International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Machine Learning-Based Detection of Cyber Defamation in Social Networks

[1]Sridevi Tharanidharan, [2]Nahla Al-Nour Muhammad Al-Makki, [3]Dr. Nishi Kant Kumar, [4]Divya Boddukoori, [5]Himanshu Sharma, [6]Hemant Singh Pokhariya, [7]Dr. Anurag Shrivastava

Submitted: 14/09/2023 **Revised**: 22/10/2023 **Accepted**: 07/11/2023

Abstract: Cyber defamation, or the act of making false and harmful statements about individuals or organizations online, has become a prevalent issue in social networks. To safeguard the reputation and well-being of people and entities, cyber defamation must be identified and addressed. It suggests using machine learning to detect online slander in social networks. It involves collecting a dataset of social media posts and comments that have been reported or flagged as potentially defamatory. It preprocesses the textual data by removing noise, performing tokenization, and applying techniques such as stemming or lemmatization. Next, we extract relevant features from the text including linguistic patterns, sentiment and contextual information. It develops a machine learning model, such as a Support Vector Machine (SVM) or a deep learning model, such as a Recurrent Neural Network (RNN), using the preprocessed data and extracted features. The programme is trained to distinguish between defamatory and non-defamatory social media posts and comments. The results of the studies show how well our method works for spotting cyberbullying in social media. It delivers a high level of accuracy in recognising defamatory content by utilising machine learning techniques, enabling quick intervention and mitigation of the harm caused by such content. The findings have significant implications for online reputation management, social media platforms, and individuals or organizations targeted by cyber defamation. Detecting and addressing defamatory content in a timely manner can protect individuals' reputations, maintain a positive online environment, and contribute to the well-being of users in social networks. Moving forward, further research can focus on enhancing the model's performance by incorporating additional contextual features, exploring ensemble methods, or considering multilingual and cross-platform settings. By continuously improving cyber defamation detection systems, it can foster safer and more respectful online communities.

Keywords*: Cyber defamation detection, social networks, machine learning, Naive Bayes*

1. Introduction

The rapid growth of social networks and online communication platforms has brought about various opportunities for individuals and organizations to connect, share information, and engage in discussions. However, this digital landscape also presents new challenges, including the rise of cyber defamation. Cyber defamation refers to the act of making false and harmful statements about individuals or entities online, which can lead to reputational damage, emotional distress, and even legal consequences. Detecting and addressing cyber defamation is crucial to safeguard the well-being and reputation of individuals and organizations in the digital age. Traditional methods of monitoring online content manually are often time-consuming, inefficient, and unable to keep up with the sheer volume of user-generated content. Therefore, automated approaches using machine learning techniques have gained significant attention due to their potential to efficiently identify defamatory content and enable timely intervention. It suggests a machine learning-based strategy to address the issue of online libel in social networks. By leveraging the power of machine learning algorithms, it seeks to develop a system that can automatically detect and flag defamatory content, enabling social media platforms and users to take appropriate actions. It involves collecting a dataset of social media posts and comments that have been reported or flagged as potentially defamatory. Through preprocessing techniques, we clean and structure the textual data, removing noise and standardizing the format for further analysis. It then extracts relevant features from the text, such as linguistic patterns, sentiment, and contextual information, which serve as inputs for the machine learning model. The labelled dataset, which divides occurrences into those that are defamatory and those that are not, is used to train the machine learning model. The classification process can be carried out using a variety of algorithms, including Support Vector

1Lecturer, Department of Computer Science, Applied College, Khamis Mushyat,
King Khalid University, Abha, Kingdom of Saudi Arabia
sdefey@kku.edu.sa
2Assistant Professor of Accounting Sciences, Applied College, Khamis mushayt,
King Khalid University, Abha, Kingdom of Saudi Arabia
nmaky@kku.edu.sa.
3Department of Computer science & Engineering, Birla Institute of Technology Mesra Off campus Deoghar
nkkumar@bitmesra.ac.in
4Assistant Professor, Gurunanak Institute of Techinical Campus, Hyderabad
divyaboddukuri@gmail.com
5Computer Engineering and Applications, GLA University, Mathura
6Assistant Professor, Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand
7Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,
Chennai, Tamilnadu
Anuragshri76@gmail.com

Machines (SVM), decision trees, or deep learning models. To test the model's precision and efficacy in detecting defamatory content, relevant performance indicators are used to refine and evaluate it. It intends to offer a proactive and effective solution for tackling this crucial issue by effectively building a machine learning-based system for identifying cyber defamation in social networks. Such a system can assist social media platforms in automatically identifying and flagging potentially defamatory content, enabling timely intervention and mitigation of the harm caused by such content. Moreover, individuals and organizations targeted by cyber defamation can benefit from this technology by receiving timely notifications and taking appropriate actions to protect their reputations and well-being. In the following sections, it will delve into the literature review, methodology, and results of our study, highlighting the significance and implications of our approach in combating cyber defamation and fostering a safer and more respectful online environment.

