AUTOMATIC DETECTION OF CYBER SECURITY EVENTS FROM TURKISH TWITTER STREAM AND TURKISH NEWSPAPER DATA

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS

OF

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

ÖZGÜR URAL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF MASTER OF SCIENCE

IN

CYBER SECURITY

MAY 2019

Approval of the thesis:

**AUTOMATIC DETECTION OF CYBER SECURITY EVENTS FROM TURKISH TWITTER STREAM AND TURKISH NEWSPAPER DATA**

Submitted by **ÖZGÜR URAL** in partial fulfillment of the requirements for the degree of **Master of Science in Cyber Security Department, Middle East Technical University** by,

Prof. Dr. Deniz Zeyrek Bozşahin

Dean, **Graduate School of Informatics**

Prof. Dr. Aysu Betin Can

Head of Department, **Cyber Security**

Assist. Prof. Dr. Cengiz Acartürk

Supervisor, **Cognitive Science Dept., METU**

Assoc. Prof. Dr. XXX

Co-Supervisor, **Computer Engineering Dept., METU**

**Examining Committee Members:**

Prof. Dr. XXX (\*)

Computer Engineering Dept., METU

Prof. Dr. XXX (\*\*)

Medical Informatics Dept., METU

Prof. Dr. XXX

Cognitive Science Dept., METU

Prof. Dr. XXX

Computer Engineering Dept., Boğaziçi University

Prof. Dr. XXX

Computer Engineering Dept., Bilkent University

**Date: \_***Write your defense date!*

*\*Write the name of the head of the examining committee in the first row.*

*\*\*Write ten name of the supervisor in the second row.*

**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

**Name, Last name : ÖZGÜR URAL**

**Signature :**

# ABSTRACT

AUTOMATIC DETECTION OF CYBER SECURITY EVENTS FROM TURKISH TWITTER STREAM AND TURKISH NEWSPAPER DATA

Ural, Özgür

MSc., Department of Cyber Security

Supervisor: Assist. Prof. Dr. Cengiz Acartürk

May 2019, XX pages

The Internet has different kinds of timely information. Every day, security experts scan the internet and face with security events that affect people, institutions, and governments. An information analyst regularly examines sources to stay up to date on security events require. This situation may lead to a heavy workload for the information analysts if they have not proper tools. For example, an information analyst might want to be aware of cybersecurity incidents, such as a DDoS attack on a government agency website. The earlier they detect and understand the threats, the longer time remaining to alleviate the obstacle and to investigate the incident by means of forensics analyses methods. Therefore, information security analysts need to establish situation awareness of the security events and their likely effects. However, due to volume of information flow, it may be difficult for security analysts and researchers to detect and analyze security events appropriately. There are academic and commercial successful researches to solve this problem. Information analysts actively use such technical solutions in their daily routine.

On the other hand, the internet uses different languages to share information. For instance, information about security events, which effects citizens, institutions and the government in Turkey, are shared on the internet mainly in the Turkish. The present thesis investigates automatic detection of security incidents in Turkish by processing Twitter and news media. It proposes an automatic, Turkish -specific software system that is able to detect cybersecurity events in real time.

Keywords: Cyber Security, Event Detection, Turkish, Twitter, Hurriyet Newspaper.

# ÖZ\_\_

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

Ural, Özgür

Yüksek Lisans, Siber Güvenlik Bölümü

Tez Yöneticisi: Yrd. Doç. Dr. Cengiz Acartürk

Mayıs 2019, XX sayfa

İnternet farklı ve zamana bağlı bilgiler içerir. Güvenlik uzmanları her gün interneti tarıyor ve insanları, kurumları ve hükümetleri etkileyen güvenlik olaylarıyla karşı karşıya kalıyorlar. Bir bilgi analisti gereken güvenlik olayları hakkında güncel kalmak için kaynakları düzenli olarak inceler. Bu durum, uygun araçlara sahip olmadıkları takdirde bilgi analistleri için ağır bir iş yüküne yol açabilmektedir. Örneğin, bir bilgi analisti, bir devlet kurumu web sitesine yapılan DDoS saldırısı gibi siber güvenlik olaylarının farkında olmak isteyebilir. Tehditleri ne kadar erken saptarsa ve anlarlarsa, problemleri hafifletmek ve adli olarak soruşturmak için o kadar uzun süreye sahip olurlar. Bu nedenle, mevcut güvenlik olayları ve olası etkileri hakkında durum bilgisine sahip olmaları gerekir. Ancak, çok sayıda olay nedeniyle, güvenlik analistlerinin ve araştırmacıların bu bilgi akışını yeterli şekilde ele alması zor olabilir. Bu sorunu çözmek için akademik ve ticari başarılı araştırmalar var. Bilgi analistleri bu tür teknik çözümleri günlük rutinlerinde aktif olarak kullanırlar.

Öte yandan, internet bilgi paylaşmak için farklı dilleri kullanır. Örneğin, Türkiye'deki vatandaşları, kurumları ve hükümeti etkileyen güvenlik olayları hakkındaki bilgiler internette çoğunlukla Türkçe olarak paylaşılmaktadır. Bu tez, Türkçe kullanılan Twitter akışlarını ve haber medyalarını işleyerek, güvenlik olaylarının otomatik olarak algılanmasını araştırıyor. Siber güvenlik olaylarını gerçek zamanlı olarak algılayabilen otomatik, Türkçe'ye özgü bir yazılım sistemi önermektedir.

Anahtar Sözcükler: Siber Güvenlik, Olay Tespiti, Türkçe, Twitter, Hürriyet Gazetesi.

# DEDICATION

To My Family

# ACKNOWLEDGMENTS

First of all, I would like to express …..

Besides my supervisor, I would like to thank …..

I would also like to thank all of colleagues from …..

To my wife, …..

