CYBER HARASSMENTDETAILANALYSIS AND PREDICTOIN USING MACHINE LEARNING

Dr J REDDEPPA REDDY [1], N SRIKANTH [2],V NARESH [3]

1 & 2, Associate Professor, CSE department, Brilliant Institute of Engineering & Technology, Hyderabad, TS.

3 Assistant Professor, CSE department, Brilliant Institute of Engineering & Technology, Hyderabad, TS.

ABSTRACT

Child kidnapping, missing child and child harassment are the world wide problem related child safety.The children of age group 4 to 8 years are innocent and subject to kidnapping in frequent cases . Parents are always worried regarding their children's security mainly when they visit crowded public places and travel in widely physically located places . Number of applications is being developed to guard children in every manner . This paper introduces a Parent - Hook product which is designed for child tracking if the child is lost.The Parent-Hook is a safety band without the sensor or any chip harmful for the children can be put on the whist of the children . This band is easy to carry which is made of soft cotton webbing with parent contact information with QR Code and Cloud URL.

1. INTRODUCTION

Researchers can interpret massive data with the use of machine or deep learning techniques [1]. In the age of big data, it is now feasible to get a wealth of knowledge about people and their society that was before unimaginable [2]. Social media is one of the primary sources of information on people (SM). We may use historical data to forecast the future of a broad variety of applications by applying machine learning algorithms to SM data. Machine learning algorithms provide us the chance to predict and identify harmful human behavior, including cyberbullying, with greater accuracy [3]. Using deep learning from raw data, big data analysis can reveal information that was previously unknown [1]. The use of big data analytics has enhanced a number of applications, and the combination of big data with machine learning has even made future forecasting conceivable.

In order to detect and control violent behavior, an effective study of data on human interaction and behavior must take into account a variety of viewpoints, factors, and approaches from several disciplinary and interdisciplinary fields. Large-scale data are easily accessible, leading to new research issues, cutting-edge computational techniques, collaborative strategies, and exceptional chances to uncover numerous crucial problems statistically. Unfortunately, the size and accuracy of employing conventional techniques (statistical techniques) in this situation are difficult. These techniques frequently rely on small-scale human networks and structured data on human behavior (traditional social networks). There are various problems with using these approaches on massive online social networks (OSNs), both in terms of volume and scope. On the one hand, the rapid development of OSNs promotes and spreads aggressive types of behaviour by offering venues and networks on which to engage in and spread such conduct. On the other hand, OSNs provide crucial information for studying human behaviour and interaction on a broad scale. Researchers may utilise this information to create efficient strategies for identifying and controlling inappropriate and/or hostile conduct. OSNs give criminals the means to act violently and the networks to behave badly. The detection and control of aggressive behaviour in complex systems should thus be improved using approaches that take into account both aspects (content and network).

2. LITERATURE SURVEY

This chapter describes the research literature relevant to the primary aspects of this thesis. Although there are many different types of machine learning algorithms, practically all research on cyberbullying prediction in SM websites utilised the most well-established and extensively used type, supervised machine learning algorithms. The accuracy with which the model transforms various sorts of past observation or information about the job determines the success of machine learning techniques. Most of the practical application of machine learning is concerned with the specifics of a given situation. Then, an algorithmic paradigm that allows for correct fact encoding is chosen. Unfortunately, no one machine learning technique is optimum for all problems. As a result, most researchers chose and compared a large number of supervised classifiers to find the best ones for their task. As a result, most researchers chose and compared a large number of supervised classifiers to find the best ones for their task. The most widely used classifiers in the area, as well as the data attributes accessible for trials, are utilised to pick classifiers. Nevertheless, researchers

can only pick which algorithms to use for building a cyberbullying prediction model after conducting a full practical trial.

The machine learning methods frequently employed to create cyberbullying prediction models are described in the sections that follow.