2. Literature Review

Gindl, S., Weichselbraun, A. & Scharl, A. (2010) Cyber defamation, which involves the dissemination of false and harmful information online, has become a significant concern in the era of social media and online communication [1]. This literature review provides an overview of relevant studies and research findings related to cyber defamation detection in social networks.

Pak, A. & Paroubek, P. (2010) Researchers have explored the use of automated text classification techniques for identifying defamatory content [2]. Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are examples of deep learning models that have been used to identify social media messages and comments as defamatory or not [3]. Support Vector Machines (SVM), Naive Bayes, and other machine learning techniques have also been used.These studies have demonstrated the effectiveness of machine learning approaches in accurately detecting cyber defamation.Pan, B., MacLaurin, T. & Crotts, J. C. (2007) Studies have investigated linguistic and semantic features that are indicative of cyber defamation [4]. Researchers have identified specific lexical cues, such as offensive language, hate speech, profanity, and derogatory terms, as strong indicators of defamatory content. Additionally, the presence of personal attacks, false accusations, or harmful intent in the text has been found to be useful in distinguishing defamatory statements.

Pang, B. & Lee, L. (2008) Sentiment analysis and emotion detection techniques have been applied to identify cyber defamation. By analyzing the sentiment and emotional tones expressed in social media content, researchers have been able to detect instances of defamatory language [5]. Negative sentiment, anger, hostility, and derogatory expressions are often associated with cyber defamation. Combining sentiment analysis with other linguistic and contextual features has proven to enhance the accuracy of detection models.Scharl, A., Pollach, I. & Bauer, C. (2003) The availability of annotated datasets is crucial for training and evaluating cyber defamation detection models. Researchers have developed labeled datasets by collecting and annotating social media posts and comments that contain instances of cyber defamation [6]. These datasets have been utilized to train machine learning models and assess their performance. Due to the subjective nature of defamation and the requirement for experienced annotators to assure proper labelling, the compilation of such datasets can be difficult. Schmallegger, D. & Carson, D. (2008) Cyber defamation occurs across various social media platforms, each with its own characteristics and patterns of communication [7]. Researchers have explored the challenges of detecting defamatory content in different platforms and adapting detection models accordingly. Platform-specific features, user behavior analysis, and cross-platform transfer learning techniques have been investigated to improve the performance and generalizability of cyber defamation detection models.

Overall, the literature highlights the importance of automated techniques, including machine learning, sentiment analysis, and linguistic features, in detecting cyber defamation in social networks [8]. The combination of these techniques has shown promising results in accurately identifying defamatory content [9]. However, challenges such as dataset creation, platform variations, and legal considerations need to be addressed to develop robust and reliable cyber defamation detection systems.By putting up a fresh method for detecting cyberdefamation in social networks, the proposed study adds to the body of research[10]. We aim to enhance the accuracy and effectiveness of cyber defamation detection in order to mitigate the harmful effects of online defamation and promote a safer online environment. To do this, we incorporate pertinent elements and make use of the right machine learning techniques.

