A Systematic Review of Machine Learning Algorithms in Cyberbullying Detection: Future Directions and Challenges

Muhammad Arif*
Department of Computer Science, College of Computers and Information Systems, Umm Al-Qura University, Mecca, Saudi Arabia.

Received 07. Apr. 2021 ; Accepted 20. May. 2021 ; Available Online 01. Jun. 2021

Abstract
Social media networks are becoming an essential part of life for most of the world's population. Detecting cyberbullying using machine learning and natural language processing algorithms is getting the attention of researchers. There is a growing need for automatic detection and mitigation of cyberbullying events on social media. In this study, research directions and the theoretical foundation in this area are investigated. A systematic review of the current state-of-the-art research in this area is conducted. A framework considering all possible actors in the cyberbullying event must be designed, including various aspects of cyberbullying and its effect on the participating actors. Furthermore, future directions and challenges are also discussed.

I. INTRODUCTION
Bullying refers to aggressive behavior, which can be physical, verbal, or social [1]. Bullying is distinguished by three criteria, aggressive motive, repetition, and imbalance of power. It hurts individuals physically, mentally, or emotionally [2]. A bullying culture can develop in any environment where humans interact with each other. It may happen in the family, school, or workplace. Sometimes it is also referred to as peer abuse. If bullying behaviors prevail in society, it may affect the mental health of the underprivileged portion of the community in many ways. People who face bullying in their childhood or at the adolescent age are at higher risk of suffering from anxiety, depression, and low esteem than those who are not bullied [3]. Children or youth bullying others may also face psychological problems in their later years [4]. Even bystanders to bullying also develop mental stress and fear [5].

With the advancement of technology, the use of social media is growing every day. We are living in the internet-enabled world in which reaching other people is just a click away. People can openly share on social media, websites, and community forums. Although digital media offers various resources, many people misuse it in the name of freedom of speech or hatred towards a particular race, social group, or individual. Cyberbullying is a bullying action performed through digital means to embarrass, threaten, or socially exclude others [6]. In cyberbullying, elements of repetition, power differential, and motive are considered essential fac-

Keywords: Cybercrime, Information Security, Cyberbullying, Social media, machine learning, natural language processing.

* Corresponding Author: Muhammad Arif
Email: mahamid@uqu.edu.sa
doi: 10.26735/GBTv9013

1658-7782© 2021, JISCR. This is an open access article, distributed under the terms of the Creative Commons, Attribution-NonCommercial License.
Cyberbullying victims report a higher level of depression and anxiety, suicidal trends and attempts, academic performance, work performance, and poorer physical and mental health. The harmful effects of cyberbullying are more severe than traditional bullying because of the broader audience on the internet and the faster spread of messages. The harmful effects of cyberbullying are more stringent than conventional bullying because of a wider audience on the internet. Tommy et al. described triadic reciprocal relationships between perpetrators, victims, and bystanders. This framework consolidated personal factors, environmental events, and behavioral patterns that influence each other in a triadic manner.

Early detection of different social anomalies, including cyberbullying, hate speech, trolling, fake news, rumors, counterfeit profile detection, misogyny, etc., is becoming a trend in recent social media-based research. Abusive text can be detected in the messaging/comments on social media by maintaining a list of offensive words. However, words and phrases can be obfuscated by the users. The human readers can easily understand these confused words but extremely difficult for an automated system. One solution to this problem is by updating the word list continuously. A survey on hate speech detection using natural language processing can be found in [21]. Cyberbullying can take different forms, including flaming (online fights), harassment, denigration, impersonation, outing (sharing secrets of someone to others), trickery, exclusion, and cyberstalking [22]. A good list of 118 causes of cyberbullying and methods are given in [23]. The role of a person’s personality is also important to predict whether he/she may engage in the activity of cyberbullying [24]. Personality traits related to the dark triad (psychopathy, Machiavellianism, and narcissism) may influence a person’s cyberbullying behavior.

A systematic review is conducted to identify and compare different machine learning methods used to detect cyberbullying. This methodological review is undertaken to answer the following questions:

**RQ1:** What are the existing machine learning methods applied to detect cyberbullying in social media?

**RQ2:** What are the possible applications of cyberbullying detection tools?

**RQ3:** What are the challenges and future perspectives of the cyberbullying detection frameworks?

The systematic review consisted of three steps. In the first step, three major research databases, IEEE explore, ScienceDirect, and Springer was searched through queries and collected as many papers as possible. The search queries are "cyberbullying detection machine learning," "cyberbullying detection," and "Cyberbullying natural language processing." Based on initial exclusion criteria, papers were selected after carefully reading the abstract of the papers in the second step. A final list of papers is prepared after reading the full articles and applying further exclusion criteria.

Exclusion criteria in the first and second steps include:

**EC1.** Studies must be peer-reviewed articles published in the English and Arabic languages.

**EC2.** Books, notes, theses, letters, and patents are not included in this review.

**EC3.** Only papers focusing on applying machine learning methods to the problem of cyberbullying are considered.

Three further exclusion criteria are used in the final step as follows:

**EC4.** A unique contribution is considered for inclusion, and repeated studies are not included.

**EC5.** Those articles which do not describe the methodology and result sufficiently are excluded.

**EC6.** Those articles that do not address the research questions mentioned above are not included. Cyberbullying research on languages other than English and Arabic is excluded.

Fig. 1 depicts the literature review process. Query searches on the three databases produced a total of 1032 articles. Article search is not limited to any specific period. In these articles, some of the articles are repeated. After carefully reading the papers’ title and abstract, 803 articles are excluded based on the exclusion criteria EC1, EC2, and EC3.
algorithms are required to extract and select useful features from the data. Once important features are collected from the data, a classifier must be trained on this feature set to predict the correct events.

Performance analysis can be based on different performance metrics in machine learning and may include classification accuracy, precision, recall, or F-Score. Classifier structure can be fine-tuned to achieve an optimal performance of the cyberbullying detection and monitoring framework. In the following sub-sections, the use of different feature extraction and classification methods in cyberbullying detection literature is described in detail.

### A. Feature Extraction

Features for cyberbullying detection can be broadly classified into Content features, Network features, Activity features, User profile features, and sentiment features. Table I summarizes a list of features used in cyberbullying detection in the literature. Word embedding features are the most common features used for cyberbullying detection in the literature.

Further details about different types of features used in cyberbullying research can be found in the following subsections.

#### 1) Content features

Content features may include textual features, emoji-based features, and features extracted from audio, images, or video contents. Many valuable features can be extracted from the text posted by the user based on natural language processing. Some features may depend on the word dictionary, and some features also consider the context of a sentence. Based on the vulgar/profane words dictionary, the vulgarity feature can be calculated by the number of offensive words present in the user’s post.

