**ABSTRACT**

In an era marked by the relentless evolution of cyber threats, phishing attacks continue to pose a significant risk to individuals and organizations alike. Conventional methods of detecting phishing URLs often struggle to keep up with the dynamic strategies employed by malicious entities. This paper introduces Phish Not, a cutting-edge cloud-based machine-learning solution meticulously crafted to enhance the precision and agility of phishing URL detection.

Phish Not employs sophisticated machine-learning algorithms that delve into the intricate dynamics of URLs, scrutinizing their characteristics to discern potential threats. Leveraging the power of cloud computing, the system conducts real-time analyses, enabling the prompt identification and neutralization of phishing threats. Through a combination of lexical analysis, content inspection, and the incorporation of historical URL behavior patterns, Phish Not aspires to provide a robust and adaptable solution to the ever-evolving landscape of phishing attacks.

The cloud-centric architecture of Phish Not not only ensures scalability but also facilitates seamless integration into existing security infrastructures for organizations. Furthermore, the system incorporates continuous learning mechanisms, enabling it to stay abreast of emerging phishing techniques. PhishNot's user-friendly interface and flexible integration capabilities empower security professionals with a potent tool to proactively defend against phishing threats.

In rigorous evaluations, Phish Not demonstrated impressive results, showcasing high accuracy rates in differentiating between legitimate and phishing URLs. The cloud-based deployment model enhances the system's adaptability and responsiveness to the evolving threat landscape, establishing it as a valuable asset in the ongoing battle against cyber threats.

**CHAPTER 1**

**INTRODUCTION**

* 1. **INTRODUCTION**

As the digital landscape continues to evolve, so do the tactics employed by malicious actors seeking to compromise sensitive information through cyber threats. Among these, phishing attacks stand out as a persistent and pervasive menace, exploiting human vulnerabilities to deceive individuals and organizations. Traditional methods of detecting phishing URLs often fall short in keeping pace with the ever-adapting strategies of cybercriminals. In response to this pressing need, we present "PhishNot," an innovative cloud-based machine-learning solution specifically engineered to enhance the accuracy and agility of phishing URL detection.

Phishing attacks commonly involve the use of deceptive URLs designed to mimic legitimate websites, making manual identification challenging. Existing solutions often rely on static analysis or signature-based approaches, struggling to keep up with the dynamic nature of modern phishing campaigns. PhishNot represents a paradigm shift by leveraging advanced machine-learning algorithms to discern patterns and anomalies in URL characteristics, enabling it to make real-time, data-driven decisions regarding the potential threat posed by a given URL.

The cloud-based architecture of PhishNot provides several advantages, including scalability and real-time analysis capabilities. By harnessing the power of cloud computing, the system can efficiently process vast amounts of data, ensuring swift and accurate identification of phishing URLs. This approach not only enhances the efficiency of detection but also facilitates seamless integration into diverse security infrastructures, making it an adaptable solution for organizations of varying sizes and complexities.

This paper delves into the core mechanisms of PhishNot, detailing how it combines lexical analysis, content inspection, and historical URL behavior patterns to create a robust and dynamic defense against phishing threats. The continuous learning capabilities of PhishNot further set it apart, allowing the system to evolve and adapt to emerging tactics employed by cyber adversaries.

In the subsequent sections, we explore the components of PhishNot in detail, presenting experimental results that validate its effectiveness in discerning between legitimate and phishing URLs. As cyber threats continue to evolve, PhishNot stands as a proactive and intelligent defense mechanism, embodying the fusion of cutting-edge machine learning and cloud computing in the realm of cybersecurity.

* 1. **PHISHING**

Phishing is a social engineering attack that exploits the weakness in system processes caused by system users [1]. An attacker can send a phishing Uniform Resource Locator (URL) such that when the user clicks on that link, it takes the user to a phishing website. Phishing URLs are delivered in various ways, including emails, text messages, or on other suspicious websites, with email being the primary phishing medium. The phishing website might have a URL that resembles a legitimate link, such as a social media website, banking website, or an email website, and the webpage on the phishing URL would resemble a legitimate service webpage. It would typically ask the user to log in. At this stage, once the users type their login credentials, they are stolen, and the users are usually redirected to the original login page. In other phishing attacks, clicking on a link could download malware or spyware, install backdoors, or steal session information.

