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

Internet has many different kind of timely information. Every day, security experts scan the internet and face with lots of security events that effect people, institutions and governments. An information analyst constantly scan many sources to staying up to date on security events require, which leads to information overload to them. For example, an information analyst might want to be aware of cyber security incidents such as a DDOS attack on a government agency website. The earlier they are able to detect and understand the threats, the longer time remaining to alleviate the obstacle and to investigate them forensic. Therefore, they need to have a situation awareness of the existing security events and their possible effects. However, due to the large number of events, it can be difficult for security analysts and researchers to handle this flow of information in an adequate manner. Moreover, internet uses different languages to share informations, like the humans do. As expected, security events related informations which effect Turkish people, Turkish institutions and Turkish government also share in internet mostly in Turkish language. In this thesis, I investigate detection of existing security incidents with using Turkish language, ITU NLP Api, Twitter social network and Hürriyet Turkish newspaper. I propose an automatic, Turkish language specific software system that can detect cyber security events in real time over the Twitter stream in Turkish language and Hurriyet newspaper stream.

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

# ÖZ\_\_

TÜRKÇE TWITTER AKIŞI VE TÜRKÇE GAZETE VERİLERDEN 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 birçok farkı zamana bağlı bilgi içerir. Güvenlik uzmanları her gün interneti tarıyor ve insanları, kurumları ve hükümetleri etkileyen birçok güvenlik olayıyla karşı karşıya kalıyorlar. Bir bilgi analisti, gerekli olan güvenlik olayları hakkında güncel bilgi sahibi olmak için sürekli olarak birçok kaynak taramakta ve bu da onlarda aşırı bilgi yüklenmesine neden olmaktadır. 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. Ayrıca internet, insanlar gibi bilgileri paylaşmak için farklı dilleri kullanır. Beklenildiği gibi, Türk halkını, Türk kurumlarını ve Türk hükümetini etkileyen güvenlik olayları ile ilgili bilgiler de çoğunlukla Türkçe olarak internette paylaşılmaktadır. Bu tezde, mevcut güvenlik olaylarının tespitini Türk dilini, İTÜ NLP Api, Twitter sosyal ağı ve Hürriyet gazetesini kullanarak araştırıyorum. Türk dilindeki Twitter akışında ve Hürriyet gazetesi akışında siber güvenlik olaylarını gerçek zamanlı olarak algılayabilen otomatik, Türkçe’ye özgü bir yazılım sistemi öneriyorum.

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](#_Toc5813557)

[ÖZ\_\_ vi](#_Toc5813558)

[DEDICATION viii](#_Toc5813559)

[ACKNOWLEDGMENTS ix](#_Toc5813560)

[TABLE OF CONTENTS x](#_Toc5813561)

[LIST OF TABLES xi](#_Toc5813562)

[LIST OF FIGURES xii](#_Toc5813563)

[LIST OF ABBREVIATIONS xiii](#_Toc5813564)

[1 INTRODUCTION 14](#_Toc5813565)

[1.1 Motivation 14](#_Toc5813566)

[1.2 Problem Definition 16](#_Toc5813567)

[1.3 Objectives 16](#_Toc5813568)

[1.4 Contributions of the Thesis 16](#_Toc5813569)

[1.5 Use Cases 17](#_Toc5813570)

[1.6 Outline 17](#_Toc5813571)

[2 BACKGROUND INFORMATION 18](#_Toc5813572)

[2.1 What is anInformation Security Analyst? 18](#_Toc5813573)

[2.2 What does an Information Security Analyst do? 18](#_Toc5813574)

[2.3 What is Natural Language Processing? 19](#_Toc5813575)

[2.4 Why do we need Natural Language Processing? 20](#_Toc5813576)

[2.5 Sample Tweets Related with a Security Incident 21](#_Toc5813577)

[2.6 Why is NLP Hard? 23](#_Toc5813578)

[2.7 Twitter Social Network 23](#_Toc5813579)

[2.7.1 Mechanism and Specific Terminology 23](#_Toc5813580)

[2.7.2 Working with Twitter Data 25](#_Toc5813581)

[2.7.3 Twitter, a Social Network? 25](#_Toc5813582)

[2.8 Hürriyet Turkish Newspaper as a Data Source 26](#_Toc5813583)

[3 LITERATURE REVIEW 27](#_Toc5813584)

[4 SYSTEM ARCHITECTURE AND DESIGN 27](#_Toc5813585)

