BULLY NET: UNMASKING CYBER BULLIES ON SOCIAL NETWORKS

Sanjeevini S.H¹, T. Pavani², P. Keerthana², A. Rachana²

¹Assistant Professor, ²UG Students, Department of Cyber Security Engineering.
¹,²Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Kompally, Secunderabad-500100, Telangana, India.

To Cite this Article


ABSTRACT

In the rapidly evolving landscape of online communication, the surge in cyberbullying has emerged as a critical challenge, necessitating innovative solutions for detection and prevention. Existing approaches often rely on simplistic keyword-based filters or rule-based methods, struggling to keep pace with the dynamic nature of cyberbullying scenarios. The intricate and varied nature of online harassment demands a more sophisticated system capable of discerning subtle nuances within social media interactions. Recognizing this gap, the proposed BullyNet system introduces a character-level convolutional neural network (CNN) approach to enhance the accuracy and adaptability of cyberbullying detection. By incorporating both word-based and character-based models, BullyNet aims to provide a holistic understanding of language expression and contextual cues, offering a nuanced solution to the complex challenges posed by cyberbullying. This system’s multifaceted approach, encompassing preprocessing, training, and evaluation of CNN models, is designed to address the shortcomings of existing systems and contribute to the creation of a safer online environment. BullyNet stands as a promising stride towards unmasking cyberbullies on social networks, emphasizing the need for advanced tools capable of navigating the intricate landscape of digital communication.

INTRODUCTION

Cyberbullying is an increasingly important and serious social problem, which can negatively affect individuals. It is defined as the phenomena of using the internet, cell phones and other electronic devices to willfully hurt or harass others. Due to the recent popularity and growth of social media platforms such as Facebook and Twitter, cyberbullying is becoming more and more prevalent. Many applications of the World Wide Web need to discover the envisioned meaning of certain textual resources (e.g., data to be annotated, or keywords to be searched) in order to semantically describe the result causing the effects, such as the abusive words usage causes to create the impact of cyberbullying. However, this cyberbullying detection is more complicated because current search engine focuses only on retrieving the results containing the user keywords, and lots of data that may carry the desired semantic
information remains overdue. The cyber cyberbullying detection is an advanced topic in Artificial Intelligence research and related fields, which is a major problem not only in NLP but in the Semantic Web services as well. Disambiguation methods mean to get the most suitable sense of an ambiguous word according to the context. Cyberbullying is bullying that takes place over digital devices such as cell phones, computers, and tablets [1]. Cyberbullying can be achieved in various ways, such as sending a message containing abusive or offensive content to a victim, and some labeled posts are shown in Table 1. In a 2018 statistical report, during the 2015-16 school year, approximately 12% of public schools reported that students had experienced cyberbullying on and off campus at least once a week, and 7% of public schools reported that the school environment was affected by cyberbullying [2]. It can create negative online reputations for victims, which will impact college admissions, employment, and other areas of life, and can result in even more serious and permanent consequences such as self-harm and suicide [3]. Cyberbullying events are hard to recognize. The major problem in cyberbullying detection is the lack of identifiable parameters and clearly quantifiable standards and definitions that can classify posts as bullying [4]. As people spend increasingly more time on social networks, cyberbullying has become a social problem that needs to be solved, and it is very necessary to detect the occurrence of cyberbullying through an automated method. Our research focuses on textual cyberbullying detection because text is the most common form of social media. In text-based cyberbullying detection, capturing knowledge from text messages is the most critical part, but it is still a challenge. The first challenge that cannot be ignored is dealing with unstructured data. The content information in social media is short, noisy, and unstructured with incorrect spellings and symbols [5] such as the instances in Table 1. Social media users intentionally obfuscate the words or phrases in the sentence to evade manual and automatic detection as in R3. These extra words will expand the size of the vocabulary and influence the performance of the algorithm. Emojis made up of symbols such as :) in R4, which definitely convey emotional features, are always hard to distinguish from noise.

