**EGERTON UNIVERSITY**

**SOFTWARE REQUIREMENTS SPECIFICATION**

**FOR**

**ONLINE SUSPECIOUS DISCUSSIONS DETECTOR**

## PREPARED BY: S13/15358/16 BRENTONE ALISTAR

**SUPERVISOR: DR. PHOEBE ONGALO**

**COORDINATOR: DR. ENG. W. GIKARU**

**November 2019**

**Version 1.0**

# Table of Contents

[Table of Contents ii](#_TOC_250042)

[Revision History iii](#_TOC_250041)

1. [Introduction 2](#_TOC_250040)
   1. [Purpose 2](#_TOC_250039)
   2. [Document Conventions 2](#_TOC_250038)
   3. [Intended Audience and Reading Suggestions 2](#_TOC_250037)
   4. [Project Scope 2](#_TOC_250036)
2. [Overall Description 3](#_TOC_250035)
   1. [Product Perspective 3](#_TOC_250034)
   2. [Product Features 3](#_TOC_250033)
   3. [User Problem statement 4](#_TOC_250032)
   4. [User Objectives 5](#_TOC_250031)
   5. [Operating Environment 5](#_TOC_250030)
   6. [Design and Implementation Constraints 5](#_TOC_250029)
   7. [User Documentation 5](#_TOC_250028)
   8. [Assumptions and Dependencies 6](#_TOC_250027)
   9. [User Constraints 6](#_TOC_250026)
3. [System Features 7](#_TOC_250025)
   1. [Generalized Model of operation 7](#_TOC_250024)
   2. [Use case User Registration - Account Sign up(U1) 8](#_TOC_250023)
      1. [Objective 8](#_TOC_250022)
      2. [Priority 8](#_TOC_250021)
      3. [Source 8](#_TOC_250020)
      4. [Actors 8](#_TOC_250019)
4. [External Interface Requirements 10](#_TOC_250018)
   1. [User Interfaces 10](#_TOC_250017)
   2. [Hardware Interfaces 10](#_TOC_250016)
   3. [Software Interfaces 10](#_TOC_250015)
   4. [Communications Interfaces 11](#_TOC_250014)
5. [Other Nonfunctional Requirements 12](#_TOC_250013)
   1. [Performance Requirements 12](#_TOC_250012)
   2. [Safety Requirements 12](#_TOC_250011)
   3. [Security Requirements 12](#_TOC_250010)
   4. [Software Quality Attributes 13](#_TOC_250009)
   5. [Other requirements Attributes 14](#_TOC_250008)
6. [Preliminary Object-Oriented Domain Analysis 15](#_TOC_250007)
   1. [Inheritance relationships 15](#_TOC_250006)
   2. [User Classes and Characteristics 15](#_TOC_250005)
7. [Preliminary Budget and Schedule 18](#_TOC_250004)
8. [Other Requirements 19](#_TOC_250003)
   1. [References 19](#_TOC_250002)
   2. [Appendix A: Glossary of definitions, Acronyms and abbreviations 20](#_TOC_250001)

[Appendix B: Issues List 20](#_TOC_250000)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
| Brentone Alistar | 12/11/19 | Initital Version | 1.0 |
|  |  |  |  |

**Overview**

SRS is the official statement of what the system developers should implement. SRS is a complete description of the behavior of the system to be developed. SRS should include both a definition of user requirements and a specification of the system requirements.

The SRS fully describes what the software will do and how it will be expected to perform. The SRS precisely defines the software product that will be built. SRS used to know all the requirements for software development and thus that will help in designing the software. It provides feedback to the customer. Documents that describe the functions of the SRS include the Software Requirements Document (SRD), Functional Requirements Document (FRD), Functional Requirements Specifications document (FRS), among other synonyms.

The SRS defines the contract between the developer and the owner of the system.

# Introduction

## Purpose

The Online Suspicious Discussion Detector (OSDD) is intended to provide an effective security control mechanism over the internet for the internet users against abuse and with a great length work towards minimizing illegal uses of the internet such as hacking, sexuality, religious, piracy, gambling, fraud by analyzing for provoking posts using a set of keywords in the algorithm.

This system will analyze text sources from social media and online platforms then classify the text into different groups. The system will distinguish between legal and illegal data using Stop-Words Selection, Stemmer algorithm, and Levenshtein algorithm.

