Cyberbullying Conceptualization, Characterization and Detection in Social Media – A Systematic Literature Review

Wai Hong Woo, Hui Na Chua, May Fen Gan*
Department of Computing and Information Systems, Sunway University, Malaysia.

*Corresponding author: ganmayfen@gmail.com
(Received: 9th January 2023; Accepted: 19th January 2023; Published on-line: 28th January 2023)

Abstract— Social media has become the primary form of communication wherein users can share intimate moments online through photos, videos, or posts. At a glance, while this greatly improves interconnectivity between people, it also increases the propensity towards unrestricted acts of Cyberbullying, prompting the need for a data-centric detection system. Unfortunately, these sites generate much metadata, which begs the need for complex Machine Learning (ML) classifiers to categorize these acts accurately. Prior studies on the subject matter only target the topics of Conceptualization, Characterization, and Classification of Cyberbullying individually, so this research aims to provide a more holistic understanding of the subject matter in a continuous, synthesized format. This study found that Cyberbullying differs from Traditional Bullying in key areas of Repetition and Intention. Moreover, multimodal feature sets, as opposed to single feature sets, significantly improve ML classifiers’ performance. Lastly, the selection of appropriate ML classifiers and performance metrics is context-dependent. The result of this study presents a consolidated view of relevant parties tackling different aspects of an ML-based automated Cyberbullying detection system so that those assigned tasks can approach them strategically.

Keywords— Cyberbullying, systematic literature review, Social Media, Conceptualization, Characterization, Classification, Machine Learning

1 INTRODUCTION

One of the main channels for human communication today is none other than through various social media platforms such as Facebook, Douyin, Twitter, and Reddit. Through these platforms, people can keep in touch with their loved ones, network with like-minded individuals across the globe, and share their opinions and ideas online through site postings. However, despite all its advantages, social media, too, has its pitfalls. For example, the issue of cyberbullying, which, quite menacingly, increases the rate of suicide attempts by 8.7% [1], causes anxiety [2], increases the propensity of substance abuse by 2.5% [3], adversely affects academic performance [4], and a host of other issues.

According to [5], Cyberbullying is defined as a belligerent act performed over and over again with time, with intent, and using an electronic communication medium by an individual or a group of individuals towards a victim who is unable to defend himself or herself. Cyberbullying victims, as such, often feel defenceless, unable to do anything to parry the onslaught of negativity and toxicity directed toward them. Furthermore, most cyberbullying occurrences go unnoticed as an implication of the nature, complexity, and sheer volume of the frequency of its happenings [6]. As bullies can also remain anonymous online, they can leverage this anonymity to go under the radar and become more offensive perpetrators [2]. Moreover, cyberbullying, for instance, via text, usually brings more profound and longer-lasting negative effects compared to traditional bullying because victims and bystanders can see traces of the deed repeatedly as it gets propagated online [8]. The gravity of the issue, it’s mishandling, and the desire to curtail its undesirable effects further amplifies the need to develop more intelligent tools and techniques capable of characterizing and detecting cyberbullying using present social media datasets.

Findings from our literature study show that different detection techniques have been employed to detect cyberbullying in social media. These techniques range from textual analysis methods to more complex and elaborate Machine Learning methods. Although previous literature reviews mainly focused only on the detection process, there is a lack of a study that systematically reviews the conceptualization and characterization processes involved in detecting cyberbullying. Conceptualization, characterization, and detection, when reviewed collectively and sequentially, are complementary and supplementary to a more comprehensive understanding of cyberbullying in the ever-changing technological landscape. Thus, the primary motivation of this systematic literature review is to provide an overview of the current state of affairs concerning the conceptualization, characterization, and detection of cyberbullying. In addition, this review is a
starting point to ascertain gaps in the field of study and incentivize future work and improvements in the three respective disciplines.

This study aims to differentiate the conceptualization of cyberbullying from traditional bullying and compare and contrast different cyberbullying characterization methods and different Machine Learning algorithms for cyberbullying detection. This study tackles the three research questions (RQ) as follows, listed along with the motivation for each RQ:

RQ 1: How is the conceptualization of cyberbullying different from traditional bullying?

Motivation for RQ 1: To identify meta-themes from prior studies contributing to cyberbullying and traditional bullying, and compare their similarities and differences. By distinguishing between the two, feature ambiguity can be significantly reduced, and cyberbullying can be characterized more accurately.

RQ 2: How do we characterize cyberbullying?

Motivation for RQ 2: Identify textual and non-textual characterization methods used for cyberbullying detection in the current literature to establish a more holistic and multimodal approach to cyberbullying characterization. This study also analyses the features used in each characterization method and suggests the rationale for the relevance of the feature in denoting cyberbullying in social media postings.

RQ 3: How can Machine Learning (ML) algorithms be used to detect cyberbullying in social media? and what are the common algorithms used for its detection?

Motivation for RQ 3: Provide a thorough, state-of-the-art look into the process of using ML algorithms to detect cyberbullying in social media through four sequential steps of data collection, feature engineering, ML and evaluation, and in doing so, disseminate the knowledge used in each area to assist in the direction of future research.

2 RELATED WORK

Cyberbullying detection in SM is the title and objective of this study but instead of directly addressing the ML methods used in the detection of cyberbullying, a three-pronged approach is implemented in this study including the conceptualization of cyberbullying, characterization of cyberbullying and detection of cyberbullying, which are highly coupled with each other. This is because better understanding of the definition of cyberbullying leads to better characterization of cyberbullying and better characterization results in improved feature extraction in the eventual detection ML algorithm. Therefore, implementing a three-pronged approach.

A. THE CONCEPTUALIZATION OF CYBERBULLYING

The conceptualization of cyberbullying is an essential precursor to the other two elements because having a set of meta-themes to identify and compare traditional bullying or cyber aggression. Common meta-themes or foundational elements indicative of cyberbullying include intent, repetition, accessibility, anonymity, barriers to disclosure, and power imbalance.

The intent is a common recurring meta-theme, especially in how young people conceptualize cyberbullying [9-13]. The intent, in itself, can take varying forms. For example, [14] found that jealousy drives cyberbullying propensity, and [15] reported that vengeance as the intent is a motivating factor. In contrast, [16] emphasized the intent of amusement. Langos [17], on the other hand, discusses how in the absence of intent, accidental behaviours and usual jests are labelled as cyber aggression instead of cyberbullying. Finally, [18] further reinforces the idea, finding that intention is a differentiating factor and a binding agent that verifies an act as cyberbullying. Therefore, all other meta-themes of cyberbullying, despite being present, will be invalidated without intention.

Repetition as a meta-theme of cyberbullying usually indicates some significant intention because cyberbullying is usually not a one-off event. Naruskov et al. [10] and Nocentini et al. [11] recognized that repetition could differentiate between wisecracks and full-blown cyberbullying. SM, unfortunately, promotes this repetition because of its fundamental nature, allowing users to create posts and forward or share the posts of others multiple times, causing these posts to be viewed over and over again. A single-act transition into a repetitive one the more frequently the post, video, or photo is viewed [19].