# TABLE OF CONTENTS

[ABSTRACT iv](#_Toc6798692)

[ÖZ\_\_ vi](#_Toc6798693)

[DEDICATION viii](#_Toc6798694)

[ACKNOWLEDGMENTS ix](#_Toc6798695)

[TABLE OF CONTENTS x](#_Toc6798696)

[LIST OF TABLES xii](#_Toc6798697)

[LIST OF FIGURES xiii](#_Toc6798698)

[LIST OF ABBREVIATIONS xiv](#_Toc6798699)

[1 INTRODUCTION 15](#_Toc6798700)

[1.1 Motivation 15](#_Toc6798701)

[1.2 Objectives 19](#_Toc6798702)

[1.3 Use Cases 19](#_Toc6798703)

[1.4 Outline 20](#_Toc6798704)

[2 BACKGROUND INFORMATION 21](#_Toc6798705)

[2.1 What is an Information Security Analyst? 21](#_Toc6798706)

[2.2 What is Natural Language Processing? 22](#_Toc6798707)

[2.3 What is Text Mining? 23](#_Toc6798708)

[2.4 Twitter Social Network 24](#_Toc6798709)

[2.4.1 What is Twitter? 24](#_Toc6798710)

[2.4.2 Twitter API 25](#_Toc6798711)

[2.5 Hürriyet Turkish Newspaper as a Data Source 26](#_Toc6798712)

[2.5.1 What is Hurriyet Newspaper? 26](#_Toc6798713)

[2.5.2 Hurriyet Newspaper API 26](#_Toc6798714)

[2.5.3 What is OData 26](#_Toc6798715)

[2.5.4 Hürriyet API - OData Usage 27](#_Toc6798716)

[2.6 Python Programming Language 28](#_Toc6798717)

[2.7 Istanbul Technical University NLP API 28](#_Toc6798718)

[2.8 SQLite Database 29](#_Toc6798719)

[2.9 Other Technologies Used in the Thesis Project 29](#_Toc6798720)

[3 LITERATURE REVIEW 30](#_Toc6798721)

[3.1 Weakly Supervised Extraction of Computer Security Events from Twitter 30](#_Toc6798722)

[3.2 Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an Example 32](#_Toc6798723)

[3.3 DDoS Event Forecasting using Twitter Data 32](#_Toc6798724)

[3.4 Prediction of drive-by download attacks on Twitter 33](#_Toc6798725)

[3.5 SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream 33](#_Toc6798726)

[3.6 Crowdsourcing Cybersecurity: Cyber Attack Detection using Social Media 35](#_Toc6798727)

[4 SYSTEM ARCHITECTURE AND DESIGN 36](#_Toc6798728)

[4.1 Approach 36](#_Toc6798729)

[4.2 Taxonomy 38](#_Toc6798730)

[4.3 Data Collection 38](#_Toc6798731)

[4.4 Data Preprocessing 38](#_Toc6798732)

[4.5 Cybersecuirty Related Event Detection 38](#_Toc6798733)

[5 IMPLEMENTATION 38](#_Toc6798734)

[6 RESULTS 38](#_Toc6798735)

[7 CONCLUSION AND FUTURE WORK 39](#_Toc6798736)

[7.1 Conclusion 39](#_Toc6798737)

[7.2 Future Work 39](#_Toc6798738)

[REFERENCES 39](#_Toc6798739)

[APPENDICES 42](#_Toc6798740)

[APPENDIX A 42](#_Toc6798741)

[APPENDIX B 43](#_Toc6798742)

# LIST OF TABLES

[Table 1: Example high-confidence events extracted using the system published within this paper. 31](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015531)

[Table 2: Example of high-weight features. Context words other than nouns and verbs are replaced with their part of speech tags for better generalization. 32](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015532)

[Table 3 Seed Instances for DDoS Attacks. 32](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015533)

[Table 4 Tweet Examples with Attack Targets. 33](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015534)

# LIST OF FIGURES

[Figure 1: Tweets in Turkish After the TurkTrust Vulnerability Announcement on 3 January 2013 17](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015927)

[Figure 2 : Hürriyet Newspaper News after the Turktrust SSL Vulnerability is Detected 18](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015928)

[Figure 3: Research results of IBM Security Lab about Cyber Security Analysts 23](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015929)

[Figure 4: A Simple diagram to explain what NLP does. 24](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015930)

[Figure 5 Sample Turkish Tweets Related with a Security Incident 26](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015931)

[Figure 6: Architecture of the Keyword Finder Component. 35](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015932)

[Figure 7: Technical Overview of Sonar. 36](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015933)

[Figure 8: A Schematic Overview of Cybersecurity Event Detection System from The Publication. 36](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015934)

[Figure 9: Streamgraph Showing Normalized Volume of Tweets (September 2015 through October 2016) Tagged with Data Breach (red), DDoS Activity (grey) and Account Hijacking (blue) Types of Cybersecurity Events. 37](file:///C:\Users\Ozgur\source\repos\MSThesis\thesis\ozgur_ural_cybersecurity_thesis%20-%20Copy.docx#_Toc7015935)

# LIST OF ABBREVIATIONS

|  |  |
| --- | --- |
| **DDOS** | Distributed Denial of Service |
| **DOS** | Denial of Service |
| **REST** | Representational State Transfer |
| **API** | Application Programming Interface |
| **HTTP** | Hyper-Text Transfer Protocol |
| **OData** | Open Data Protocol |
| **JSON** | JavaScript Object Notation |
| **IDE** | Integrated Development Environment |

**CHAPTER 1**C

# INTRODUCTION

## Motivation

Security awareness tools help security analysts to protect an institution's sensitive and mission-critical data from being stolen, damaged or compromised by attackers. The duration between the disclosure of a new vulnerability and the moment when the security analyst becomes aware of it is crucial for taking appropriate countermeasures in a timely manner.

On 3 January 2013, Google announced a security vulnerability which could allow spoofing using fraudulent digital certificates issued by TURKTRUST Inc.[1] Other companies like Microsoft and Mozilla which may affect this vulnerability followed Google and announced the vulnerability, shared their affected software and devices and suggested actions. After these announcements, Twitter and Turkish newspapers showed a quick reaction. As shown in Figure 1, Twitter users shared the information on the same day immediately after the announcement on 3 January 2013. Since TurkTrust certificates were a major part of certificate use market in Turkey, numerous Tweets circulated in Turkish related to the vulnerability.