## Document Conventions

This document follows the MLA Format. The bold-faced text has been used to emphasize section and sub-section headings. Highlighting is to point out words in the glossary and italicized text is used to label and recognize diagrams. When writing the SRS document for Online Suspicious Discussion Detector the following styles were used to make the document more effective and readable Times New Roman font size 12 and headings which are bold and elegantly placed have been used.

The following terminologies are also used:

|  |  |
| --- | --- |
| DB | Database |
| DDB | Distributed Database |
| ER | Entity Relationship |
| User | Anyone who uses the application |
| OS | Operating System |
| OSDD | Online Suspicious Discussion Detector |

## Intended Audience and Reading Suggestions

The intended readers of this document are the developers of the system, testers, social media/online forum users, law and enforcement agencies as well as other readers who seek to gain knowledge and all the information about the system.

## Project Scope

There is no such platform that is currently popular for providing a cushion to the internet users against cyber-crimes as well as an extension for cyber-crime branches for detecting an implementing laws on proper usage of the internet. The proposed system will monitor for suspicious postings, collect it from a few discussion forums, implement techniques of data mining and extract meaningful data. This would provide cyber-crime branches with ways of detecting these forums for illegal feedbacks, comments or reviews and download questionable postings as verification for their investigation.

This application will provide the users a social platform that they can communicate to the relevant authorities for filing complaints and giving out feedbacks which in essence is subjective towards better performance of the application and effective control of the internet usage. The system is an online social platform text-analyzing and processing system which is intended to solve the problems described above. The system provides a mobile platform in which people can easily register and use.

When the users register, their user credentials will be used for the monitor purpose, not only as culprits but also as victims of cyberbullying and cyber-crimes. The user account credentials will be accessible only to the relevant authorities and there will exists no privacy issues with regards to this information. For transparency, accountability, and integrity, the system will include an additional feature for a follow up on the victim’s side to ensure that the correct measures have been taken against the offender. This would be in terms of feedback from the authority to the offended with pieces of information on the penalties the offender has paid for.

# Overall Description

## Product Perspective

The software product being developed is platform-independent equipped with relevant and stable algorithms that function as a text and discussion analyzer application for text input and common signs. The product works with other software products like an Embedded Operating System, Databases for text and speech, Recognition and Translation Software.

This product is aimed at upgrading the security standards to safeguard social media users against cyber-crimes, social and political assaults. Implicitly, this system will be incorporated into already existing self-independent systems especially social media categorically. With the addition of more features, the system is objectively oriented towards the provision of a better experience to its users and generally towards enhancing better performance.

Currently, there is no device, which combines all functionalities the way the OSDD does. Therefore, it is a prototype of a new product that merges social media families with internal security control services for cyber-crimes and other internet related misuses. Refer to the attached *use case diagram* for further information.

## Product Features

The OSDD contain the following features:

* + 1. Recognizes and captures suspicious texts on online forum platforms using text mining and translated voice data from the online hosted public meetings and shows.
    2. Use data mining algorithms and techniques with an already existing database with rules and references to categorize the identified text/discussion or voice data into specific cybercrime threats following a collection of predefined laws governing online safety and usage.
    3. Associate the identified cybercrime with a relevant cybersecurity agency for submission after downloading the material in audio format for spoken data inputs and a screenshot for the data captured from text-mining. In both cases, there will be an attached information explaining the reasons for the verdict, time for the event the targeted victim and the convict.
    4. Prompt the to chose whether the event was exceptional and should be regarded as non-offensive, for example when connecting and talking to friends where the number of the recipients of the information does not exceed seven. This typically halts the system and the iteration begins from the start. This feature is only available when the number of recipients of the information is at most seven.
    5. Should the system user select the option to proceed with the submission, the information is submitted to the already associated cybersecurity agents for action and measures to be applied. For example, domestic violence will implicitly be submitted to the department of cybersecurity dealing with domestic violence.
    6. Moreover, the system will have a comment and feedback section from which the users will press charges for online bullying and inappropriate use of the internet giving relevant evidences.
    7. A response mechanism will be configured from the cybersecurity side showing the validity of the charged and the taken actions. This is to provide the users with a sense of satisfaction and transparency.

## User Problem statement

The users of the system can be anybody with the capability of accessing the internet, specifically the social media platform with high anticipation of online abuse resulting in both social and emotional affliction. These users are in need of protection from redundant occurrences of these common and devastating oppressions. It is with accuracy that the users know the working environment and standards of these platforms and thus won't need much expertise in incorporating the system to work side by side with the already existing platforms.