Accessibility is another symbolic element in cyberbullying. Mishna et al. [20] and Pelfrey Jr and Weber [21] argue that feelings of isolation in younger people increase with the absence of SM. Mishna et al. [20] further added that SM becomes an inviting space for them to openly and unspiringly indulge in derogating their peers. Pelfrey Jr and Weber [21] also concluded that perpetrators of cyberbullying are empowered to continue with their acts upon returning to cyberspace.

Anonymity is another prominent feature and progenitor of cyberbullying. According to [22], the detrimental effects of cyberbullying are compounded by an unknown factor, which increases victims’ distress. Similarly, [23] provided examples of different forms of anonymity, such as deception and hacking are prime motivators for cyberbullying as the perpetrators do not need to identify as in real life and can still get away without having to deal with the consequences of their actions.

In the context of barriers to disclosure, [24] argued how fear of repercussions would prevent young people from telling adults that they are victims of cyberbullying. They also found out that this lack of disclosure is because adults are often perceived as incompetent in dealing with matters
on SM. Studies like [14] and [22] also reported how refusal to part with SM or the Internet is another significant barrier to cyberbullying disclosure.

Lastly, power imbalance or discrepancies in capacity between victim and perpetrator is evident in many instances of cyberbullying. Distinct differences in physique, popularity, gender, and intelligence between perpetrators and victims of cyberbullying in favour of the perpetrators can create an imbalance and render the victims powerless in the face of their offenders [25]. Additionally, sometimes a power differential can be made through self-victimization on the victim’s part in cases where the victim has poor social interaction skills [26]. Sometimes, the situation is not within their control, as online posting times do not follow a predictable pattern [27].

B. THE CHARACTERIZATION OF CYBERBULLYING

Cyberbullying characterization looks into establishing an understanding of the features of cyberbullying for detection. More specifically, what features are extracted, are there any pre-processing requirements, and did the prior study use external resources [28]? Preliminary research into several prior studies for this literature review shows that there are generally four different types of features: content-based, sentiment-based, user-based, and network-based.

1. CYBERBULLYING CONTENT-BASED FEATURES

Content-based features include cyberbullying keywords, profanity, pronouns, n-grams, Bags-of-Words (BoW), Term Frequency Inverse Document Frequency (TFIDF), length of a document, and spelling. Profanity lexicons were created using libraries such as noswearing.com and urbandictionary.com to detect profanity features [29-31]. Rafiq et al. [32], however, were not in favour of using profanity because not all profanities are indicative of cyberbullying, which are just means of expression. Studies such as [29] and [33] used n-grams as the feature of choice in detecting cyberbullying. However, [34] do not favour n-grams, choosing to implement TFIDF instead, claiming that it outperforms n-grams due to its establishment of word importance relative to the document. Sood et al. [35] and Huang et al. [36] are novel studies using less common features, Levenshtein Distance and emoticons, respectively. According to [37], sentiment or emotion-based analysis has applications in product reviews in SM, whereas [38] found that it can be used to dissect patterns in the financial market.

2. CYBERBULLYING SENTIMENT-BASED FEATURES

Sentiment or emotion-based features, through the identification of keywords, were used in most of the studies screened [39-41]. Nevertheless, this approach is not utilized in [42], which used Probabilistic Latent Semantic Analysis (PLSA) instead to extract the emotive features from the SM postings. In general, sentiment-based features are found to improve the subsequent detection process. However, improvements were insignificant because sentiments can be shrouded in sarcasm, and emotions are not always genuinely expressed, making this feature subpar at best [29, 43, 44].

3. CYBERBULLYING USER-BASED FEATURES

Besides content-based and sentiment-based features, user-based features such as age, sex, ethnicity, and sexual preference are also used to detect cyberbullying. Studies like as [45], [46], and [47] used either age or sex or both, with these two features being the most commonly used user-based feature from all the studies screened. Salawu et al. [28] proved that user-based features, like age and sex, substantially improved the detection of cyberbullying trained using ML classifiers.

4. CYBERBULLYING NETWORK-BASED FEATURES

Lastly, several studies have also reflected the use of network-based features such as the number of likes, friends, followers/following, uploads, and comments. For example, [45] used the network-based feature such as the amount of time spent online, whereas [42], [36], and [48] used ego networks, a type of social network. In particular, [36] found that a higher degree of interconnectedness in an ego network correlates to lower occurrences of cyberbullying, potentially due to better social support. However, more communication between users in that scenario led to more remarkable occurrences of cyberbullying, which is a contrary effect.

Predominantly speaking, earlier works did not limit themselves to only using a single feature type but rather a combination (two or more) of different features for detection. For instance, one of the studies used content-based, sentiment-based, and network-based features to perform detection using ML techniques such as Naïve Bayes, RandomForest, and Decision-Tree [32].

C. THE DETECTION OF CYBERBULLYING

Machine Learning (ML) comprises several but typically four main steps: 1) Data collection, 2) Feature Engineering, 3) Learning, and 4) Evaluation. Data collection is a process by which data is pooled from online databases. A glance into the prior studies screened showed that most of the data were obtained from either SM sites, media sharing platforms, or online databases like Kaggle, with each study dealing with enormous amounts of data, justifying the need for an automated approach in detection. After data is collected, features are extracted in the feature engineering process. According to [49], feature engineering is a process of tweaking the feature space in a dataset to boost the performance of the eventual modelling task. For modelling,
this study focuses on none other than ML. ML approaches can be further categorized into supervised and unsupervised learning approaches.

In terms of supervised learning approaches, the Support Vector Machine (SVM) and Naïve Bayes (NB) classifiers are the two most commonly used techniques for detecting cyberbullying in social media [8, 29, 43, 44, 50]. Studies done using SVM and NB only differs from each other in terms of features. Nandhini and Sheeba [51], a study that used NB, used the Levenshstein Distance, a content-based feature, whereas another NB study, by [46], trained its model using gender, a user-based feature. Even amongst studies that use the SVM approach, the feature engineering process may differ. For instance, [52] relied on keywords on cyberbullying (content-based feature), whereas [35] made use of TFIDF and n-grams (content-based features).

Likewise, between studies that use the NB approach. Notably, [53] used likes and followers/following, a network-based feature, but [54] utilized n-grams, a content-based feature. After SVM and NB, Decision Tree (DT) appeared as another supervised learning approach used, though not as frequent as the two former, in studies like [32], [47], and [55]. Galán-García et al. [55], in particular, incorporated the J48, a DT classifier. According to [28], DT ensembles such as the J48 are often used because, unlike SVM, they can classify non-linear data without having to map the dataset into a higher dimension. The study also added that the typical reason why SVM and NB are often selected is that both are responsive toward any optimization in their parameters. However, if speed is of concern, NB is preferred over SVM. Preliminary screening into several prior studies did not seem to single out any supervised machine learning techniques in terms of performance because performance ultimately boils down to feature engineering.