**N-gram features:** N-gram is the probabilistic model of a sequence of n adjacent items (words, phonemes, syllables, letters, etc.). In the linguistic sense, n-grams are collected from text or speech corpus. In n-gram, n refers to the number of items or words in the text. N-gram features have numerous applications in natural language processing and other areas [51-53]. In this model, conditional...
probabilities of a word given all the previous words \( P(W_i|W_{i-(n-1)}, \ldots, W_{i-1}) \) are calculated. Probability distribution is further smoothed for unseen n-grams. Through these conditional probabilities, we can predict the next most likely word. Binary features can be presence or absence or n-grams in the text. N-gram frequency profile is the frequency of presence of the n-grams in the text.

**Word Embedding Techniques:** Word embedding is a vector representation of the text where words with similar meanings have similar representations. Words are represented as real-valued vectors in a vector space. According to the usage of the words, the similarity of the context of the words is learned. By word embedding, the semantic and syntactic similarity of the word in the corpus can be understood. It can also capture the relation of a word with other words. There are different methods to learn this representation from the text corpus. Word2Vec [54, 55] is a statistical method to learn word embedding from the text corpus using neural networks. The Skip-gram model [55] predicts the context words for a target word. It is an unsupervised learning technique that can learn the context of any word. The bag of words (BoW) model extracts features from the text by occurrence frequency of words in the text. A histogram of words can be used as an input to the classifiers [56]. BoW model does not consider the context of the word in the sentence, and hence semantic of the word is lost. Continuous Bag Of Words (CBOW) [55] predicts the current word by using the contexts (surrounding words). Both methods are used to learn the usage context of a word. Global vector space
representations of words can be constructed [57]. Word-word co-occurrence counts are tabulated from the corpus. The probabilities of a word i appearing in the context of a word j are calculated and called co-occurrence probabilities. The ratio of these probabilities can be used to model the context of the words. Distance between the words relates to the semantic similarity of the words. Term Frequency-Inverse Document Frequency (TF-IDF) finds the importance of the word in the document or corpus [58]. Term frequency (TF) measures the frequency of occurrence of a term or word in the document. Whereas inverse document frequency (IDF) measures how important this term or word is? It is calculated by taking the logarithm of the ratio of the total number of documents in the corpus and the number of documents having this term or word. TF-IDF score is calculated for each word in the corpus by multiplying TF and IDF. Fasttext [59] is an extension of the word2vec model. In this model, every word is represented as an n-gram of characters. A skip-gram is used to learn the embedding. Zhou et al. [37] proposed a new word embedding method called Locality Sensitive Hashing Word Embedding (LSHWE) to represent obfuscated words in cyberbullying events. The method assumes that deliberately obfuscated words have a high context similarity with their corresponding actual word. The assumption is fair; otherwise, the victim may not be understanding this word either. Based on the co-occurrence matrix and rare word list, a nearest neighbor matrix is generated through locality-sensitive hashing from the corpus. A LSH based autoencoder model is used to learn every word representation.

**Sentiment Analysis:** Sentiment is a feeling provoked by text, image, or video. Positive, neutral, or negative scores of the sentiments can be used as features towards cyberbullying detection [60].

**Media Related Features:** In the case of media (audio/image/video) sharing by the user, features such as a number of likes/dislikes, comments, and sharing, the subjectivity of the media caption are important in the prediction of the cyberbullying associated with it [40]. Further features can be extracted from the comments section of the media, including a percentage of negative comments, profane words in the comments, average polarity/subjectivity of the comments, top topics using Latent Dirichlet Allocation (LDA) from all the comments, etc.

**Vulgar Feature:** Vulgar words represent hostile or aggressive behavior and can be related to the perpetrator’s cyberbullying effort. Based on a dictionary of vulgar or profane words, the vulgarity feature can be a number of vulgar or offensive words present in the post’s content.

2) **User Network Features**

There is a strong correlation between cyberbullying and how social a perpetrator is on the social network [61]. Therefore, the social network features of users are essential for the detection of cyberbullying. It includes followers of a person, the number of users a person follows. A following to follower ratio is also an important feature. The popularity of the user plays a vital role in the severity of cyberbullying. Any attack from a popular user hurts the victim more as the perpetrator’s popularity creates the power imbalance between the perpetrator and the victim [62].

3) **User Profile Features**

Various features can be extracted from the user profile and his/her activity on social media. The age and gender of the user can be important of the cyberbullying perpetrator and victims. The age difference between the perpetrator and the victim sometimes plays a vital role in assessing the severity of the bullying. Types of social groups of the user can be predicted from his/her social network [32]. Many researchers have worked on predicting the personality of the user by his/her social activity data. By knowing the character of the person, we can understand human behavior. Cyberbullying sometimes correlates with the aggressive or hostile behavior of the user [63].

Similarly, neurotic people show anger, anxiety, and moodiness and can engage in an activity leading to cyberbullying [64]. Many studies have shown that there is no relationship between gender and cyberbullying. However, few experts suggest that including gender in the machine learning models may
improve cyberbullying detection [47]. Gender information of a user can be predicted by his/her writing style [65, 66]. There may exist some correlation between cyberbullying and age groups of the social media user [67]. Therefore, prediction of the age group from the social media data can be beneficial in cyberbullying classification [68]. Personality traits also correlate with the bullying activity of the person. Big Five model [69] identifies five personality traits: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. Mitsopoulou and Giovazolias [70] found that lower levels of Agreeableness and Conscientiousness and higher levels of Neuroticism and Extraversion are associated with bullying behavior. Researchers have tried to predict these five personality traits from a person’s digital footprint on social media that includes posted text, images, videos [68, 71, 72]. Contextual features may consist of the profession, religion, family, and financial factor of the user.

4) User Activity features
Activity features can measure the online communication activity of a user. It may include the number of posts/tweets, the number of posts/tweets liked or disliked, and hashtag activity.

5) Sentiment features
Sentiment features can also help detect aggressive and abusive behaviors [32, 60]. The post’s sentiment can be decided by a well-trained classifier or from a dictionary of the words in which sentiments are related to the words [73]. Jain et al. [74] compared various word embedding techniques for hate speech detection. Few works are reported about the use of personality features in cyberbullying detection. Personality prediction from the social media traces can help predict the roles of users in a cyberbullying event. Recent advances in increased internet speed, and users more frequently sharing video clips and other visual content forms. Hence, more research is needed to identify cyberbullying events through images or videos.

B. Classification
A range of classifiers is available for the detection and monitoring of cyberbullying events on social media. The feature extraction section mentions that textual features can be converted into vectors by embedding techniques and other features are also numeric, categorical, or binary values. Hence, many well-known classifiers, already proven in various real-life applications, can be used to classify the presence of cyberbullying events, the severity of the cyberbullying events, and the identification of perpetrators and victims.