OSDD system domain comprises major online platforms used for social media interactions and information broadcasting such as using Facebook to host a live political rally event. It is in this domain that will be the major source of data and information input for the system. Hate speeches, online scams from various adverts and other related cybercrimes are implicitly the targeted data for the system as input.

At the other end of the domain is a cybersecurity agency. The processed data, raw data(the actual crime) with embedded pieces of information such as the violated edict, time and the convict/culprit will be sent to the relevant cybersecurity agency for implementing and ensuring that the directives are upheld.

## User Objectives

1. To provide a reliable system that is easy to use and work with
2. To ensure 24 x 7 availability of the system
3. Provide a secure system that doesn’t lead to further complications
4. Provide a system that help implement online safety and regulations
5. Provide an interactive system that has good performance and minimum system requirements such as memory size, processor speed, and data.

## Operating Environment

### Operating environment for the Online Suspicious Discussions Detector is as listed below.

* distributed database
* client/server system
* Operating system: Windows.
* database: MySQL database
* platform: python

## Design and Implementation Constraints

1. **Synchronization:** the system will be structured to monitor multiple platforms at a go for complete utilization of its resources and consistency in performance.
2. **Memory requirements**: the device will have a minimum 2GB internal hard drive requirement. Software and database cannot exceed this amount.
3. **Permissions**: the user has to give/enable the application permissions to collect data from the targeted social media platform applications and to write on the storage.
4. **Language requirements**: for better performance and scope accuracy to ensure all user needs are put into consideration the software should be multilingual, taking into account considerations the major national languages.

## User Documentation

For user documentation and information, please consult section 4: External Interface

*Requirements and attached user manual.*

## Assumptions and Dependencies

It is assumed that the user of the system will have strong internet connectivity and some knowledge and expertise on the usage of the targeted online social platforms because this system is client/server- based extracting inferences and deploying the algorithms on the servers on the client's data obtained from the social media servers.

Moreover, the implementation of these regulations by the relevant cybersecurity agencies is assumed to be tight and no offender should be exempted without proper justifications. The interactions between the OSDD system with the agency’s system is also assumed to be real-time with the provision of feedback to the victims.

## User Constraints

* The interactions with the social platform will be a single way.
* Users have to provide unique credentials such as ID number for purposes of uniquely identifying the users.
* In cases of feedbacks, substantial evidence should be provided to support the claim.

# System Features

## Generalized Model of operation

#### Description and Priority

The OSDD system monitors the social media platforms for suspicious discussions and illegal internet usages using text mining, this acts as the inputs for the text processing using data-mining with relevant algorithms and sentimental analysis. The performance of this system is majorly prioritized to be real- time due to the dynamic characteristics of the internet contents and materials.

#### Stimulus/Response Sequences

* Automated Monitoring of Suspicious Discussions Using Data Mining Statistical Corpus- Based Approach
  + For an immediate user, if manual submission is the user preference, the system prompts the user to confirm an identified potential harm or abuse to the relevant authority.
  + The system categorizes the abuse into either of the five predefined categories and downloads the supporting evidence to support the charges.
  + Finally, the submission is made to the cybersecurity authorities for actions and measures to be taken against the offender.
  + Offer follow up activities for the victims

#### Functional Requirements

Other system features include:

**DISTRIBUTED DATABASE:**

A distributed database implies that a single application should be able to operate transparently on data that is spread across a variety of different databases and connected by a communication network hosted on different servers.

**CLIENT/SERVER SYSTEM**

The term client/server refers primarily to an architecture or logical division of responsibilities, the client is the application (also known as the front-end), and the server is the DBMS (also known as the back-end).

A client/server system is a distributed system in which,

* Some sites are client sites and others are server sites.
* All the data resides at the server sites.
* All applications execute at the client sites.

#### Technical Issues

It is in good practice for the users of the system product to keep up with newer released versions to ensure efficient compatibility and configuration accuracy with the dynamic changes and updates of the social media platforms that are related to the system’s operation*.*

#### Dependencies with other requirements

The system requires a good internet connection as an external dependency with enough memory storage for good operation and performances.

## Use case User Registration - Account Sign up(U1)

#### Objective

The purpose of the U1 use case is to provide relevant fields to the user for capturing user credentials to ensure the unique identity of each and every user of the system that will facilitate correct user reference.