The selection of different features under different circumstances will yield different performance results. Thus, in the prior studies screened, there were no supervised ML techniques that consistently came up on top in terms of performance. Besides, there were also no unsupervised ML techniques in the prior studies screened simply because supervised ML techniques were more commonly used. Di Capua et al. [56] and Cheng et al. [57] are two studies favoring the paradigm shift from supervised to unsupervised learning approaches. Di Capua et al. [56] argued that an unsupervised ML approach in the form of an Artificial Neural Network (ANN) could easily outperform its supervised counterparts as it does not need to deal with the complexities of having to label the dataset manually. When dealing with colossal amounts of SM data, this task becomes unfeasible and cannot be generalized for future use cases when the SM evolves.

On the other hand, [52] proposed an unsupervised learning framework called UCD based on time series processing. Therefore, the efficacy of the ML algorithm must be evaluated using several metrics. Commonly used metrics to evaluate the performance of ML algorithms include true positive (TP), true negative (TN), false positive (FP), false negative (FN), recall, specificity, precision, F-score or F-measure, receiver operating characteristic (ROC) curves, area under ROC curves (AUC) and overall accuracy [58, 59].

D. Systematic Literature Review (SLR)

An SLR is a type of literature review that groups all empirical data according to some pre-indicated inclusion criteria to answer a particular set of research questions [60]. An SLR is a meta-analysis with qualities such as having a set of research questions. To which the study will attempt to answer a set of goals that are explicit and easily replicated that meet the eligibility criteria, a quality assessment of the mined literature, a synthesized presentation of data obtained from the selected works, and a high research value [61-63].

3 Research Methodology

We adopted the SLR model for this study to provide a synthesized view of three separate yet interrelated research areas. The SLR protocol in this study has a few stages:

- Identification and Specification of Research Questions
- Sourcing Process
- Inclusion and Exclusion Criteria
- Search and Selection Process
- Quality Assessment
- Data Extraction, Aggregation, and Analysis

For the identification and specification of Research Questions (RQ), RQ1, RQ2, and RQ3, have been detailed in the Introduction section.

A. Sourcing Process

The following are the e-journal databases used in the SLR of this study: IEEE Xplore (https://ieeexplore.ieee.org), Google Scholar (https://scholar.google.com), ScienceDirect (https://www.sciencedirect.com), and ACM Digital Library (https://dl.acm.org/).

B. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria will differ between the three areas of research in the study: conceptualization, characterization, and detection of cyberbullying in SM. Nonetheless, the general criteria for inclusion and exclusion, are shown in TABLE.

After the first pass of filtering using EC1 to EC6, the pool of available articles to work with is of higher quality and relevance to the study. Therefore, the next step was to
performed specific filtering using additional exclusion criteria to aggregate further the papers based on the three different RQ areas of conceptualization, characterization, and detection. These criteria are described in Table I, II, and IV.

### C. SEARCH AND SELECTION PROCESS (SSP)

The SSP can be divided into several distinct stages, as shown in Fig. 1. Papers excluded from Stage 8 and papers found via backward searching are fed again into Stage 1 of the cycle, and the whole SSP repeats itself, leading to the next iteration.

#### TABLE I
**General Exclusion and Inclusion Criteria**

<table>
<thead>
<tr>
<th>Exclusion Criteria</th>
<th>Inclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC1: Paper is not written in the English Language</td>
<td>IC1: Paper is written in the English Language.</td>
</tr>
<tr>
<td>EC2: Paper is not fully accessible.</td>
<td>IC2: Paper is fully accessible.</td>
</tr>
<tr>
<td>EC3: Paper is not peer-reviewed.</td>
<td>IC3: Paper is peer-reviewed.</td>
</tr>
<tr>
<td>EC4: Paper is not published in any of the above listed databases.</td>
<td>IC4: Paper is published in one of the above listed databases.</td>
</tr>
<tr>
<td>EC5: The content of the paper is not related to the topic and area of study. Paper does not have keywords such as &quot;cyberbullying&quot;, &quot;social&quot;, &quot;media&quot;, &quot;literature&quot;, &quot;review&quot;, &quot;meta-analysis&quot;, &quot;data&quot;, &quot;mining&quot;, &quot;systematic&quot;, &quot;multimodal&quot;, &quot;problems&quot;, &quot;challenges&quot; or &quot;holistic&quot; in its title.</td>
<td>IC5: The content of the paper is related to the topic and area of study. Paper has keywords such as &quot;cyberbullying&quot;, &quot;social&quot;, &quot;media&quot;, &quot;literature&quot;, &quot;review&quot;, &quot;meta-analysis&quot;, &quot;data&quot;, &quot;mining&quot;, &quot;systematic&quot;, &quot;multimodal&quot;, &quot;problems&quot;, &quot;challenges&quot; or &quot;holistic&quot; in its title.</td>
</tr>
</tbody>
</table>

#### TABLE II
**Exclusion and Inclusion Criteria for RQ1 (Cyberbullying Conceptualization)**

<table>
<thead>
<tr>
<th>Exclusion Criteria</th>
<th>Inclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC7: Paper does not have keywords such as &quot;conceptualization&quot;, &quot;v.s.&quot;, &quot;difference&quot;, &quot;nature&quot;, &quot;motives&quot;, &quot;principles&quot;, &quot;factors&quot;, &quot;meta-themes&quot;, &quot;concept&quot;, &quot;features&quot; or &quot;themes&quot; in its title.</td>
<td>IC7: Paper has keywords such as &quot;conceptualization&quot;, &quot;v.s.&quot;, &quot;difference&quot;, &quot;nature&quot;, &quot;motives&quot;, &quot;principles&quot;, &quot;factors&quot;, &quot;meta-themes&quot;, &quot;concept&quot;, &quot;features&quot; or &quot;themes&quot; in its title.</td>
</tr>
</tbody>
</table>

#### TABLE III
**Exclusion and Inclusion Criteria for RQ2 (Cyberbullying Characterization)**

<table>
<thead>
<tr>
<th>Exclusion Criteria</th>
<th>Inclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC8: Paper does not have keywords such as &quot;characterization&quot;, &quot;analysis&quot;, &quot;textual&quot;, &quot;sentiment&quot;,</td>
<td>IC8: Paper has keywords such as &quot;characterization&quot;, &quot;analysis&quot;, &quot;textual&quot;, &quot;sentiment&quot;, &quot;lexicon&quot;,</td>
</tr>
</tbody>
</table>

#### TABLE IV
**Exclusion and Inclusion Criteria for RQ3 (Cyberbullying Detection)**

<table>
<thead>
<tr>
<th>Exclusion Criteria</th>
<th>Inclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC9: Paper does not have keywords such as &quot;detection&quot;, &quot;machine&quot;, &quot;learning&quot;, &quot;supervised&quot;, &quot;unsupervised&quot;, &quot;comparative&quot;, &quot;analysis&quot;, &quot;comparison&quot;, &quot;models&quot;, &quot;training&quot; or &quot;automated&quot; in its title.</td>
<td>IC9: Paper has keywords such as &quot;detection&quot;, &quot;machine&quot;, &quot;learning&quot;, &quot;supervised&quot;, &quot;unsupervised&quot;, &quot;comparative&quot;, &quot;analysis&quot;, &quot;comparison&quot;, &quot;models&quot;, &quot;training&quot; or &quot;automated&quot; in its title.</td>
</tr>
</tbody>
</table>

