TÜRKÇE TWİTTER AKIŞI VE TÜRKÇE GAZETE VERİLERİNDEN SİBER GÜVENLİK OLAYLARININ OTOMATİK TESPİT EDİLMESİ

Jüri Sonrası Tez Düzeltmesi Kapsamında Yapmış Olduğum Çalışmalar:

# takip listelerinin oluşturulması

Bu kapsamda geçmişte gerçekleşen siber güvenlik olaylarını içeren datasetler oluşturmam gerekmekteydi. Geçmiş tarihli istediğim ölçütlerde ve kısıtlamalarda Türkçe datasetler online ortamda bulunmamakta ve bu sebeple dataset oluşturma yazılımını kendim yazmam gerekmekteydi. Tezde o ana kadar Twitter Standart API’sini kullanmaktaydım. Twitter’da geçmiş bir olay üzerinden analiz yapmak Twitter'ın Standart Api'si sadece son 7 gün verilerini çekmemize izin verdiği için API’nin ücretsiz versiyonunda yapılabilir bir şey değildi. İstenen geçmiş tarihli verilere ancak ücretli versiyon olan Twitter Premium API ile erişim sağlayabilirdim. Twitter’a yapmış olduğum akademik çalışmayı açıklayan, yazmış olduğum tezden bölümler içeren bir mail attım. Twitter çalışmama destek olmayı kabul etti ve aylık 50 sorgu atabileceğim Premium API’yi ücretsiz olarak verdi.

Analizimde kullanmak için nic.tr DDOS saldırısını seçtim. Nic.tr saldırıları 14 Aralık 2015 de başlamış ve yaklaşık 2 hafta devam etmişti. 14.12.2015-29.12.2015 tarihleri arasında içinde "nic.tr" geçen Türkçe tweetleri çektim. Daha sonra saldırı öncesi geçmiş 1 yılın verilerini çektim. Ve son olarak saldırının başladığı gün olan 14 Aralık 2015 tarihindeki tweetleri çektim. Bu 3 ayrı database’i analiz ederek içlerinden siber güvenlikle ilgili kullanabileceğimiz kelimeleri seçmemiz gerekmekteydi. Bu aşamada TF-IDF (Term Frequency-Inverse Document Frequency) tekniği kullanarak kelimeleri seçmeye karar verdik. İlgili datasetleri kullanarak TF-IDF analizi yaptık ve siber güvenlikle ilgili anahtar kelimeler listemizi bu analiz doğrultusunda güncelledik.

Daha sonra oluşturmuş olduğumuz anahtar kelimeler listesiyle yazılım çözümümüzü test etmek için nic.tr DDOS saldırısı ile ilgili databaseler oluşturmam gerekmekteydi. Ancak ilgili databaseleri oluştururken Twitter’ın bana verdiği aylık 50 sorguluk Premium API hakkı bitti. Twitter Premium API 100-1900 dolar arasında değişen bir aylık ücrete sahip. Bu sebeple satın almak yerine alternatif çözümler aramaya başladım. Bu esnada Selenium otomasyon aracının bu tür bir iş için kullanılabileceğini farkettim. Selenium ve Chrome driver kullanarak Twitter’dan data çekmek için bir Python kodu yazdım. Çözümüm Api ile çekmek yerine normal bir kullanıcı gibi, Chrome browser ı açıp, Twitterın arama kutusuna belirlediğim query i yazıyor ve daha sonra html sayfasını parse ediyor. Bu çözüm daha önce aklıma gelmişti ama html dinamik olarak yaratıldığı için sayfayı nasıl aşağı kaydırabileceğimi bulamamıştım. O yüzden api çözümüne yönelmiştim. Selenium ve chrome web driver bunu yapabiliyormuş. Selenium kullanarak Twitter dataseti oluşturma daha önce yapılmış bir çözüm değil. İlgili yazılımı diğer kodlarla birlikte Github’da paylaşacağım. Data analizi ile uğraşanlar tarafından Premium API satın almak yerine kullanılabileceğine inanıyorum.