According to Statistia, Twitter has 321 million monthly active users at worldwide[2]. Turkey is the fifth country in the list of leading countries with nearly 9 million active users, as of January 2019.[3] Twitter users can tweet in any languages they select. Although there is no statistics about the use of Turkish by Twitter users from Turkey, it is very likely that most of the Turkish Twitter users share their tweets in their native language.

A review of the literature and recent state of technology reveals that most of the research conducted on security event detection focus on English. As of our knowledge, research is lacking on real-time security event detection in Turkish language streams. With emerging internet adoption in Turkey, there are much timely information shared in Turkish. This Turkish information not much help without automated event detection systems Turkish tweets can also be used to detect cyber security events if Turkish language specific steps and requirements shall be added to the detection systems and algorithms.



Figure 1: Tweets in Turkish After the TurkTrust Vulnerability Announcement on 3 January 2013

Of course, social media is not the only option to learn such information. The security analyst has a wide range of sources available like the specialized press, blogs, forums, news agencies, newspapers and so on to gather cyber threat information. However, their first reference to detecting such security events is generally social networks. After a trending event occurred, people increasingly share posts about it on social media. To illustrate, A DDOS attack to a service or a website generally firstly recognized and reported by users and they share that on online platforms like tweeting "X website is unreachable."

An alternative way to learn such information is newspapers. After the Türktrust SSL vulnerability in 2013, the newspapers also share that information as fast as possible. In Figure 2, we can see news published in Hurriyet newspaper related to the vulnerability.[4]



Figure 2 : Hürriyet Newspaper News after the Turktrust SSL Vulnerability is Detected

An autonomous system which can use a different kind of data source for security event detection would be beneficial for a security analyst. We designed and developed a software system capable of detecting and monitoring cybersecurity-related events over the Twitter Stream in Turkish. It can technically process millions of documents per day and detect security events. To gain more accurate results, we added the Hürriyet Turkish newspaper stream to analyze and detect security events. The software solution’s infrastructure supports adding new data resources quickly. For example, we can add LinkedIn, Facebook, Eksisozluk website streams to gain more accurate results.

## Objectives

The objectives of this thesis are the followings.

* We research and compare “state of the art” studies and software systems in real time event detection with literature review.
* We research possible data sources to determine the most suitable ones to use it for real-time event detection with the Turkish language.
* We research useful studies and API's related to NLP to use it for normalization of Turkish texts.
* We design and develop the software system to use its real-time cybersecurity event detection using Turkish texts.
* We design the system as a framework to make useable it for other researches. Turkish datasets are useful for various research areas like text classification, author detection, automatic question answering and so on. However, finding datasets in the Turkish language is extremely hard because there are not enough shared datasets online. With the thesis software framework researchers effortlessly get datasets in the Turkish language. Moreover, they can select and modify their queries by changing keyword vectors.
* We validate the proposed approach using several detected events within shared in the Turkish language.

## Use Cases

Cybersecurity is an emerging topic in Turkey just like the rest of the world. There are a few kinds of research about automated security event detection system in the world. However, these studies focus on data mining in the English language. Even if these systems can be beneficial for detecting global level cyber security events, such systems cannot be used with other languages like Turkish, because data mining is a language-specific area. Security analysts who work in Turkey or just interested in Turkey specific security events can use data in the Turkish language to detect such events. With observing these, a security analyst gets situation awareness in cyberspace and take actions against new threads. For example, assume that a security analyst works for a Turkish company and his company uses local websites API like Ekşi Sözlük API e-Devlet API or libraries/frameworks developed for focused Turkish people. If these API's, libraries or frameworks have vulnerabilities and someone discovers them, they are probably discussed and announced within social media like Twitter in Turkish. Turkish newspapers are published it as breaking news and so on. The software system shall listen to Turkish data sources and process the data specific to the Turkish language. Our research meets these requirements to develop such a software system and framework.

## Outline

* Chapter 2 is related to background information. Technologies, terminologies and standard terms discussed and explained in this section.
* In Chapter 3, we share literature researches related to the thesis.
* In Chapter 4, we explain the software system in both architectural and design perspective.
* In Chapter 5, we explain the software system in the implementation perspective.
* In Chapter 6, we discuss thesis results.
* Finally, in chapter 7, we state the conclusion and explain possible future works.

**CHAPTER 2**

# BACKGROUND INFORMATION

## What is an Information Security Analyst?

According to careerexplorer website[5] an information security analysts, the primary responsibility is taking measures to protect his company’s mission-critical and sensitive information and be prepared for a cyber attack. To be prepared for the cyber attack, they use different tools and systems. One of their responsibility is analyzing data and recommending changes to higher-ups. However, they are not authorized and implement changes. Their main job is keeping cyber attacks out.

Security analysts spend nearly one hour with getting caught up on the latest security news through bulletins, forums, news, social networks an so on to identify new threads. They spend two or three hours with the repeated investigation of potential security incidents using online resources. They spend the rest of their daily time with manually copying and pasting information from disparate and siloed tools to correlate data. They generally face with ten to twenty challenge daily. Their investigation time gives cyber attackers advantages, and it is tough for them to keep up with threads.

In Figure 3[6] below, there is a result of research about security analysts to explain why security analysts need automated systems.



Figure 3: Research results of IBM Security Lab about Cyber Security Analysts

It is not sustainable without automated systems.

## What is Natural Language Processing?

NLP is “the ability of machines to understand and interpret human language the way it is written or spoken”[7]. In figure 4[8], can be seen as a simple explanation of What NLP does. In this thesis, we used a few NLP techniques and Istanbul Techincal University’s NLP Api[9] for normalization of the texts.



Figure 4: A Simple diagram to explain what NLP does.

