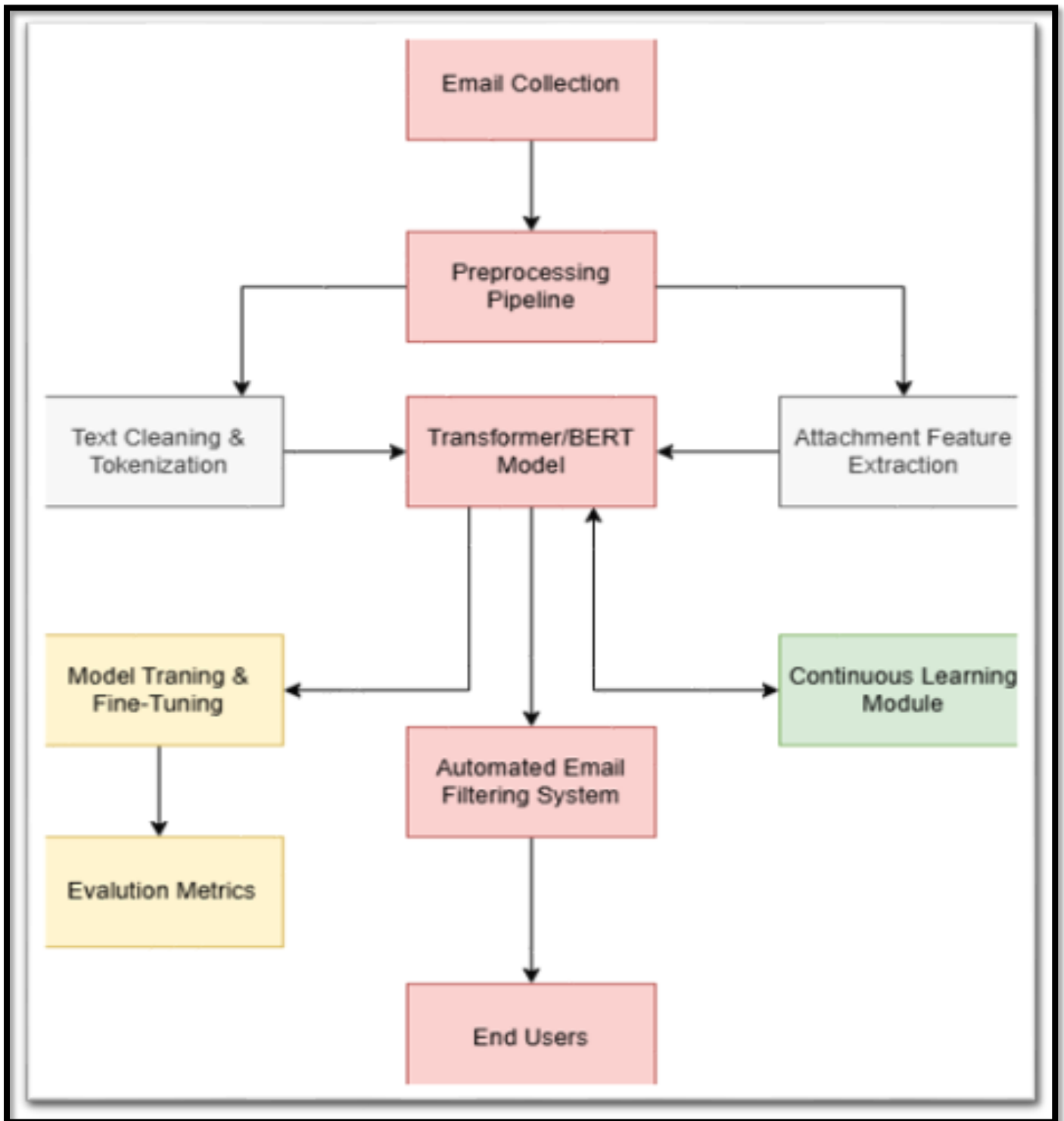
- A dashboard (using tools like Dash or Kibana) should be included to visualize phishing threats.
- Users ought to be able to filter and analyze detected phishing emails with ease.
- The system should automatically generate reports for cybersecurity teams.

Category	Requirement
Functional	Data collection, preprocessing, phishing detection, model fine-tuning, evaluation, continuous learning, integration with security systems
Performance	Real-time processing, scalability for high email volumes
Accuracy	High precision/recall, minimal false positives
Security	Data encryption, compliance with GDPR
Maintainability	Easy model updates, API support
Usability	Dashboard, visualization, reporting

Overall System Diagram



Component System Diagram



8. Anticipated Benefits

Successfully completing this research will lead to several key advantages

Improved Phishing Detection Accuracy: The fine-tuned BERT model is likely to achieve better accuracy in spotting phishing emails compared to traditional machine learning systems, significantly lowering the chances of successful phishing attacks.

Proactive Defense: The model's capacity to learn and adapt to new techniques will enable us to take proactive measures against zero-day attacks and changing phishing campaigns, effectively reducing the impact of new phishing threats.