One of the main challenges is the network perimeter can be protected with state-of-the-art firewalls and intrusion detection systems but could still suffer from phishing. Phishing penetrates these protected network borders through encrypted web traffic or via emails. Once the user clicks this phishing URL, malicious activity proceeds to infect the target’s device with malware or perform other harmful actions. Hence, protecting users from phishing is an integral part of securing the network. With the increasing reliance on technology, phishing has become more wide-ranging, intense, and sophisticated. Spear phishing attacks have increased in number and improved in quality. In a spear-phishing attack, the attacker gathers information about a specific user or a small group of users and creates highly-crafted spoofed emails, usually impersonating well-known companies, trusted relationships, or contexts [2]. Another type of phishing is called Vishing, which is Voice-phishing. In vishing, the attack vector is a phone call instead of an email. Lack of user awareness contributes heavily to the success rates of phishing. According to [3], only 52% of users raise an alarm upon receiving a suspected phishing email within 5 min. This behavior indicates weak user awareness about phishing and its potentially harmful impact. It became increasingly challenging when many organizations moved to work from home due to the Covid-19 pandemic. Phishing has become the most widely used attack vector to deliver malicious payloads to targets. According to the 2022 Verizon Data Breach Report, 82% of data breaches involved a human element

* 1. **OBJECTIVES**
* **Enhanced Phishing URL Detection Accuracy**: Develop advanced machine-learning algorithms capable of accurately distinguishing between legitimate URLs and phishing URLs.

Improve detection accuracy by analysing dynamic URL characteristics, including lexical features, content inspection, and historical behaviour patterns.

* **Real-time Phishing Threat Mitigation**: Implement a cloud-based architecture to enable real-time analysis of URLs, ensuring prompt detection and mitigation of phishing threats.

Leverage the scalability of cloud computing to handle large datasets efficiently and enhance the system's responsiveness to emerging threats.

* **Adaptability and Integration**: Design PhishNot to be seamlessly integrable with existing security infrastructures, facilitating easy adoption by organizations with diverse cybersecurity frameworks.

Ensure the system's adaptability to evolving phishing tactics through continuous learning mechanisms, allowing it to stay ahead of emerging threats.

* **User-Friendly Interface**: Develop an intuitive and user-friendly interface for security professionals, enabling them to interact with and manage the PhishNot system effectively.

Provide clear and actionable insights into the analysis results, empowering users to make informed decisions in response to potential phishing threats.

* **Scalability and Resource Efficiency**: Design the system to be scalable, accommodating the varying needs of organizations with different sizes and complexities.

Optimize resource efficiency in cloud-based deployment, ensuring effective URL analysis without compromising system performance.

* **Security and Privacy Considerations**: Implement robust security measures to safeguard the PhishNot system from potential attacks or unauthorized access.

Ensure compliance with privacy regulations by adopting measures that protect sensitive information during the URL analysis process.

* **Validation and Performance Metrics**: Conduct rigorous evaluations to validate the effectiveness and reliability of PhishNot in detecting phishing URLs.

Define and measure performance metrics, such as detection accuracy, false positive rates, and response times, to quantify the system's success in mitigating phishing threats.

**CHAPTER 2**

**LITERATURE REVIEW**

**2.1 EXISTING SYSTEM**

There are various existing systems commonly found in the literature for machine learning based phishing detection.

**Multilayer phishing detection system named PhiDMA:**

PhiDMA provides a model to detect phishing by incorporating five layers: Auto upgrade whitelist layer, URL features layer, Lexical signature layer, String matching layer, and Accessibility Score comparison layer. They built a prototype implementation of the proposed PhiDMA model. The testing results showed that the model could detect phishing sites with an accuracy of 92.72

**Phishing detection system relying on Software Defined Networks (SDN) and Deep Packet Inspection (DPI) named Phishlimiter:**

Phishlimiter starts with DPI and then leverages it with SDN to identify phishing activities through e-mail and webbased communications. The proposed DPI approach consists of two components, phishing signature classification and real-time DPI. The proposed system performs well in the SDN environment but is not suited for applications in end-user environments that are not reliant on SDNs.

**a lightweight deep learning algorithm to detect the malicious URLs and enable a real-time and energy-saving phishing detection sensor**

The proposed deep learning classifier achieved an accuracy of 86.630%. The focus of the study was to create a low-power phishing detector for sensors and Internet of Things (IoT) devices. Although the proposed system acquitted itself well as a lightweight solution, it has a relatively lower and less practicable accuracy performance.

**Presented a machine-learning-based phishing URL detector based on Natural Language Processing (NLP)**

The proposed system used seven classification algorithms and natural language processing (NLP) features. Testing showed the proposed system could achieve an accuracy of 97.98% using an RF classifier, with a relatively high false-positive rate of 3%. These results were achieved using 27 features.