## What is Text Mining?

The Oxford English Dictionary defines text mining as “the process or practice of examining large collections of written resources to generate new information, typically using specialized computer software.”[10] Text mining consists of a broad variety of methods and technologies. In this thesis, we used Keyword-based technologies and statistics technologies. According to expertsystem website, Keyword-based technologies definition is “The input is based on a selection of keywords in text that are filtered as a series of character strings, not words nor concepts.”[11] and statistics technologies definition is “Refers to systems based on machine learning. Statistics technologies leverage a training set of documents used as a model to manage and categorize text.”[11]

## Twitter Social Network

### What is Twitter?

Twitter is an online social networking service, which was created in October 2006 by Jack Dorsey, Even Williams, and Biz Stone. People use Twitter for various purposes[12].

First of all, One of its usage examples is as a social messaging service. Users can interact with the other users, communicate with their friends and family and share details of their lives. Secondly, users can use it as a microblogging service for sharing details of a person’s life. Thirdly, users can use Twitter as a marketing tool for public relations. Many celebrities and politicians use Twitter for interacting with their audience. Lastly, Twitter is an information platform on which users can get news via broadcasting agents’ or journalists’ accounts fast and efficiently. Moreover, there are Twitter bots created by developers for a precise function like Bitcoin ticker bot will tweet every hour the price of Bitcoin in Turkish Lira.

According to the first quantitative study on Twitter “What is Twitter, a Social Network or a News Media?” which is published in 2010[13], Twitter is more an information sharing network than a social network. They found that result while working on Twitter follower graph. They decided that because of the low rate of reciprocated ties. People tend to use Twitter as a news feed by following multiple online news media, but other Twitter users will only follow “real” users.

Twitter users can post a short message called tweet which is limited with 280 characters, or retweet another user tweet. Photos, videos or URLs can be added to the tweets. Users can follow other accounts and creates their networks. They can mention each other or reply to each other within their tweets. To identify what the tweet is about, users use word preceded by a hash sign (#). Twitter uses these hashtags to define trending topics both locally and globally. Users use the trending topic lists to identify favorite subjects at that time on Twitter.

In default settings, all Twitter accounts are public. Users can interact with each other like replying other user's tweets, sending a private direct message and so on.

Figure 5 Sample Turkish Tweets Related with a Security Incident

### Twitter API

The Twitter API is a set of URLs. The URLs cant take parameters and let users access Twitter features like finding tweets which contain a set of specific words and so on.

Twitter provides several APIs to get tweets:

Twitter’s REST API allows users to get tweets which or search terms which includes specific parameters. It is useful for analytics on historical data because this API does not give users live data. Moreover, this API cannot retrieve tweets older than seven days.

Twitter’s Streaming API gives users access to live data on Twitter and keeps sending it until asked it to stop. Developers can access only 1% sample of all the tweets. Its typical usage is when doing analytics over live campaigns on Twitter and so on.

## Hürriyet Turkish Newspaper as a Data Source

### What is Hurriyet Newspaper?

Hürriyet is one of the major Turkish newspapers, founded in 1948. As of January 2018, it had the highest circulation of any newspaper in Turkey at around 319,000.[14]

### Hurriyet Newspaper API

Hürriyet API is an interface which enables the usage of Hürriyet data programmatically in web, mobile, or desktop applications. It is a free service. With Hürriyet API, developers can reach news, columns, writers, photo galleries and pages. Hürriyet API has a RESTful-based, resource-oriented architecture. Developers can access Hürriyet newspaper data via standard HTTP requests. The resultant set of results is in JSON format. Requests via the API are limited to 5 per second and 500 per hour to prevent abuse.[15]

### What is OData

OData is a REST-based data source using the HTTP protocol is a global protocol for querying services. With OData standards, developers do not waste much time on basic standards such as to request and response headers, status codes, HTTP methods (GET, POST and so on), and query options. Developers can only create RESTful APIs by building business logic.

Consuming OData services is easy. Client - interpretable can quickly render OData metadata. Therefore, developers can quickly integrate it into robust and expandable client applications.

### Hürriyet API - OData Usage

The OData structure has a unique query structure. Below are some of the most basic query keywords and their functionality briefly outlined:

$ select: Limits the columns/properties in the response set from the query. Example use;

* https://api.hurriyet.com.tr/v1/articles?$select=Title

To limit relational properties such as Files, RelatedNews; it is necessary to use $ select filter with $ expand. Example use;

* https://api.hurriyet.com.tr/v1/articles?$select=Files&$expand=Files

$ filter: By adding a filter to the query, the answer set can be limited. Example use;

* https://api.hurriyet.com.tr/v1/articles?$filter=Path eq '/gundem/'

Users can also use these keywords together to increase the number of filters in the result set and make it easier to reach the desired result set.

Using OData protocol on Hürriyet API service, these can be queried and used in applications.

* Articles in the system
* Columns in the system
* In-system photo galleries
* The pages in the system and the pages assigned to the pages
* Folders in the system
* Writers

Requests via the API are restricted to block abuse. These limits are five requests per second and 500 requests per hour.

## Python Programming Language

“Python is an interpreted, object-oriented, high-level programming language with dynamic semantics.”[16] It is a multi-paradigm programming language and supports so many paradigms like object-oriented programming, structured programming, functional programming and so on. It has enough frameworks and API to work on cognitive science, text mining, NLP like areas. It is fast enough and learning it is fast. Most big companies use Python in data mining projects. To illustrate, according to a 2014 article in Fast Company magazine, Facebook chooses to use Python for data analysis because it was already used so widely in other parts of the company.[17] In this thesis, we use Python version 3.6.6.

## Istanbul Technical University NLP API

Turkish NLP Tools and APIs developed by the Natural Language Processing group at Istanbul Technical University. The program is available at “tools.nlp.itu.edu.tr” website.[9] The API is free to use for academic purposes. To be able to use the API, we need access token and an account for the token. In order to get them, we sent an email to briefly explain who we are, why we need to access the API and our affiliation. Our application seems okay for them. Therefore, they give us the credentials.

The platform operates as a Software as a Service and provides the researchers and the students the state of the art NLP tools in many layers: preprocessing, morphology, syntax and entity recognition. [18]. It is a web API; developers can access it with an HTTP request and can use GET or post method.