#### Priority

This requirement is a high priority.

#### Source

The source of this use case is the user of the system.

#### Actors

An end-user of the system(social media user) would be the relevant actor for this use case.

#### Flow of events

* + - 1. **Basic Flow**
         1. User accesses the system program registration page.
         2. the provided user credentials are captured and stored in a distributed database.
         3. a validation information is sent to the email account or phone.
         4. the validation code is the user default password and can change it after this stage.

#### Alternative Flow- At step 3.2.5.1.4, the user decides not to validate the account.

* + - * 1. User presses the cancel button.
        2. The system exits the validation process by creating an account with a pending validation.
        3. User gets a validation request to proceed for every submission and complain requests. All other system functionalities will be accessible except submission

.

#### Exception Flow – At step 3.2.5.1.4, the process encounters a problem.

* + - * 1. System provides an error message indicating the error and relevant solution.
        2. No user registration info is submitted or stored. The registration process initializes.
    1. **Includes** – None.

#### Requirements-

* + - 1. The system shall provide the option to skip registration.
      2. The system shall provide the option to register with the social media account.
      3. The system shall display a default user avatar.
      4. The system shall indicate a need for registration should the user chose to skip
    1. **Preconditions** – Good internet connection.
    2. **Postconditions** – An updated profile information reflecting the user information.

#### Nonfunctional requirements –

* + - 1. **Performance Requirements**-
         1. The maximum allowed execution time for the U1 use case is 60 seconds, starting at the time when the user presses the register button and

ending when the details have been saved and displayed.

* + - 1. **Safety Requirements**-None.
      2. **Security Requirements**-None.

#### Software Quality Requirements-None.

# External Interface Requirements

## User Interfaces

The Online Suspicious Discussion Detector(OSDD) user interface has been specifically designed with the user in mind, giving them convenience while they use the application system. The OSDD makes sure at every point, that the user spends most of the time using the system application rather than figuring out how to use it.

The home screen offers a menu with a list of functions that the system performs. The

Users can select one of the options on the menu and are taken to the respective screen. Every screen displays the menu on the bottom. The user can click on any one of the options and is taken to the screen of their choice. In addition, the application offers easy navigation options to the rest of the screens efficiently. To scroll down any screen, simply touch the scroll bar on the screen, and roll down. If the user does not know how to use any functionality or has any queries, the help option can be used. The help screen contains a text field to enter search terms. A list of search results pertaining to the query is *displayed*.

## Hardware Interfaces

This application will work on android phones and windows. Since the application must run connected to the internet and need location data, Android devices must have a GPS unit and internet connection in order to run this application.

For voice data inputs, the user requires a microphone connected to the computer. This is as a supplementary input method should the user decide to enter data via voice input which will be followed with voice translation into text and processing.

## Software Interfaces

The OSDD features revolutionary social media software technological advancement that makes it convenient to use. The OSDD also offers a voice input option that helps users enter data and information to the system via spoken words for the user who would prefer the use of a microphone over a keyboard for faster inputs and processings.

The OSDD uses synchronization software that is compatible with Windows and Android operating systems. The system contains an in-built language database containing image, text and

audio files. The database can be updated with additional data and information from the connected social media accounts by downloading them on the user’s computer through synchronizing the processing and monitoring across all connected social media accounts.

## Communications Interfaces

The application will use HTTP protocol for communication over the internet*.*

# Other Nonfunctional Requirements

## Performance Requirements

* OSDD will be able to support at least 10,000 simultaneous users. The capacity can be extended in the future if needed.
* There will be a large amount of information to be handled in the database such as social media data, user information, feedbacks, etc. and the server will be enough space to handle this occupation.
* All of the functions that are for identifying suspicious messages, illegal activities, sentimental public speeches, etc. should be performed less than 5 seconds.

## Safety Requirements

As a measure against data loss, the software application will include a backing up feature that ensures periodic backing up of data onto the google drives or accounts as an external source and copy of the information for use in instances of server problems and when the user uninstalls the program and wishes to reinstall the same.

The major threat to the system program would have to related to theft of data and unauthorized access to the information stored in the system. A security control mechanism has been put into place to ensure that only a single instance of this application can run for each and every user at a time. This ensures data integrity and restricted access to data. In some way, it makes the application thread-safe. The communication and application access between the OSDD and other social media platform is also made to be one way, the access is only allowed for the OSDD and not multiway.