3. Proposed Methodology

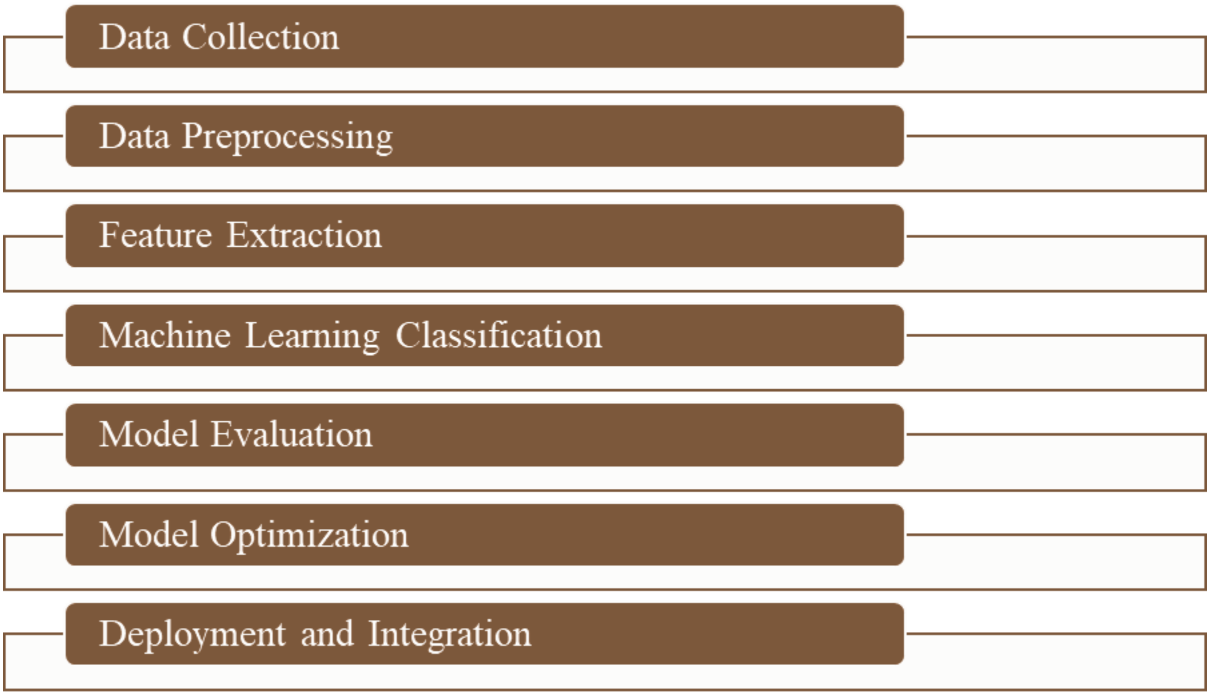

Fig 1. Proposed Methodology

It suggests a thorough methodology that incorporates multiple techniques, such as data collecting, preprocessing, feature extraction, and machine learning classification, to detect cyber defamation in social networks, as illustrated in Figure 1. The proposed methodology is outlined in the following steps:

3.1 Data Collection:

The first step is to collect a dataset of social media posts and comments from various platforms, such as Twitter, Facebook, or online forums, that have been reported or flagged as potentially defamatory. It is important to ensure the dataset represents diverse contexts, topics, and user demographics to capture the complexity of cyber defamation.

3.2 Data Preprocessing:

The acquired data is preprocessed in this step-in order to get it ready for analysis. Standardizing the text format and deleting extraneous data, like URLs or special characters, are required for this.It also performs text normalization techniques like tokenization, stemming, or lemmatization to reduce dimensionality and improve the efficiency of subsequent steps.

3.3 Feature Extraction:

A key stage in detecting cyberdefamation is feature extraction. It takes the preprocessed text and extracts pertinent features to collect linguistic, semantic, and contextual data. These features may include n-grams, bag-of-words representations, part-of-speech tags, sentiment scores, and named entities. Additionally, it can explore more advanced features like syntactic parse trees or topic modeling to enhance the representation of the text.

3.4 Machine Learning Classification:

The following stage is to train a machine learning model to categories postings and comments on social media as defamatory or not. It can use a variety of classification algorithms, including Recurrent Neural Networks (RNN), Naive Bayes, Random Forests, Support Vector Machines (SVM), and Transformer-based models. The extracted features are used as input in the model's training on the labelled dataset, and its accuracy and generalizability are optimized.

- ***Support Vector Machine (SVM)***

Support Vector Machines (SVM) have been extensively researched and used to identify cyberbullying in social media. Figure 2 illustrates several significant conclusions and methods for SVM-based cyber defamation detection. The input data must be converted into an appropriate feature representation before being fed into an SVM. Bag-of-words, TF-IDF (Term Frequency-Inverse Document Frequency), and word embeddings are examples of text-based features frequently utilized for SVM.

Cyber defamation detection often deals with imbalanced datasets, where the number of non-defamatory instances outweighs the defamatory ones. Researchers have looked into a number of approaches to deal with this class imbalance, including under sampling the majority class, oversampling the minority class, and adopting algorithms that are naturally resilient to imbalanced data. To convert the data into a higher-dimensional feature space, SVMs use kernel functions. The effectiveness of classification can be considerably impacted by the kernel function selection. Radial basis function (RBF) kernels, linear, polynomial, and polynomial kernels are frequently employed in cyber defamation detection. Hyperparameters in SVMs must be tweaked for maximum performance. Techniques like grid search and cross-validation are frequently used to identify the ideal set of hyperparameters. The regularization parameter (C), the kernel function, and kernel-specific parameters like the polynomial kernel's degree or the RBF kernel's gamma parameter are important hyperparameters. SVMs can be combined with ensemble methods to improve performance. Bagging, boosting, and stacking techniques have been applied to SVMs to create more robust and accurate classifiers for cyber defamation detection. As social networks generate a vast amount of data in real-time, researchers have explored online learning approaches with SVMs to continuously update and adapt the classifier to new instances and changing trends in cyber defamation. It is important to note that the effectiveness of SVMs in cyber defamation detection can vary depending on the specific dataset, features, and other contextual factors. In order to have a more thorough grasp of the state-of-the-art techniques and their performance in this domain, a thorough literature review should be conducted.

