DIGITAL FORENSICS:AN INVESTIGATIONON CYBERBULLYING ACTIVITIES USING MACHINE LEARNING ALGORITHM

Raja ram N[1], Praveen B[2], VishvaS[3], Mr. Santana Krishnan J[4]
[123] University college of Engineering, Thirukkuvalai, Nagapattinam, Tamilnadu, India
[4] Assistant professor, Department of computer science, University college of Engineering, Thirukkuvalai, Nagapattinam, Tamilnadu, India
E-mail: [1] rr7435925@gmail.com , [2] basspraveen2002@gmail.com , [3] sivakumar71816@gmail.com , [4]csesaki@gmail.com

ABSTRACT

Cyberbullying has become a growing concern in today's society, with more and more people turning to the internet to harass and intimidate others. Digital forensics is an essential tool for investigating cyberbullying activities, as it allows for the collection and analysis of digital evidence. However, traditional digital forensics techniques can be time-consuming and require a significant amount of human effort. In this paper, we propose the use of machine learning algorithms to aid in the investigation of cyberbullying activities. By training these algorithms on a dataset of known cyberbullying incidents, we can create a predictive model that can automatically classify new instances of cyberbullying. This can significantly reduce the time and effort required for investigations, allowing for a more efficient response to cyberbullying incidents. The challenges associated with using machine learning for cyberbullying detection, including the need for high-quality training data and the potential for bias in the algorithms. We also explore the various types of digital evidence that can be used in cyberbullying investigations, such as social media posts, emails, and instant messages. We present a case study in which we apply our proposed approach to a real-world cyberbullying incident. Our results show that the machine learning algorithm was able to accurately identify the cyberbullying activity with a high level of precision, demonstrating the potential of this approach for improving the efficiency and effectiveness of cyberbullying investigations.

I.INTRODUCTION

Digital forensics refers to the process of collecting, analysing, and preserving electronic data in order to investigate and prevent cybercrimes. One of the major cybercrimes that digital forensics can help investigate is cyber bullying, which involves the use of digital technologies to harass, intimidate, or embarrass individuals or groups.

In recent years, cyber bullying has become a growing concern, particularly among young people who spend a significant amount of time on social media platforms and other digital communication channels. To combat cyber bullying, digital forensics experts have started using machine learning techniques to identify patterns of behaviour and detect cyber bullying activities. Machine learning algorithms can analyse large volumes of data and identify suspicious patterns of behaviour that may indicate cyber bullying. For example, machine learning models can be trained to identify abusive language, threatening messages, and other indicators of cyber bullying in online communication channels. By leveraging machine learning algorithms, digital forensics experts can quickly and accurately identify cyber bullying activities, which can help law enforcement agencies and other stakeholders take appropriate action to prevent further harm. Ultimately, the use of machine learning in digital forensics can help create a safer and more secure online environment for everyone.

II.LITERATURE SURVEY

1) The study reviewed the existing literature for various machine learning algorithms and identified Light GBM as the most efficient. A model for detecting bullying tweets for real time tweets was developed.
2) The emergence of social media, particularly Twitter, has raised a slew of challenges owing to a misunderstanding of the notion of free expression. One of these difficulties is cyberbullying, which is a severe global issue that affects both individual victims and societies.
3) Cyberbullying and cyber aggression are increasingly worrisome phenomena affecting people across all demographics. More than half of all teenage social media users across the world have experienced such protracted and/or organized digital abuse.
4) In this research, a multidimensional feature set that takes into consideration individual-based, social network-based, episode-based, and linguistic content-based cyberbullying aspects is constructed.Social media networks like Facebook and Twitter create a great platform to share public views, opinions, and feelings by text message, image, and video. The public is eager to utilize these networks because of the simple Graphical User Interface (GUI) that allows them to exchange material from their electric gadgets, gizmos, and, most notably, smartphones.
5) Social media networks like Facebook and Twitter create a great platform to share public views, opinions, and feelings by text message, image, and video. The public is eager to utilize these networks because of the simple Graphical User Interface (GUI) that allows them to exchange material from their electric gadgets, gizmos, and, most notably, smartphones.

