Üniversite	**:**	**T.C. İstanbul Kültür Üniversitesi**
Enstitüsü	**:**	**Lisansüstü Eğitim Enstitüsü**
Anabilim Dalı	**:**	**Bilgisayar Mühendisliği**
Program	**:**	**Bilgisayar Mühendisliği**
Tez Danışmanı	**:**	**Prof. Dr. Özgür Koray ŞAHİNGÖZ**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – Şubat 2021**

ÖZET

İÇERİK TABANLI OLTALAMA SALDIRISI TESPİT SİSTEMİ

Son yıllarda internet teknolojilerinin kaçınılmaz büyümesi nedeniyle gerçek dünyadaki sistemlerin neredeyse tamamı dijital platformlara aktarılıyor. Bu, özellikle ilgili hizmetlere her zaman ve her yerde konsept ile bağlanmamızı sağlayan mobil cihazlarla hayatımızın her alanında siber uzay kullanımını artırıyor. Bununla birlikte, bu kaçınılmaz genişleme, özellikle standart son kullanıcılar için birçok güvenlik ihlali de beraberinde getirir. Kimlik avı, bilgisayar korsanlarının kendilerini kolayca engelleyerek kullandıkları en çok tercih edilen saldırı türlerinden biridir. Bu tür saldırı, başlangıçta basit bir e-posta veya sosyal medya mesajı ile tetiklenir ve bu mesaj, esas olarak kurbanları kötü niyetli bir web sayfasına yönlendirir. Güvenlik yöneticileri için tespit edilmesi gerçekten zor saldırı türleridir. Bu nedenle, bu makalede içerik tabanlı bir kimlik avı tespit mekanizması önerilmektedir. Teklifte, en iyi eğitim modellerini seçmek için altı farklı makine öğrenimi modeli uygulanmaktadır. Deneysel sonuçlar, önerilen yaklaşımın çok sağlam olduğunu ve güvenlik yöneticileri için kabul edilebilir doğruluklar verdiğini göstermektedir.

Anahtar Kelimeler: Makine öğrenimi, Güvenlik İhlalleri, Saldırılar, Kimlik Avı.

University : **T.C. İstanbul Kültür University**
Institute : **Institute of Graduate Studies**
Department : **Computer Engineering**
Program : **Computer Engineering**
Thesis Advisor : **Prof. Prof. Özgür Koray ŞAHİNGÖZ**
Degree Awerded And Date : **MA – February 2021**

ABSTRACT

CLASSIFICATION OF CONTENT BASED PHISHING ATTACKS BY MACHINE LEARNING METHODS

In recent years due to the inevitable growth of Internet technologies, almost all of the real world systems are transferred to digital platforms. This increases the use of cyberspace in every dimention of our lives especially with mobile devices which enable us to connect to related services in anytime and anywhere concept. However, this ineluctable expansion also brings lots of security breaches especially for standard end users. Phishing is one of the mostly preferred attack type that hackers use by easily hindering theirselves. This type attack is initilally triggered with a simple e-mail or social media message which mainly forward the victims to a malicious webpage. For security admins, they are really hard attack types to detect. Therefore in this paper a content based phishing detection mechanism is proposed. In the proposal about six different machine learning models are implemented to select the best training models. Experimental results show that the proposed approach are very robust and give acceptable accuracies for security admins.

Keywords—machine learning, security breaches, attacks, phishing.