The ITU NLP API components for stand-alone usage are the followings;

• Tokenizer

• Deasciifier

• Vowelizer

• Spelling Corrector

• Normalizer

• isTurkish

• Morphological Analyzer

• Morphological Disambiguator

• Named Entity Recognizer

Twitter API can also filter Turkish Tweets, and Hürriyet is a Turkish newspaper. Therefore, we do not need an “isTurkish” component of the API for the thesis. Currently, we only use the “Normalizer” component of the ITU NLP API.

## SQLite Database

According to SQLite.org website, SQLite is an in-process library that implements a serverless, self-contained, zero-configuration, transactional SQL database engine. Using both commercial and private is free. SQLite is the most widely deployed database in the world including high-profile projects.[19] It is an embedded database engine. Unlike most other SQL databases, SQLite reads and writes directly to ordinary disk files. SQLite does not have a separate server process. In the thesis project, we do not need the server side. Therefore, we choose SQLite to use in the thesis project.

## Other Technologies Used in the Thesis Project

We used Visual Studio Enterprise 2017 as IDE. It is handy especially for debugging the code. Moreover, we used JSON as a data-interchange format. We use gif for version service with GitHub web-based hosting service. Our repository on GitHub is currently private, but we are planning to make it public as an opensource project when we finish the thesis.

**CHAPTER 3**

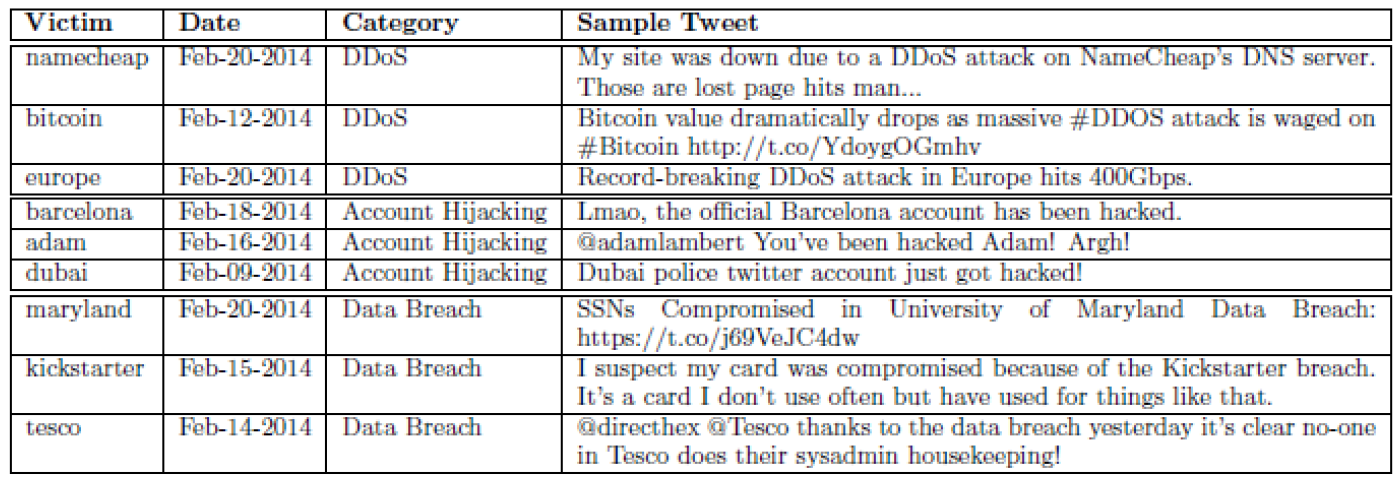
# LITERATURE REVIEW

During the bibliography study, we read and investigate more than forty academic research. They help us to understand the domain. We think some of them are closely related to our researches. These publications are as follows.

## Weakly Supervised Extraction of Computer Security Events from Twitter

Research on identifying victims affected by attacks in these categories as output, using the Twitter data and adding categories to the user without being dependent on fixed categories.[20]

Table 1: Example high-confidence events extracted using the system published within this paper.



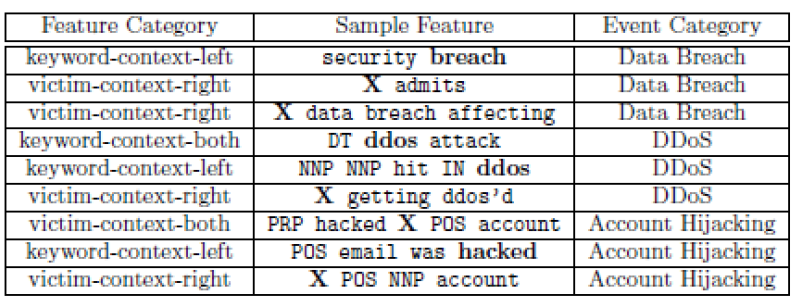
They determine candidate events as in Table 2.

Table 2: Example of high-weight features. Context words other than nouns and verbs are replaced with their part of speech tags for better generalization.

Then they are trying to find the victim, institution or program affected by these events.

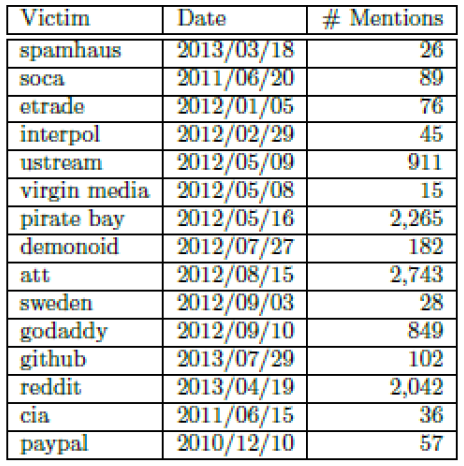


Table 3 Seed Instances for DDoS Attacks.

## Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an Example

That paper[21] is a joint publication of a Ph.D. student from Yıldırım Beyazıt University with one of the professors from his university and a professor at the University of Kent Canterbury form the UK. Using machine learning techniques, they investigated to find a method of whether social media accounts related to cybersecurity.

## DDoS Event Forecasting using Twitter Data

It is a publication[22] to estimate the DDoS attacks that have not yet taken place by processing Twitter data.