Table 1: Some instances in dataset.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Sassy.. More like trashy</td>
</tr>
<tr>
<td>R2</td>
<td>I HATE KAT SO MUCH</td>
</tr>
<tr>
<td>R3</td>
<td>Kat, a massive c*nt</td>
</tr>
<tr>
<td>R4</td>
<td>Shut up Nikki… That is all :)</td>
</tr>
</tbody>
</table>

Another key challenge in cyberbullying research is the availability of suitable data, which is necessary for developing models that can classify cyberbullying. There are some datasets have been publicly
available for this specific task such as the training set provided in CAW 2.0 Workshop and the Twitter Bullying Traces dataset [6].

Since cyberbullying detection has been fully illustrated as a natural language processing task, various classifiers have been masterly improved to accomplish this task, including the Naive Bayes [7], the C4.5 decision tree [8], random forests [9], SVMs with different kernels, and neural networks classifiers [6]. A variety of feature selection methods have also been carefully designed to improve the classification accuracy. However, previous data-based works have relied almost entirely on vocabulary knowledge, and so, the challenges that are posed by unstructured data still exist.

2. RELATED WORK

Traditional studies on cyberbullying stand more on a macroscopic view. These studies focused on the statistics of cyberbullying, explored the definitions, properties, and negative impacts of cyberbullying and attempted to establish a cyberbullying measure that would provide a framework for future empirical investigations of cyberbullying [15-18]. As cyberbullying has captured more attention, various methods have been used for the detection of cyberbullying in a given textual content. An outstanding work is the one by Nahar et al. Their work used the Latent Dirichlet Allocation (LDA) to extract semantic features, TF-IDF values and second-person pronouns as features for training an SVM [19].

Reynolds et al used the labelled data, in conjunction with the machine learning techniques provided by the Weka tool kit, to train a C4.5 decision tree learner and instance-based learner to recognize bullying content [8]. Xu et al showed that the SVM with a linear kernel using unigrams and bigrams as features can achieve a recall of 79% and a precision of 76% [6]. Dadvar et al took into account the various features in hurtful messages, including TF-IDF unigrams, the presence of swear words, frequent POS bigrams, and topic-specific unigrams and bigrams, and the approach was tested using JRip, J48, the SVM, and the naive Bayes [10].

Kontostathis et al analyzed cyberbullying corpora using the bag-of-words model to find the most commonly used terms by cyberbullies and used them to create queries [20]. In the work of Ying et al, the Lexical Semantic Feature (LSF) provided high accuracy for subtle offensive message detection, and it reduced the false positive rate. In addition, the LSF not only examines messages, but it also examines the person who posts the messages and his/her patterns of posting [12]. As the use of deep learning becomes more widespread, some deep learning-based approaches are also being used to detect cyberbullying.

The work of Agrawal and Awekar provided several useful insights and indicated that using learning-based models can capture more dispersed features on various platforms and topics [21]. The work of Bu and Cho provided a hybrid deep learning system that used a CNN and an LRCN to detect cyberbullying in SNS comments [22]. Since previous data-based work relied almost entirely on
vocabulary knowledge, the challenge posed by unstructured data still exists. Some works observed that the content information in social media has many incorrect spellings, and in some cases, the users in social media intentionally obfuscate the words or phrases in the sentence to evade the manual and automatic detection [23, 24]. These extra words will expand the vocabulary and affect the various performances of the algorithm.

Waseem and Hovy performed a grid search over all possible feature set combinations. They found that using character n-grams outperforms when using word n-grams by at least 5 F1-points using similar features [25], and it is a creative way to reduce the impacts of misspellings. Al-garadi et al used a spelling corrector to amend words, but we believe that some mistakes in this particular task scenario hide the speaker’s intentions and correcting the spelling will destroy the features in the original dataset [26]. Zhang et al innovatively attempted to use phonemes to overcome deliberately ambiguous words in their work. However, some homophones with different meanings will get the same expression after their conversion, and their methods cannot solve some misspellings that have no association in their pronunciations [24].