[4.1 Approach 27](#_Toc5813586)

[4.2 Taxonamy 27](#_Toc5813587)

[4.3 Data Collection 27](#_Toc5813588)

[4.4 Data Preprocessing 27](#_Toc5813589)

[4.5 Event Detection 27](#_Toc5813590)

[5 IMPLEMANTATION AND EVALUATION 28](#_Toc5813591)

[5.1 Implemantation 28](#_Toc5813592)

[5.2 Events Evaluation 28](#_Toc5813593)

[5.2.1 Yahoo Data Breach ie 28](#_Toc5813594)

[6 RESULTS 28](#_Toc5813595)

[7 CONCLUSION AND FUTURE WORK 28](#_Toc5813596)

[7.1 Conclusion 28](#_Toc5813597)

[7.2 Future Work 28](#_Toc5813598)

[REFERENCES 29](#_Toc5813599)

[APPENDICES 30](#_Toc5813600)

[APPENDIX A 30](#_Toc5813601)

[APPENDIX B 31](#_Toc5813602)

# LIST OF TABLES

[Table 1: Decision Making Terminology 1](#_Toc444263431)

[Table 2: xxxx 7](#_Toc444263432)

# LIST OF FIGURES

[Figure 1: Tweets in Turkish After The TurkTrust Vulnerability Announcement on 3 January 2013 15](file:///C:\Users\Ozgur\source\repos\MSThesis\tez\tez.docx#_Toc6236406)

# LIST OF ABBREVIATIONS

|  |  |
| --- | --- |
| **DDOS** | Distributed Denial of Service |
| **DOS** | Denial of Service |

**CHAPTER 1**CHAPTER

# INTRODUCTION

## Motivation

Security awareness tools helps security analysts to protect a company's sensitive and mission-critical data from being stolen, damaged or compromised by hackers. The delay between the disclosure and the moment when the security analyst is aware for each newly discovered vulnerability is very important.

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 from 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 quick reaction. As you can see in the Figure 1.1, Twitter users had shared the information on the same day immediately after the announcement on 3 January 2013. I notice that one of the profile who share information about the vulnerability was Asst. Prof. Dr. Süleyman Özarslan, one of the past instructors of METU Cyber Security Department. This is an example of even university professors share timely and valuable informations at Twitter. Because of TurkTrust directly related with Turkey, there were so many Tweets in Turkish related with that vulnerability. According to Statistia website, Twitter has 321 million monthly active users at worldwide[2] and with nearly 9 million active users Turkey is fifth country in the list of leading countries based on number of Twitter users as of January 2019.[3] Twitter users can tweet in any languages they wish. As predictable, 9 million Turkish Twitter users share their tweets generally in Turkish language.

During my literature review and commercial research and products reviews, I realized that even there are a few researches and products to focus on automatic security Event Detection, they mainly focus data mining in English language. There is no research focused on real time security event detection focused Turkish language streams. With emerging internet adoption in Turkey, there are many timely information shared within Turkish language. These Turkish informations not much useful without automated event detection systems Turkish tweets can be also 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 only option to learn such information. The security analyst has a wide range of sources available like specialized press, blogs, forums, news agencies, newspapers and so on to gather cyber threat informations. However, their first reference for detect such security events is generally social networks. After a trending event occurred, people increasingly share posts about it on social media.

In our case, an event is a phenomenon happening during a certain time period which stimulates people to post about it on social media. For example, denial of service attacks are often first reported by users of the website or service under attack. Users of online social networks witnessing or participating in an event are naturally incentivized to discuss it on social media (e.g., tweeting “I cannot reach X website” ). Moreover, Twitter act as a platform where not only cybersecurity media but also mainstream media will tweet about ongoing events and where people can react to such events. Nonetheless, dealing with document such as tweets for the purpose of detecting cyber security related events poses a wide variety of challenges. First, in order to have a general overview of the current situation, the framework must be able to proceed in real-time and in a timely manner a high-volume data. Hence, all the algorithms used should be fast and scalable.

Secondly, given the nature of tweets, documents retrieved are often unusable: there is a lot of duplicates, off-topic, badly written and incomplete documents. As we can get very valuable information (e.g., information on a data breach), we can also get a lot of irrelevant information (e.g., how I feel today). One of the main challenges lies in correctly filtering the noise from the retrieved content. Finally, the lexical field of cyber security event is growing and constantly changing which makes the tracking of new terminology a hard and time-consuming task. Having an autonomous system that leverage social network’s data for security event detection would be extremely useful for a security analyst. Moreover, the ability to have an evolving scope of detected cyber security related events represent a substantial advantage.