Table II summarizes the number of articles using different classifiers in cyberbullying detection. Naïve Bayes classifier, SVM, RF, and RNN are the most commonly used classifiers. In recent years, deep learning architecture have the attention of researchers in natural language processing. Hence,

### Table II
**Different Classification Methods in Cyberbullying Detection**

<table>
<thead>
<tr>
<th>Type of Classifier</th>
<th>Classifier</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression/Statistical Classifiers</td>
<td>Logistic Regression [75], [25], [48], [28], [38]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KNN [43], [48], [41]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Naïve Bayes [27], [43], [25], [28], [76], [29], [77]</td>
<td></td>
</tr>
<tr>
<td>Decision Tree Algorithms</td>
<td>CHAID [23]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exhaustive CHAID [23]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QUEST [23]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regression Tree [30]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>J48 [27], [45], [39]</td>
<td></td>
</tr>
<tr>
<td>Support Vector Machines</td>
<td>Random Forest [32], [45], [24], [48], [33], [41], [46], [30], [38], [39], [44]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bagging/Boosting [24], [79], [78], [44]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Voting Ensemble [33]</td>
<td></td>
</tr>
<tr>
<td>Ensemble of Classifiers</td>
<td>CNN [80], [36], [61], [28], [42], [78]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CapsNet + ConvNet [82]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RNN [33], [75], [28], [42], [49], [36], [77], [83], [64], [50]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BERT [25], [85]</td>
<td></td>
</tr>
<tr>
<td>Reinforcement Learning</td>
<td>[86]</td>
<td></td>
</tr>
</tbody>
</table>
many papers have focused on using deep learning architectures like RNN, CNN, BERT, etc., especially in text-based analysis. A detail of the classifiers is given below in the subsequent subsections.

1) Regression/Statistical Classifiers

In regression analysis, statistical methods are used to estimate the relationship between dependent and independent variables. Linear and logistic regression methods are used in classification or prediction modeling [87]. The linear regression model assumes a linear relationship between dependent and independent variables. Logistic regression [88] is an extension of the linear regression model used for classification purposes. It models the probabilities of two classes by a logistic function at the output of the linear model. Maximum likelihood estimation is one of the cost functions that can be used to find the coefficients of the logistic regression model. A proper threshold at the output of the logistic function can give binary classification. This classifier is used in the literature on cyberbullying when there are two classes, cyberbullying or no cyberbullying. K-nearest neighbor (KNN) classifier [89] is a nonparametric classifier that classifies based on the majority class of k number of nearest neighbors. Naïve Bayes classifiers [90] are based on Bayes’ theorem using conditional probabilities. All the features used in the classification are considered independent from each other. Hence, the presence or absence of any feature does not affect other features. Probability model of every feature is combined with a decision rule to select the class. The decision about the class can be taken by choosing the most probable class (Maximum a posteriori decision rule) or maximum likelihood estimate (MLE decision rule).

2) Decision tree-based Classifiers

Decision trees, more recently called Classification and Regression Tree (CART) [91], are used for classification and regression modeling. Each non-leaf node is labeled with a feature or attribute and arcs from this node are possible values of this attribute in the classification tree. The leaf nodes represent the class or the probability distribution over the classes. In the case of the regression tree, predicted output is a continuous real number. J48 classifier is an open-source implementation of C4.5 decision tree algorithm [92]. This algorithm builds a tree based on the training dataset. For every node in the tree, the algorithm selects the best attribute to split with the highest normalized information gain. More nodes are generated on the remaining attributes. Once all attributes are covered, a single pass pruning is performed on the tree to minimize the overfitting. Chi-square Automatic Interaction Detector (CHAID) algorithm [93] builds the tree to detect the relationship between independent variables. This algorithm can be applied to nominal, ordinal, and continuous data split into categories. Chi-square test of independence (p-value) is applied at each of the stages to find the association between two categorical variables, and F-test is used for continuous variables. Bonferroni corrections are calculated to counter the problem of multiple comparisons/testing. CHAID algorithm selects predictors having the strongest interaction with the dependent variable. Exhaustive CHAID [94] creates all possible splits for each predictor and groups the categories of each predictor optimally. Moreover, Bonferroni correction in exhaustive CHAID is revised to counter excessive penalization in the CHAID algorithm. Quick Unbiased Efficient Statistical Tree (QUEST) algorithm [95] is another binary-split decision tree-based algorithm. QUEST uses the ANOVA F-test for non-categorical variables and the chi-square test for categorical variables to select the splitting variables. A Variable having the smallest significance probability is assigned for the split. It has low variable selection bias and computationally simple. One of the advantages of QUEST algorithm is its unbiasedness in variable selection for the split. If there are more than two classes, then classes are grouped into two super classes before the application of quadratic discriminant analysis.

3) Support Vector Machines

Support vector machines [96] are well-known classifiers in the community of machine learning, and it is used successfully in a variety of real-life problems [97]. SVM is a supervised classifier that trains itself to find maximum margin hyperplanes.
between classes to minimize generalization errors. Training data is mapped to a higher dimension using kernels to maximize the separation between classes. With this kernel trick, SVM can classify nonlinearly separable classes. Utilizing the support vectors, which are the data points near the decision boundary, the hyperplane’s position and orientation are adjusted to maximize the separating margins. A hinge loss function for margin maximization along with a regularization parameter makes the SVM a robust classifier. A good review about variants of SVM can be found in [98].

4) Ensemble of Classifiers

In an ensemble of classifiers, individual decisions of a set of classifiers are combined in a certain way (for example, voting) to predict the class of a new data point. Ensemble of classifiers improves the predictive performance as compared to an individual classifier. The idea is to combine several weak learners to form a strong learner. Recently a lot of research has been done on the ensemble of classifiers [99]. Few of such classifiers are intensively used in cyberbullying detection.

In the bagging classifier [100], several training data subsets are chosen randomly from the training data with replacement. For each subset of data, a decision tree is trained, and hence an ensemble of classifiers is created. This ensemble of classifiers is trained independently, and prediction is based on the aggregate of their outputs. In this way, the variance of the classifier is reduced. Aggregation of the outputs of weak learners can be through hard voting (majority voting) or through soft voting. In soft voting, class probabilities of all the classifiers are averaged, and the class with the highest probability is selected. Bagging can be implemented in parallel. In boosting [101], classifiers learn sequentially. A learner learns the simpler model, and by analyzing the classification errors on this classifier, subsequent classifiers are fitted on the training data. All weak learners are combined by majority voting. There are many variants of boosting classifier including AdaBoost [102], LogitBoost, BrownBoost [103], GentleBoost [104] etc., LogitBoost [105], BrownBoost [103], GentleBoost [104] etc. The voting ensemble method uses voting of multiple classifiers to decide the class of an unknown data point. It uses different classifiers on the same dataset or uses the same base classifier on a different subset of the data. Due to the diversity of the classifier, an ensemble of classifiers performs better than a single classifier.

A random forest classifier was proposed by Ho et al. [106] and later formulated by Breiman et al. [107]. It grows a forest of decision trees that split the feature space with hyperplanes. Training data is projected to a randomly chosen subspace (a randomly selected subset of features) and used to train the decision tree using bagging. Hence, in the random forest classifier, many decision trees are trained in parallel with bootstrapping followed by bagging. The random forest classifier variance is minimized by ensuring that every decision tree in the forest is unique. It exhibits good generalization without overfitting issues. Different base classifiers can be used in the random forest classifier [108, 109]. Random forest classifier is successfully applied in many practical applications [110-112]. Several studies demonstrated the potential of using kernel functions in the random forest classifier [113, 114].