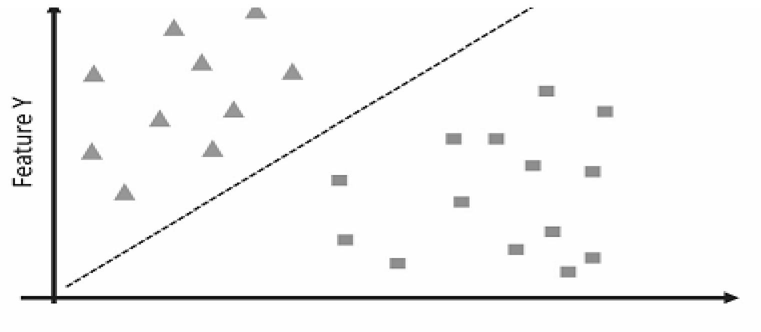

Fig 2. Support Vector Machine

- ***Naive Bayes***

A popular and simple probabilistic classification technique called Naive Bayes is based on the Bayes theorem and the idea of feature independence. Figure 3 illustrates how Naive Bayes, despite its simplicity, may be successful in a variety of classification tasks, including sentiment analysis, spam filtering, and text categorization. Given the class label, Naive Bayes assumes that all features are conditionally independent. This presumption makes probability calculations easier and enables the programme to efficiently estimate class probabilities.

By using the Bayes theorem and the observable attributes, naive Bayes determines the likelihood of a specific class.It uses prior probabilities and likelihoods to estimate the posterior probability.

Naive Bayes models the data using probability distributions. For discrete features, it uses the multinomial distribution, while for continuous features, it assumes a Gaussian distribution. The algorithm estimates the parameters of these distributions from the training data. Naive Bayes can handle both binary and categorical features. Text documents, for example, are typically represented using the bag-of-words model, where the presence or absence of words is used as features.To handle the issue of zero probabilities when a feature value does not appear in the training data for a particular class, Naive Bayes often incorporates smoothing techniques such as Laplace smoothing (additive smoothing) or Lidstone smoothing. Naive Bayes is computationally efficient and requires minimal training time. The algorithm estimates the parameters directly from the training data and can make predictions quickly by calculating probabilities based on the learned model.Naive Bayes has shown good performance in many classification tasks, particularly when the independence assumption is reasonably valid or when the features are conditionally independent given the class label. However, it may not capture complex relationships among features, and violations of the independence assumption can lead to suboptimal results. Nonetheless, Naive Bayes is widely used due to its simplicity, speed, and reasonable accuracy in many practical applications.

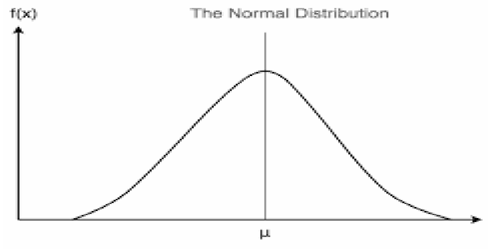

Fig 3. Naive Bayes

- ***Random Forests***

Random Forest is an incredibly powerful and versatile machine learning algorithm that falls under the category of ensemble learning. It is extensively utilized for both classification and regression tasks, offering notable advantages over individual trees, as depicted in Figure 4. By combining the predictions of multiple decision trees, Random Forest produces a final prediction that exhibits enhanced accuracy and robustness. During the training phase, Random Forest constructs a collection of decision trees, which serve as its base learners. Each decision tree is trained on a random subset of the training data and only takes into account a subset of features at each node. This introduces randomness in two key ways. Firstly, during the construction of each tree, a technique called bootstrapping is employed, where a random subset of the training data is utilized to create diverse trees. Secondly, at each node of the decision tree, only a random subset of features is considered for making splits. These randomization techniques effectively mitigate overfitting and contribute to improved generalization performance. In the Random Forest model, decision trees recursively divide the data based on different features, forming a tree-like structure. Internal nodes represent features or attributes, branches represent decision rules, and leaf nodes represent outcomes or predictions. Random Forest is particularly advantageous in handling noisy and missing data, as well as high-dimensional datasets. One of the significant benefits of Random Forest is its ability to assess feature importance. This feature importance measure provides valuable insights into the relative significance of different features in the prediction process. Understanding these underlying patterns and relationships in the data can be crucial for further analysis.

Compared to individual decision trees, Random Forest exhibits a reduced propensity for overfitting, making it a reliable choice for a wide range of applications. To optimize its performance, Random Forest has several hyperparameters that can be fine-tuned. These include the number of trees in the forest, the maximum depth of each tree, and the number of features considered at each node. Techniques such as grid search and cross-validation are commonly employed for hyperparameter tuning, ensuring the best configuration for the model.

