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

Jüri Sonrası Tez Düzeltmesi Kapsamında Yapmış Olduğum Çalışmalar:

Jürinin önerdiği üzere geçmiş siber güvenlik olaylarının Twitter ve haber sitesi verileri derlenerek olayın hemen öncesinde (öncül) ve hemen olayı müteakip (artçıl) haber ve tweetlerde frekans analizi yapılarak öncül ve artçıl belirteç kelimelerin bulunması ve bunlara bağlı takip listelerin oluşturulması üzerine bir çalışma yapabilmek için 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, içeriğinde yazmış olduğum tezden bölümler içeren bir mail attım. Twitter çalışmama destek olmayı kabul etti ve aylık 50 sorgu atabileceğim Premium API’yi ücretsiz verdi.

Analizimde kullanmak için etmek için nic.tr DDOS saldırısını seçtim. 14.12.2015-29.12.2015 tarihleri arasında içinde "nic.tr" geçen Türkçe tweetleri çektim. Daha sonra geçmiş 1 yılın verilerini çektim. Ve son olarak saldırının başladığı gün olan 14 Aralık 2015 tarihindeki tweetleri çektim. Bu 3 ayrı database i analiz edip içlerinden siber güvenlikle ilgili kullanabileceğimiz kelimeleri seçmemiz gerekmekteydi. Bu aşamada TF-IDF (Term Frequency-Inverse Document Frequency) 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 olduğum anahtar kelimeler listesiyle yazılım çözümümüzü test etmek için nic.tr saldırısı ile ilgili databaseler oluşturmam gerekmekteydi. Ancak ilgili databaseleri oluştururken Twitter’ın bana verdiği aylık 50 requestlik premium API hakkım 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 kullanarak yazılım çözümümü çalıştırdığımda kendi test kriterlerime göre başarılı sonuçlar verdi. Nic.tr saldırısını detect edebildi. Bir olay olduğunda olayın olduğu gün detect edebiliyor olmasını ve ilgili detectionın birkaç hafta boyunca devam edebilmesini duyarlılık olarak düşündüm. Bu açıdan yaptığımız testler başarılı çıktı. False positive sayısının az olmasını belirlilik olarak düşündüm. False positive oranı %25-%30 civarında, bu açıdan da çözümümüzün başarılı olduğuna karar verdik.

Jurinin bir diğer beklediği düzeltme ise tez dokümanında siber güvenlik olaylarının saptanması için kullanılan yöntemin daha detaylı olarak anlatılması ve tartışılmasıydı. Bu doğrultuda özellikler tezin 4. bölümünün (“System Architecture and Design”) ve 6. bölümünün (“Results”) daha detaylı ve kapsamlı olacak şekilde geliştirilmesi gerekiyordu.

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 detection 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 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 chapterı da Juri’nin öneri ve istekleri doğrultusunda alarak güncelledim. (Örneğin yazılım dosyalarıyla ilgili açıklamalarımı Appendix e taşıdım. Yeni oluşturduğum takip listesini Appendix e ekledim.)