### D. QUALITY ASSESSMENT (QA)

QA is an integral component of the SSP, performed throughout the SSP lifecycle whenever a set of papers gets screened using any exclusion criteria. QA aims to tackle biases and verify each selected paper's internal and external legitimacy [64, 65]. Selected academic papers for this study were written in English, fully accessible, peer-reviewed, published in one of the electronic databases between 2005 and 2021, and contain all generic and specific keywords for RQ1, RQ2, and RQ3, but that does not necessarily make it a high-quality paper. Therefore, a set of questions [66, 67] were answered for each paper to assess the quality:

- Is the objective of the research adequately described?
- Is the research methodology used in the study sufficiently described?
- Are the results of the studies presented clearly?
- Were the conclusions made by the authors supported by the results of the study?
- Are threats to the legitimacy of the study considered?

### E. DATA EXTRACTION, AGGREGATION AND ANALYSIS

Data extraction or Coding in this SLR model refers to extracting relevant information from selected papers to answer the three RQs set at the beginning of the study. It can be represented in a tabular format consisting of authors' columns, and year published, objectives, research methodology, tools used, findings, conclusion, limitations, future work, and evidence for RQ1/RQ2/RQ3. The data extraction form for each selected paper was collated into a combined dataset and aggregated based on the three different RQs.

### 4 RESULTS AND DISCUSSION

#### A. RQ1: HOW IS THE CONCEPTUALIZATION OF CYBERBULLYING DIFFERENT FROM TRADITIONAL BULLYING?

Conceptualization of Cyberbullying is paramount to establishing a ground zero on the topic of Cyberbullying.
Often, the definition is unclear, making the subsequent processes of Feature Engineering, otherwise known as Representation Learning, and then Classification, subpar in its effectiveness, as everything can be traced back to how concrete the conceptualization of Cyberbullying was made. With a clear understanding of the meta-themes that accounts for Cyberbullying, researchers can better understand the corpus they are dealing with, allowing for more accurate labelling by human annotators through some predefined criteria. These predefined criteria make up the six core meta-themes of Cyberbullying. They include themes: 1) Intent, 2) Repetition, 3) Power Imbalance, 4) Anonymity, 5) Barriers to Disclosure, and 6) Accessibility.

On the other hand, Traditional Bullying has three core meta themes which are 1) Intent, 2) Repetition, and 3) Power Imbalance. We can see that both Cyberbullying and Traditional Bullying share three similar meta-themes: Intent, Repetition, and Power Imbalance. The additional factors of Anonymity and Accessibility are present in the Cyberbullying conceptualization because they are more specific to the cyber context of SM sites, where these acts of Bullying occur. Although Barriers to Disclosure are one of the core meta themes for cyberbullying, it is but a direct consequence of Accessibility and Anonymity. Consequently, the significant glaring differences between Traditional Bullying and Cyberbullying lie among the three core meta-themes shared, particularly in Intent and Repetition, with Accessibility and Anonymity having less of an impact as much as they are apparent for the context, i.e., occurring in the cyberspace. The prior studies, along with the meta-theme(s) discussed, are shown in Table V.

In increasing order of importance, with the most important being the most frequently discussed in prior studies, the meta themes for cyberbullying can be ranked as follows: Repetition, Intent, Power Imbalance, Anonymity, Accessibility, and Barriers to Disclosure. As expected, the top 3 meta themes for Cyberbullying are all the core meta themes for Traditional Bullying because, dismissing the fact that it occurred in cyberspace, Cyberbullying is still another form of bullying hence the similarity. Barriers to Disclosure are seldom discussed, as seen from the studies in Table VII, most likely because it is related to the reasoning behind why Cyberbullying continues to be rampant rather than being a defining factor for it. On the other hand, for Traditional Bullying, Intent, Repetition, and Power Imbalance were discussed in all relevant papers. All three core meta-themes of Traditional Bullying (Intent, Repetition, and Power Imbalance) are of equal importance as they conceptualize what bullying is in general.

Where applicable, we discuss the commonalities and differences between each meta-theme in the context of both Cyberbullying and Traditional Bullying in sections 4.1.1 – 4.1.6.

Fig. I SSP Model Diagram
### TABLE V

Core Meta-Themes for Cyberbullying and Traditional Bullying

<table>
<thead>
<tr>
<th>No.</th>
<th>Study</th>
<th>Intent</th>
<th>Repetition</th>
<th>Power Imbalance</th>
<th>Anonymity</th>
<th>Barriers to Disclosure</th>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Slonje and Smith [19]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Vandebosch and Van Cleemput [13]</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Dooley et al. [27]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Mishna et al. [20]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Nocentini et al. [11]</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Burnham and Wright [24]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Hemphill et al. [68]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Langos [17]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Naruskov et al. [10]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Ševčíková et al. [69]</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Baas et al. [22]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Cassidy et al. [70]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Eden et al. [71]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Topcu et al. [12]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Berne et al. [9]</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Kowalski et al. [22]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Pelfrey Jr and Weber [31]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Rafferty and Vander Ven [16]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Thomas et al. [73]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Abu Bakar [23]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Jacobs et al. [15]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Cuadrad-Gordillo and Fernández-Antelo [74]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Fahy et al. [75]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Betts and Spenser [14]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Dennehy et al. [76]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

### Traditional Bullying Sources

<table>
<thead>
<tr>
<th>No.</th>
<th>Study</th>
<th>Intent</th>
<th>Repetition</th>
<th>Power Imbalance</th>
<th>Anonymity</th>
<th>Barriers to Disclosure</th>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aluede et al. [77]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Modecki et al. [78]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Tsagounis [79]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Salin et al. [80]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Stuart and Szaszewski [81]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **Intent**

Intent can come in a myriad of forms, but in the case of Cyberbullying and Traditional Bullying, the perpetrator's intentions are usually bad in most cases. According to [9] and [17], bad intentions in Cyberbullying include actions such as making spiteful remarks about a person's looks, sexual preference, and circle of friends. However, bad intentions can also include making sarcastic or snide comments whose reaction can go both ways; either the person receiving said remarks get offended or laugh along with the joke. Therefore, Intent cannot be a standalone criterion for both Cyberbullying and Traditional Bullying, so it has to be used alongside Power Imbalance and Repetition in conceptualizing both forms of bullying [17]. Nocentini et al. [11] further added how the notion of Intent could be individualistic and not so clear-cut in Cyberbullying because the perpetrator may regard it as a harmless prank or joke. However, the victim was offended. Thus, intent as a metatheme of Cyberbullying should focus on the perceived
intention of the perpetrator to cause harm, causing the victim to feel attacked and unsafe. In Traditional Bullying, the intent of the bully to cause harm is always concretely established [77-81].