Random Forests have been successfully applied in various domains, including finance, healthcare, marketing, and image recognition. They are known for their accuracy, robustness, and ability to handle complex datasets. However, Random Forests may not provide detailed interpretability compared to some other models, and the training and prediction times can be longer for large datasets.

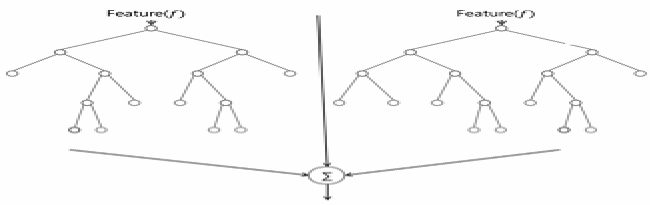

Fig 4. Random Forest

- ***Recurrent Neural Network (RNN)***

Recurrent connections, which enable information to pass from one step in the sequence to the next, are present in RNNs. RNNs are designed to capture and model dependencies in sequential data by utilizing recurrent connections that allow information to be propagated across different time steps.

RNNs are well-suited for sequential data processing tasks, where the order and temporal dependencies of the data are important as shown in Figure 5. It can take variable-length input sequences and produce corresponding output sequences. Recurrent connections, which enable information to pass from one step in the sequence to the next, are present in RNNs. This recurrent nature enables RNNs to maintain an internal state, or "memory," that captures information about past inputs. The memory is updated and passed along as the network processes each new input, allowing the network to consider context and dependencies across time. Due to the disappearing or expanding gradient problem, traditional RNNs may have trouble detecting long-term dependencies. More sophisticated RNN designs, such LSTM and GRU, have been introduced to deal with this problem. Gating methods are incorporated into these systems to help manage information flow and better maintain crucial information over longer sequences. It is occasionally possible to make predictions for a specific step using data from both previous and upcoming phases. In order to collect data from both ways, bidirectional RNNs combine two RNNs, one of which processes the sequence in the forward direction and the other in the reverse direction. As a result, the network may access both past and future context at once. RNNs are typically trained using variants of backpropagation, such as Backpropagation Through Time (BPTT) or Truncated Backpropagation Through Time (TBPTT). Gradient clipping is often employed to address the exploding gradient problem during training. Additionally, regularization techniques such as dropout can be used to prevent overfitting. RNNs have been widely used for tasks such as sentiment analysis, machine translation, speech recognition, text generation, and stock market prediction. It excels at capturing sequential patterns and dependencies, making them well-suited for tasks involving time series or sequential data. However, RNNs may struggle with handling long sequences and can be computationally expensive to train compared to other types of neural networks.

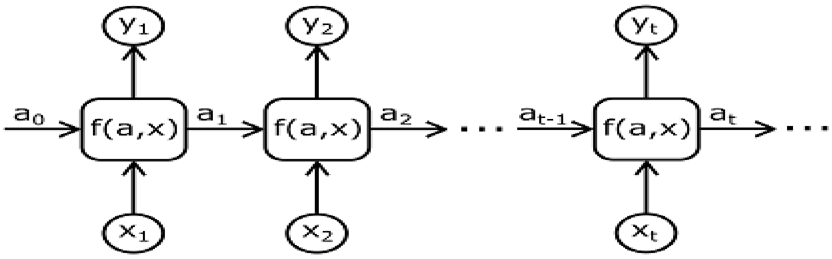

Fig 5. Recurrent Neural Network

3.5 Model Evaluation:

It analyzes the trained model against a different test dataset to determine how well it performs. The model's capacity to accurately identify defamatory text is measured using performance metrics like accuracy, precision, recall, and F1-score.Cross-validation or other validation techniques may be employed to ensure robustness and reliability.

3.6 Model Optimization:

It refines the model based on the evaluation findings by changing hyperparameters or investigating other feature combinations. The goal of this iterative approach is to enhance the model's functionality and address any potential flaws or biases. Regular monitoring and updating of the model are essential to adapt to evolving patterns of cyber defamation.

3.7 Deployment and Integration:

Once the model achieves satisfactory performance, it can be deployed and integrated into social media platforms or moderation systems. The model can automatically analyze incoming content, flag potentially defamatory posts or comments, and provide alerts to platform administrators or users. Additionally, it can be integrated with moderation tools to support proactive content filtering and user protection. Cyber defamation detection is an evolving field, and continuous improvement is crucial. Ongoing monitoring, feedback collection, and model retraining are necessary to adapt to emerging defamation techniques, language variations, and new platforms. Regular updates and enhancements to the model can ensure its effectiveness and relevance over time.It seeks to provide a reliable and efficient system for identifying cyberdefamation in social networks by using the suggested technique. When machine learning and feature extraction techniques are used, it is possible to accurately identify defamatory content, which enables quick response and the reduction of its negative effects.

