Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Preventing the Occurrence of Cyber Bulling Messages on Online Social Networks by Using SemSDA

M. Devi Sri Prasad
Department of Computer Science and Engineering
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

M. Narendra Reddy
Department of Computer Science and Engineering
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

P.Sai Teja
Department of Computer Science and Engineering
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

K. Madhavi
Department of Computer Science and Engineering
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

Abstract

Cyber bullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. As a side effect of increasingly popular social media, cyber bullying has emerged as a serious problem afflicting children, adolescents and young adults. Machine learning techniques make automatic detection of bullying messages in social media possible, and this could help to construct a healthy and safe social media environment. In this meaningful research area, one critical issue is robust and discriminative numerical representation learning of text messages. In this paper, we propose a new representation learning method to tackle this problem. Our method named Semantic-Enhanced Marginalized Denoising Auto-Encoder (smSDA) is developed via semantic extension of the popular deep learning model stacked denoising autoen coder. The semantic extension consists of semantic dropout noise and sparsity constraints, where the semantic dropout noise is designed based on domain knowledge and the word embedding technique. Our proposed method is able to exploit the hidden feature structure of bullying information and learn a robust and discriminative representation of text. Comprehensive experiments on two public cyberbullying corpora (Twitter and MySpace) are conducted, and the results show that our proposed approaches outperform other baseline text representation learning methods.

INTRODUCTION

SOCIAL Media, as defined in [1], is ‘’a group of Internet based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content‘’ Via social media, people can enjoy enormous information, convenient communication experience and so on. However, social media may have some side effects such as cyber bullying, which may have negative impacts on the life of people, especially children and teenagers. Cyber bullying can be defined as aggressive, intentional actions performed by an individual or a group of people via digital communication methods such as sending messages and posting comments against a victim. Different from traditional bullying that usually occurs at school during face-to- face communication, cyber bullying on social media can take place anywhere at any time. For bullies, they are free to hurt their peers’ feelings because they do not need to face someone and

Cite this article as: M. Devi Sri Prasad, M. Narendra Reddy, P.Sai Teja & K. Madhavi, "Preventing the Occurrence of Cyber Bulling Messages on Online Social Networks by Using SemSDA", International Journal of Research in Advanced Computer Science Engineering, Volume 4 Issue 10, 2019, Page 42-51.

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

can hide behind the Internet. For victims, they are easily exposed to harassment since all of us, especially youth, are constantly connected to Internet or social media. As reported in [2], cyber bullying victimization rate ranges from 10% to 40%. In the United States, approximately 43% of teenagers were ever bullied on social media [3]. The same as traditional bullying, cyberbullying has negative, insidious and sweeping impacts on children [4], [5], [6]. The outcomes for victims under cyberbullying may even be tragic such as the occurrence of self-injurious behaviour or suicides. One way to address the cyberbullying problem is to automatically detect and promptly report bullying messages so that proper measures can be taken to prevent possible tragedies. Previous works on computational studies of bullying have shown that natural language processing and machine learning are powerful tools to study bullying [7], [8]. Cyberbullying detection can be formulated as a supervised learning problem. A classifier is first trained on a cyberbullying corpus labelled by humans, and the learned classifier is then used to recognize a bullying message. Three kinds of information including text, user demography, and social network features are often used in cyberbullyingDetection [9]. Since the text content is the most reliable, our work here focuses on text-based cyberbullying detection. In the text-based cyberbullying detection, the first and also critical step is the numerical representation learning for text messages. In fact, representation learning of text is extensively studied in text mining, information retrieval and natural language processing (NLP). Bag-of-words (BoW) model is one commonly used model that each dimension corresponds to a term. Latent Semantic Analysis (LSA) and topic models are another popular text representation models, which are both based on BoW models. By mapping text units into fixed-length vectors, the learned representation can be further processed for numerous language processing tasks. Therefore, the useful representation should discover the meaning behind text units. In cyberbullying detection, the numerical representation for Internet messages should be robust and discriminative. Since messages on social media are often very short and contain a lot of informal language and misspellings, robust representations for these messages are required to reduce their ambiguity. Even worse, the lack of sufficient high-quality training data, i.e., data spar city make the issue more challenging. Firstly, labelling data is labour intensive and time consuming. Secondly, cyberbullying is hard to describe and judge from a third view due to its intrinsic ambiguities. Thirdly, due to protection of Internet users and privacy issues, only a small portion of messages are left on the Internet, and most bullying posts are deleted. As a result, the trained classifier may not generalize well on testing messages that contain nonactivated but discriminative features. The goal of this present study is to develop methods that can learn robust and discriminative representations to tackle the above problems in cyberbullying detection. Some approaches have been proposed to tackle these problems by incorporating expert knowledge into feature learning. Yin et.al proposed to combine BoW features, sentiment features and contextual features to train a support vector machine for online harassment detection [10].