5) Deep Learning Classifiers

Traditionally, features are designed by a human to train the machine learning algorithms, which require a lot of expertise and domain knowledge. Deep learning architectures exploit powerful neural networks containing multiple layers without the burden of feature engineering. Several useful deep learning architectures are successfully used in natural language processing [115, 116], image, and video processing. These deep learning architectures include Convolutional neural networks [113], Deep belief networks [115], Deep recurrent neural networks [113], Deep stacking networks [117], Generative Adversarial networks [118], LSTM [117] and variants of LSTM [119, 120], etc.

Convolutional neural networks were originally designed for image processing [121]. It contains many hidden layers, including convolution layers which perform convolution on the input, pooling layers, fully connected layers, and normalization layers. Convolution layers contain filters to learn features from the input (feature map). Pooling layers reduce the
dimensions of data. Max pooling, sum pooling, and average pooling are the common operations in the pooling layers. Fully connected layers are the same as the multi-layer perceptron. There are different types of normalization layers in deep learning architectures [122]. In batch normalization, input to any layer is normalized to have a pre-defined mean and variance. Another type of normalization is weight normalization, in which weights are normalized to improve convergence [123]. Layer and group normalization normalize the activations in feature direction [124, 125]. Existing popular CNN architectures are AlexNet [126], VGGNet [127], ResNet [128] etc. A good survey can be found in [129].

Recurrent neural networks (RNN) are designed to handle the temporal sequences of the inputs, which is very important in natural language processing. The recurrent neural network allows the previous outputs to be used as inputs by looping the output to the input of the network. Hence, an input of any length can be handled by RNN. RNN usually has short-term memory and cannot tackle long-term dependencies. Vanishing gradients, when backpropagated through time, cannot contribute to the learning. Sometimes long-term dependencies also matter in the correct prediction of the output. These scenarios exist more frequently in natural language processing. Long short-term memory (LSTM) networks are widely used in applications requiring temporal processing of the inputs and outputs [130]. These networks are especially suited to learn the long-term dependencies. LSTM consists of connected subnet call memory blocks, and each block contains one or more self-connected memory units comprising a cell, an input gate, an output gate, and a forget gate. Information flows from the input to the output through cells and removing information or adding new information is done through gates. LTSM stores information in these gated cells and passes the long chains of sequences to make the prediction. Bidirectional LSTM (Bi-LSTM) is an extension of classical LSTM in which two independent RNN structures are used to forward and backward the information at every time step. Bi-LSTM learns the context in the text better than LSTM [131]. Encoder-Decoder LSTM [132] reads the input sequence and encodes it to a fixed-length vector. The decoder part decodes the vector into the predicted sequence. In the context of machine learning, concentrating relevant concepts in the data and ignoring the irrelevant ones is done by an attention mechanism. Attention network is used between encoder and decoder layers of LSTM by Google neural machine translation. Attention network is a single layer RNN encoder whose weights are adjusted using a fully connected shallow network and a softmax function [85]. The attention mechanism does not consider the order of the sequence and model the relevance between representation pairs.

The transformer model [85, 133] uses the attention to boost the training speed. It transforms one sequence into another sequence by using encoder and decoder layers. Bidirectional Encoder Representations from Transformers (BERT) [134] learns the text representation bidirectionally. By doing so, BERT captures the language context more accurately. BERT uses an attention mechanism called a transformer to understand the contextual relationship between words. It is trained by the text sequence with a certain percentage of the masked tokens, and the network must predict the masked tokens. Moreover, pairs of sentences as input and target sentences are used in the training process. Few recent works have used more advanced language models like BERT and variants of BERT. Due to the BERT model's high computational cost and larger memory footprint, many lighter versions of BERT are also proposed [135-137]. Hardware acceleration of the BERT model is also an active area of research [138]. Emotion detection using BERT-based models is presented in a recent paper [74], which may help extract the sentiment features for cyberbullying detection.

6) Reinforcement Learning

Reinforcement learning [139] is another paradigm of artificial intelligence in which an agent learns an optimal or near-optimal policy to maximize a reward function. For each action of the agent, there is either a positive or negative reward associated with it. Hence reinforcement learning uses a balance between exploration and exploitation and generates a sequence of actions to maximize the cumulative reward function. Q-learning is an algorithm that does not require a model to learn action. Based on the actions of the agent to enter
a new state, the Q value is updated accordingly using the Bellman equation. Deep reinforcement learning [140] proposed recently will be a new area to build more autonomous systems with a high level of understanding.

III. TEXT-BASED CYBERBULLYING DETECTION

Balakrishnan et al. [45] described various feature sets that can be useful in cyberbullying detection. These features include user personality (Big Five model [69]), Twitter features (Text/content features, user features, network features), emotion analysis, and sentiment-based features. After a comparative study of different combinations of the features, the authors have identified ten key features using the best-first search method. J48 classifier has shown promising results on the features set (Classification accuracy of 92.88% on four classes).

Lee et al. [20] integrated various filters to detect the abusive text by using unsupervised learning of abusive words. These filters include blacklist [141], n-gram [142], edit-distance, list filtering, and text features. The word2vec skip-gram module is applied in unsupervised learning, and cosine similarity is used as a similarity measure. The best setting produced f-scores on the news article, community comments, and Twitter are 0.869, 0.85, and 0.92, respectively, by trying different combinations of models. In some cases, words only do not carry any positive or negative meaning. But if these words are used in a specific context, they may express harmful meanings. Therefore, Plaszynski et al. [143] used phrases consisting of morpheme pair in a dependency relation (in Japanese language) to define a harmful polarity score. Therefore, Plaszynski et al [143] used phrases consisting of morpheme pair in a dependency relation (in the Japanese language) to define a harmful polarity score. However, the precision and recall of this method on abusive and non-abusive phrases are not very significant (70% precision on 50% recall).

Fortuna et al. [144] have conducted an interesting study on the generalization of various language classification models to different datasets. They have investigated Bidirectional Encoder Representations from Transformers (BERT), A Lite BERT (ALBERT), FastText, and support vector machine (SVM) with different settings. BERT comprises of multi-layered bidirectional transformer encoder that can learn general language representations. A sentence or bunch of sentences can be input sequence to the BERT. Nine publicly available datasets (Table II of the reference) from Twitter mainly covering different classes, including racism, sexism, hate, misogynous, aggression toxic, obscene, spam, etc., are used in this study. BERT and ALBERT performed better than other classification models in the intra-dataset classification. In some cases, FastText performed better than others. Although hate speech is not the topic of this paper, these findings can be beneficial in the cyberbullying datasets also. Paul and Saha [85] fine-tuned the BERT model for cyberbullying detection. BERT comes with high computational complexity due to millions of parameters. In this paper, the knowledge distillation method [145], a simpler version of BERT, is used to minimize the computational cost of the process. A fully connected layer is added for classification. The simplified BERT method is tested on three datasets from Twitter, Wikipedia, and FormSpring. F1-score of the proposed method is comparable with the original BERT method with 30 times less computational complexity.