6) The purpose of this study is to highlight prior researchers and to provide a method for detecting cyberbullying that includes sarcasm. The findings demonstrated that the SVM classifier outperformed other classifiers.
7) Prior to the development of information and communication technology (ICT), social connections were limited to local cultural boundaries such as geo-spatial places. Recent advancements in communication technology have significantly surpassed conventional communications' time and geographical limits.
8) The purpose of this paper is to investigate several methodologies that take into account time in the identification of cyberbullying in social networks. We use a supervised learning strategy with two distinct early detection models, threshold and dual.
9) Cyberbullying has greatly affected people's daily lives. This study is being conducted to determine whether online comments contain cyberbullying behaviors and to characterize cyberbullying in order to reduce this problem. An increased information gain approach is employed for feature selection, while the bidirectional LSTM neural network is used for classification.
10) This study employs supervised machine learning (ML) and Natural Language Processing (NLP) to identify cyberbullying in the Malay language. Because of the rising number of cyberbullying incidents in Malaysia throughout the years, as well as the idea that there are an increasing number of unreported cyberbullying cases, an intelligent method to identify cyberbullying on social media is required.

III.EXISTING SYSTEM

Experts believe that every government should take this issue seriously and work to find a solution. In 2016, an incident known as the Blue Whale Challenge resulted in a large number of juvenile suicides in Russia and other countries. In recent years, individuals have expressed and shared their thoughts freely over the Internet. Yet, due to the characteristics of social media, it appears that harmful usage of social media is occurring. If we can create useful tools for detecting cyberbullying on social media, we can reduce cyberbullying. As a result, in this study, we offer a method for detecting cyberbullying based on social network analysis and data mining. The method will look at three basic strategies for discovering cyberbullying: keyword matching, opinion mining, and social network analysis.

Cyberbullying is a recurrent act of harassing, humiliating, threatening, or bothering someone using electronic devices and online social networking websites. Cyberbullying is more destructive than conventional bullying because it has the capacity to spread shame to an infinite online audience. According to UNICEF and an Indonesian Ministry of Communication and

Information study, 58% of 435 teenagers are unaware about cyberbullying. Some of them may have even been bullies, but since they did not understand cyberbullying, they were unable to see the detrimental consequences of their actions. Bullies may fail to see the consequences of their acts because they may not witness quick reactions from their victims. Our study attempted to discover cyberbullying actors using texts and user credibility analysis and to inform them about the dangers of cyberbullying. We gathered information from Twitter. Because the data was unlabelled, we created a web-based labelling tool to categorise tweets as cyberbullying or non-cyberbullying. The programme provided us with 301 cyberbullying tweets, 399 non-cyberbullying tweets, 2,053 bad terms, and 129 curse words. Following that, we used SVM and KNN to learn about and recognise cyberbullying texts. SVM has the greatest f1-score (67%), according to the data. We also conducted a user credibility study and discovered 257 Normal Users, 45 Harmful Bullying Actors, 53 Bullying Actors, and 6 Potential Bullying Actors.

DISADVANTAGE

- Machine learning algorithms are only as good as the data they are trained on. If the data used to train the algorithm is incomplete, biased, or otherwise flawed, the algorithm may produce inaccurate or unreliable results.
- The require significant computational resources and may not be feasible for smaller organizations or investigations. In addition, there may be technical challenges in collecting and analysing digital evidence, particularly if the evidence has been deleted or encrypted.

IV.PROPOSED SYSTEM

A proposed system for using digital forensics and machine learning to investigate cyberbullying activities. To investigate cyberbullying activities, digital forensics techniques can be applied to gather evidence from electronic devices such as smartphones, computers, and social media accounts. Machine learning algorithms can be used to analyse the collected data and identify patterns and trends in the behaviour of the cyberbully. Collecting data on cyberbullying activities from various sources, such as social media platforms, messaging apps, and email accounts. Cleaning and preparing the data for analysis, which may involve removing irrelevant or duplicate data, standardizing the data format, and converting the data into a machine-readable format. Identifying key features and patterns in the data, such as the frequency and nature of the cyberbullying messages, the identity of the sender, and the social network of the victim. Using the extracted features to train machine learning algorithms to detect cyberbullying activities and to identify potential cyberbullies. Testing the machine learning models on a separate dataset to evaluate their accuracy and performance. Interpreting the results of the analysis and making informed decisions based on the evidence gathered. This may involve identifying the sources of cyberbullying, gathering additional evidence, and taking appropriate actions to stop the cyberbullying. It is important to note that the proposed system would need to be designed with careful consideration of ethical and legal issues, such as privacy, consent, and due process. It is also important to involve human expertise and judgment throughout the investigation process to ensure that the results of the analysis are interpreted and applied in a fair and ethical manner.

ADVANTAGE

- The identify patterns and trends in cyberbullying activities that may not be immediately apparent to human investigators. This can help to identify cyberbullies who may be using multiple accounts or disguising their identities.
- The can be used to identify potential cyberbullying incidents before they occur, which can help to prevent or mitigate the impact of cyberbullying.
- It used to identify potential cyberbullying incidents before they occur, which can help to prevent or mitigate the impact of cyberbullying.

