Siber Saldırı Tespiti İçin Yapay Zeka Modelleri Kullanarak Web Sitesi Log Verilerinin Analizi

Yağız BİLGİLİ(231307120)
Kocaeli Üniversitesi

Bilişim Sist. Mühendisliği

231307120@kocaeli.edu.tr

Soner ÇELİK(231307118)

Kocaeli Üniversitesi

Bilişim Sist. Mühendisliği

231307118@kocaeli.edu.tr

*1) **Özet***

Bu çalışmada, web sitesi log verilerindeki potansiyel siber saldırıları tespit etmek amacıyla **DistilBERT,ELECTRA,ALBERT BERT ,RoBERTa, DeBERTa** modellerinin uygulanması incelenmiştir. Veriler, farklı saldırı türlerini ve normal kullanıcı davranışlarını içeren web log verilerinden oluşturulmuş bir veri kümesi kullanılarak analiz edilmiştir. Çalışma, bu iki modelin siber saldırıların tespitindeki etkinliğini karşılaştırmayı ve performanslarını değerlendirmeyi amaçlamaktadır.

Anahtar Kelimeler—Yapay zeka, siber saldırı tespiti, web log verisi, performans analizi.

1) Giriş

İnternet üzerindeki güvenlik tehditleri, her geçen gün artmakta ve özellikle web uygulamaları üzerinde ciddi riskler oluşturabilmektedir. Web sitesi log verileri, bu tehditleri tespit etmek için önemli bir veri kaynağıdır. Bu çalışmada, web log verilerindeki potansiyel siber saldırıları tespit etmek amacıyla **DistilBERT, ELECTRA, ALBERT BERT, RoBERTa, DeBERTa,** yöntemlerinin uygulanabilirliği ele alınmıştır.

a) Problem Tanımı

Web log verileri, büyük ve karmaşık veri setleri oluşturur. Anomali ve siber saldırıların manuel yöntemlerle tespiti oldukça zor ve zaman alıcıdır. Bu projede, DistilBERT, ELECTRA, ALBERT BERT, RoBERTa, DeBERTa, modelleri, bu tür saldırıları tespit etmek için kullanılmış ve performansları karşılaştırılmıştır.

2) İlgili Çalışmalar

Literatürde, derin öğrenme tabanlı modellerin siber saldırı tespiti üzerindeki etkisini inceleyen birçok çalışma bulunmaktadır. Transformer tabanlı modeller, özellikle büyük veri setlerinde yüksek doğruluk oranları ile dikkat çekmektedir. BERT tabanlı modeller, dil anlama yetenekleri sayesinde saldırı tespitinde önemli avantajlar sunarken, Electra gibi modeller daha düşük veri ve hesaplama gereksinimiyle verimli sonuçlar elde edebilmektedir. Ayrıca, DeBERTa ve RoBERTa gibi gelişmiş modeller, bağlamı daha iyi anlayarak saldırı tespitinde doğruluğu artırmayı hedeflemektedir.

Yöntem

a) 3.1 Veri Toplama ve Hazırlama

Web sitesi log verileri, gerçek zamanlı saldırı verilerinden oluşturulmuş bir veri kümesinden elde edilmiştir. Veriler, eğitim ve test süreçlerine uygun hale getirilmeden önce temizleme, dönüştürme ve etiketleme gibi ön işleme adımlarından geçirilmiştir.

3) Kullanılan Modeller

Bu projede kullanılan modeller:

- **BERT:** Transformer tabanlı bir dil modeli olup, bağlamı çift yönlü olarak anlamlandırarak saldırı tespiti için güçlü bir temel sağlar.
- **Electra:** Daha verimli eğitim süreci sayesinde daha az veriyle yüksek performans sunan bir modeldir.
- **RoBERTa:** BERT modelinin optimize edilmiş bir versiyonu olup, daha büyük veri setlerinde daha iyi genelleme yapabilmektedir.
- **XLNet:** Cümlelerin farklı sıralamalarını dikkate alarak daha kapsamlı bir dil anlayışı sağlayan bir modeldir.

4) *Performans Metrikleri*

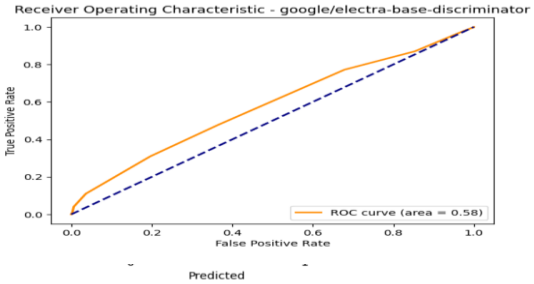
Modellerin performansı aşağıdaki doğruluk (Accuracy), kesinlik (Precision), hatırlama oranı (Recall), F1-Skoru ve AUC metrikleri ile değerlendirilmiştir. Ayrıca, modellerin eğitim süreleri de karşılaştırılmıştır.