2. REPETITION

According to [9], SM sites can become a venue for perpetrators, friends of perpetrators, enablers, and mindless bystanders to disseminate information repeatedly. [11] also concurred with the study, adding that there is an element of Repetition in Cyberbullying through the persistent forwarding posts on SM sites. Cyberbullying detection aims to create a failsafe mechanism that, in an ideal world, will detect instances of Cyberbullying at the earliest so that these posts can either be changed or deleted to keep exposure to audiences of the Internet at a minimum. However, according to [17], this could be hard to achieve as most of the time, Cyberbullying posts tend to remain in cyberspace eternally.

Another thing to note is that Repetition in Cyberbullying is often not characterized by actions performed repeatedly by the malefactor. However, it is usually the case where past deeds may have an incessant effect [22]. In Traditional Bullying, bullying is always set in stone when there is an element of repetitiveness inflicted by the perpetrator toward the victim, which consolidates the victim’s perception of the perpetrator’s intent to cause harm [77-81].

3. POWER IMBALANCE

Power Imbalance exists when the victim is in a vulnerable position, unable to stand up for himself or herself during the perpetrator’s display of power toward the victim [17]. In that same vein, even though the victim has perceived differences in power, if he or she is not rendered defenseless, then a power differential does not exist. Langos [17] further added that stark differences in age, gender, physique, mental capacity, sociability, and social standings lead to disparities in power between aggressor and victim in most cases studied. The factors above are valid for both Cyberbullying and Traditional Bullying. Nocentini et al. [11], however, took a different approach in their studies, researching whether victims of Cyberbullying can quickly end the negative interactions between them and the perpetrators, thereby reducing or eliminating any power imbalances. Despite their efforts, the study concluded that Power imbalance still exists in Cyberbullying, as posts on SM sites can propagate like wildfire, leading to more exposure and deepening of the issue. In Traditional Bullying, Power Imbalance exists as well and is a crucial feature in its conceptualization [77-81].

4. ANONYMITY

An easy way to comply with the journal paper formatting requirements is to use this document as a template and simply type your text into it.

According to [5], the probability that an anonymous person becomes a victim of Cyberbullying is equal regardless of how authoritative he or she is deemed in real life. This is closely related to identity forgery, which, as discussed in [10], enables people to do the unthinkable and act in ways they would never do in reality. The term Anonymity can also literally refer to the notion that the perpetrator of Cyberbullying commits derogatory acts while on the keyboard, unbeknownst to the victims. Cuadrado, Cordillo and Fernández-Antelo [20] further added that this Anonymity could serve as a "safe house" for the perpetrators, which only works in their favor, making it harder for authorities to rat them out as aggressors. Moreover, this "safe" setting made possible through Anonymity gives perpetrators the impression that they have the authority to hound others without repercussions. Furthermore, this can make it seem like the acts of Cyberbullying are non-orchestrated. However, this is not the case for Traditional Bullying, as the perpetrator's identity is always known [13].

5. BARRIERS TO DISCLOSURE

Barriers to Disclosure, in most cases, are a direct consequence of both Accessibility and Anonymity, or it pertains more to why Cyberbullying is still at large rather than being a defining cause of it. Out of all the studies screened, only two, [22] and [20], stood out as the two with the most explanatory takes on Barriers to Disclosure. According to [22], Barriers to Disclosure take the form of the victim’s reluctance to seek assistance. Mishna et al. [20] touched on several Barriers to Disclosure, including victims of Cyberbullying are hesitant to report their bullying to parents and other adult figures because it is a problem that is incomprehensible to them due to generational differences. Furthermore, victims of Cyberbullying are afraid to disclose any information concerning their bullying for fear of having their computer privileges stripped from them. There was also a point made on how victims of Cyberbullying do not bother with telling the truth as the perpetrators will most likely be disingenuous, leveraging on the power of Anonymity. Finally, the study also brought up how most victims of Cyberbullying take a non-disclosure disposition when it comes to experiences such as Cyberbullying in order to be self-sufficient so as not to worry their folks.
6. Accessibility

An easy way to comply with the journal paper formatting requirements is to use this document as a template and simply type your text into it.

Accessibility, like Anonymity, is also one of the meta-themes specific to the cyber context. However, unlike Anonymity, Accessibility can be quite multi-faceted, referring to several aspects that can explain why Cyberbullying has occurred. The first aspect of Accessibility is related to the ease of access by which perpetrators can commit their heinous acts of Cyberbullying. According to [14], Accessibility refers to the absence of a cut-off time for Cyberbullying, which perpetrators of Cyberbullying can leverage. Traditional bullying often occurs in a physical setting with different cut-off times, such as when one is asleep or engaged in other activities, and facilities restrictions, such as closing hours and barring people from being around the physical compound, thus halting the act of Traditional Bullying. Unlike Cyberbullying, acts can go on around the clock in cyberspace. The second aspect of Accessibility is related to the ease of publicizing the acts of Cyberbullying, forwarding the same post a hundred to a thousand times over through SM, garnering huge volumes of bystanders who may or may not aggravate the situation [10, 74].

B. RQ2: How do we characterize Cyberbullying?

In the lens of an automated Cyberbullying detection framework, the Characterization of Cyberbullying is essentially the process of Feature Extraction or Feature Engineering in the landscape of the Cyberbullying detection framework. It is the crucial step that precedes the Classification of Cyberbullying in detection. Feature Extraction converts the data corpus into a format that can be fed into the various Machine Learning algorithms. In addition, various features can be extracted from the corpus. However, features used in prior studies typically fall into one or more of four types of features: 1) Content-based features, 2) sentiment/emotion-based features, 3) user-based features, and 4) network-based features.

Content-based features are an umbrella term for features extracted from the content of the post or corpus, such as pronouns, n-grams, Bag-of-Words (BoW), and Term Frequency-Inverse Document Frequency (TF-IDF). Sentiment/emotion-based features, on the other hand, include features such as Cyberbullying-specific keywords, Polarity, and outputs of any Semantic Analysis. In addition, features specific to users, like age, gender, and sexual orientation, make up what is known as user-based features. Finally, network-based features or social network features encompass (but are not limited to) the follower count, the following count, and the number of likes. As content-based features make up anything that can be extracted from the content of SM sites, they can include both textual/lexicon and contextual/non-textual features. For example, BoW (Bag-of-Words) is a textual, content-based feature, whereas an audio file is a contextual, content-based feature. This distinction is crucial in understanding the differences between the two terms. Thus, contextual features include various feature types: network-based, sentiment/emotion-based, user-based, and all image and visual features.