1)Support Vector Machine in Cyberbullying

Text categorization frequently makes use of the supervised machine learning classifier known as the support vector machine (SVM). A separating hyperplane is created in the feature characteristics of two classes, and the distance between the hyperplane and the adjacent data point of each class is then maximised to create a support vector machine (SVM). SVM was theoretically created using statistical learning theory. The SVM algorithm's "optimal separation hyperplane" refers to the separating hyperplane that is attained during the training phase and minimises misclassifications. Based on reduced categorization risks, the methodology. SVM was developed initially to categorise classes with linear separability. Objects from various classes that may be linearly separated are included in a 2D plane (e.g., positive or negative). SVM seeks to effectively divide the two classes. By increasing the distance between the exceptional hyperplane and the closest data point of each class, SVM determines the hyperplane that offers the greatest margin.In real-time applications, precisely determining the separating hyperplane is difficult and nearly impossible in several cases. SVM was developed to adapt to these cases and can now be used as a classifier for non-separable classes. SVM is a capable classification algorithm because of its characteristics. Specifically, SVM can powerfully separate non-linearly divisible features by converting them to a high-dimensional space using the kernel model .

The advantage of SVM is its high speed, scalability, capability to predict intrusions in real time, and update training patterns dynamically.

SVM has been used to develop cyberbullying prediction models and found to be effective and efficient. For example, Chen et al.applied SVM to construct a cyberbullying prediction model for the detection of offensive content in SM. SM content with potential cyberbullying were extracted, and the SVM cyberbullying prediction model was applied to detect offensive content. The result showed that SVM is more accurate in detecting user offensiveness than naïve Bayes (NB). However, NB is faster than SVM. Chavan and Shylaja proposed the use of SVM to build a classifier for the detection of cyberbullying in social networking sites. Data containing offensive words were extracted from social networking sites and utilized to build a cyberbullying SVM prediction model. The SVM classifier detected cyberbullying more accurately than LR did. Dadvar et al.used SVM to build a gender specific cyberbullying prediction model. An SVM text classifier was created with gender specific characteristics.

The SVM cyberbullying prediction model enhanced the detection of cyberbullying in SM. Hee et al. developed an SVM-based cyberbullying detection model to detect cyberbullying in a social network site. The SVM-based model was trained using data containing cyberbullying extracted from the social network site. The researchers found that that the SVM-based cyberbullying model effectively detected cyberbullying. Mangaonkar et al. constructed an SVM-based cyberbullying detection model for YouTube. Data were collected from YouTube comments on videos posted on the site. The data were used to train SVM and construct a cyberbullying detection model, which was then used to detect cyberbullying. The results suggested that the SVM-based cyberbullying model is more reliable but not as accurate as rule-based Jrip. However, the SVM-based cyberbullying model is more accurate than NB and tree-based J48. Dinakar et al.proposed the use of SVM for the detection of cyberbullying in Twitter. An SVM-based cyberbullying model was constructed from data extracted from Twitter. The SVM-based cyberbullying prediction model was applied to detect cyberbullying in Twitter. SVM detected cyberbullying better than NB- and LR-based cyberbullying detection models did.

3. EXISTING SYSTEM

In the recent years, a lot of research has been done on the role that machine learning algorithms play in OSN content analysis. With the successful development of multiple models, tools, and algorithms for processing massive volumes of data to address practical issues, machine learning research has become essential in a wide range of fields.

According to recent research, the majority of specialists support monitoring cyberbullying automatically. The urgent need for autonomous monitoring and prediction models for cyberbullying was validated by a study that looked at 14 groups of adolescent participants. The study found that conventional methods for dealing with cyberbullying in the age of big data and networks do not function effectively.

DISADVANTAGES OF EXISTING SYSTEM

SM websites provide a lot of textual and/or non-textual content, as well as information about aggressive conduct. As a result, cyberbullying has become more severe on SM platforms that encourage open and anonymous cyberbullying. These features

make social media platforms (SM) like Twitter risky places to engage in cyberbullying

3.2PROPOSEDSYSTEM

In this study, aggressive conduct is predicted via content analysis of SM websites. Such an analysis for predicting cyberbullying behaviour is restricted to textual OSN material. Given how simple it is to engage in cyberbullying, it is regarded as a hazardous and quickly proliferating hostile behaviour.

To find published works on cyberbullying prediction models, two steps were used. Finding reliable academic databases and search engines was part of the initial phase. the academic databases and search engines employed for the retrieval of pertinent documents.

Cyberbullying, aggressive behaviour, big data, and cyberbullying models were the main terms that were coined in connection to social media and used for the literature search.