3. PROPOSED SYSTEM

The proposed architecture for cyberbullying detection as shown in Figure 3 is broadly divided into four stages namely data storage stage, data preprocessing stage, data detection stage and output stage. In the data storage stage, data will be trained based on word, character and synonyms. Finally creates the three individual trained datasets such as word level trained dataset, character level trained dataset and synonym level trained dataset. These trained data sources consisting of malicious data generated by numerous attackers and contains the spelling and grammatical errors, these datasets available from the different sources of social networking platforms.

3.1. Data preprocessing stage

In the data preprocessing stage, input test data \(T\) will be applied and will be spitted into words. Then white space will be removed using padding extraction operation. In the extracted words, there might be the special characters, unknown symbols, and encrypted format data. This may cause to creation of abusive content in text generates bullying. Thus, these missing unknown text data will be replaced by the known relevant text. The text data is in ASCII format generally, but neural networks neither be trained nor be tested with the text content. Thus, the input text data will be converted into special type of non-ASCII value and will be represented in digital numeric’s for every character like “a will be transformed to 0”, similarly b:1, c:2, d:3 and goes on for all characters.

 Tokenization
Over here the input text data is split into a set of words by removing all punctuation marks, tabs and other non-text characters and replacing them with white spaces. The part-of-speech (POS) tagging is also applied in some cases where words are tagged according to the grammatical context of the word in the sentence, hence dividing up the words into nouns, verbs, etc. This is important for the exact analysis of relations between words. Another approach was to ignore the order in which the words occurred and instead focus on their statistical distributions (the bag-of-words approach). In this case it is necessary to index the text into data vectors. The POS becomes important if the research is related to NLP. In one algorithm as part of extension work POS has been implemented.

**Padding extraction**

Padding refers to the white space between words, thus in padding extraction the space between two conjugative words will be extracted. In most of the times, the attackers wantedly use the whiter space to utilize the abusive text in the data. Thus, by using the padding extraction, the words contain white space will be precisely analyzed for cyberbullying detection.

![Diagram](Figure 3: Proposed cyberbullying detection architecture.)

**Word signature**

Unknown word handling module Unknown words are defined as the words which are not in the lexicon or in reference sentences. Since CNN algorithm generate error as it detects unknown word therefore a separate module is required for tag decision for unknown word. In case of cyberbullying scenario, the
attackers use the complicated abusive words; they may not be presented in the vocabulary. Thus, out of vocabulary words also considered for cyberbullying detection.

**Non-ASCII conversion**

Electronic processing of text in any language requires that characters (letters of the alphabet along with special symbols) be represented through unique codes, this is called encoding. Usually, this code will also correspond to the written shape of the letter. A NON-ASCII conversion is basically a number associated with each letter so that computers can distinguish between different letters through their codes.

3.2. Data detection stage

In the data detection stage character level, word level and synonym level embedding operation will be performed. In this embedding character recognition, word recognition and synonym recognition operations will be performed parallel manner to give the maximum efficiency to detect the cyberbullying. Then the data groups will be formed as 3D array using pattern matching operations. The selection of character level or word level or synonym level cyberbullying detection is performed by the user through user interface. Then corresponding 3D group array will be applied CNN.

**Data Clustering**

Clustering is a powerful and broadly acceptable data mining technique which is used to partition voluminous data into different classes, known as clusters, to support the businessman or an end user by providing different views and various patterns of same data suitable to the requirements. The cyberbullying detection focuses on the different levels clustering’s such as character level, word level and synonym-character level.

Phase I: The set of prototype vectors are much higher than the expected number of clusters. The prototypes are grouped to form the actual character-based clusters.

Phase II: In this phase word level clustering algorithm is executed on the prototypes vectors to find clusters' word centroid. Clustering of vast amount of words in text samples is a key process in providing a higher level of knowledge about the underlying inherent classification of the abusive content causes to create cyberbullying.

Phase III: The word-based cluster centres obtained in Phase II are used in phase III. Synonym-character identification algorithm utilizing the high standard vocabulary is applied in this phase to generate the actual synonym-character-based clusters. The result from word level clustering which is found in phase II is used as the initial seed of the Synonym-character identification algorithm. Phase III converges quickly when the centroids from Phase II are used.
A normalized longest common subsequence (NLCS) based string approximation method is proposed for indexing multidimensional data cube. In this indexing system, the reference table is made, and dimensional key values are stored for each dimension. A dimensional reference table is a set of dimensional key values stored in sorted order. The slot number of a key value in the dimensional reference table will be the index of the key value on the axis of multidimensional array. NLCS based string approximation is used to search a nearest keyword for a misspelled keyword, in the reference table and gets its slot number.