According to [36], a multimodal approach must be taken regarding what features are used to train Classification algorithms because the efficacy of using textual features alone is relatively poor. In that study, the contextual feature used in tandem with the traditional textual features is social network features (or network-based features). This multimodal approach led to marked improvements in the classification accuracy of the classifiers employed in the study. Furthermore, Cyberbullying is considered a social issue, so information on the social context encompassing the textual information may offer critical insights which can help improve its detection. In layperson’s terms, having social network features paints a complete picture in prior studies on Cyberbullying detection, so its inclusion was justified. Rezvani et al. [82] also, second this, claiming to implement a multimodal or combined feature set. Their research on the inclusion of image metadata features to traditional textual features yielded similar improvements. Prior studies relevant to the features used are detailed in Table VI.

<table>
<thead>
<tr>
<th>STUDY</th>
<th>TYPE OF FEATURE</th>
<th>CONTENT</th>
<th>TYPE OF FEATURE</th>
<th>USER</th>
<th>NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAYZICK ET AL. [83]</td>
<td>INSULT WORDS, SWEAR WORDS, 2ND PERSON PRONOUNS, CAPITALIZATION</td>
<td>SENTIMENT/EMOTION</td>
<td>-NIL-</td>
<td>-NIL-</td>
<td>-NIL-</td>
</tr>
<tr>
<td>REYNOLDS ET AL. [84]</td>
<td>NUM (#BAD WORDS), NORM (DENSITY OF BAD WORDS), SUM (OVERALL BADNESS OF POST), TOTAL (#WORDS IN A POST)</td>
<td></td>
<td>-NIL-</td>
<td>-NIL-</td>
<td>-NIL-</td>
</tr>
<tr>
<td>Authors</td>
<td>Tweet Content</td>
<td>Metadata</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dadvar et al. [8]</td>
<td>Profane words, 2nd person pronouns, other pronouns, term frequency – inverse document frequency (TF-IDF)</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dadvar and De Jong [46]</td>
<td>Profane words, 2nd person pronouns, other pronouns, TF-IDF</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dinakar et al. [85]</td>
<td>Profanity, TF-IDF, negativitiy (Ortony Lexicon), subtext (label specific features)</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dadvar et al. [86]</td>
<td>Profane words, normalized 1st &amp; 2nd person pronouns, profanity window, # emoticons, # cyberbullying words, ratio of capital letters in a comment</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kontostathis et al. [87]</td>
<td>Bag of Words (BoW), TF-IDF</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nahar et al. [88]</td>
<td>Binary representation of keywords, normalized value of keywords, pronouns, normalized value of capital letters, messages’ metadata</td>
<td>Normalized values of emotions (happy &amp; angry)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosseinmardi et al. [53]</td>
<td>Profanity, linguistic, image, cyberagression, # wordspysychological measurements</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ptaszyński et al. [89]</td>
<td>Disjoint elements</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Squicciarini et al. [47]</td>
<td>Post length, offensive words, 2nd person pronouns</td>
<td>Normalized sentiment (measured using Semantria)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Van Hee et al. [90]</td>
<td>BoW</td>
<td>Normalized values of emotions (happy &amp; angry)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Van Hee et al. [91]</td>
<td>BoW</td>
<td>Age, gender, location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al-Garadi et al. [92]</td>
<td>Vulgarity, words, acronyms and abbreviations of cyberbullying-specific words, 1st &amp; 2nd person pronouns</td>
<td>Degree centrality, closeness centrality, between-ness centrality, eigenvector centrality, clustering coefficient</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zhao et al. [93]</td>
<td>BoW, word embeddings</td>
<td>Profile Specific Representation (PSR), Subprofile Specific Representation (SSR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escalante et al. [94]</td>
<td>n-grams, TF-IDF</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Haidar et al. [95]</td>
<td>Tweet content, language (English &amp; Arabic), cyberbullying keywords</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Özel et al. [96]</td>
<td>BoW, TF-IDF, emoticons</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rasi and Huang [97]</td>
<td>Bullying bigrams</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singh et al. [98]</td>
<td>Informal language, sexual words, 3rd person singular pronouns, tone, psychological words, words that show personal concern, image category, image type, sexual content</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rosa et al. [99]</td>
<td>BoW, TF-IDF, inverse class frequency (ICF)</td>
<td>-Nil-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hani et al. [100]</td>
<td>N-grams, TF-IDF</td>
<td>Polarity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balakrishnan et al. [101]</td>
<td>Characters, uppercase characters, lowercase characters, hashtags, symbols, user mentions, URLs, media</td>
<td>Sentiment analysis, emotion analysis, verified status, status count, list count, user favourite count, # followers, # following-followers ratio</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
It was found that content-based features were adopted in all papers gathered, sentiment/emotion-based and user-based features were 30%, and network-based features were 23.3% of total papers gathered for Cyberbullying detection. The evolution graphs in Fig. 2, 3, and 4 show how different features used in the Characterization or Feature Engineering process have evolved over the years. Fig. 2 depicts the evolution in the usage of the four types of features over the years. In contrast, Fig. 3 portrays the evolution in the usage of textual and non-textual features over the years. Finally, Fig. 4 displays the evolution of using single and multimodal feature sets over the years. Based on the graph, we observe an apparent tendency that the multimodal features approach is likely to be the direction of future studies for Cyberbullying classification.

As observed in Fig. 3, except for the 2018 study, [99] see the inclusion of contextual/non-textual features in the feature sets used to train the classifiers. Contextual/non-textual features are never used alone but are always used in tandem with textual features. However, in many studies, textual features are used in isolation which is traditionally how most studies were in the earlier times before they evolved to include newer features, both contextual/non-textual features and reengineered textual features in their feature sets. Nonetheless, incorporating contextual/non-textual features improves the ensuing Classification performance [46, 82, 101].

As seen in Fig. 4, except in the 2018 study, [99] evaluated the efficacy of a combined or multimodal feature set, in which case a multimodal/combined feature set is pitted against other multimodal/combined or single feature sets. Cyberbullying detection using ML techniques generally falls into either one of three categories: 1) evaluate the effectiveness of a new/proposed feature by comparing different feature sets, i.e., baseline vs. [baseline + new/proposed feature]. 2) assess the effectiveness of a new/proposed Cyberbullying detection framework/classifier by comparing different classifiers. 3) compare the performance of different classifiers. We discuss the first category in this section, then the second and third categories in the following section on RQ3.

A multimodal/combined feature set is a union between textual and contextual/non-textual features in comparing different feature sets. According to [91], the best Classification performance was achieved with a multimodal/combined approach, merging all the different features and not when the features are used separately or in smaller combinations. According to [82], adding contextual/non-textual features to textual features yielded better results than when using contextual/non-textual features alone or textual features alone, wherein only subpar results were obtained for both cases. Another study by [88] showed that when used on their own, textual features outperformed contextual/non-textual features, contrary to the initial expectations of the researchers. However, the best performance across all classifiers is still observed only with a combined usage of the textual and contextual/non-textual features.
It is observed that the combination of contextual/non-textual features and textual features can also be a novel feature on its own, not necessarily a multimodal/combined feature set. For example, in [94], two inventive features called PSR and SSR are by-products of the amalgamation between textual and contextual/non-textual features, which remarkably improved the performance of the classifiers across all measures.