## Security Requirements

#### In the application side,

* The system must not request unnecessary permissions from the user in order to prevent unwanted attacks.
* Stored data of the application should not be reached by other applications that is installed in

the user’s mobile device.

* Stored data in the mobile device and sent data via the internet should be encrypted. Send and received data should be transferred via HTTPS connection. And also authenticated and encrypted socket-level communication should be implemented.

#### In the database side,

* SQL codes should not be stored in the application in case of application can be affected by malware software.
* Data that come from the application should be encrypted again on the database side.

## Software Quality Attributes

Some of the software quality attributes that make the system an exemplary to some of the best and preferred software products include:

#### Availability;

* + the system will be a configuration product that will be made available to all users for free download and installations. thus no acquisition charges incurred by the user.
  + The system should be available for 7 days and 24 hours.
  + In the application side, the system should be tested against probable failures before publishing the first version or updated versions of the application. Published version should be error-free.
  + In the database side, in case of a failure, the system should recover any information for the user and system.

#### Portability;

* + the product is platform-independent and portable to devices that meet the hardware and software requirement specifications for the installation and usage of the software program.
  + %100 percent of the program depends on the host. In order to change the host, all the components of the database should be transferred.

#### Security;

in addition to several server firewalls and thread-safe mechanisms, several security control mechanisms have been implemented to safeguard users from intentional and unintentional security breaches.

#### Flexibility;

the features of the system are user-customizable to meet the desired user preferences and ensure users’ maximum satisfaction and user-controlled usage.

#### Adaptability;

frequent product updates on the product features and functionalities with regards to the changing technological advancements to ensure a software product with efficient and maximized user requirements.

#### Maintainability;

* + the software maintainability will only involve downloading updates and installing these updates at free costs.
  + An SVN software should be used in the development phase in order to reduce complexity, make the system traceable and recover the code from an unwanted crash while more than one developer is dealing with the code.
  + Design elements should be documented well.
  + Since programming language is object-oriented, program tasks are independent of each other and therefore easier to maintain.
  + All parts of the code should be easy to read.

#### Performance;

in terms of requests and responses, advanced and most current algorithms have been implemented to facilitate faster processing of all user requests resulting in giving out feedbacks/responses in time.

## Other requirements Attributes

For information regarding functional requirements, refer to section 3: System Features.

Each feature has its requirements listed alongside the feature information. Special requirements

for each system feature are also mentioned in section 3. There are no additional Functional requirements.

# Preliminary Object-Oriented Domain Analysis

This section presents a list of the fundamental objects that must be modeled within the system to satisfy its requirements. The purpose is to provide an alternative ‘structural’ view on the requirements stated above and how they might be satisfied in the system.

## Inheritance relationships

System Admin Cybersecurity agency System user

Social platform & feedbacks Data

## User Classes and Characteristics

The users of the system will be able to create a user account, link all the social media platforms to be monitored to the application system and manually send complains to the relevant cybersecurity agencies providing all the supporting materials for the claim. The users will have access to all of the users' functions. This includes choosing whether the identified sentimental comments and speeches should be submitted automatically or manually via the user’s approval. This includes all the cases the user has chosen to be exceptionally out of the monitoring. The system will ignore the exception and only captures all the remaining contents from social media.

With the comments and feedback mechanism and as a feature of the system, the major fraud and unethical advertisements and subscription activities will be included on the monitor algorithms to help warn the user should the same be found on the user’s social media wall.

The system will support three types of user privileges, the subscriber user, cybersecurity agency and the management privilege. The subscribed user, at the lowest level, will have normal user functions and privileges. These mainly include the provision of all the input data for processing and relevant permissions for access to the connected social media accounts. On the other hand, as a third party system class, the cybersecurity agency will have the middle-level class to access user information but only the allowed contents and validate claims giving out validation feedbacks and sometimes inquiries concerning a particular claim.

Right at the top-level exists the management class, responsible for all system updates and will full access privileges can modify the database when the is need and monitor server logs and activities. He is also responsible for finetuning the monitoring algorithms and with updates to the current identified threats and risks.

#### Class descriptions

The main classes associated with the system and have direct influences on the general performance of the ystem as identified during the OO Domain Analysis are the user class and the cybersecurityagency class.