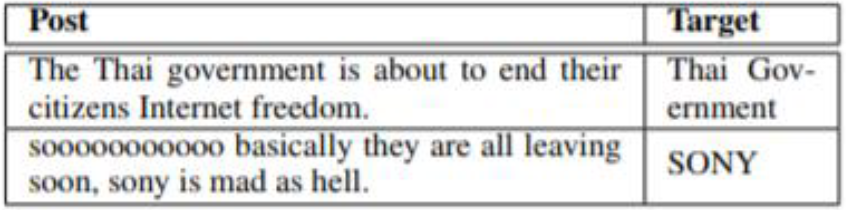


Table 4 Tweet Examples with Attack Targets.

They tried to obtain this information using six popular supervised classification models. To illustrate, one of the models which they used is the “negative term count.”. Neg-Term-count is the baseline sentiment-based model. They count the negative words from tweets each day, forecasting an attack if the number of negative words is more significant than a threshold α, which is the average number of negative words on training data.

## Prediction of drive-by download attacks on Twitter

Some cyber attackers use the URL abbreviation method to show malicious websites as if a harmless website and share them on twitter as an abbreviated URL. Some Twitter users may believe in this deception and click on such website abbreviations, and these links can harm the users. They have explored what we can do to prevent such malicious websites from being clicked like a safe website due to this kind of abbreviation. They try various methods such as detecting malicious software infection from the increase in the use of CPU or RAM with using Honeypot. [23]

## SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream

They developed a self-learning framework called Sonar.[24] Sonar can automatically capture events related to cybersecurity by processing twitter data. Developers give the system some keywords to follow. The system can find other keywords to followed related to cybersecurity with the help of previously given keywords.

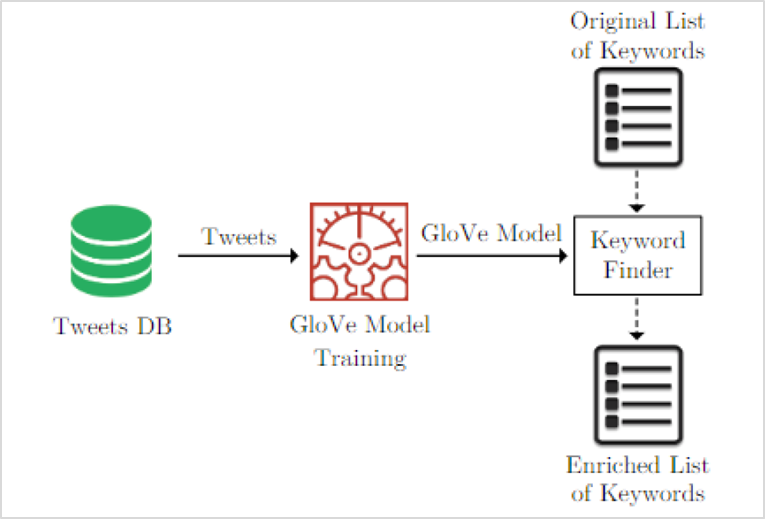


Figure 6: Architecture of the Keyword Finder Component.

They have also benefited from many big data technologies to do their researches.

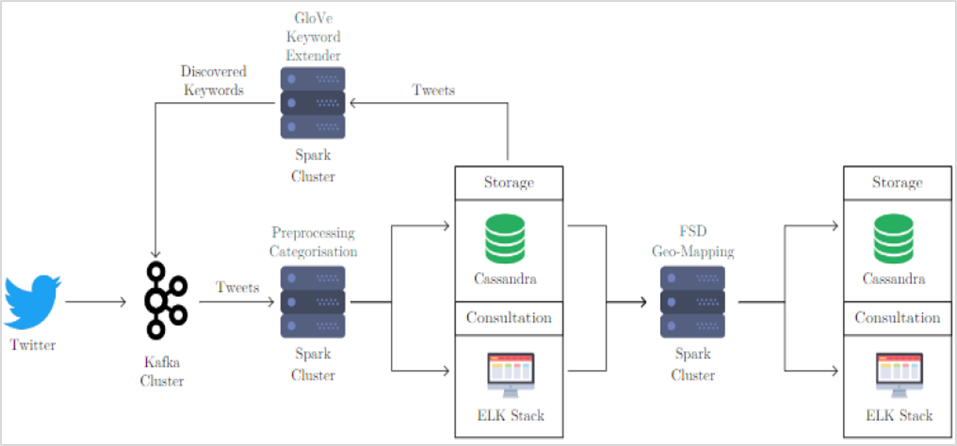


Figure 7: Technical Overview of Sonar.

## Crowdsourcing Cybersecurity: Cyber Attack Detection using Social Media

It is another study on detecting cybersecurity attacks by processing Twitter data. They acknowledge that their work is similar to that of previous studies, but they claim to have more successful results. [25]

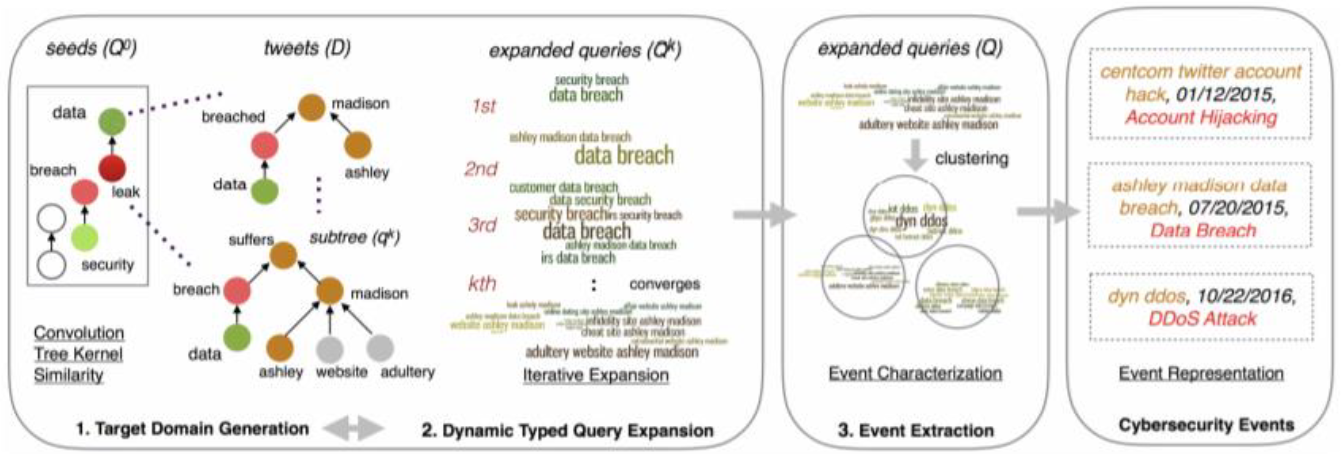


Figure 8: A Schematic Overview of Cybersecurity Event Detection System from The Publication.