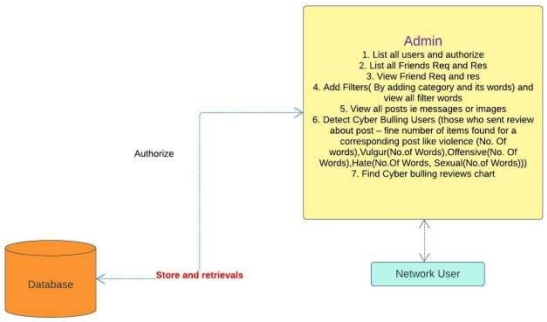
The second stage entailed using the digital library at Qatar University to look up literature. To make sure the articles matched the inclusion requirements, the search results were carefully examined.

PROPOSED SYSTEM BENEFITS

High speed, scalability, real-time intrusion prediction, dynamic updating of training patterns.

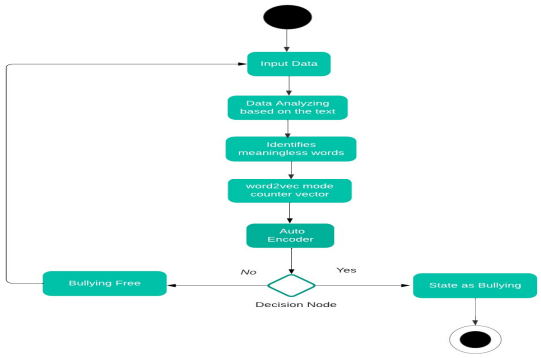
The concept has been utilised to create prediction models for cyberbullying, and it has been discovered to be successful and efficient.

4.SYSTEM ARCHITECTURE .



Activity Diagram

A graphical representation of the work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5. SYSTEM IMPLEMENTATION

- Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as view and authorize users, view all friends request and responses, Add and View Filters, View all posts, Detect Cyber Bullying Users, Find Cyber Bullying Reviews Chart.

Viewing and Authorizing Users

In this module, the admin views all users details and authorize them for login permission. User Details such as User Name, Address, Email Id, Mobile Number.

Viewing all Friends Request and Response

In this module, the admin can see all the friends' requests and response history. Details such as Requested User Name and Image, and Requested to User Name and Image, status and date.

Add and View Filters

In this module, the admin can add filters (like Violence, Vulgar, Offensive, Hate, and Sexual) as Categories with the words those related to corresponding filters.

View all posts

In this module, the admin can see all the posts added by the users with post details like post name, description and post image.

Detect Cyber Bullying Users

In this module, the admin can see all the Cyber Bullying Users (The users who had posted a comment on posts using cyber bullying words which are all listed by the admin to detect and filter). In this, the results shown as, Number of items found for a corresponding post like Violence (no. of words belongs to Violence Filter used in comments by the users), Vulgar (no. of words belongs to Vulgar Filter

used in comments by the users), Offensive (no. of words belongs to Offensive Filter used in comments by the users), Hate (no. of words belongs to Hate Filter used in comments by the users), Sexual (no. of words belongs to Sexual Filter used in comments by the users).

Find Cyber Bullying Reviews Chart
In this module, the admin can see all the posts with number of cyber bullying comments posted by users for particular post.

 User
In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user can perform some operations like viewing their profile details, searching for friends and sending friend requests, Posting Your Messages as Posts by giving details, View and Comment on Friend Posts, viewing all friends posts and comment, view all your cyber bullying comments on your friend posts.
Viewing Profile Details, Search and Request Friends
In this module, the user can see their own profile details, such as their address, email, mobile number, profile Image.
The user can search for friends and can send friend requests or can accept friend requests.
Add Posts
In this, the user can add their own posts by giving post details such as, post title, description, uses, and image of post.
View and Comment on Your Friends Post
In this, the user can see his entire friend's post details (post title, description, uses, creator and image of post) and can comment on posts.
View all Friends Posts and Comment (Cyber bullying Related)
In this, the user can see his all friend's post details (post title, description, uses, creator and image of post) and can comment on posts.
Don't Post If the comment consists of Cyber bullying words and Shows the reason why comment is not posted by indicating Detected Cyber Bullying Words like Numbers of Cyber Bullying words Related to Filter Violence found in comment, Numbers of Cyber Bullying words Related to Filter Vulgar found in comment, Numbers of Cyber Bullying words Related to Offensive found in comment, Numbers of Cyber Bullying words Related to Hate found in comment, Numbers of Cyber Bullying words Related to Sexual found in comment,