V.ALGORITHM USED

- ➢ Logistic Regression
- ➢ Random Forest
- ➢ ADABOOST
- ➢ Decision Tree

LOGISTIC REGRESSION

Cyberbullying is a growing concern in today's digital age, with a significant number of people being subjected to it. As a result, there is a need for effective methods to investigate and prevent cyberbullying activities. Digital forensics is one such method that involves the analysis of digital devices and data to gather evidence in a legal investigation. Machine learning, on the other hand, is a technique that enables computers to learn from data and improve their performance over time. Logistic regression is one such algorithm that is widely used in machine learning for classification tasks. Combining digital forensics and machine learning techniques can provide a powerful tool for investigating cyberbullying activities. This approach can help in identifying patterns and trends in the data that may not be apparent to human analysts. In this context, logistic regression can be used to classify cyberbullying-related activities based on various features such as the content of the messages, the sender's profile, and the frequency of the messages. By training the model on a large dataset of cyberbullying activities, the algorithm can learn to accurately identify and classify new instances of cyberbullying. The combination of digital forensics and machine learning can be a powerful approach to investigate and prevent cyberbullying activities, which can have severe psychological and emotional consequences for the victims.

RANDOM FOREST

Cyberbullying is a serious problem that has become more prevalent with the rise of digital communication technologies. Digital forensics is one approach that can be used to investigate cyberbullying activities, which involves the analysis of digital devices and data to gather evidence in a legal investigation. Machine learning is another tool that can be used to analyse large amounts of data and identify patterns and trends that may not be apparent to human analysts. One popular machine learning algorithm is the Random Forest algorithm, which is a decision tree-based approach that can be used for both classification and regression tasks. In the context of investigating cyberbullying activities, the Random Forest algorithm can be trained on a large dataset of cyberbullying-related activities, including features such as the content of the messages, the sender's profile, and the frequency of the messages. By training the model on this dataset, the algorithm can learn to accurately classify new instances of cyberbullying. The Random Forest algorithm is that it can handle high-dimensional datasets and can identify important features that contribute to the classification accuracy. This information can be useful for understanding the underlying factors that contribute to cyberbullying activities and can help inform prevention strategies. The Random Forest algorithm, can be a powerful approach to investigate and prevent cyberbullying activities. By identifying patterns and trends in the data, this approach can help law enforcement agencies and other stakeholders to take proactive measures to prevent cyberbullying and protect the well-being of victims.

ADABOOST

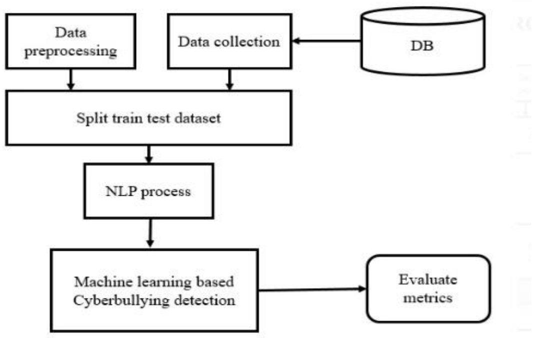
Cyberbullying is a significant problem that has become more prevalent with the widespread use of digital communication technologies. Digital forensics is one approach that can be used to investigate cyberbullying activities, which involves the analysis of digital devices and data to gather evidence in a legal investigation. Machine learning is another tool that can be used to analyse large amounts of data and identify patterns and trends that may not be apparent to human analysts. One popular machine learning algorithm is AdaBoost, which is an ensemble method that combines multiple weak classifiers to create a stronger classifier. In the context of investigating cyberbullying activities, AdaBoost can be trained on a large dataset of cyberbullying-related activities, including features such as the content of the messages, the sender's profile, and the frequency of the messages. By training the model on this dataset, the algorithm can learn to accurately classify new instances of cyberbullying. AdaBoost is that it can improve the classification accuracy by combining multiple weak classifiers. This can be useful for identifying complex patterns and trends in the data that may be difficult to identify with a single classifier. Where the number of positive instances (cyberbullying activities) is much smaller than the number of negative instances (non-cyberbullying activities). This is important because cyberbullying activities are often rare events, making it difficult to collect a large dataset of positive instances.The combining digital forensics and machine learning techniques, such as AdaBoost, can be a powerful approach to investigate and prevent cyberbullying activities. By identifying patterns and trends in the data, this approach can help law enforcement agencies and other stakeholders to take proactive measures to prevent cyberbullying and protect the well-being of victims.