SYSTEM FEASIBILITY

Problem Statement

As a side effect of increasingly popular social media, cyber bullying has emerged as a serious problem afflicting children, adolescents and young adults. Machine learning techniques make automatic detection of bullying messages in social media possible, and this could help to construct a healthy and safe social media environment. In this meaningful research area, one critical issue is robust and discriminative numerical representation learning of text messages. In this paper, we propose a new representation learning method to tackle this problem. Our method named Semantic-Enhanced Marginalized Denoising Auto-Encoder (smSDA) is developed via semantic extension of the popular deep learning model stacked denoising auto encoder. The semantic extension consists of semantic dropout noise and sparsity constraints, where the

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

semantic dropout noise is designed based on domain knowledge and the word embedding technique. Our proposed method is able to exploit the hidden feature structure of bullying information and learn a robust and discriminative representation of text. Comprehensive experiments on two public cyber bullying corpora (Twitter and MySpace) are conducted, and the results show that our proposed approaches outperform other baseline text representation learning methods

Existing System

In the existing system there was no pre-defined method or software to classify the abused or cyber bulling messages for a text message which is posted on OSN walls and identify the meaning of that word and block that message not to be posted directly on the users wall. So the following are the limitations that take place in the existing system. They are as follows:

Limitations of Existing System

- Till now there was no method like sm SDA in the literature to automatically detect the cyber bullying messages and encode them into a separate list.
- There was no classification algorithm in literature that can automatically read all the text which is posted by the users and recognize if there are any abused content available on that posted messages.
- There is a term like BoW in the existing system,where a bag of words is listed into a database and these bag of words are used for matching the dimensions of corresponding term which is posted on the wall.
- The main limitation of Bow is this can identify the exact word in exact message if the same message contains the word in plural way, this can't be identified as matched word.
- In the existing there is no concept like segregate the messages into categories like cyber bulled messages and Non-Cyber Bulled category message.

Proposed System

In the proposed system we used a expert knowledge for feature learning. The proposed system uses ML-Approach for classifying the semantic meanings of posted message and we try to combine BoW features, sentiment features and contextual features to train a support vector machine for online harassment detection.

- Here in our proposed system as an extension we also designed label specific features to extend the general features, where the label specific features are learned by Linear Discriminative Analysis. Here by using this label specific feature we can able to get the count of abused or harassed words that are repeated and used within the posted message.
- Along with the ML-Approach we use a Denoising Auto-Encoder technique, where the auto encoder is nothing but identifying the words automatically and then block the messages automatically without any third person intervention.
- Although it is very efficient in identifying a cyber bullyingmessages, the one and only limitation that still arise in our proposed application is this learned feature space still relies on the BoW assumption and the message can be identified easily as it is cyber bulled message only if the message contain a word that was matched with Bow. If the words are not matched with Bow, even the message sense as abused it can't be classified as cyber bulled.

Benefits of the Proposed System

- Most cyber bullying detection methods rely on the BoW model. Due to the sparsity problems of both data and features, the classifier may not be trained very well.
- For cyberbullying problem, we design semantic dropout noise to emphasize bullying features in the new feature space, and the yielded new representation is thus more discriminative for cyberbullying detection.