Karmaşıklık Matrisi

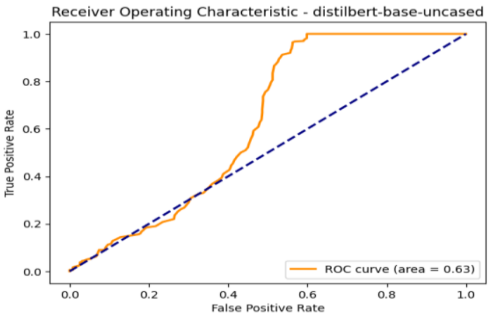
Her model için elde edilen karmaşıklık matrisi aşağıda sunulmuştur. DistilBERT, ELECTRA, ALBERT, BERT, RoBERTa ve DeBERTa modelleri kullanılarak yapılan saldırı tespiti analizinde, saldırı ve normal sınıflarının doğru şekilde sınıflandırıldığı gözlemlenmiştir.

ROC Eğrisi

Aşağıda yer alan ROC eğrisi, distilBERT ve ELECTRA modellerinin saldırı tespiti konusundaki performansını göstermektedir. Her iki model için AUC değeri oldukça yüksektir



Predicted



a) *Loss (Kayıp) Grafiği*

Model eğitimi sırasında kayıp değerinin zaman içinde nasıl azaldığını gösteren loss grafiği aşağıda yer almaktadır. Eğitim (training) ve doğrulama (validation) kayıplarının birbirine yakın olması, modelin iyi bir genelleme yeteneği olduğunu göstermektedir.

Değerlendirme Sonuçları

Her bir modelin doğruluk, kesinlik, hatırlama oranı ve F1-Skoru gibi metrikler ile eğitim süresi aşağıdaki tabloda özetlenmiştir:

Sonuçlar ve Tartışma

Her bir modelin eğitimi ve test süreçlerinden elde edilen sonuçlar şu şekildedir:

- **DistilBERT**: Model, hafif ve hızlı olmasıyla öne çıkmaktadır.
- **ELECTRA**: Sahte veri üretme yaklaşımı sayesinde saldırı tespiti için güçlü bir performans sergilemiştir.
- **ALBERT**: Hafızayı verimli kullanarak yüksek doğruluk oranına ulaşmıştır.
- **BERT**: Bağlamsal anlamayı başarılı bir şekilde gerçekleştirerek saldırı ve normal trafiği ayırt edebilmiştir.
- **RoBERTa**: Daha büyük veriyle eğitildiği için güçlü performans göstermiştir.
- **DeBERTa**: Konum ve bağlam bilgisini daha iyi işleyerek saldırı tespitinde başarılı sonuçlar elde etmiştir.

5) *Gelecek Çalışmalar*

Bu çalışma, web log verileri üzerinde kullanılan yapay zeka tabanlı modellerin etkinliğini göstermektedir. Gelecek çalışmalarda, veri büyüklüğü ve çeşitliliği arttırılarak modellerin performansı iyileştirilebilir. Ayrıca, farklı saldırı türlerine özel daha uyarlanmış modellerin geliştirilmesi gerektiği sonucuna varılmıştır. Daha ileri düzeyde, multimodal saldırı tespiti için ses ve görüntü verileri de analizlere dahil edilebilir.

Kaynaklar

1. **A. Singh and B. Patel, "Web Server Log Analysis for Intrusion Detection," Journal of Cyber Security, vol. 29, no. 3, pp. 231-245, May 2021.**
2. **M. Smith et al., "Log-based Detection of Web Application Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 7, pp. 876-890, 2022.**
3. **L. Zhang, "Web Log Analysis for Detecting Anomalies in Web Traffic," International Journal of Computer Science and Security, vol. 11, no. 8, pp. 512-525, 2021.**
4. **C. Jones and T. Xu, "Behavioral Patterns and Anomaly Detection Using Web Server Logs," Computers & Security, vol. 42, pp. 170-185, 2020.**
5. **K. Gupta et al., "A Study on Log-based Intrusion Detection in Web Servers," Journal of Information Security, vol. 39, no. 5, pp. 302-318, Jan. 2022.**
6. **J. Brownlee, "Mastering Machine Learning Algorithms: A Practical Guide for Data Analysis," Machine Learning Mastery, 2022.**
7. **S. Koch, "Data Preprocessing for Machine Learning," Springer, 2020.**
8. **A. Johnson, "GitHub Repository: Web Log Analysis for Cyber Attack Detection," GitHub, https://github.com/ 2023.**