Coi et al. [146] proposed a method to identify the cyberbullies by text mining their comments through the Losada ratio (Positive to negative comments ratio), cyberbullying index (Insulting words rate of the comments), and social network analysis (connection relationship between commenters). A dictionary of insulting words is used to calculate the cyberbullying index. Random forest, logistic regression, and SVM are tested on the features of the comments of 3200 users. Random forest outperformed other classifiers (F-score 0.8, precision 0.81, and recall 0.78). Song et al. [23] implemented the decision tree analysis methods of data mining to predict cyberbullying’s risk factors. Causal factors of cyberbullying are used to construct the decision tree. Chi-square Automatic Interaction Detection (CHAID), Exhaustive CHAID, Quick Unbiased Efficient Statistical Tree (QUEST), and Classification and Regression Tree (C&RT) are the decision tree methods used in this study. All methods showed comparable classification accuracy with CR&T showing the best classification accuracy of 74.5%.
Al-Garadi et al. [43] used a more extensive feature set, including network information, activity information, user information, and tweet content, to classify tweets containing cyberbullying or not. Publicly available Twitter data of two months in 2015 within California, USA, is collected through Twitter API. Information gain, chi-square test, and Pearson correlation are used to select the significant features. The top ten features are used to classify cyberbullying or not using LibSVM, random forest, Naïve Bayes, and K-nearest neighbor classifier. The class imbalance was treated by SMOTE (oversampling the minority class). Random forest showed the best results (AUC was 0.943 and f-measure was 0.936).

Yokotani and Takano [147] studied the spread of cyberbullying trends via online social networks. They used a 2-dimensional convolutional neural network, bidirectional long-short term memory (LSTM), and an attention framework to identify the perpetrator-to-victim relationship. Relational patterns, gender/sexual orientation, and Pigg party usage by room owner and visitor are used. A similar classifier is used to identify the victim-to-perpetrator relationship. Data is collected from the users of the Pigg party. The gender/orientation classifier showed 99.69% accuracy. Classifiers for perpetrator-to-victim relationship and victim-to-perpetrator relationship achieved an accuracy of 88.47% and 85.32%, respectively.

Sanchez-Medina et al. [24] studied the causal relationship between dark triad and cyberbullying behaviors. They used “The Dirty Dozen” method [148] to measure the dark triad and questionnaire based on research in [149, 150] to detect cyberbullying and studied the causal relationship between dark triad and cyberbullying behaviors. Various ensemble classifiers, including random forest, bagging, boosting, and logistic regression, are used. Random forest performed best with AUC equals to 0.983. Agarwal et al. [28] identified four classes from different datasets, including Formspring, Twitter, and Wikipedia. Based on features extracted using word embedding, different classifiers are tried on the datasets and found that Bidirectional Long Short-Term Memory (BLSTM) with attention and feature level transfer learning outperformed other classifiers with an f1-score of more than 90%. Chatzakou et al. [33] distinguished cyberbullying from aggressive behaviors on a large dataset collected from Twitter users (1.2 million users, 2.1 million tweets). They have extracted a large set of features including user profile, network-based features, sentiment emotions, and content-based features. Out of these features, important features are selected for the classification. After removing spam tweets, a good classification is obtained between offensive (bullying + aggressive) and normal with AUC of 0.91 using random forest classifier.

Most of the cyberbullying detection is based on training a classifier of a feature set. Cheng et al. [151] introduced an approach of unsupervised cyberbullying detection. Multi-modal features (bag of words representation of text, social network analysis, and time of comments). The proposed learning framework estimates the likelihood of cyberbullying by using the Gaussian mixture model. The performance of the proposed framework (AUC is 0.74) was comparable with other supervised learning methods.

Yuvaraj et al. [46] proposed a framework integrating artificial neural network (ANN) and deep reinforcement learning (DRL) and achieved an accuracy of 98% on the Twitter data (30,384 tweets) with 90% training and 10% testing datasets. Feature sets include content features, user features, network features, and sentiment features. Zhao and Mao [34] developed an extension of a deep learning model called semantic-enhanced marginalized denoising auto-encoder (smSDA). It learns a robust discriminative representation of the text. The proposed method is applied to the Twitter dataset (7321 tweets) and MySpace dataset (800 instances) and obtained an accuracy of 84.9% and 89.7%, respectively. Raisi and Huang [35] proposed a weakly-supervised framework in which an ensemble of two deep learners co-training one and the other. One learner analyzes the content of the message, whereas the other learner considers the user’s social structure. Data from Twitter, Instagram and Ask.fm (total 260,800 users and 2,863,801 question-answer pairs) are manually annotated to bullying or not bullying. Experiments showed that the proposed ensemble learner performed better than other classifiers.

The deep neural network model with Gradi-
ent Boosted Decision Trees [42] has shown better accuracy (F1 Score is 0.93) on a similar data set. Zhao et al. [37] proposed a new embedding LSHWE to tackle the problem of obfuscated bullying words and showed that this embedding also improves the computational efficiency of text representation learning on large-scale datasets. Deep learning detector, Bidirectional LSTM with attention, performed better than other LSTM based detectors using cosine similarity distance function in LSHWE (F1-score is 0.8629). Cheng et al. [83] proposed Hierarchical Attention Networks for Cyberbullying Detection (HANCD) containing different layers, word sequence encoder, word-level attention layer, comment sequence encoder, comment level attention layer, contextual layer, and social media attributes embedding layer. [83] proposed Hierarchical Attention Networks for Cyberbullying Detection (HANCD) containing different layers, word sequence encoder, word-level attention layer, comment sequence encoder, comment level attention layer, contextual layer, and social media attributes embedding layer. Finally, a weighted loss function to optimize cyberbullying detection and time interval prediction. The model is compared with other methods on a dataset of Instagram (2218 sessions) and achieved a good F1-score of 0.783. This model may be tested on bigger datasets to prove its efficacy.

Most of the research mentioned above focuses on detecting cyberbullying on datasets collected from one or two social media platforms. Bruwaene et al. [78] collected a text-based dataset from VISR tool of SafeToNet that monitors the social media activity of a child on various social media platforms. They received an F-Score of 0.885 to classify bullying and non-bullying using CNN. Talpur and O’Sullivan [39] classified the severity of cyberbullying as non-cyberbullying, low, medium, and high levels. From the dataset already categorized into types of harassment contents, they ranked the severity of cyberbullying. It is debatable that how the severity of cyberbullying is linked with the types of harassment content. The severity of cyberbullying may depend on various factors, and there is no consistent definition of such classes. After extracting features based on word embedding, sentiment, Lexicon, and semantic orientation, they tried various classifiers to classify cyberbullying severity. Random forest classifier performed the best among these classifiers with a classification accuracy of 91%. Aind et al. [86] used the Q-learning method (a type of reinforcement learning) on the dataset of comments tagged as offensive or non-offensive. Misspelled words are also corrected with the closest words according to their probability. Based on the penalty/reward policy, the Q-learning method learns the sentence as offensive or not offensive (F1-score is 0.86).