Normalized LCS based string approximation is used to design a character, word, and synonym (CWS) searching algorithm. This CWS searching algorithm gives near optimal solution to the string approximation problem. The algorithm finds the NLCS values of searched keyword with all the stored keywords in the set. The keywords in the set having NLCS value between 0.5 and 1 are the nearest neighbor of the searching keyword. The keyword closest to the searching keyword having highest NLCS value will be the optimal keyword. The CWS searching, finds the index of keyword, like searching keyword from the set of stored keywords and creates the 3d array group for easily detection of cyberbullying. So, the abusive words and its synonyms will be identified easily.

3.3 Deep-learning CNN

The selection of character level (C) or word level (W), synonym level (S) cyberbullying detection is performed by the user through user interface, and then selected cyberbullying detection operation will be performed on the predefined trained model. There is common deep learning architecture for word, character and synonym-character level cyberbullying detection, if the user selects word level cyberbullying detection, then entire operation will be performed on word level trained dataset. If the user selects character level cyberbullying detection, then entire operation will be performed on character level trained dataset. But, if the user selects synonym-character level cyberbullying detection, then entire operation will be performed on three trained datasets such as character level, word level and synonym-character level trained datasets. The CNN can take predefined features of synonyms and n-grams features of each word and character, the applied to multiple layers of various filters to build feature vector. The advantage of this technique is each word, character and synonym similarity will be checked with CNN trained model and if attacker is using more cyberbullying content then it can be easily detected. With the help of this technique any spelling variations used by attacker to avoid detection also detected very easily. Apart from spelling mistake malicious users, we are building CNN to one more extra step by utilizing similar synonym words of cyberbullying text to mislead and missed detector words as detector trained model with original words and also with various similar synonyms of original word. Users can understand that text contains cyberbullying with synonyms words, but model do not know. Thus, we are building CNN model with synonyms of all possible ways for detection
with characters to prevent malicious user from sending cyberbullying text in no possible way. Finally, in the output stage the detected cyberbullying words (CB) will be generated. If the CNN model generates $CB$ as 1 it indicates cyberbullying word else generates $CB$ as 0 it indicates non-cyberbullying word. Then qualitative evaluation operation will be performed to measure the efficiency of the system.

**Proposed CNN**

Convolutional neural networks Convolutional neural network (CNN), originally created for image processing, have performed very well in natural language processing (NLP), especially in sentiment analysis and question classification. Convolutional neural networks with end-to-end training were used in NLP for the first time in other works [31, 32]. heir ground-breaking work introduced a new global max-pooling operation, which has been proved to be effective for text, as an alternative to the conventional local max-pooling of the original LeNet architecture [33]. As a brilliant variant, Kim proposed a simpler multichannel architecture with varying size filters [34]. Kalchbrenner et al proposed a wide convolution operation and dynamic k-max pooling structure to handle variable-length input sentences [35]. These classical works have proved that CNNs have excellent performance in text classification tasks, and they are constantly being updated by the efforts of many researchers.

In NLP, capturing features from text is a critical part. Thanks to the work on distributed representations, which are also known as word embeddings, the initialization of embedding vectors has become more efficient with the help of open tools such as word2vec and Glove. Essentially after word embedding, vocabularies are combined into a set of vectors in a relatively low-dimensional space, and the distance between these vectors is determined by their semantic relationship. However, some works further noted that word-based input representations may not be very well adapted to social media inputs such as Twitter, where the token usage may be extremely creative [36].