DECISION TREE

Cyberbullying is a growing problem in today's digital age, with a significant number of people being subjected to it. Digital forensics is one approach that can be used to investigate cyberbullying activities, which involves the analysis of digital devices and data to gather evidence in a legal investigation. Machine learning is another approach that can be used to analyse large amounts of data and identify patterns and trends that may not be apparent to human analysts. One popular machine learning algorithm is the Decision Tree algorithm, which is a tree-based approach that can be used for both classification and regression tasks.

In the context of investigating cyberbullying activities, the Decision Tree algorithm can be trained on a large dataset of cyberbullying-related activities, including features such as the content of the messages, the sender's profile, and the frequency of the messages. By training the model on this dataset, the algorithm can learn to accurately classify new instances of cyberbullying. One advantage of using the Decision Tree algorithm is that it can handle both categorical and numerical data, making it useful for analysing a wide range of features that may be relevant to cyberbullying activities. Additionally, decision trees can be visualized, which can help investigators to understand how the algorithm is making its classification decisions. The digital forensics and machine learning techniques, such as the Decision Tree algorithm, can be a powerful approach to investigate and prevent cyberbullying activities. By identifying patterns and trends in the data, this approach can help law enforcement agencies and other stakeholders to take proactive measures to prevent cyberbullying and protect the well-being of victims.

ARCHITECHTURE DIAGRAM



VI.MODULE LIST

- Data collection
- Pre-processing of data
- NLP processing
- Model selection

MODULE DESCRIPTION

DATA COLLECTION

- ➢ Data for our project is gathered from the Kaggle website.
- ➢ The dataset contains 16858 records.

DATA PREPROCESSING

- ➢ The dataset contains only text data which contains some special cases.
- ➢ We need to remove those special case.

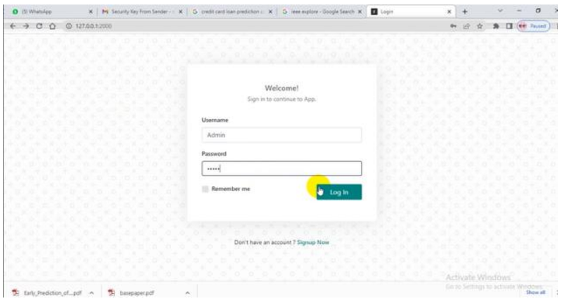
NLP PROCESSING

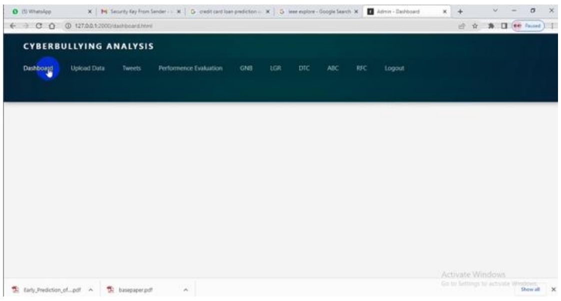
- ➢ Because text data cannot be used to develop a machine learning model, we must convert it to vector format.
- ➢ In this process, the NLP toolkit is used to perform the vectorization operations.

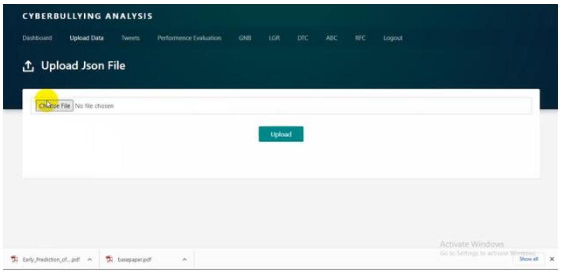
MODEL SELECTION

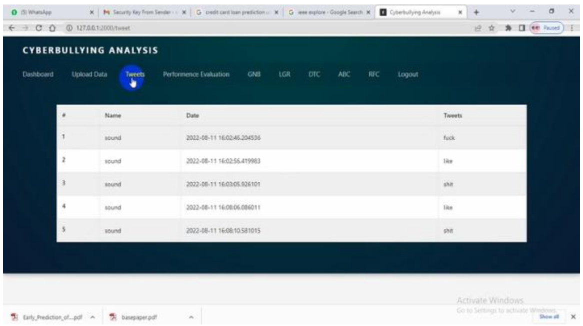
- ➢ ADABoost and Random Forest based model is compared in theapplication in order to build the efficient machine learning models
- ➢ Based on the better performance with cross validation, the model will be selected.