Table III summarizes most of the current research conducted in the English-based cyberbullying detections on various social media content data containing more than 5000 tweets, comments, posts/instances. Deep learning architectures like LSTM and its variants, CNN, and BERT (including its variants) are prevalent in recent years. Safa et al. [25] built a small Arabic textual corpus by crawling data from Twitter and labeled it with a three-hierarchical annotation scheme. Features are extracted using n-gram, contextual word embedding, and word embeddings. The performance of various machine learning algorithms (SVM, Naïve Bayes, LR, CNN, LSTM, and GRU) on this data is analyzed on multi-classes. Word/Char-n-grams features with SVM classifier, AUC is 0.84 for hate/offensive and clean classes. For three classes (hate, offensive, and clean), the same model produced AUC equals 0.78. These works on the Arabic language can contribute to further research in cyberbullying detection on social media in Arabic-speaking people. Haider et al. [76] collected tweets in the Arabic language from Twitter (35273 tweets) and manually annotated them as bullying and not bullying. F-measures for Naïve Bayes and SVM classifiers are 0.905 and 0.927, respectively. They also enhanced cyberbullying detection performance in the Arabic language using ensemble machine learning [79]. Mouheb et al. [77] detected cyberbullying in the Arabic tweets and YouTube comments (25000 comments and tweets) based on keywords and the Naïve Bayes classifier with an accuracy of 95%. Rachid et al. [36] applied different deep learning methods on a dataset consisting of 32000 comments deleted by a news channel as offensive or obscene. So, their work identifies inappropriate comments that may not be targeted to-
<table>
<thead>
<tr>
<th>Reference</th>
<th>Data Size</th>
<th>Features</th>
<th>Classifier</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>[45]</td>
<td>9484 tweets</td>
<td>Features (Personality, net- 10 work, user) Cyberbullying index + Losada ratio + sentiment analysis, social network analysis</td>
<td>J48</td>
<td>Accuracy = 92.8% (Classes 4)</td>
</tr>
<tr>
<td>[146]</td>
<td>650000 posts and comments</td>
<td>-</td>
<td>Random Forest</td>
<td>F-Score = 0.80 (Classes 2)</td>
</tr>
<tr>
<td>[23]</td>
<td>103212 buzzes</td>
<td>Casual factors of cyberbullying</td>
<td>CRT</td>
<td>Accuracy = 74.5%</td>
</tr>
<tr>
<td>[43]</td>
<td>10,606 tweets</td>
<td>Multiple types of Features</td>
<td>Random Forest</td>
<td>F-Score = 0.936 (Classes 2)</td>
</tr>
<tr>
<td>[32]</td>
<td>10,000 tweets</td>
<td>User, Text, Network features</td>
<td>Random Forest</td>
<td>Accuracy = 91% (Classes 3)</td>
</tr>
<tr>
<td>[28]</td>
<td>12,000 Posts</td>
<td>-</td>
<td>CNN</td>
<td>F-Score = 0.93 (Classes 2)</td>
</tr>
<tr>
<td>[33]</td>
<td>2.1 Million tweets</td>
<td>User, Text, Network features</td>
<td>Random Forest</td>
<td>F-Score = 0.902 (Classes 2)</td>
</tr>
<tr>
<td>[46]</td>
<td>30,384 tweets</td>
<td>Content, user, network, sentiment features</td>
<td>ANN + DRL</td>
<td>Accuracy = 80.7% (Classes 2)</td>
</tr>
<tr>
<td>[34]</td>
<td>7,321 Tweets and 800 instances (MySpace)</td>
<td>-</td>
<td>SmSDA</td>
<td>Accuracy = 84%, 89% (Classes 2)</td>
</tr>
<tr>
<td>[86]</td>
<td>184,349 comments</td>
<td>Textual features</td>
<td>Reinforcement Learning</td>
<td>Accuracy = 89% (Classes 2)</td>
</tr>
<tr>
<td>[37]</td>
<td>9,600 tweets</td>
<td>LSHWE word embedding</td>
<td>BLSTM with attention network</td>
<td>F-Score = 0.863 (Classes 2)</td>
</tr>
<tr>
<td>[78]</td>
<td>14,899 Posts</td>
<td>LIWC features</td>
<td>CNN</td>
<td>F-score = 0.885 (Classes 2)</td>
</tr>
<tr>
<td>[38]</td>
<td>37,373 tweets</td>
<td>TF-IDF, Word2Vec</td>
<td>LR</td>
<td>F-Score = 0.928 (Classes 2)</td>
</tr>
<tr>
<td>[49]</td>
<td>2188 Instagram 7321 Tweets</td>
<td>Context2vec features</td>
<td>LSTM</td>
<td>F-Score = 0.85 (Classes 2)</td>
</tr>
<tr>
<td></td>
<td>16090 tweets (C1) 115854 Wikipedia corpus (C2)</td>
<td>-</td>
<td>BERT</td>
<td>F-Score = 0.94 (C1: 4 Classes)</td>
</tr>
<tr>
<td>[85]</td>
<td>12773 instances FormSpring (C3)</td>
<td>-</td>
<td>BERT</td>
<td>F-Score = 0.91 (C2: 2 Classes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F-Score = 0.92 (C3: 2 Classes)</td>
</tr>
</tbody>
</table>
wards anyone. But it can be considered as relevant research towards cyberbullying identification in the Arabic language. On the original dataset, they could not find a good combination to get a better F1-score but on the balanced dataset (number of offensive and non-offensive comments are same), they claimed a good F1-score of 0.84 using RNN/CNN and Fasttext embedding.

Table IV summarizes the research in cyberbullying detection involving Arabic-speaking individuals. Only a few papers have shown considerable success in Arabic language-based cyberbullying detection. A lot of work is needed to create a good corpus of Arabic language related to cyberbullying, modify existing classifiers (possibility of transfer learning in the existing Deep learning architecture for NLP), and perform performance analysis on more extensive datasets. Many valuable works already exist in Chinese [152, 153] and other languages [154, 155].

IV. Multi-modal Cyberbullying Detection

Due to diversity in the types of communication platforms and allowable content types, people are engaging with different kinds of content to maximize their social impact on the community around them. Multi-modal content makes cyberbullying detection and monitoring more challenging for the researchers.

Manuel et al. [40] detected cyberbullying in a publicly available dataset collected from Vine social network, which comprises social media sessions of videos posted, and all the likes and comments associated with this video. The feature set consisted of profile features, media session features, video features, Latent Dirichlet Allocation (LDA) features, bag-of-words similarity, and time aspects of the comments. Random Forest (RF), AdaBoost (AB), Extra Tree (ET), linear Support Vector Classification (SVC), and Logistic Regression (LR) are considered for the binary classification of cyberbullying or no bullying events. Early detection problem is considered as detecting the cyberbullying in the first few comments. A Dual model [156] classifier based on ET produced the best results, and the best F-latency metric was 0.5217. Dual models use different models with different feature sets for each class.