To address these challenges, I designed and developed a software system capable of detecting and monitoring cyber security 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, I added Hürriyet Turkish newspaper stream to analyze and detect security events. The software solution’s infrastructure supports adding new data resources. For example, it can be added LinkedIn, Facebook, Ekşisözlük website streams to gain more accurate results.

## Problem Definition

Everyday, thousands of cyber security events happen in the world. Being able to follow all of them in real-time is humanly impossible. Moreover, in a lot of cases the delay between the moment a vulnerability is found and the moment the investigator learns about it is critical. In our case, a digital forensic is interested in knowing in real-time what are the current security events happening in the world. SONAR aims to fix this problem by giving the investigator a framework to see in real-time the cyber security events. Each event is automatically detected using social network. We choose Twitter because it’s the biggest and the easier to access as well as for his uniqueness, meaning how information/news and chatter are tied together. In order to extract as much information from Twitter as possible, we choose to retrieve tweets per keywords. This gives us up to 1% of relevant tweets.

## Objectives

Regarding the previously stated problems, we define here the objectives that we wish to achieve.

In particular, this thesis aims at:

Conducting a comparative study of the state-of-the-art techniques in real-time event detection in Twitter

Elaborating a framework for cyber security events detection in Twitter

Designing and implementing the proposed framework

Validating the proposed approach using several detected events

## Contributions of the Thesis

This section list the main contributions of this thesis regarding the objectives stated above. Our

contributions in this thesis are the following:

The design of a novel, automatic, self-learned, cyber security event detection framework from

social media feeds

A self-learned keywords mechanism based on word embedding to discover new relevant keywords over a corpus of short documents

The development and implementation of this framework

The evaluation of SONAR on 12 months of Twitter data demonstrating the effectiveness of the tool

## Use Cases

A cyber security situation awareness tool provides to the expert a situation awareness capability on what is currently happening in the cyberspace and prioritize their actions toward the new threat. In addition, it is a tool for forensics to observe the chronology of cyber threats on social media and identify potential suspects (for example the first person talking about a newly data breach or malware). Finally, it is a very convenient tool for security teams as it can help them protecting their organization from newly discovered vulnerabilities.

## Outline

The remainder of the thesis is structured as follows. In Chapter 2, we discuss the related work and background knowledge used for this work. Then, in Chapter 3, we detail the architecture and design of our solution. Finally, in Chapter 4 we implement it and evaluate the performance of SONAR before presenting concluding remarks in Chapter 5.

**CHAPTER 2**

# BACKGROUND INFORMATION

## What is anInformation Security Analyst?

An information security analyst is someone who takes measures to protect a company's sensitive and mission-critical data, staying one step ahead of cyber attackers. They do this by coming up with innovative solutions to prevent critical information from being stolen, damaged or compromised by hackers.

Note the differences between a Security Analyst and a Security Administrator:

* Security Analysts - are responsible for analyzing data and recommending changes to higher ups, but do not authorize and implement changes. Their main job is keeping attackers out.
* Security Administrators - ensure that systems are working as designed by making changes, applying patches and setting up new admin users. Their main job is keeping systems up.

## What does an Information Security Analyst do?

The analyst challenge:

* A typical day involves 10 to 20 challange
* Errors such as false positive and false negative are common
* Investigating incidents takes time, giving attackers an advantage

A day in the life of thread investigator:

* 1 hour of a thread investigator spends with getting cought up on the latest security news through bulletins and social networks in order to identify new threads.
* 3 hours of a thread investigator spends with repeatedly investigatation of potential security incidents via online sources.
* 4 hours a thread investigator spends with manually copying and pasting information from disparate and siloed tools to correlate data

All this mundane time spent and unable to keep up with threads.



It is not sustainable without a cognative soultion.

## What is Natural Language Processing?

Natural Language Processing (NLP) is “ability of machines to understand and interpret human language the way it is written or spoken”[4].