RESULT:

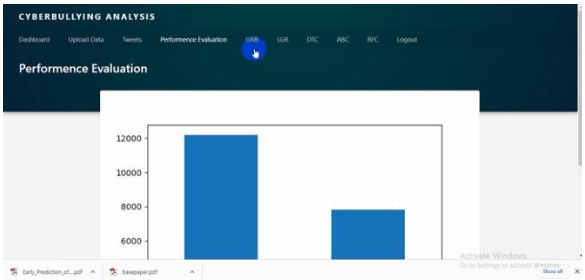

Welcome!
Sign in to continue to App.
Username: Admin
Password: •••••
☐ Remember me
Don't have an account ? Signup Now
(5) WhatsApp
Security Key From Sender
credit card loan prediction
ieee explore - Google Search
Login
127.0.0.1:2000
Paused
Log In
Activate Windows
Go to Settings to activate Windows.
Early_Prediction_of....pdf
basepaper.pdf
Show all

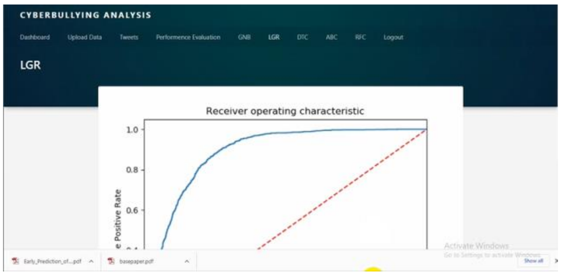



Upload Json File
Choose File No file chosen



#	Name	Date	Tweets
1	sound	2022-08-11 16:02:46.204536	fuck
2	sound	2022-08-11 16:02:56.419983	like
3	sound	2022-08-11 16:03:05.926101	shit
4	sound	2022-08-11 16:08:06.086011	like
5	sound	2022-08-11 16:08:10.581015	shit





VII.CONCLUSION

In conclusion, the use of digital forensics and machine learning techniques can be very effective in investigating cyberbullying activities. By collecting electronic data from devices and social media accounts, digital forensics experts can identify evidence of cyberbullying and extract relevant features for training a machine learning model. Machine learning algorithms can then be used to analyse the data and identify patterns and trends in the cyber bully’s behaviour. This approach can be particularly effective in cases where the cyberbully is using anonymous accounts or trying to hide their identity. The proposed system for investigating cyberbullying activities using digital forensics and machine learning has the potential to greatly improve the ability of law enforcement and school officials to address cyberbullying and protect victims. It is important to continue to develop and refine these techniques to stay ahead of cyberbullies and keep up with the constantly evolving digital landscape.

VIII.REFERENCE

1) John Hani Mounir, Mohamed Nashaat, Mostafa Ahmed, ZeyadEmad, EslamAmer and Ammar Mohammed, "Social Media Cyberbullying Detection using Machine Learning", *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 10, pp. 703-707, 2019.

2) T. K. Chan, C. M. Cheung and Z. W. Lee, "Cyberbullying on social networking sites: A literature review and future research directions", *Information & Management*, vol. 58, no. 2, 2021.

3) C. Van Hee, G. Jacobs, C. Emmery, B. Desmet, E. Lefever, B. Verhoeven, et al., "Automatic detection of cyberbullying in social media text", *PLoS ONE*, vol. 13, no. 10, 2018.

4) H. Ahmad Ghazali, A. Abu Samah, S. Z. Omar, H. Abdullah, A. Ahmad and H. A. Mohamed Shaffril, "Predictors of Cyberbullying among Malaysian Youth", *Journal of Cognitive Sciences and*

Human Development, vol. 6, no. 1, pp. 67-80, 2020.

5) H. Margono, "Analysis of the Indonesian Cyberbullying through Data Mining: The Effective Identification of Cyberbullying through Characteristics of Messages", *Dissertation*, 2019.

6) A &. F. S. M. Muneer, "A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter", *Future Internet*, vol. 12, no. 11, 2020.

7) O. Habimana, Y. Li, R. Li, X. Gu and G. Yu, "Sentiment analysis using deep learning approaches: an overview", *Science China Information Sciences*, vol. 63, no. 1, pp. 1-36, 2020.

8) H. Rosa, N. Pereira, R. Ribeiro, P. C. Ferreira, J. P. Carvalho, S. Oliveira, et al., "Automatic cyberbullying detection: A systematic review", *Computers in Human Behavior*, vol. 93, pp. 333-345, 2019.

9) V. Ashok, "Nexus of advanced technology platforms for strengthening cyber-defense capabilities" in Practical applications of advanced technologies for enhancing security and defense capabilities: Perspectives and Challenges for the Western Balkans, IOS Press, pp. 14-31, 2022.

10) A. Agarwal, "Information technology vis-a-vis human rights: an analytical and legal approach", *Int'l JL Mgmt. & Human*, vol. 5, no. 2, 2022.