**Machine-learning phishing URL detector named HEFS**

The proposed work suggests a feature reduction from 48 to 10 using a Cumulative Distribution Function gradient (CDF-g) algorithm. Testing showed that the proposed model achieved 94.6% accuracy with 48 features, while accuracy dropped to 94.60% when the features were reduced to 10. They performed another testing phase with a second dataset, where the proposed system achieved 94.27% accuracy with 30 features.

**Machine learning phishing URL detection based on analysis of the HTML code of the web page**

The proposed approach extracts 12 features from the HTML code of the page linked by the URL and feeds that information into a classifier. It achieved 98.4% accuracy on the logistic regression classifier. However, this method is considered high-risk because it reads the actual page contents before deciding whether it is a phishing or benign link. This process can be particularly dangerous if the phishing page contains malware or is used for drive-by attacks.

**A case-based reasoning Phishing detection system (CBR-PDS**)

CBR-PDS aims to improve the detection accuracy and the reliability of the results by identifying a set of discriminative features and discarding irrelevant features. CBR-PDS relies on a twostage hybrid procedure using Information gain and Genetic algorithms. The reduction of the data dimensionality results in an improved accuracy rate and a reduced processing time. Testing shows that CBR-PDS can achieve an accuracy of 95%. However, the system requires high processing power and high memory.

**Decision Tree and Optimal Features based Artificial Neural Network (DTOF-ANN)**

to target proper feature selection to help the ANN classifier perform better [14]. The proposed system starts with improving the traditional k-medoids clustering algrowth with an incremental selection of initial centres to remove duplicate points from the public datasets. Then, an optimal feature selection algorithm based on the newly defined feature evaluation index, decision tree, and local search method prunes out the negative and useless features. Finally, an optimal structure of the neural network classifier is constructed through finely-tuned parameters and trained by the selected optimal features. Testing results demonstrated that DTOF-ANN could achieve an accuracy of 97.80%.

**A hybrid Rule-Based Solution for phishing URL detection using Convolutional Neural Networks (CNN)**

The proposed system extracts 37 features from seven different methods, including the blacklisted method, lexical and host method, content method, identity method, identity similarity method, visual similarity method, and behavioural method. When tested, the proposed system achieved 97.945% with the CNN model and 93.216% for the MLP model.

**SDN-based phishing detection technique based on clustering and CNN**

The proposed work uses Recursive Feature Elimination (RFE) with a Support Vector Machine (SVM) algorithm for feature selection. The SDN transfers the URLs phishing detection process out of the user’s hardware to the controller layer, continuously trains on new data, and then sends its outcomes to the SDN-Switches. RFE-SVM and CNN increase the accuracy of phishing detection. The experimental results showed 99.5% phishing detection accuracy. The proposed work consumed about 500MB of memory, which could heavily overload SDN devices where the classifier operates. Another shortfall of the proposed system is that it uses online training, which can make the classifier model susceptible to adversarial ML attacks

* 1. **DRAWBACKS**

**Static Analysis Limitations**

Many traditional systems relied heavily on static analysis, which involves examining the URL's structure and comparing it to known phishing patterns. This approach struggled to adapt to the evolving and polymorphic nature of phishing URLs, making it less effective against sophisticated attacks.

**Signature-Based Approaches**

Signature-based systems often used known patterns or signatures of phishing URLs to identify threats. However, these systems were prone to false negatives when encountering new or modified phishing techniques that did not match existing signatures.

**Limited Adaptability**

Some existing systems lacked the adaptability to swiftly respond to emerging phishing tactics. As phishing techniques evolved, these systems required manual updates to incorporate new detection methods, leading to delays in protecting against novel threats.

**Inefficiency in Handling Large Datasets**

Systems that did not leverage cloud-based architectures often faced challenges in efficiently processing and analysing large datasets of URLs. This limitation hindered real-time analysis and responsiveness to rapidly changing phishing campaigns.

**Insufficient Behavioural Analysis**

Systems that primarily focused on static or signature-based analysis often lacked the depth of behavioural analysis needed to understand the dynamic aspects of URLs. This made it difficult to identify subtle changes in phishing campaigns, such as modifications in content or redirection patterns.

**Complex Integration Processes**

Integrating some existing solutions into diverse security infrastructures was a complex and time-consuming process. This complexity posed challenges for organizations with varying cybersecurity frameworks, hindering the widespread adoption of these systems.

**False Positive Rates**

Many systems struggled with high false positive rates, flagging legitimate URLs as phishing threats. This not only led to a waste of resources but also eroded the trust of security professionals in the efficacy of the detection systems.

**Limited User-Friendly Interfaces**

The user interfaces of some existing systems were not intuitive or user-friendly, making it challenging for security professionals to interpret results and take appropriate actions effectively.