The user class primary performs subjectively to avail all the required data for processing by the system. The availability of these data can be via monitor-controlled functionality of the system or user provided as in the cases of user feedbacks. Likewise, at the other end of the system is cybersecurity agency class tasked with implementing the rules and regulations on the internet usage. It also serves as the source for the logic and definition rules for the system algorithms in identification and legislation of improper usage of the internet.

#### User Class

* + - * 1. **Abstract or Concrete:**

the user class is an abstract class with methods and attributes that can be inherited by other classes.

#### List of Superclasses:

social media platform and cybersecurity agency

#### List of Subclasses:

feedbacks & comments

#### Purpose:

this class is the major source of data for the sytem processing. It serves a purpose of initiating the system with reference of system processing and other functionalities.

#### Collaborations:

this class interacts and indirectly dependent with the system administrative class to inherit methods and features that are critical and essential for the general goals of the system application.

#### Attributes: user information

Name

Age

Gender

UserID

#### Other information

Linked account

Identified threats

Feedbacks

#### Operations:

As an operation within the scope of this class, the monitor operation is initiated once the user links and provides read permissions to social media accounts and other relevant and required permissions for the operation. The return types of this operation includes: sexuality, hacking, fraud,religion and political sentiments among others

#### Constraints:

the user class would only collect informations from the allowed accounts and platforms. There would be no third party accessing the user class to enforce security standards.

# Preliminary Budget and Schedule

This section provides an initial budget, itemized by cost factor and schedule including major tasks to be accomplished, their interdependencies and their tentative start/stop dates. The plan/schedule should also include information on hardware, software and other resources required.

|  |  |
| --- | --- |
| **Item** | **Cost** |
| Computer/Smartphone | Ksh. 25,000 |
| Windows / Android OS | Ksh. 10,000 |
| Internet Bundles | Ksh. 5,000 |
| Microphone | Ksh. 3000 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Duration Activity** | **Oct 2019** | **Nov 2019** | **Dec 2019** | **Jan 2019** | **Feb 2020** | **March 2020** |
| **Problem definition** |  |  |  |  |  |  |
| **Feasibility study and analysis** |  |  |  |  |  |  |
| **Requirement Analysis** |  |  |  |  |  |  |
| **System Design** |  |  |  |  |  |  |
| **Coding** |  |  |  |  |  |  |
| **Compiling and Testing** |  |  |  |  |  |  |
| **System Integration** |  |  |  |  |  |  |
| **Testing** |  |  |  |  |  |  |
| **Presentation and Deployment** |  |  |  |  |  |  |
| **Maintenance** |  |  |  |  |  |  |

# Other Requirements

## References

1. Murugesan, M. Sururthi, R. Pavitha Devi, S. Deepthi, V. Shri Lavanya, and Annie Princy. Automated

Monitoring Suspicious Discussions on Online Formus Using Data Mining Statistical Corpus Based Approach. 259

Imperial Journal of Interdisiplinary Research (IJIR) Vol2, Issue-5, 2016

1. Harika Upgaganlawar, Nilesh Sambhe. Surveillance of Suspicious Discussions on Online Forums Using Text Mining. International Journal of Advances in Electronics and Computer Science,

Volume4, Issue-4, April-2017

1. Suhas Pandhe and Sahil Pawar. Algorithm to Monitor Suspicious on Social Networking Sites Using Data Mining Techniques. International Journal of Computer Applications. Volume 116 – No. 12, April 2015
2. Javad Hosseinkhani, Mohammad Koochakazei, Solmaaz Keikhaee and Yahaya Hamedi Amin. Detecting Suspicion Information on Web Crime Using Crime Data Mining Techniques. International Journal of Advanced

Computer Science and Information Technology (IJACSIT) Vol.-3, No. 1, 2014, Page 32-41

1. G.Vinodhini, R.M Chandrasekran. Sentiment Analysis and Opinion Mining: A Survey. International

Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 6, June-2012

## Appendix A: Glossary of definitions, Acronyms and abbreviations

**Glossary**

1. API – Application Programming Interface
2. OS – Operating System
3. DB – Database
4. DDB – Distributed Database
5. HTTP – HyperText Transfer Protocol
6. URI – Uniform Resource Identifier
7. SQL – Structured Query Language

# Appendix B: Issues List

This is a dynamic list of the open requirements issues that remain to be resolved, including TBDs, pending decisions, information that is needed, conflicts awaiting resolution, and the like.

* + Exceptions handing of identified threats with proper reasons
  + Synchronization with the third party databases (social media platforms)