Kumari et al. [157] classified the social media posts containing images into non-aggressive, medium aggressive, and high-aggressive classes using different classifiers. Text features from comments are extracted by an optimized convolutional neural network (CNN), and VGG-18 [127] model is used to extract the features from images. A binary particle swarm (BPSO) algorithm is used to extract the most relevant features. Random forest classifier model with optimized features achieved F1-Score of 0.74. Li et al. [31] collected 3000 images from Instagram and extracted features from the images, captions, and comments. Features are extracted from the comments using Bag of words, Offensiveness level, and Word2vec. Comments-based features produced the best results using SVM with radial basis kernel. Latent Dirichlet allocation (LDA) is used to extract main topics from the image captions’ text, Scale-Invariant Feature Transform (SIFT), GIST, color histogram features from the images. But features based on caption and images have not performed well. Kumar et al. [82] pre-
sented a combined deep neural network model for textual, visual, and infographics (embedded text in graphics) modalities of social media. CapsNet deep neural network [158] with dynamic routing predicts the cyberbullying from the textual content, and ConvNet [159] predicts the cyberbullying from visual contents. A Late-fusion Perceptron decision layer fuses both decisions. Based on 10,000 comments, the proposed model has achieved AUC equal to 0.98 and an accuracy of 97%.

Multimodal cyberbullying detection, including text (comments, tweets, posts, etc.), images, and videos, is summarized in Table V. More extensive datasets of multimodal content are required to formulate better techniques and performance analysis. Different deep learning architectures are used to tackle the multimodal content’s diversity, and few works have shown promising results.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Data Size</th>
<th>Features</th>
<th>Classifier</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>[157]</td>
<td>3600 images with comments</td>
<td>Text features/ Image features</td>
<td>Random Forest</td>
<td>F-Score = 0.74</td>
</tr>
<tr>
<td>[31]</td>
<td>3000 images with comments</td>
<td>Text features/ Image features</td>
<td>SVM, Deep learning</td>
<td>Accuracy = 95%</td>
</tr>
<tr>
<td>[82]</td>
<td>10,000 comments, images</td>
<td>-</td>
<td>CNN</td>
<td>Accuracy = 97%</td>
</tr>
<tr>
<td>[41]</td>
<td>733 sessions with 15 posts or more</td>
<td>Textual, Visual, Audio features</td>
<td>LR</td>
<td>AUROC = 0.834 (Classes 2)</td>
</tr>
<tr>
<td>[160]</td>
<td>2100 images with comments</td>
<td>Image embedding, Text embedding (TD-IDF)</td>
<td>CNN</td>
<td>F-Score = 0.68 (Classes 2)</td>
</tr>
<tr>
<td>[49]</td>
<td>2218 sessions (Instagram)</td>
<td>LIWC, Word embedding</td>
<td>HANCD</td>
<td>F-Score = 0.778 (Classes 2)</td>
</tr>
<tr>
<td>[50]</td>
<td>969 video sessions with comments</td>
<td>-</td>
<td>Recurrent-CNN</td>
<td>ResidualBiLSTM</td>
</tr>
</tbody>
</table>

V. AUTOMATED CYBERBULLYING MONITORING AND INTERVENTION SYSTEM

In Japan, the parent-teacher association (PTA) monitors the website activities through net-petrol. Any offensive text is requested to remove from the net-petrol member [143]. But this activity is done manually and hence requires a lot of time and effort. Tommy et al. In Japan, the parent-teacher association (PTA) monitors the website activities through net-petrol. Any offensive text is requested to remove from the net-petrol member [143]. But this activity is done manually and hence requires a lot of time and effort. Tommy et al. [12] described triadic reciprocal relationships between perpetrators, victims, and bystanders. This framework consolidated personal factors, environmental events, and behavioral patterns that influence each other in a triadic reciprocal manner. Perpetrators bully the victims through any social media platform, and victims react to this bullying behavior in many ways. A bystander who is watching this bullying episode through social media platform may confront the perpetrator or remain silent against him. Similarly, he/she may comfort or stand with the victim or remain silent. Moreover, it was found that a higher rate of cyberbullying victims among the peer networks increases the risk of victimization of cyberbullying [147]. Similarly, more perpetrators among
the person’s peer network may increase the risk of victimization. Potha et al. [81] recognized bullying temporal patterns in the predator’s questions using time series modeling methodology. Jacobs et al. [161] tried to identify automatically different participants in a cyberbullying event from textual cyberbullying traces. [161] tried to identify automatically various participants in a cyberbullying event from textual cyberbullying traces. Although the F1-score of their best model is not very high (56.7%), there is a lot of scope in this area.

Developing a complete automated cyberbullying monitoring and intervention system is the need of the day. More and more people worldwide are joining social media actively, and massive data makes it impossible to monitor social media behaviors manually. Natural language processing algorithms, statistical analysis of social media activity, and deep learning may be the target areas to build such a system. We can train the system on a broader international population, and transfer learning can fine-tune the system for the local population. Interactions among perpetrator, victim, and bystander are very complicated, and a high level of artificial intelligence modeling is required to understand such interactions.

The automated cyberbullying system will focus on the following area:

- Interaction monitoring.
- Mental health monitoring.
- Intervention policies.

A. Interaction Monitoring

Simple detection of cyberbullying is not enough. We should also consider the capacity of the victim to absorb and respond to the bullying. Hence, it is crucial to monitor the interaction among the perpetrator, victim, and bystander to predict the damage done by the bullying.

1) Perpetrator and victim interaction monitoring

Interaction between the perpetrator and the victim will be monitored to detect the presence and absence of cyberbullying. In case of cyberbullying, the system will also assess the severity of the bullying towards the victim. The victim’s response to the perpetrator will also be monitored to determine the effect of cyberbullying on the victim. The victim’s reaction may be classified as appropriate, not enough, depressing, aggressive, etc. Furthermore, the victim’s interaction with his/her social circle, including family, friends, peers, etc., will be monitored to quantify the psychological damage done to the victim’s personality.

2) Bystander and victim interaction monitoring

If there is any interaction between bystander (witness of bullying on social media) and victim, either positive or negative should be monitored to assess the severity of cyberbullying on the victim. Positive interaction includes consoling the victim. Negative interaction is joining the perpetrator and bullying the victim, mockery, or spreading the event to others on social media. Blackmailing the victim on this event may also be part of the negative interaction with the victim.

3) Bystander and perpetrator interaction monitoring

Bystanders may be just witnessing the event without any interaction. In some cases, bystanders can interact with the perpetrator in a positive or negative sense. Positive interaction may include stopping the perpetrator and counseling the perpetrator. Bystanders can also become part of the cyberbullying process and encourage the perpetrator. Bystanders can also cyberbully the perpetrator in return for changing his/her behavior towards the victim.

B. Mental Health Monitoring

The victim’s mental health also plays a crucial role in an increase in the severity of cyberbullying. Furthermore, monitoring the perpetrator’s mental health can help him/her mitigate his/her aggressive behavior towards others. A proper intervention may also improve the overall community environment. Different machine learning algorithms are successfully used to monitor a person’s mental health [162-165].