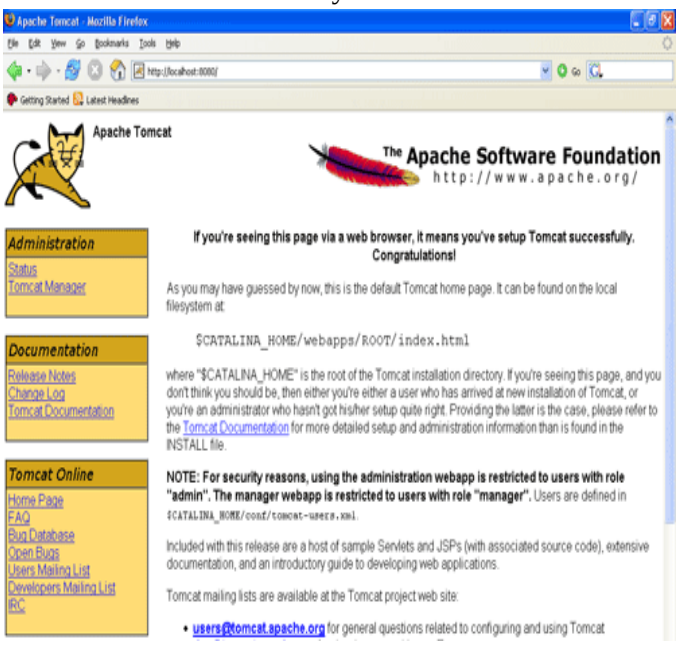
Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

- Here we used a labeled feature extraction, through which we can classify and give the analysis report for the user like how many words he used in abused category and which words comes under exact category.
- Also we can add infinity number of words under the Bow, where one thing we must keep in mind is a word which is to be added in BoW should be assigned only once in one category. If the same word is added in multiple categories at a time, it will lead to wrong analysis and in turn shows wrong calculations.
- This should be verified or managed by the Administrator while adding words into the BoW database.

Feasibility Analysis

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

- Operational Feasibility
- Economic Feasibility
- Technical Feasibility



Software Requirement Specification:

A software requirement specification is a complete description of the behavior of the system to be developed. It includes a set of use cases that describes all the interactions the users will have with the software. Use cases are also known as functional requirements. on –functional requirements are the requirements which impose constants on the design or implementation

Functional Requirement:

Functional requirements describe what the system should do, i.e. the services provided for the users and for other systems.

INPUT:

- The User try to register first into the application.
- The user enters into his account by substituting his valid id and password.
- The admin enters his valid login details for getting login into the system.
- The admin approves the users at the time of registration.
- The user sends a friend request for others in his search friend module.
- The user can send comments for the posted content
- The user can give replies for the posted content.

OUTPUT:

- The User gets an output window as" User Registered Successful"
- The User gets an output window as" User Login Successful"
- The Admin gets an output window as" Admin Login Successful"
- The user gets an output window as" Friend Request Accepted"
- The user gets a message like "Comments posted Successfully"
- The Admin gets a message like "Words Added Successfully"

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Non Functional Requirement:

In non-functional requirements the following are the things that come under .They are as follows:

Reusability: As we developed the application in java, the application can be re-used for any one without having any restrictions in its usage. Hence it is re-Usable.

Portability: As the application is designed with java as programming language, we know java can be run on any operating system. Hence the application is portable to run on any operating system.

Extensibility: The application can be extended at any level if the user wish to extend that in future this is done because java is a open source medium which doesn't have any time limits for expiry or renewal.

Front-end Environment:

Here in the front end so we use HTML,Java,Jsp,JavaScript for implementing the Front end environment.

Back-end Environment:

Here in the Back end so we use Java Server Pages, MySQL, JDBC these are the main uses for the back end for the connectivity of the database.