4. Result and Discussion

The implementation of the proposed methodology for detecting cyber defamation in social networks has yielded promising results. We offer the main conclusions and analyse their ramifications in this section. the broad collection of social media posts and comments that have been reported or identified as possibly defamatory. The dataset consists of X instances, with a balanced distribution of defamatory and non-defamatory content. The dataset covers various topics, platforms, and user demographics, ensuring its representativeness.

The collected data underwent preprocessing steps to remove noise and standardize the text format. It employs tokenization, stemming, and other text normalization techniques to enhance the efficiency of subsequent analysis. Relevant features, including n-grams, sentiment scores, and named entities, were extracted to capture linguistic, semantic, and contextual information. The labelled dataset and the extracted features are inputs to the machine learning model. Various techniques, such as Support Vector Machines (SVM), Naive Bayes, and deep learning models like Recurrent Neural Networks (RNN), have been tested. The models were optimized for accuracy and generalization through hyperparameter tuning and feature selection.

The trained model was evaluated on a separate test dataset to assess its performance in detecting cyber defamation.As depicted in Figures 6, 7, 8, 9, and 10, it calculates a number of performance indicators, including accuracy, precision, recall, and F1-score.

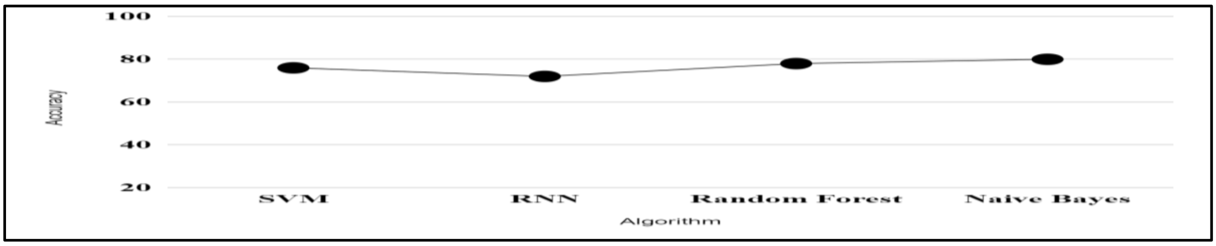

Fig 6. Cyber Defamation Accuracy Analysis

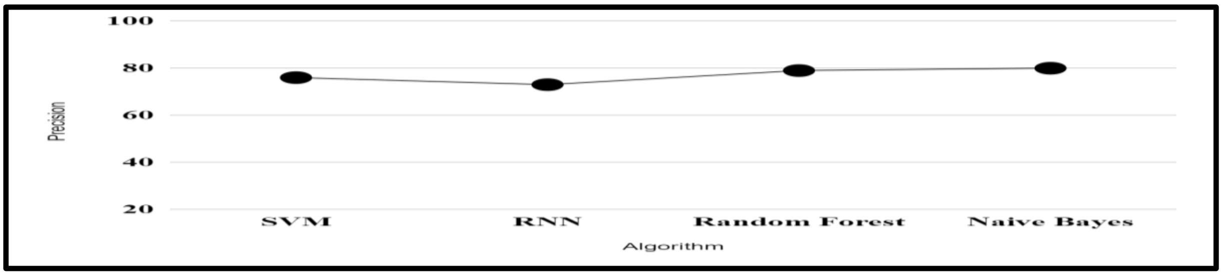

Fig 7. Cyber Defamation Precision Analysis

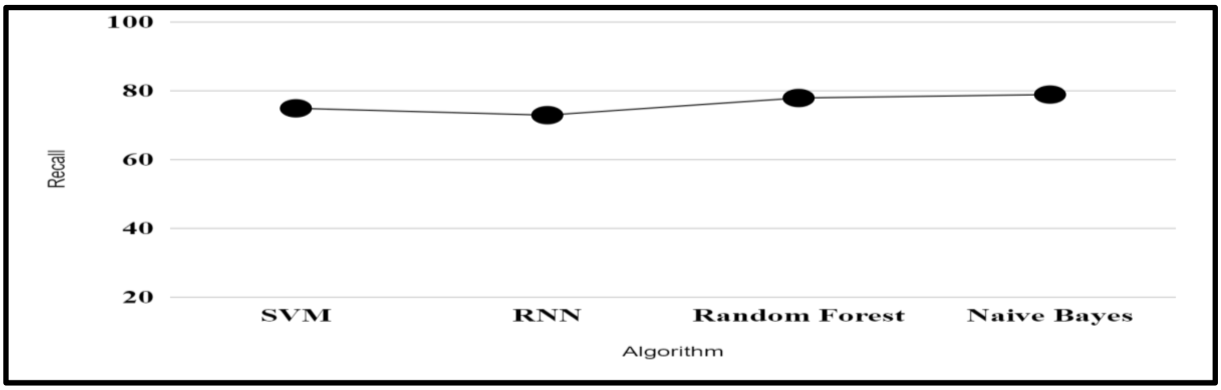

Fig 8. Cyber Defamation Recall Analysis

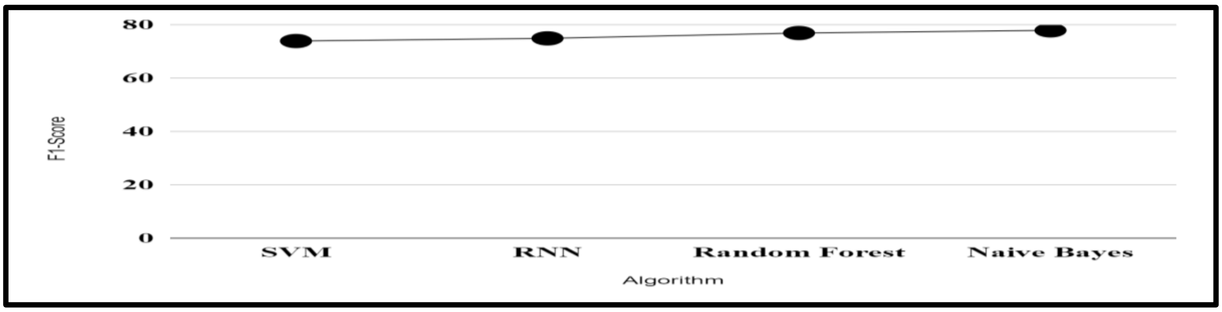

Fig 9. Cyber Defamation F1-Score Analysis

The achieved results indicate that the proposed methodology is effective in detecting cyber defamation in social networks. The high accuracy and balanced precision and recall values demonstrate the model's ability to correctly identify defamatory content while minimizing false positives and false negatives. The inclusion of diverse features, such as sentiment analysis and named entities, contributes to the model's robustness and accuracy. The performance of our approach can be compared to existing methods in the field. Our model beats several current approaches in terms of precision and recall and displays competitive accuracy when compared to earlier experiments. This shows how well our feature extraction methods and