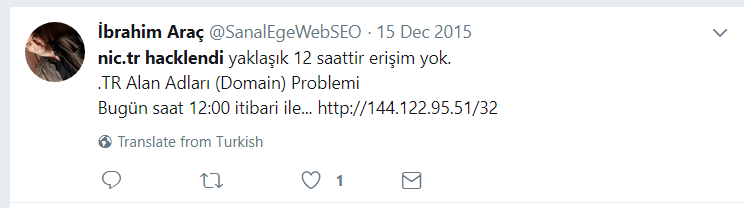


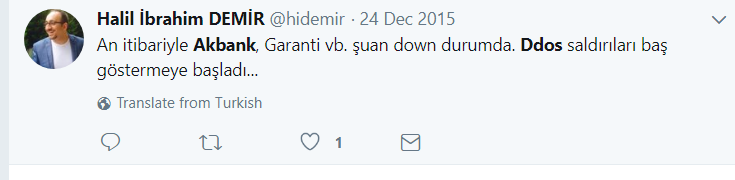
## Why do we need Natural Language Processing?

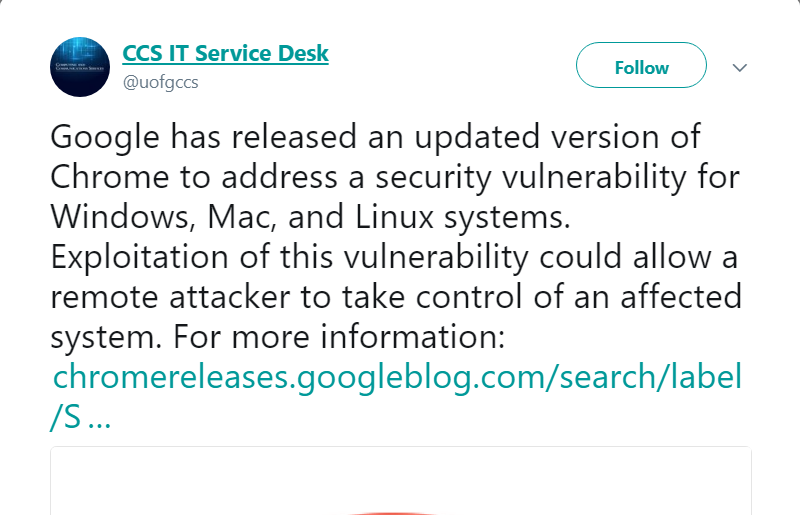




## Sample Tweets Related with a Security Incident









Sample False Positive:



A cognative solution that learns about security from structured and unstructured information sources, and empower security analysts with insights to respond to incidents with speed and accurancy like never before.

## Why is NLP Hard?

Language is highly ambiguous– it relies on subtle cues and contexts to convey meaning.

Take this simple example: “I love flying planes.”

Do I enjoy participating in the act of piloting an aircraft? Or am I expressing an appreciation for man-made vehicles engaged in movement through the air on wings?

A single sentence can carry different meanings. After thousands of years of evolution, languages have evolved to become shorter and less explicit. For humans, this is very efficient.

## Twitter Social Network

* + 1. What is Twitter?

Twitter is an online social networking service, which was created in October, 2006 by Jack Dorsey, Even Williams and Biz Stone. Twitter can be used for various purposes[5].

First of all, It can be used 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, It can be use as a micro blogging service for sharing details of a person’s life. Thirdly, Twitter can be used 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 easily. Moreover, there are lot of Twitter bots created by developers for a precise function like Bitcoin ticker bot will tweet every hour the price of Bitcoin in USD.

According to the first quantitative study on Twitter “What is Twitter, a Social Network or a News Media?” which is published in 2010[6], 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.

### Mechanism and Specific Terminology

On Twitter, any registered user can post a short message called a Tweet (Figure 2.1), this message cannot be more than 280 characters. Files like photos or videos can be added to the tweets and are not counted is the number of characters. Users can also add URL, which are automatically shortened in order to save space using Twitter’s URL shortening service. These hyperlinks usually start with “https://t.co/XX” where XX is a random sequence of characters.

Figure 2.1: Screenshot of a Tweet Containing the Number of Replies, Retweets and Likes

As soon as they register on Twitter, the users are prompted to follow accounts they might be interested in (usually classified by category such as sport or high-tech). By following other accounts, the users create their own network (which forms a simple directed graph) and subscribe to the other users’ Tweets. At first the connection is unilateral, followed accounts can decide to follow back if they are interested in the content of their follower. Each Twitter account maintain a count of followers (the number of people following the account) and following (the number of people the account is following), see Figure 2.2 for an example. When they register, Twitter users can write a short description about them and precise where they live.