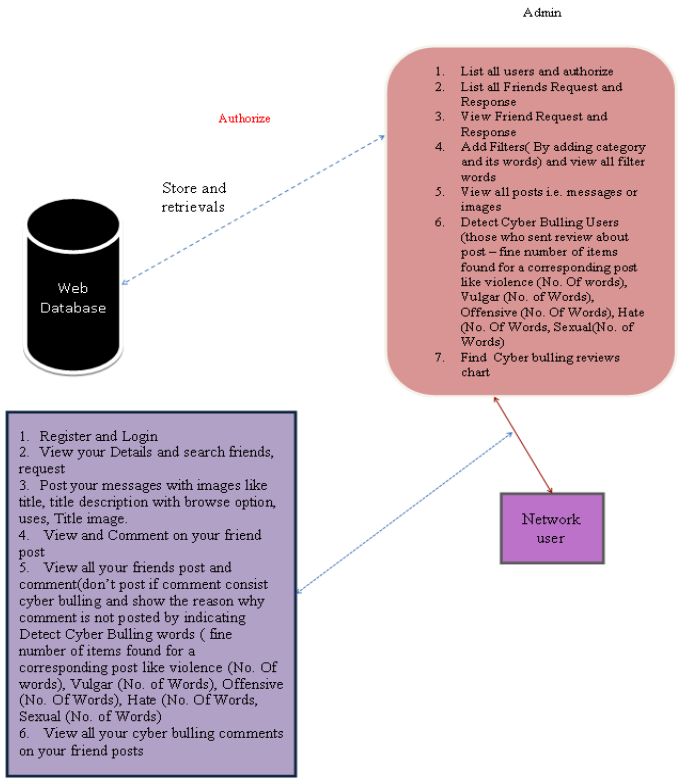
Data Storage:

Here we use MY Sql as back end so we use Heidi sql as back end GUI tool for implementing the current application with easy of use. application. Here we use MY-SQL as back end data base that is due to because of various advantages, they are as follows:

- It has featured like auto commit.
- It is GUI in nature (Common line Interface).
- It occupies very less size for installation.
- It is cross platform in nature

SYSTEM DESIGN

System Architecture:



Sequence Diagram:

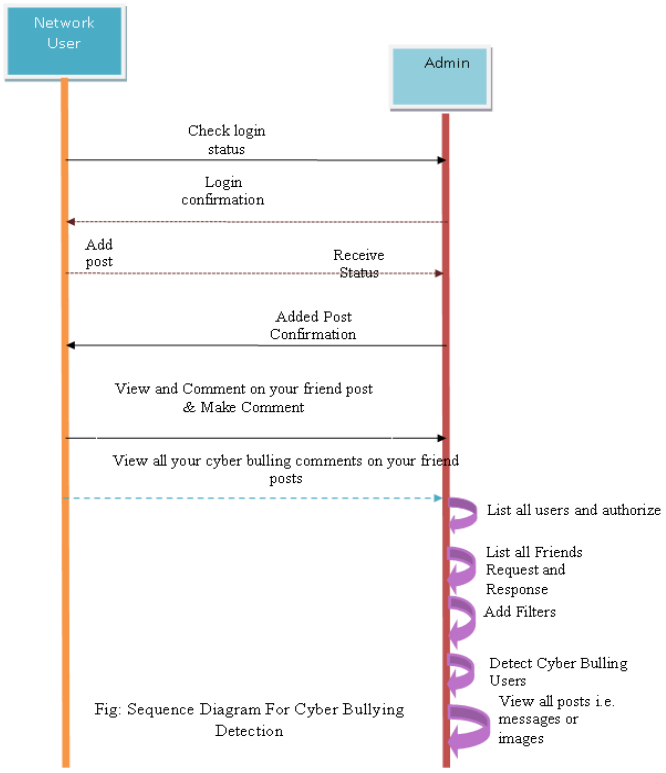


Fig: Sequence Diagram For Cyber Bullying Detection

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules Used:

- Network Construction Module
- Marginalized Stacked De-noising Auto-encoder
- Semantic Enhancement for mSDA
- Construction of Bullying Feature Set
- smSDA for Cyberbullying Detection

Modules description

Network Construction Module

In this module initially we need to construct a network containing single admin and multiple users. Where the admin has the facility to add a set of words into each BoW database based on individual category. The admin should add each and every word into the database individually. Once if a word is added in one category the same word shouldn't be added on another category. So this should be mandatory step for the admin while adding words into the database. Also admin has the facility to authorize each and every user at the time of registration. The user who got activated by admin only can access his profile by login into the site. Those users who are not authorized cant be enter into their individual accounts at any cost.