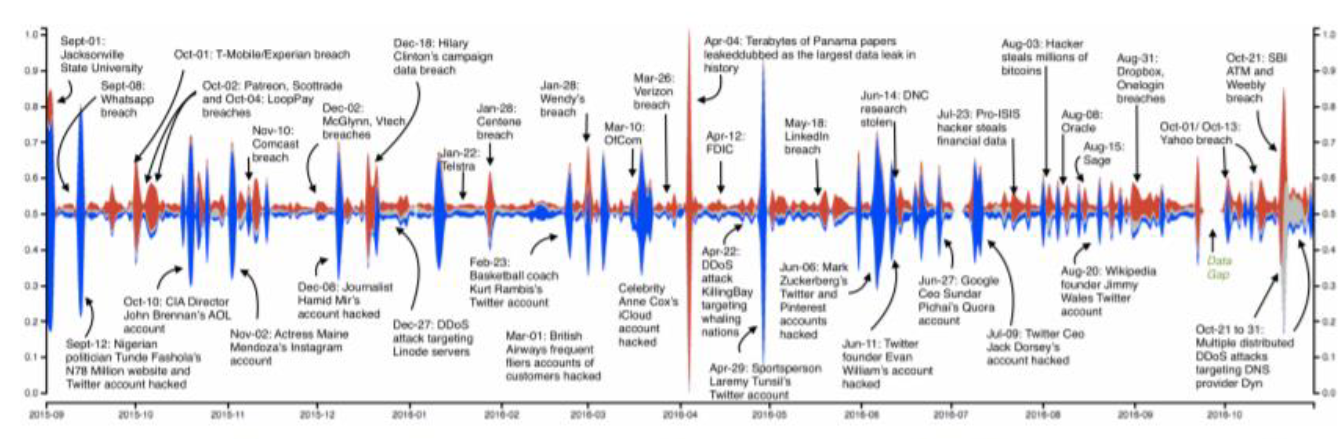


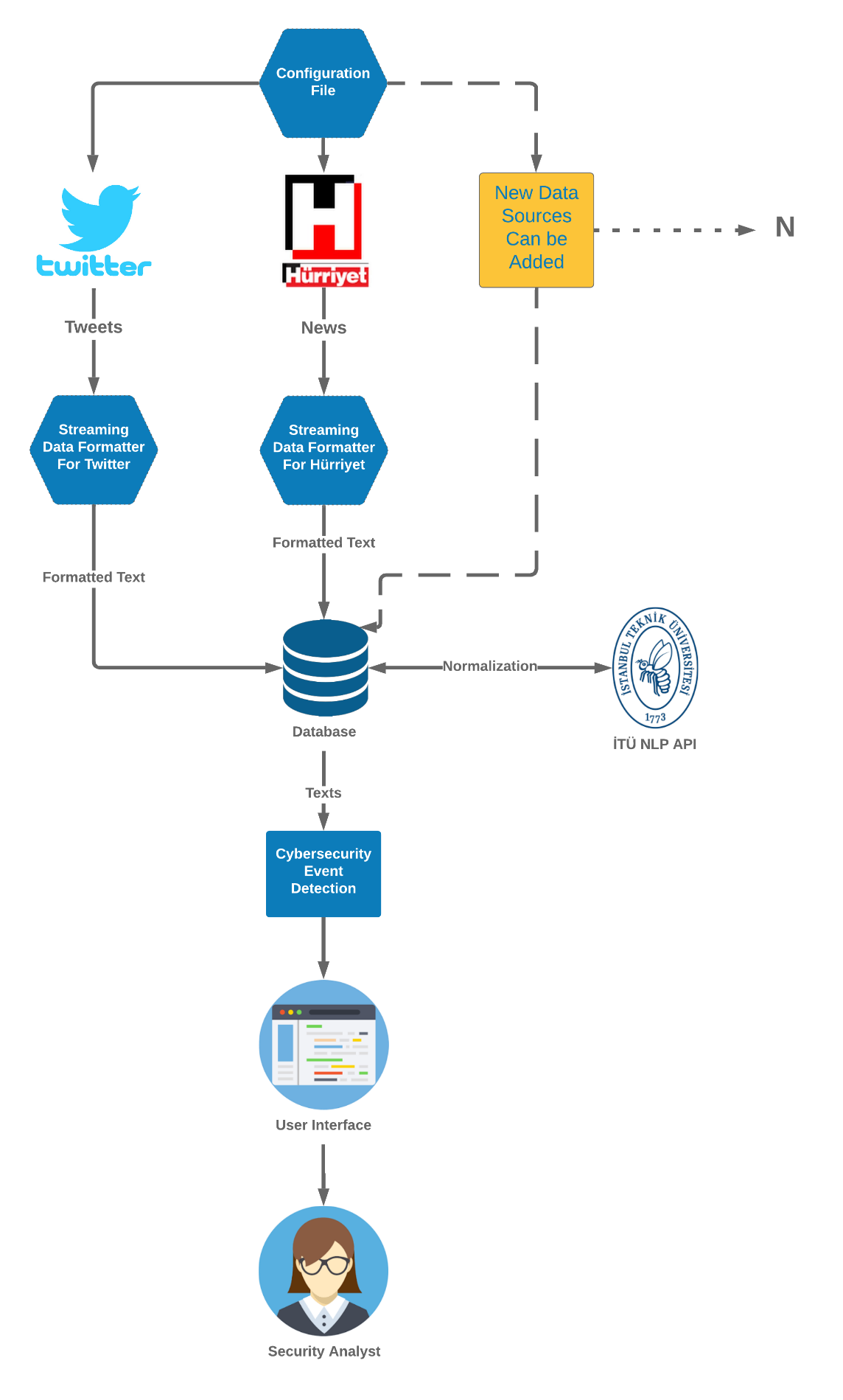
Figure 9: Streamgraph Showing Normalized Volume of Tweets (September 2015 through October 2016) Tagged with Data Breach (red), DDoS Activity (grey) and Account Hijacking (blue) Types of Cybersecurity Events.