Adaptability: Thanks to the continuous learning mechanism, the system will remain responsive to the ever-shifting landscape of phishing attacks, ensuring long-term effectiveness and ongoing protection.

Reduced Human Intervention: Automating the detection and mitigation of attacks lessens our dependence on manual labor, saving time and resources. It also minimizes the risk of human error by automating many processes within the pipeline, making everything more efficient.

Enhanced APT Defense Framework: Improved phishing detection will bolster a stronger and more effective defense framework, safeguarding against the initial delivery vectors of Advanced Persistent Threats.

9. Research Constraints

Here are a few potential limitations we've noticed for this research project:

Data Collection Challenges: It can be tough to find real-world phishing emails, and putting together a varied and representative dataset isn't easy either. To tackle this, we'll use publicly available data sources and keep looking for new samples to train our models.

Technical Complexity: Getting BERT models up and running, plus fine-tuning them, demands a good amount of technical know-how and computational power. We'll address this by making use of modern machine learning tools and libraries and optimizing the models for better efficiency [10].

Integration Hurdles: Merging the model with existing security systems, like email gateways and SIEM platforms, might bring along some technical obstacles and may

need further research and development. Our research will be designed for modular integration with current systems.

Computational Resources: Fine-tuning deep learning models needs a lot of computational resources, particularly GPUs. We plan to use high-performance computing systems to tackle this limitation.

10. Project Plan

The research project is organized into several phases, with a 12-month timeline

Phase 1: Data Collection and Preprocessing (Months 1–3)

- Gathering datasets of phishing and legitimate emails.
- Prepping the email dataset, which includes text cleaning, tokenization, and feature extraction.

Phase 2: Feature Extraction and Model Preparation (Months 4–5)

- Extracting and transforming key features from the preprocessed data.
- Implementing attention mechanisms to focus on the most relevant features.
- Configuring and getting the BERT model ready for fine-tuning.

Phase 3: Model Training and Fine-Tuning (Months 6–8)

- Training and refining the BERT model with the prepared data.
- Continuously testing and adjusting the model's parameters to enhance performance.

Phase 4: Model Evaluation and Testing (Month 9)

- Conducting thorough testing and validation of the model using metrics like precision, recall, F1-score, AUC, and confusion matrix.
- Analyzing the testing results and developing suggestions to improve the model.

Phase 5: Integration and Development of Continuous Learning (Months 10–12)

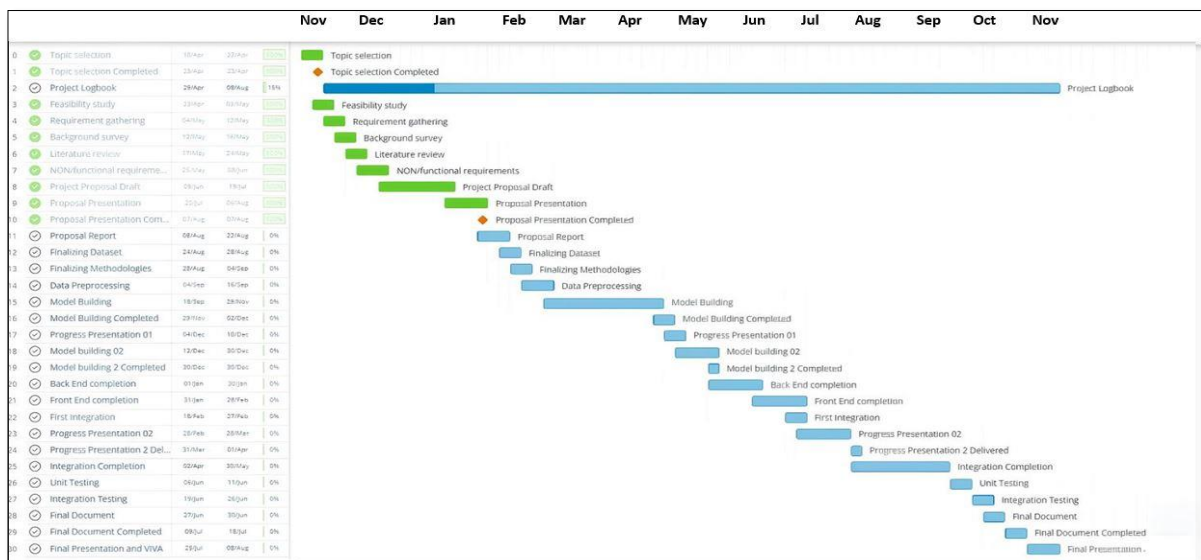
- Setting up a pipeline for the ongoing integration of newly identified phishing methods.
- Creating a procedure for incremental model updates to support continuous learning.
- Integrating the phishing detection system into a broader security framework.