View all Your Cyber bullying comments on your friend posts
The user can see all his posted cyber bullying comments on their friend created posts.
6.1 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:

7.RESULTS

fig.7. 1 Home page

fig.7.2 This fig shows the remote users data

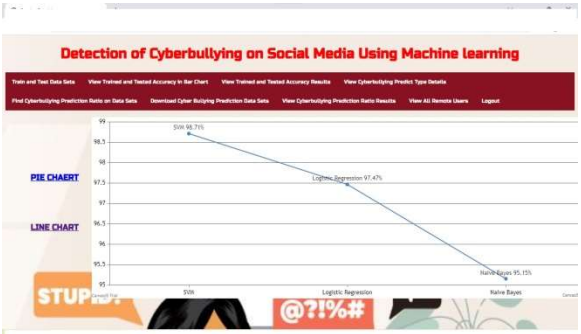


Fig 7.3 This fig shows the line chart and pie chart

Fig 7.4 This fig shows the trained and tested data.

8. CONCLUSION & FUTURE WORK

By the use of machine learning techniques, this study evaluated the body of literature to identify hostile conduct on SM websites. With regard to utilising machine learning techniques to identify cyberbullying texts, we primarily looked at four aspects: data collecting, feature engineering, building a model to detect cyberbullying, and assessing the model. Also, a summary of several categories of discriminative traits that were employed to identify cyberbullying in online social networking sites was provided. Also, the best supervised machine learning classifiers for categorising messages from online social networking sites that contain cyberbullying were found. The definition of evaluation metrics to properly identify the relevant parameter so that the various machine learning algorithms can be compared to one another is one of the primary contributions of the current study. Most crucially, using machine learning approaches, particularly supervised learning, we summarised and identified the critical elements for identifying cyberbullying. In order to simulate the behaviours involved in cyberbullying, we have employed accuracy, precision recall, and f-measure, which provides us with the area under the curve function. The primary concerns and unresolved research problems were then outlined and debated. To build extremely efficient and reliable cyberbullying detection methods, significant research is needed. We are certain that the current study will offer important information and suggest fresh approaches to the problem of identifying violent human behaviour, including cyberbullying on online social networking sites.

REFERENCES

[1] V. Subrahmanian and S. Kumar, ``Predicting human behavior: The nextfrontiers," Science, vol.355, no. 6324, p. 489, 2017.

[2] H. Lauw, J. C. Shafer, R. Agrawal, and A. Ntoulas, ``Homophily in thedigital world: ALiveJournal case study," IEEE Internet Comput., vol. 14,no. 2, pp. 15_23, Mar./Apr. 2010.

[3] M. A. Al-Garadi, K. D. Varathan, and S. D. Ravana, ``Cybercrime detectionin online communications: The experimental case of cyberbullyingdetection in the Twitter network," Comput. Hum. Behav., vol. 63,pp. 433_443, Oct. 2016.

[4] L. Phillips, C. Dowling, K. Shaffer, N. Hodas, and S. Volkova, ``Usingsocial media to predict the future: A systematic literature review," 2017,arXiv:1706.06134. [Online]. Available: https://arxiv.org/abs/1706.06134

[5] H. Quan, J. Wu, and Y. Shi, ``Online social networks & social networkservices: A technical survey," in Pervasive Communication Handbook.Boca Raton, FL, USA: CRC Press, 2011, p. 4.

[6] J. K. Peterson and J. Densley, ``Is social media a gang? Toward a selection,facilitation, or enhancement explanation of cyber violence," AggressionViolentBehav., 2016.

[7] BBC. (2012). Huge Rise in Social Media. [Online]. Available:http://www.bbc.com/news/uk-20851797

[8] P. A.Watters and N. Phair, ``Detecting illicit drugs on social media usingautomated social media intelligence analysis (ASMIA)," in CyberspaceSafety and Security. Berlin, Germany: Springer, 2012, pp. 66_76.