Selenium çözümünü kullanarak ilgili databaseleri oluşturdum. Saldırı öncesi 1 yıllık süreçteki tweetleri çektiğinde 2310 tweet buldu. Saldırının başlaması sonrası 2 haftalık süreçteki tweetleri çektiğinde 400 tweet buldu. Saldırı günü ise 38 tweet buldu.

Bu databaseleri ve belirlemiş olduğumuz anahtar kelimeleri kullanarak yazılım çözümümüzü çalıştırdığımızda belirlediğimiz test kriterlerine göre başarılı sonuçlar verdi. Nic.tr saldırısını hassaslık ve duyarlılık açısından başarılı şekilde tespit edebildi. Bir olay olduğunda olayın olduğu gün tespit edebiliyor olmasını ve ilgili tespitin birkaç hafta boyunca devam edebilmesini duyarlılık olarak düşündük. Bu açıdan yaptığımız testler başarılı çıktı. False-positive sayısının az olmasını belirlilik olarak düşündük. False-positive oranı denemiş olduğumuz datasetlerde %30 civarında, bu açıdan da çözümümüzün başarılı olduğuna karar verdik.

# System Archıtecture and Desıgn and Methodology düzeltmeleri

System Architecture and Design chapterını System Architecture and Design and Methodology olarak değişitirdim.

* **Approach** u güncelledim.
* **Determination of Cybersecurity Related Keywords Vector** adında bir başlık ekledim.
* **Data Collection**’ı daha detaylı olarak açıkladım. Bu kapsamda karşılaştığım problemlerden ve nasıl çözdüğümden bahsettiğim bir bölüm ekledim.
* **Data Processing** kısmında kullanmış olduğum NLP ve text mining tekniklerini daha ayrıntılı olarak açıkladım.
* **Cybersecurity Related Event Detection**’da tespit için kullandığım tekniklerden bahsettim. (Term frequency-inverse document frequency (TF-IDF) technique, keyword-based analysis, the statistical technique, and A/B testing ve Machine Learning tekniklerinden Anomaly Detection)

# Results düzeltmeleri

Results kısmına daha önceki çalışmalarıma ilave olarak geçmiş siber güvenlik olaylarını kullanarak oluşturduğum training datasetlerin sonuçlarını ekledim. Geliştirmiş olduğumuz çözümün hangi açılardan başarılı hangi açılardan başarısız olduğuna değerlendirme kriterlerini de belirterek açıkladım. Birtakım trade-off’ lardan bahsettim, takip listelerinin daha geniş tutulmasının veya daha dar tutulmasının geliştirmiş olduğumuz yazılımı nasıl etkilediğinden bahsettim.

# Diğer Düzeltmeler

Diğer chapterları da Juri’nin öneri ve istekleri doğrultusunda düzelttim ve güncelledim. Örneğin yazılım dosyalarıyla ilgili açıklamalarımı Appendix e taşıdım. Yeni oluşturduğum takip listesini Appendix e ekledim.

# tezin Kaynak kodlarının paylaşımı

Geliştirmiş olduğum yazılımı, oluşturduğum ve kullandığım datasetleri, analiz sonuçları gibi bilgileri GitHub private repository’de tutuyorum. Tez ile ilgili çalışmalarım devam ettiği için public erişime açmadım. İlgili kaynak kodları, datasetleri ve analizleri görebilmeniz için repo’nun ilgili bölümlerini Google Drive a yükledim. Aşağıdaki link üzerinden erişim sağlayabilirsiniz.

<https://drive.google.com/drive/folders/1nqLzdiSt8oiKLupq_et71mKc4eG17hu0?usp=sharing>

Juri talep ederse ve Github hesaplarını benimle paylaşmaları halinde tez çalışmalarımın bulunduğu Github repo’suna collaborator olarak da ekleyebilirim.