Figure 2.2: Screenshot of the Twitter Account of Barack Obama

Twitter accounts are by default public and anyone can see a user’s post. Users can interact by replying to each other’s tweets with the reply button or by writing a tweet starting with a “@” and the user screen name. They can also send a private direct message (DM) to other accounts which are also constrained within 140 characters. User can also mention other user in their tweet by writing “@” followed by the user screen name. A mention is constructed the same way as reply, but the Twitter handle is not the first thing in the post. When a Twitter user want to share another user tweet with his followers, he can retweet the tweet. In general popularity of a tweet is measured by the number of retweets.

Finally, the last important concept in Twitter is the hashtag. A hashtag is a word or a sequence of word preceded by a hash sign (#). Hashtags are used to identify tweets on a specific topic. Twitter automatically uses these hashtags to create geolocated trending topics: a list of the most used hashtags per place (see Figure 2.3). This is especially useful to quickly identify which subjects are currently discuss on the social network.

Figure 2.3: Screenshot of the Worldwide Trending Topics in Twitter

Tweets can also be geolocated. On mobile client, a user can share his exact location (GPS

coordinates) or manually select a place near him. On desktop, users can decide to turn on their location and choose from a predefined list of cities around them.

In January 2017, Twitter had 317 million monthly active users, 500 millions tweets per day with 80% of the twitters tweeting from mobile devices1.

### Working with Twitter Data

Twitter provides several Application Programming Interfaces (APIs) to get tweets:

1See https://www.omnicoreagency.com/twitter-statistics/.

A REST (REpresentational State Transfer) API2 designed to read and write Twitter data.

With this API a developer can control his own account and access Twitter Data such as other persons tweets or descriptions. This API also contains the Twitter Search API, allowing “queries against the indices of recent or popular Tweets and behaves similarly to, but not exactly like the Search feature available in Twitter mobile or web clients, such as Twitter.com search”. This last API will not retrieve tweets older than 7 days. A Streaming API3 which gives developers access to realtime data in Twitter such as a 1%

sample of all the tweets. This API also allows developers to get all the tweets from a user or for a specific set of keywords (up to 1% of the Twitter volume). The GNIP API4 is a pay-per-use API. GNIP, a company purchased by Twitter in 2014, is specialized in social media API aggregation. GNIP API for Twitter is the same as REST and STREAMING APIs without any limitations.

## Hürriyet Turkish Newspaper as a Data Source

* + 1. 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.[7]

* + 1. Hurriyet Newspaper API

Hürriyet API (application programming interface) is an interface which enables the usage of Hürriyet data programmatically in web / mobile / desktop applications. It is a free service for now. With Hürriyet API, can be reached news, columns, writers, photo galleries and pages. Hürriyet API was established with a RESTful-based, resource-oriented architecture. Hürriyet data can be accessed 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.[8]

* + 1. What is OData

The OData (Open Data Protocol) REST-based data source using the HTTP protocol is a global protocol for querying services.

With the OData standards, you can quickly, without wasting much time on basic standards such as request and response headers, status codes, HTTP methods (GET, POST and so on), and query options. you can only create RESTful APIs by building business logic.

It is easy to consume OData services. OData metadata is easily rendered by the client - interpretable. Therefore, integration into powerful and expandable client applications can be done quickly and easily.

* + 1. 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/'

ball -> Limit the number of records in the response set that will be returned from the query. Example use;

* https://api.hurriyet.com.tr/v1/articles?$top=3

You 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. Example use;

https://api.hurriyet.com.tr/v1/articles?$select=Title&$filter=ModifiedDate ge Datetime'2014-10-10T10: 41: 31Z '& $ top = 3

Using OData protocol on Hürriyet API service;

News in the system (Articles),

Columns in the system,

In-system photo galleries (NewsPhotoGalleries),

The pages in the system and the pages assigned to the pages (Pages),

Folders in the system (Paths),

Writers

you can query and use them in your applications.

**CHAPTER 3**

# LITERATURE REVIEW

**CHAPTER 4**

# SYSTEM ARCHITECTURE AND DESIGN

## Approach

## Taxonamy

## Data Collection

## Data Preprocessing

## Event Detection

**CHAPTER 5**

# IMPLEMANTATION AND EVALUATION

## Implemantation

## Events Evaluation

### Yahoo Data Breach ie

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

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

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

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

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

# APPENDICES

# APPENDIX A

**TITLE**

xxx

# APPENDIX B

**TITLE**

xxx