In addition to word-level inputs, character-level inputs can also build a language model. The idea of character-level language modeling comes from signal processing. The grammar and word semantics in the text are simply ignored because it is widely believed that the model can capture this grammar and word semantic information. The challenge of character-level language modeling is that it requires a large amount of data and enough training time to make the model smart enough to extract the grammatical information and word semantic information from the text. In addition, it also requires data expansion to avoid generalization errors. The work of Zhang et al is the first to apply a CNN only on characters [30], and their innovative work indicated that deep convolutional neural networks do not rely on word knowledge. They also suggested that ConvNets may have better applicability to real-world scenarios. They coded the characters in the alphabet to quantify the characters and fixed the input length to 1014 since it seems already capture most of the text of interest. However, their work focused on large-scale datasets and the parameters they designed are oversized for a corpus such as the comment text of a social media platform. Johnson and Tong compared the performance of a CNN text
classification model on the word-level and character-level. In their results, the shallow word-CNNs generally achieved better error rates and higher speed than those of the very deep char-CNNs, but they used more parameters and therefore require more memory [37]. Especially for corpus of a social media, the method uses a huge, embedded table that contains many noise words.

4. RESULTS AND DISCUSSION

Convolution Neural Networks was designed for image processing but it also giving best performance in Natural Language Processing to detect sentiments from text or cyberbullying. Existing techniques were using words vector to embed or feed data into CNN networks and these networks may not predict correct class due to small spelling mistakes available in train data and sometime some users may give spelling mistakes to avoid detection process. To allow CNN network to predict spelling mistakes or shortcuts data we are building Character Based CNN networks.

To design character-based CNN we will split text data into words and then extract characters from each work and build a vector. CNN embedding layer can be created using all characters available in English language and this embedding layer act as vocabulary for CNN. CNN filter all text data based on embedding layer.

Vocabulary example for CNN
‘a:0,b:1,c:2,d:3 and goes on for all characters’

If user give input as ‘bc’ then CNN convert ‘b, c’ with embedding weight such as ‘1,3’ as b is available at index 1 and c available at index 2. Similarly, CNN will build model by scanning embedding vocabulary.

MODULES

To implement this paper following modules are used:

1) Upload Dataset: Using this module text-based dataset can be uploaded to application.
2) Clean Module: Using this module we will apply various NLP techniques to remove stop words, special symbols etc.
3) Generate Vocabulary and Embedding Vector: using this module we will build vocabulary with all English characters set. Convert all text-based data to numeric by obtaining text numeric value from vocabulary and build a training vector.
4) Generate Character Based CNN Model: Using this module we will create CNN layers with vocabulary input and output sizes and then give train data as input to build CNN model.
5) Metrics Calculation: Using this module we will calculate various metric such as ACCURACY, PRECISION, RECALL and FMEASURE.
6) Predict Cyberbullying: Using this module we will ask user to enter any text message and then apply pre-processing technique to clean text and then convert text into one hot encoding or numeric vector. This numeric vector will be applied on CNN trained model to predict whether text contains any cyber bulling words or not.

**Formulas to calculate metrics**

Accuracy = correctly_classified_records / total_no_of_test_records

Precision = TruePositives / (TruePositives + FalsePositives)

Recall = TruePositives / (TruePositives + FalseNegatives)

F-Measure = (2 * Precision * Recall) / (Precision + Recall)

While calculating accuracy suppose we have 20 test records and model able to predict 18 records correctly then the accuracy of model can be 18 / 20 = 0.90%. Similarly, to get Precision, Recall and F-Measure we need to calculate 4 values based on prediction.

**UI RESULTS**
In above screen I entered message as ‘I hate you .. you are a bitch’ and below is the result.

In above screen we got prediction result as given message contains Cyber Bullying words. Below is an example of predicting bullying with shortcuts.
5. CONCLUSIONS

In conclusion, cyberbullying is a serious issue that can have devastating effects on individuals and society as a whole. Therefore, effective methods for detecting and predicting cyberbullying are essential to prevent its harmful consequences. The use of deep learning models such as word-based and char based CNNs with shortcuts has shown promising results in accurately identifying instances of cyberbullying. These models utilize the power of natural language processing and deep learning techniques to analyze text data and classify it as either cyberbullying or non-cyberbullying. By incorporating shortcut connections, these models can learn complex features and relationships in the text data, enabling them to accurately predict and classify instances of cyberbullying.

REFERENCES