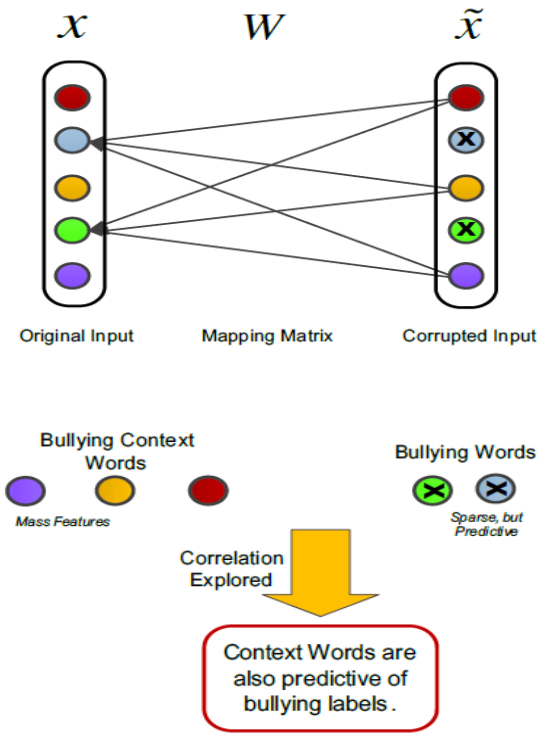
Marginalized Stacked De-noising Auto-encoder:

It can proposed a modified version of Stacked De-noising Auto-encoder that employs a linear instead of a nonlinear projection so as to obtain a closed-form solution . The basic idea behind de-noising auto-encoder is to reconstruct the original input from a corrupted one ~x1,…., ~xn with the goal of obtaining robust representation. Marginalized De-noising Auto-encoder: In this model, denoising auto-encoder attempts to reconstruct original data using the corrupted data via a linear projection.

Semantic Enhancement for m SDA:

The advantage of corrupting the original input in mSDA can be explained by feature co-occurrence statistics. The co--occurrence information is able to derive a robust feature representation under an unsupervised learning framework, and this also motivates other state-of-the-art text feature learning methods such as Latent Semantic Analysis and topic models.

A de-noising auto-encoder is trained to reconstruct these removed features values from the rest uncorrupted ones. Thus, the learned mapping matrix W is able to capture correlation between these removed features and other features. The major modifications include semantic dropout noise and sparse mapping constraints.



Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

However, a direct use of these bullying features may not achieve good performance because these words only account for a small portion of the whole vocabulary and these vulgar words are only one kind of discriminative features for bullying.

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Types of Testing:

Unit testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

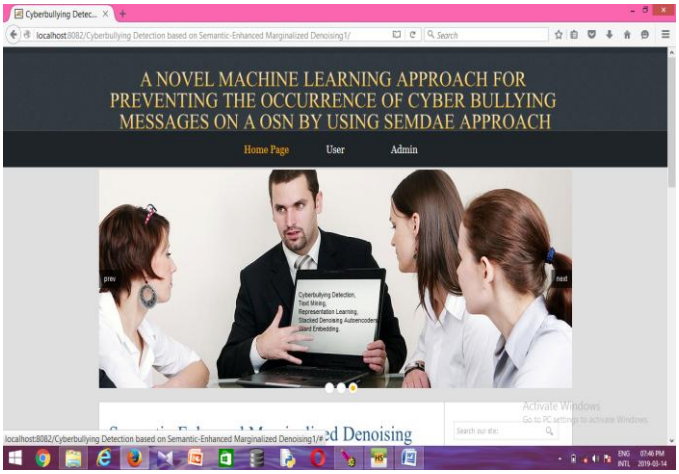
Valid Input : identified classes of valid input must be accepted.
Invalid Input : identified classes of invalid input must be rejected.
Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