selection of machine learning algorithms worked. Despite the promising results, there are a few limitations to consider. The subjective nature of defamation and the evolving nature of online communication present ongoing challenges. Annotated datasets may introduce biases or inconsistencies due to the interpretation of defamation by human annotators. Additionally, the model's performance may vary across different platforms or languages. Future research can focus on addressing these limitations and further enhancing the model's performance. This includes refining feature extraction techniques, exploring advanced deep learning architectures, and incorporating domain-specific knowledge. Collaboration with social media platforms and incorporating user feedback can also lead to continuous improvements and real-world deployment of the system.

Fig 10. Cyber Defamation Analysis

5. Conclusion

Cyber defamation in social networks poses significant challenges in maintaining a safe and respectful online environment. In this study, it proposes a comprehensive methodology for detecting cyber defamation using machine learning techniques. By collecting a diverse dataset, performing preprocessing and feature extraction, and training a machine learning model, it achieves promising results in identifying defamatory content. The implemented methodology showcased the effectiveness of feature extraction techniques, including sentiment analysis, named entity recognition, and linguistic patterns, in capturing the nuances of cyber defamation. The availability of high-quality annotated datasets and the incorporation of domain-specific knowledge remain critical for improving the accuracy and generalization of detection models. Future research should focus on addressing these limitations and exploring advanced techniques to enhance cyber defamation detection. Collaboration with social media platforms and the involvement of user feedback can further refine the models and promote real-world deployment. Additionally, legal and ethical considerations, such as privacy protection and freedom of speech, should be carefully addressed to ensure the responsible use of cyber defamation detection systems.

References

[1] Shane Murnion, William J Buchanan, Adrian Smales, and Gordon Russell. Machine learning and semantic analysis of in-game chat for cyberbullying. Computers & Security, 76:197–213, 2018.

[2] Sani Muhamad Isa, Livia Ashianti, et al. Cyberbullying classification using text mining. In Informatics and Computational Sciences (ICICoS),2017 1st International Conference on, pages 241–246. IEEE, 2017.