**CHAPTER 4**

# SYSTEM ARCHITECTURE AND DESIGN

In this chapter, we explain the software system’s architecture and design.

## Approach



## Taxonomy

## Data Collection

## Data Preprocessing

## Cybersecuirty Related Event Detection

**CHAPTER 5**

# IMPLEMENTATION

**CHAPTER 6**

# RESULTS

**CHAPTER 7**

# CONCLUSION AND FUTURE WORK

## Conclusion

## Future Work

# REFERENCES

[1] A. Langley, “Enhancing digital certificate security,” 2013. [Online]. Available: https://security.googleblog.com/2013/01/enhancing-digital-certificate-security.html. [Accessed: 15-Apr-2019].

[2] Twitter, “Twitter: Number of active users 2010-2017,” *statista.com*, 2019. [Online]. Available: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/. [Accessed: 15-Apr-2019].

[3] “Countries with most Twitter users 2019 | Statistic,” *Statista*, 2019. [Online]. Available: https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/. [Accessed: 15-Apr-2019].

[4] “Yanlış sertifika Google’dan döndü - Teknoloji Haberleri.” [Online]. Available: http://www.hurriyet.com.tr/teknoloji/yanlis-sertifika-googledan-dondu-22290509. [Accessed: 16-Apr-2019].

[5] “What does an information security analyst do? ‐ CareerExplorer.” [Online]. Available: https://www.careerexplorer.com/careers/information-security-analyst/. [Accessed: 18-Apr-2019].

[6] M. Borrett, “Security in the Cognitive Era BRINGING THE POWER OF COGNITIVE SECURITY TO THE SECURITY ANALYST Motivations for Change,” 2017.

[7] “International Journals of Management, IT et Engineering IJMIE.” International Journals of Multidisciplinary Research Academy, IJMRA.

[8] “Overview of Artificial Intelligence &amp; Role of NLP in Big Data - XenonStack Blog.” [Online]. Available: https://www.xenonstack.com/blog/ai-nlp-big-deep-learning/. [Accessed: 18-Apr-2019].

[9] “ITU Turkish Natural Language Processing Web Interface.” [Online]. Available: http://tools.nlp.itu.edu.tr/index.jsp. [Accessed: 18-Apr-2019].

[10] Stephanie Prato, “What is Text Mining? - Information Space,” 2013. [Online]. Available: https://ischool.syr.edu/infospace/2013/04/23/what-is-text-mining/. [Accessed: 18-Apr-2019].

[11] “Text mining vs data mining: discover the differences -.” [Online]. Available: https://www.expertsystem.com/text-mining-vs-data-mining-differences/. [Accessed: 18-Apr-2019].

[12] B. A. Huberman, D. M. Romero, and F. Wu, “Social Networks that Matter: Twitter Under the Microscope,” *SSRN Electron. J.*, 2008.

[13] H. Kwak, C. Lee, H. Park, and S. Moon, *What is Twitter, a Social Network or a News Media?* .

[14] “Tiraj | MedyaTava - Yazmadıysa Doğru Değildir.” [Online]. Available: http://www.medyatava.com/tiraj/2018-01-08. [Accessed: 11-Apr-2019].

[15] “Hurriyet Developers API v1.0 Docs — Hürriyet Public API.” [Online]. Available: https://developers.hurriyet.com.tr/docs/versions/1.0. [Accessed: 11-Apr-2019].

[16] Python, “What is Python? Executive Summary | Python.org,” *Python Software Foundation*. 2017.

[17] “Businesses Can Now Use The Same Stats Language As Universities, Thanks.” [Online]. Available: https://www.fastcompany.com/3030877/businesses-can-now-use-the-same-stats-language-as-universities-thanks-to-pandas. [Accessed: 19-Apr-2019].

[18] G. Eryiğit, “ITU Turkish NLP Web Service,” 2015, pp. 1–4.

[19] Sqlite.org, “About SQLite,” 2013. [Online]. Available: https://www.sqlite.org/about.html. [Accessed: 19-Apr-2019].

[20] A. Ritter, E. Wright, W. Casey, and T. Mitchell, “Weakly Supervised Extraction of Computer Security Events from Twitter,” 2016, pp. 896–905.

[21] Ç. B. Aslan, R. B. Sağlam, and S. Li, “Automatic Detection of Cyber Security Related Accounts on Online Social Networks,” 2018, pp. 236–240.

[22] Z. Wang and Y. Zhang, “DDoS event forecasting using twitter data,” in *IJCAI International Joint Conference on Artificial Intelligence*, 2017, pp. 4151–4157.

[23] A. Javed, P. Burnap, and O. Rana, “Prediction of drive-by download attacks on Twitter,” *Inf. Process. Manag.*, vol. 56, no. 3, pp. 1133–1145, 2019.

[24] J. Petersen, “Sonar,” *Handb. Surveill. Technol. Third Ed.*, no. August, pp. 223–291, 2017.

[25] R. P. Khandpur, T. Ji, S. Jan, G. Wang, C.-T. Lu, and N. Ramakrishnan, “Crowdsourcing Cybersecurity: Cyber Attack Detection using Social Media,” 2017.

# APPENDICES

# APPENDIX A

**TITLE**

xxx

# APPENDIX B

**TITLE**

xxx