11. Budget and Justification

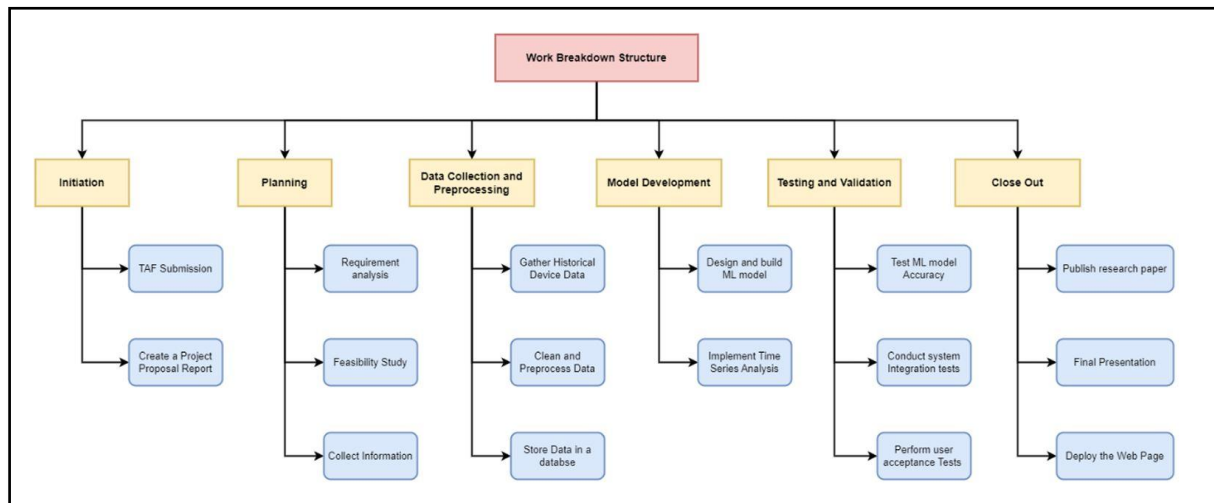
Below is a detailed budget for the project:

- **High-Performance Server:** LKR 20,000. This amount will cover the purchase of a server equipped with GPUs to meet the BERT model's heavy computational requirements. This investment is essential for effective model training and fine-tuning.
- **Machine Learning Tools and Libraries:** LKR 15,000. This funding will go towards licenses and access to vital machine learning and NLP tools and libraries, like TensorFlow, PyTorch, and the Transformers library for implementing BERT.
- **Data Collection and Labeling Tools:** LKR 10,000. This will cover the expenses for tools to gather, label, and manage diverse email datasets from different sources, including tools needed for labeling newly discovered phishing emails for continuous learning.
- **Miscellaneous Expenses:** LKR 5,000. This is for any unexpected project-related costs.

12. Gantt Chart



13. Work breakdown Structure



14. Conclusion

This research project aims to enhance phishing email detection, which is a crucial method used in APT attacks, through the implementation of a finely-tuned BERT model within a comprehensive APT security framework. By utilizing BERT and NLP techniques, our system can adapt to the latest phishing tactics. The automated pipeline for continuous learning will ensure the model stays updated with evolving attack patterns. This project has the potential to significantly boost the effectiveness of APT detection and mitigation by providing a more resilient and adaptable security framework. Its modular design will facilitate easy integration into existing systems, and the automation of processes is likely to improve operational efficiency. In short, we expect this research to create a system that greatly enhances organizations' ability to defend against phishing attacks [11].

15. References

- [1] J. H. A. a. M. K. Rasmussen, "Advanced Persistent Threats and the Need for Phishing Detection," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 45-53, 2024.
- [2] R. D. a. H. J. Lee, "Transformer Architectures: Enhancing Email Security," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 4, pp. 1165-1176, 2024..
- [3] S. Gupta and L. Y. Chen, "The Role of Natural Language Processing in Cybersecurity," *IEEE Transactions on Cybernetics*, vol. 546, pp. 1132-1143, 2023.
- [4] T. O. a. A. Patel, "Comparative Analysis of Phishing Detection Mechanisms," in *Proc. of the IEEE International Conference on Communications*, pp. 207-212, 2024.
- [5] E. Thompson, "Data Preprocessing for Machine Learning in Cybersecurity Applications," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 9, pp. 2454-2466, 2023.
- [6] F. M. a. J. Arnold, "Continuous Learning in Phishing Email Detection Systems," *IEEE Transactions on Learning Technologies*, vol. 7, no. 3, pp. 230-242, 2023.
- [7] C. W. a. B. Zhao, "Evaluating the Effectiveness of Phishing Detection Models," *IEEE Access*, vol. 11, pp. 3987-3998, 2024.
- [8] N. F. a. D. Green, "Utilizing BERT in Cybersecurity:," *A Case Study*, in *Proc. of the IEEE Symposium on Security and Privacy*, pp. 332-337, 2023.
- [9] G. S. a. R. Kaur, "Feature Extraction Techniques for Phishing Email Identification," *IEEE Transactions on Cybernetics*, vol. 55, no. 2, pp. 721-733, 2024.
- [10] V. P. a. J. Thompson, "Integrating Machine Learning Models with SIEM Systems for Enhanced Phishing Detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 6, pp. 1042-1053, 2024.
- [11] M. R. a. K. Lee, "K. Lee, "The Impact of AI on Phishing Detection and Response," *EEE Computer*, vol. 58, no. 3, pp. 48-55, 2024.