With the findings above, one may tempt to infer: 1) all classifiers unanimously well on a particular feature set, especially the multimodal/combined feature set; 2) adding just about any contextual/non-textual features to current baseline textual features would significantly improve classification performance. Nevertheless, several studies rebuked the previously mentioned inferences. For example, in [100], it was observed that a classifier might perform well on a particular feature set but not on other sets. This finding shows that while it may appear that all classifiers, without opposition, would perform well on one feature set, usually a multimodal/combined feature set; however, it cannot be generalized. So, it is worth conducting a study to ascertain and not make assumptions based on another study.

Regarding the second inference on guaranteed improvements with the addition of contextual/non-textual features as part of the multimodal/combined feature set, [53] demonstrated that incorporating such features led to non-statistically significant improvements in the performance of the classifiers. On the other hand, [101] dispelled the second claim by showing that only some contextual/non-textual features give meaningful boosts to the classifiers' performances. This study brings up a need for some way to select only important features from a pool of several features, otherwise known as Feature Selection.

In summary, the features used to train the classifiers responsible for the Cyberbullying prediction in SM postings to fall into either textual or contextual/non-textual instances or, in some fringe cases, a combination of both. The justification for creating these instances is always related to the combined process of conceptualization and characterization of Cyberbullying, i.e., what features can we characterize using the available source of information to help understand, denote or give better context to Cyberbullying? Using textual and contextual/non-textual features results in a multimodal/combined feature set; broadly speaking, ML classifiers tend to perform the best using it as opposed to single feature sets. That said, one should always run an experiment to verify the facts because results may vary from the norm depending on the corpus and classifier used.
C. **RQ3:** HOW MACHINE LEARNING (ML) ALGORITHMS CAN BE USED TO DETECT CYBERBULLYING IN SOCIAL MEDIA, WHAT ARE THE COMMON ALGORITHMS USED AND WHICH ALGORITHM(S) IS THE MOST EFFECTIVE FOR THE PURPOSE OF ITS DETECTION?

The prior two sections, 4.1 and 4.2, lay the grounds for understanding the prerequisites for an ML-based automated Cyberbullying detection system. An ML-based automated Cyberbullying detection system is bipartite. The first component is Representation Learning (used interchangeably with Feature Engineering), including the Conceptualization and Characterization of Cyberbullying (or Feature Extraction). The second component is Classification. Classification aims to produce a system adept at categorizing Cyberbullying given a corpus or SM content and generating results of Classification or other statistical measures. The ML-based classifiers, which are the tools for Classification, fall into either one of two categories: 1) Traditional ML classifiers and 2) Deep Neural Network (DNN) or Deep Learning (DL) approaches. Traditional ML classifiers include Naïve Bayes, Support Vector Machine, and Logistic Regression. In contrast, DNN/DL approaches include Convolutional Neural Networks, Multilayer Perceptron, Kohonen, or Self Organizing Map.

Where applicable, Table VII below shows the relevant prior studies with points of contention including types of features used (Content-based (Cb), User-based (Ub), Network-based (Nb), and Sentiment-based (Sb)), type of classifiers used (ML or DL or NLP or Mixed), and their classification algorithm(s).

Regarding the feature types used, we observe that all relevant prior studies (40 papers) collected used content-based features for automatic Cyberbullying detection, followed by the network-based with 30% of the total papers, 25% for user-based and sentiment-based features.

Furthermore, we found that of the papers collected on automated Cyberbullying detection using ML classifiers, 65% of them used pure ML classifiers. However, none used purely the DL/DNN approaches. For the mixed classifiers approach, we encountered 35% of studies. In the matter of Classification algorithms used, we summarize the overall adoption rates (among all relevant 40 papers gathered) by ML and DL approaches in Table VIII.
<table>
<thead>
<tr>
<th>Authors</th>
<th>Platform(s)</th>
<th>Method(s)</th>
<th>Approach(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cornet el al. [119]</td>
<td>Ragnarok, DotA</td>
<td>Cb</td>
<td>Mixed CNN, NB</td>
</tr>
<tr>
<td>Haidar et al. [120]</td>
<td>Twitter</td>
<td>Cb</td>
<td>ML Stacking Ensemble (Simple LR, K-NN, RF, SVM, Bayesian LR, SGD), Boosting &amp; Bagging Ensemble (NB, SVM, K-NN)</td>
</tr>
<tr>
<td>Hani et al. [100]</td>
<td>Kaggle</td>
<td>Cb, Sb</td>
<td>Mixed SVM, NN</td>
</tr>
<tr>
<td>Kumar et al. [121]</td>
<td>YouTube</td>
<td>Cb, Sb</td>
<td>ML RF, SMO, K-NN, NB</td>
</tr>
<tr>
<td>Liu et al. [122]</td>
<td>MySpace, Twitter, Facebook, Formspring, Ask.fm, Instagram, Vine, 2 unspecified sources</td>
<td>Cb, Nb, Sb</td>
<td>ML NB, DT, RF, Tree Ensemble, LR, SVM</td>
</tr>
<tr>
<td>Yao et al. [123]</td>
<td>Instagram</td>
<td>Cb</td>
<td>ML RDFS Classifier, RF, Dynamic LR, TM, CONCISE Classifier</td>
</tr>
<tr>
<td>Zhang et al. [124]</td>
<td>Twitter</td>
<td>Cb, Sb, Nb</td>
<td>Mixed Linear SVM, LR, DT, RF, Gradient Boosting Regression Tree, MLP</td>
</tr>
<tr>
<td>Alasadi et al. [125]</td>
<td>Instagram</td>
<td>Cb</td>
<td>ML NB, Baseline classifier (Bayesian Fusion Model with ( \lambda = 0 )), Bayesian Fusion Model</td>
</tr>
<tr>
<td>Ali and Syed [126]</td>
<td>Twitter, Formspring</td>
<td>Cb, Sb</td>
<td>ML RF, NB, SVM, LR, Ensemble Classifier</td>
</tr>
<tr>
<td>Balakrishnan et al. [101]</td>
<td>Twitter</td>
<td>Cb, Ub, Nb, Sb</td>
<td>ML RF, J48</td>
</tr>
<tr>
<td>Islam et al. [127]</td>
<td>Facebook, Twitter</td>
<td>Cb</td>
<td>ML DT, NB, RF, SVM</td>
</tr>
<tr>
<td>Kumar and Sachdeva [128]</td>
<td>Twitter, Facebook</td>
<td>Cb</td>
<td>ML MIIL-DNN, NB, DT, MLP, SVM, CNN, LSTM</td>
</tr>
<tr>
<td>Van Bruwaene et al. [129]</td>
<td>Instagram, Facebook, Pinterest, Twitter, Gmail, YouTube, Tumblr, other unspecified resources</td>
<td>Cb</td>
<td>Mixed ZeroR, SVM, XGBoost, CNN</td>
</tr>
<tr>
<td>Wang et al. [130]</td>
<td>Instagram, Vine</td>
<td>Cb</td>
<td>Mixed SVM, NB, LR, RF, LSTM, Text-CNN, HAN, MMCD Framework (BiLSTM + HAN + other embeddings)</td>
</tr>
<tr>
<td>Ahmed et al. [131]</td>
<td>Facebook</td>
<td>Cb</td>
<td>ML DNN, Ensemble Classifier</td>
</tr>
<tr>
<td>Alsubait and Alfageh [132]</td>
<td>YouTube</td>
<td>Cb</td>
<td>ML Multinomial NB, Complement NB, LR</td>
</tr>
<tr>
<td>Azeez et al. [133]</td>
<td>Twitter</td>
<td>Cb, Nb, Ub</td>
<td>ML Multinomial NB, K-NN, LR, DT, RF, LinearSVC, AdaBoost, SGD, Bagging Classifier, Ensemble Classifier</td>
</tr>
<tr>
<td>Ge et al. [135]</td>
<td>Instagram</td>
<td>Cb, Nb, Ub</td>
<td>Mixed LR, SVM, XGBoost, CNN, LSTM, SelfAtt, HAN, SIDC, Soni &amp; Sign (temporal model), HANCD, TGBully (temporal model)</td>
</tr>
<tr>
<td>Ghosh et al. [136]</td>
<td>various unspecified sources</td>
<td>Cb</td>
<td>ML SVM, LR, RF, PA</td>
</tr>
<tr>
<td>Chong et al. [137]</td>
<td>various unspecified sources</td>
<td>Cb</td>
<td>ML Rule-based and Zero-shot classifier</td>
</tr>
</tbody>
</table>