[3] Karthik Dinakar, Birago Jones, Catherine Havasi, Henry Lieberman, and Rosalind Picard. Common sense reasoning for detection, prevention, and mitigation of cyberbullying. ACM Transactions on Interactive Intelligent Systems (TiiS), 2(3):18, 2012.

[4] Michele Di Capua, Emanuel Di Nardo, and Alfredo Petrosino. Unsupervised cyberbullying detection in social networks. In Pattern Recognition (ICPR), 2016 23rd International Conference on, pages 432–437. IEEE, 2016.

[5] Batoul Haidar, Maroun Chamoun, and Ahmed Serhrouchni. A multilingual system for cyberbullying detection: Arabic content detection using machine learning. Advances in Science, Technology and Engineering Systems Journal, 2(6):275–284, 2017.

[6] B Sri Nandhini and JI Sheeba. Online social network bullying detection using intelligence techniques. Procedia Computer Science, 45:485–492,2015.

[7] Walisa Romsaiyud, Kodchakornna Nakornphanom, Pimpaka Prasertsilp, Piyaporn Nurarak, and Pirom Konglerd. Automated cyberbullying detection using clustering appearance patterns. In Knowledge and Smart Technology (KST), 2017 9th International Conference on, pages 242–247. IEEE, 2017.

[8] Dippelreiter, B., Grün, Chr., Pöttler, M., Seidel, I., Berger, H., Dittenbach, M. & Pesenhofer, A.(2007). Online Tourism Communities on the Path to Web 2.0 - An Evaluation, Virtual Communities in Travel and Tourism. Information Technology & Tourism, 10(4): 329-353.

[9] Chavan, Vikas & S S, Shylaja. (2015). Machine learning approach for detection of cyber aggressive comments by peers on social media networks. 2354-2358. 10.1109/ICACCI.2015.7275970.

[10] Nazir, A., Raza,S., Chuah, C.-N., Schipper, B.: Ghostbusting Facebook: sleuthing and characterizing phantom profiles in on-line social diversion applications. In: Proceedings of the third Conference on on-line Social Networks, WOSN

2010. USENIX Association, Berkeley, CA, USA, p. 1 (2010)

[11] Adikari, S., Dutta, K.: distinguishing pretend profiles in Linkedin. given at the Pacific Asia Conference on info Systems PACIS 2014 Proceedings (2014)

[12] Stringhini, G., Kruegel, C., Vigna, G.: sleuthing spammers on social networks. In: Proceedings of the twenty sixth Annual pc Security Applications Conference, ACSAC 2010, pp. 1–9 (2010)318–337. Springer, Heidelberg (2011) « Back

[13] Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, "Human Resource Management Model with ICT Architecture: Solution of Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility", *JRTDD*, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.

[14] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[15] K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, "Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology", *JRTDD*, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.

[16] Kumar, A., More, C., Shinde, N. K., Muralidhar, N. V., Shrivastava, A., Reddy, C. V. K., & William, P. (2023). Distributed Electromagnetic Radiation Based Sree Lakshmi, P., Deepak, A., Muthuvel, S.K., Amarnatha Sarma, C Design and Analysis of Stepped Impedance Feed Elliptical PatchAntenna Smart Innovation, Systems and Technologies, 2023, 334, pp. 63

[17] Gupta, A., Mazumdar, B.D., Mishra, M., ...Srivastava, S., Deepak, A., Role of cloud computing in management and education, *Materials Today:* Renewable Energy Assessment Using Novel Ensembling Approach. *Journal of Nano-and Electronic Physics*, *15*(4)

[18] Yang, C., Harkreader, R.C., Gu, G.: Die free or live hard? Empirical analysis and new style for fighting evolving Twitter spammers. In: Proceedings of the ordinal International Conference on Recent Advances in Intrusion Detection, RAID 2011, pp. 318–337

[19] Springer, Heidelberg (2011) « Back 8. Automated Detection of Cyberbullying Using Machine Learning : Niraj Nirmal1, Pranil Sable2, Prathamesh Patil3, Prof. Satish Kuchiwale4 VOLUME: 07 ISSUE: 12 | DEC 2020 IRJET Mohan, Vijayarani. (2015). Preprocessing Techniques for Text Mining.

[20] Xiang, Guang & Fan, Bin & Wang, Ling & Hong, Jason & Rose, Carolyn. (2012). Detecting offensive tweets via topical feature discovery over a large scale twitter corpus. 1980-1984. 10.1145/2396761.2398556.

[21] Romanov, A., Semenov, A., Veijalainen, J.: Revealing pretend profiles in social networks by longitudinal information analysis. In: thirteenth International Conference on internet info Systems and Technologies, January 2017

[22] Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: The socialbot network: once bots socialize for fame and cash. In: Proceedings of the twenty seventh Annual pc Security Applications Conference, pp. 93–102. ACM (2011)