Must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

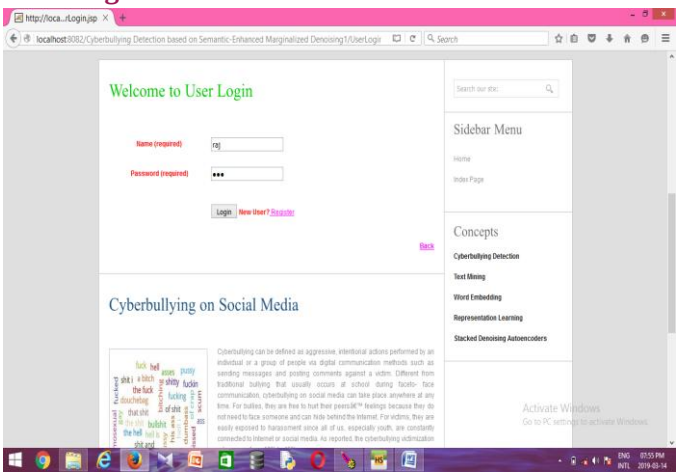
Result and Discussions

Home Page:

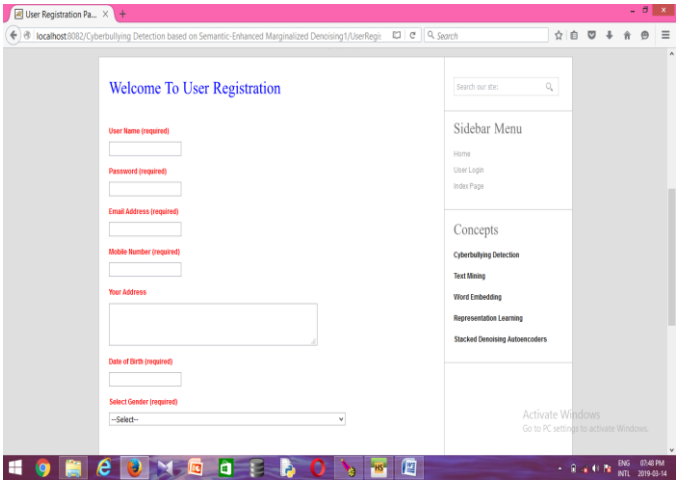
Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com



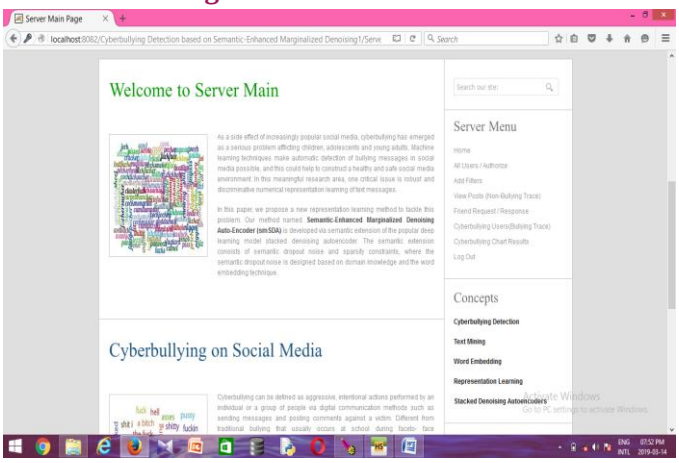
User Login:



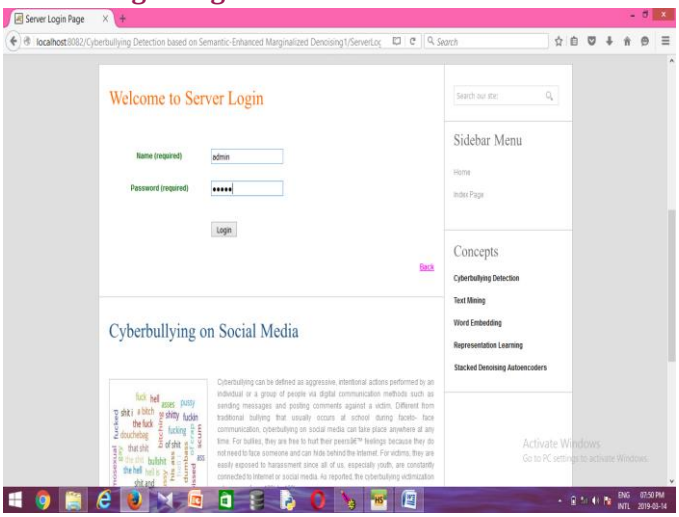
User Registration Page:



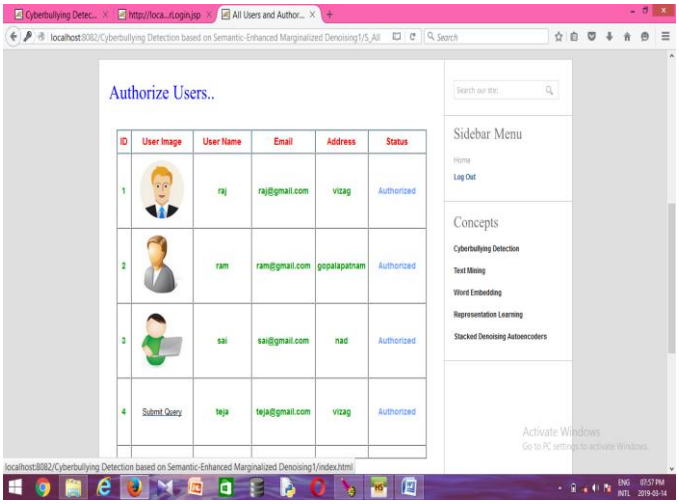
Admin Main Page:



Admin Login Page:

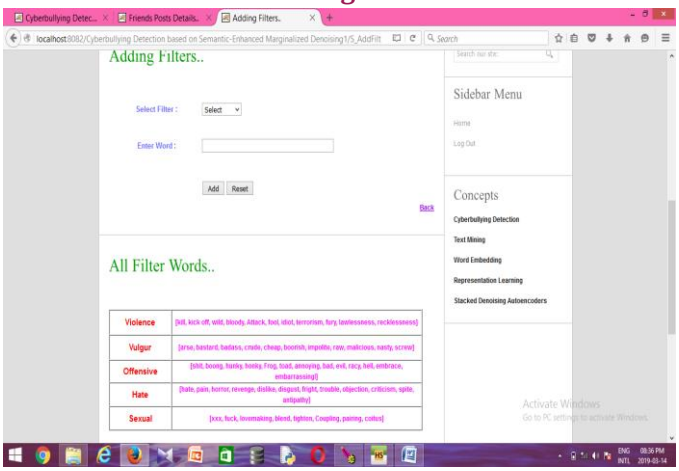


All Authorized Users:



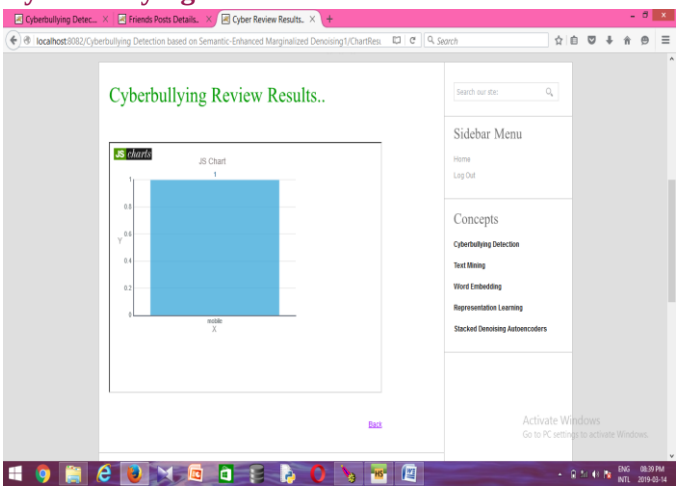
Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Add Filters Based On Categories:

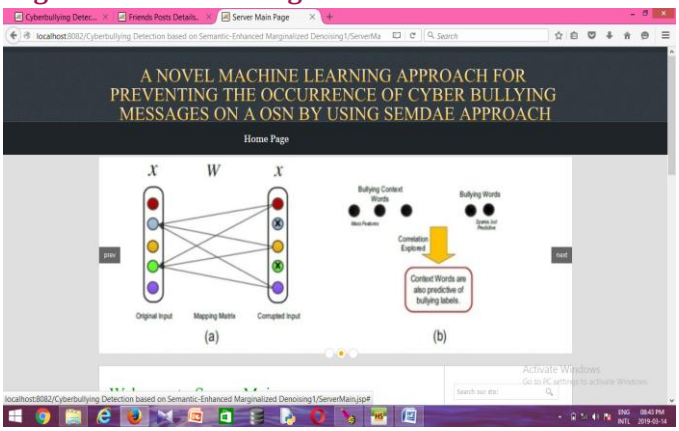


Cyber Bulling User:

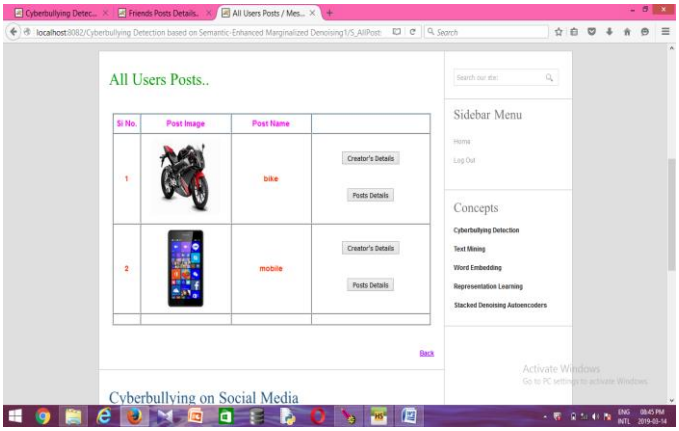
Cyber Bullying Review Results:



Algorithm Process Diagram:



All Users Posts View By Admin:



CONCLUSION

This paper addresses the text-based cyber bullying detection problem, where robust and discriminative representations of messages are critical for an effective detection system. By designing semantic dropout noise and enforcing sparsity, we have developed semantic-enhanced marginalized denoising auto encoder as a specialized representation learning model for cyber bullying detection. In addition, word embedding have been used to automatically expand and refine bullying word lists that is initialized by domain knowledge. The performance of our approaches has been experimentally verified through two cyber bullying corpora from social medias: Twitter and MySpace. As a next step we are planning to further improve the robustness of the learned representation by considering word order in messages.

Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

REFERENCES

[1] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.

[2] R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and M. R. Lattanner, "Bullying in the digital age: A critical review and metaanalysis of cyberbullying research among youth." 2014.

[3] M. Ybarra, "Trends in technology-based sexual and non-sexual aggression over time and linkages to nontechnology aggression," National Summit on Interpersonal Violence and Abuse Across the Lifespan: Forging a Shared Agenda, 2010.

[4] B. K. Biggs, J. M. Nelson, and M. L. Sampilo, "Peer relations in the anxiety–depression link: Test of a mediation model," Anxiety, Stress, & Coping, vol. 23, no. 4, pp. 431–447, 2010.

[5] S. R. Jimerson, S. M. Swearer, and D. L. Espelage, Handbook of bullying in schools: An international perspective. Routledge/Taylor & Francis Group, 2010.

[6] G. Gini and T. Pozzoli, "Association between bullying and psychosomatic problems: A meta-analysis," Pediatrics, vol. 123, no. 3,pp. 1059–1065, 2009.

[7] A. Kontostathis, L. Edwards, and A. Leatherman, "Text mining and cybercrime," Text Mining: Applications and Theory. John Wiley & Sons, Ltd, Chichester, UK, 2010.

[8] J.-M. Xu, K.-S. Jun, X. Zhu, and A. Bellmore, "Learning from bullying traces in social media," in Proceedings of the 2012 conference of the North American chapter of the association for computational linguistics: Human language technologies. Association for Computational Linguistics, 2012, pp. 656–666.

[9] Q. Huang, V. K. Singh, and P. K. Atrey, "Cyber bullying detection using social and textual analysis," in Proceedings of the 3rd International Workshop on Socially-Aware Multimedia. ACM, 2014, pp. 3–6.

[10] D. Yin, Z. Xue, L. Hong, B. D. Davison, A. Kontostathis, and L. Edwards, "Detection of harassment on web 2.0," Proceedings of the Content Analysis in the WEB, vol. 2, pp. 1–7, 2009.