1) Mental state monitoring of the victim.

The mental state of victims should be monitored...
to predict depression severity, suicidal tendency, or aggression towards his/her social circle. Victim interaction with family, friends, peers about bullying event or general interaction may also be assessed to predict the severity of the depression if exits. Any aggressive behaviors may result from the cyberbullying to the victim, which he/she shows to his connections.

2) Mental state monitoring of the perpetrator
A person becoming used to perform cyberbullying on others and enjoying the event may cause harm to his/her mental health. Early detection of such behaviors may help the perpetrator to recover from this state.

3) Mental state monitoring of the bystander
Witnessing a cyberbullying act also left unpleasant marks on the psychological state of the bystander. A positive, negative, or no response by such person may affect his/her mental health. So, monitoring bystander mental health is also essential for a healthy society.

C. Intervention policies
Once an event of cyberbullying is detected and its severity is assessed, an intervention is required to ensure the victim and other parties’ safety and mental wellness. A decision support system may decide the type of intervention. Different types of interventions are possible. An automatic decision-making system can inform the family member of the victim so that the family member may take corrective actions. Depending on the severity of the cyberbullying, the system can inform law enforcement agencies to intervene in this matter. If the victim, perpetrator, or bystander is already taking some medical treatment, the system may notify the medical staff to intervene.

VI. CONCLUSIONS
This study reviewed various aspects of machine learning-based cyberbullying detection. Most of the work is focused on classifying bullying or non-bullying events based on textual, user activity, and network information. Few research works are reported on multi-modal content extracted from social media networks. Deep learning architectures designed for natural language processing are also getting popular to understand the bullying intentions towards the victim. A strong need exists for a comprehensive dataset based on actual events involving victim’s perception of the cyberbullying efforts. Unintended biases may exist in the data annotations by a third person not involved in these events. Moreover, the victim’s mental state also plays an essential role in the severity of the cyberbullying that victims feel. Therefore, it is desirable to make the cyberbullying detection mechanism more intelligent in understanding the context of the cyberbullying attack and the mental status of the victim and his/her response to such an attack.

VII. FUTURE DIRECTIONS AND CHALLENGES
With the advancement in deep learning algorithms and their high performance in the natural language processing tasks, many new directions are opened for research to monitor social media for harassment, cyberbullying, hate crimes, etc.

Handling of a dynamic corpus: It is observed in this literature review that ways of social interaction and use of language are constantly updating. Many new slang words, intentionally misspelled or words with missing letters, use of new emojis/emoticons are continuously evolving, posing more significant challenges for monitoring systems. Therefore, language corpus should be dynamic, constantly updating with time, and retraining/incremental training of the machine learning algorithms. Transfer learning is an exciting aspect of deep learning algorithms. Pre-trained models on a language can be used for many tasks with further fine-tuning and training. On social media, many users communicate in mixed languages [166]. For example, in Asian countries like India and Pakistan, people mix English with the Urdu language. Hence multilingual identification of cyberbullying is a challenging task. In the last couple of years, few researchers have published papers in this direction [167-169].

Unintended Biasness of the detection system: Machine learning methods may contain an unintended bias towards demographic groups due to biases in the datasets on which these methods
A cyberbullying detection system is considered biased if it performs better for some demographic groups than others. Reasons for biasedness can be at the feature extraction level (bias in embedding algorithms) or classification level (bias in the human annotators or the machine learning algorithm). Gencoglu [170] suggested that unintended bias in the cyberbullying detection models can be mitigated if the model is trained with fairness constraints. Gencoglu [170] indicated that unintentional bias in the cyberbullying detection models could be mitigated if the model is trained with fairness constraints. Few works are found to solve this problem, and more research is required to produce the cyberbullying detectors using machine learning algorithms that are unbiased and transparent. Several works proposed methods to mitigate the unintended bias in the word embeddings [171-173]. Similarly, measuring and mitigating the classification algorithms’ bias is also important for a fairer performance of the classifier [173]. Data is collected and annotated by subjective human annotations. These annotations may have an unintended bias as human annotators who may not feel the victim’s pain [174, 175]. Therefore, it is essential to collect real reported data from the victims and properly annotate them. Generalization of machine learning models to various datasets, languages, and countries should also be studied further.

### Handling of obfuscated language:
Social media users use obfuscated words to bypass the automated screening software for toxic language [176]. Shorter words, conveying the semantic of a sentence, are also used to speed up the typing speed and avoid content moderation [177]. Such words pose a challenge to word embedding methods and understanding the semantic of the sentence for automated systems.

### Detection of coordinated bullying towards a specific person:
In many cyberbullying cases, more than one user targets a victim for bullying. Such collaborative cyberbullying needs more sophisticated social network analysis and understanding of messages with a common goal towards the victim. Highly coordinated groups create false impressions in the community by flooding objectionable content, making content popular, bullying, and harassing people [178]. Detection of highly coordinated groups is necessary to mitigate the bullying inside a community.

### Behavior modifications through virtual learning communities:
Helping the perpetrators involved in cyberbullying is also the community’s responsibility and the state. Behavior modification of the perpetrators through counseling, using social media, engaging them in constructive ways can be a few of the things done. Recently Nikiforos et al. [179, 180] investigated the possibility of engaging persons in the virtual learning communities who show aggressive behaviors in their physical learning communities. Teacher’s early intervention in bullying events is done through automated detection of bullying. They have shown improvement in the behaviors with such a framework. The big question arises, whether artificial intelligence can teach manners or instill moral values in a person?

### Social media’s ethical and legal issues:
Monitoring social media can prevent cyberbullying events, harassment, victimization, etc. But there are specific ethical and legal issues involved in safeguarding the students’ privacy and free speech on social media [181]. Absolute privacy of the people on social media may poses threats to the community. Hence, every country decides its ethical and legal guidelines for monitoring social media and respecting their citizens’ privacy. Monitoring social media with the perception of privacy can create a healthy environment. R. Clarke [182] coined the term dataveillance in 1988 to systematically use personal data to monitor communication among people. A good description can be found in [183].

### Policymaking to mitigate cyberbullying:
Big data analytics can give the policymakers the luxury to study various aspects of cyberbullying through automated data analytic tools. Cyberbullying events in different age groups, genders, education level based, workplaces, etc., can be analyzed to create efficient pre-emptive policies that
can reduce cyberbullying. Many societies consist of many racial groups, observing different religions and having different nationalities. In such diverse communities, monitoring cyberbullying becomes essential to foresee any mishaps in the future. Victims of cyberbullying may get depressed and tend toward suicide or may become violent and commit crimes. Therefore, such statistical analysis of the data is a necessity for effective policymaking.

REFERENCES


A Systematic Review of Machine Learning Algorithms in Cyberbullying Detection: Future Directions and Challenges


[68] H. A. Schwartz et al., "Personality, gender, and age in the language of social media: The open-vocabulary
A Systematic Review of Machine Learning Algorithms in Cyberbullying Detection: Future Directions and Challenges


[165] M. Arif, A. Basri, and G. Melibari, “Classification of