The current state of the art shows that traditional ML classifiers are more popular than DNN/DL approaches. Lastly, for the Classification model evaluation metrics used, we summarize the usage rate as follows: Accuracy 67.5% (of 41 total papers gathered, applied to the rest of this list), F/F1-measure/score 67.5%, Recall 62.5%, Precision 60%, Area Under Receiver Operating Characteristic Curve (AUC) 27.5%, True Positive (TP) 15.5%, Confusion Matrix: 7.5%, Error 7.5%, True Negative (TN) 5%, False Positive (FP) 5%, False Negative (FN) 2.5%, and other evaluation metrics: 10%.
Most of the studies' dataset is manually labelled by either field domain experts or non-professionals from crowdsourcing platforms of Amazon's Mechanical Turk and CrowdFlower [46, 56, 84, 86, 93, 112, 113, 120-125, 129, 131, 134, 136]. Novel labelling techniques also used automated code observed [110, 133] and a score-based system [119]. However, labelling is not always necessary, such as in [101], whose authors used an annotated dataset from a previous study. Romsaiyud et al. [111] worked with both annotated and non-annotated variants of the dataset and concluded that the labelling of datasets led to higher Classification accuracy.

We notice that features extracted fall into one of four broad categories: content-based features, network-based features, sentiment-based features, and user-based features. Moreover, using multiple features together tends to give the best performance compared to using them in isolation [46, 86, 101, 108, 114, 122, 124]. Different features are selected based on the type of classifier used in the studies, even though its underlying type may be the same. For example, the textual content-based features commonly used are Natural Language Processing (NLP) features such as n-gram, BoW, and TF-IDF for traditional ML. For DNN/DL classifiers, it is customary to use textual content-based features in the form of word embeddings such as Word2Vec, Doc2Vec, and GloVe [110]. In [115], an unorthodox approach called Linguistic Inquiry Word Count (LIWC) was used to extract features to avoid a skewed perception that profanity is a defining characteristic of Cyberbullying.

Work in [137] adopted the Zero-shot topic classifier and rule-based methods using Natural Language Processing (NLP) for comparing the accuracy of classifying cyberbullying. The result in [137] shows that the information extraction rule-based model applied provides limited assistance in categorizing cyberbullying behaviours. The Zero-shot model presented a better rate of recognizing the flaming behaviour compared to rule-based modelling, but its accuracy rate dropped when identifying the other cyberbully behaviours. Nevertheless, the finding of [137] concluded that Zero-shot text classification model is useful for predicting flaming behaviour. Additionally, most studies suggest that non-textual and textual features used in a Multimodal/Combined feature set seem to be the trend. The addition of such features led to statistically significant enhancements in the performance of ML classifiers [46, 86, 96, 101, 108, 114, 122, 124, 130]. When it comes to features, however, adding more and more in combination may not always be suitable for the given context, so sometimes less is more. To [133], the approach proposed can achieve high Classification accuracy with the bare minimum number of features, making the model ideal for large-scale datasets. Strangely as well, some features work better in one language but not as good in other languages, so besides context dependency, there is also some level of language (that of the dataset(s) used) dependency when it comes to features used in a study [134].

### 5 Implications for Practice

Regarding the Conceptualization of Cyberbullying, we saw the delineation of the differences between Traditional Bullying and Cyberbullying through the lens of various meta-themes such as Intent, Repetition, Power Imbalance, Accessibility, Anonymity, and Barriers to Disclosure. Through a simple one-on-one comparison between the two, it is clear that it would be folly to assume that Cyberbullying is the online equivalent of Traditional Bullying due to the differences in conceptualizations between the two. That said, researchers looking to improve the initial annotation process of Cyberbullying/Non-Cyberbullying should be looking into key factors such as Repetition and Intent in...
deciphering whether the text is Cyberbullying or Non-Cyberbullying. Non-Cyberbullying is a blanket term that can include posts containing harmless pranks, satire, or sarcasm to posts that are non-bullying altogether. Traditional Bullying is a subset of Non-Cyberbullying, so the distinction between Cyberbullying and Traditional Bullying is crucial to the success of the forthcoming ML procedure. Suppose researchers only filter through posts with cyberspace-specific meta-themes such as Accessibility and Anonymity. In that case, there is a chance that they will mislabel a Non-Cyberbullying post as a Cyberbullying post simply because Accessibility and/or Anonymity factors are present and vice versa. This finding indicates that any volunteers or experts who perform labelling on a dataset should be briefed beforehand in taking such cautions when evaluating an SM post based on the six different meta themes.

We learned two lessons for the Characterization of Cyberbullying, otherwise known as the process of Feature Engineering or Representation Learning. The first lesson is that contextual/non-textual features complement textual features. They are not replacements. Secondly, we have also established that using a multimodal/combined feature set, in comparison to single feature sets, greatly improved the performance of ML classifiers. However, there should not be a misconception that any contextual/non-textual features would suffice in its supplementary action to textual features in increasing the performance of said classifiers. Some contextual/non-textual features are more relevant than others; this is where the importance of Feature Selection comes in, to select only the significant contextual/non-textual features and discard irrelevant ones. Feature Selection has been shown repeatedly in several studies to benefit the forthcoming Classification step significantly by ensuring that the classifiers are trained with the cream of the crop, regardless of whether it is contextual/non-textual or textual features. All in all, researchers looking to: i) perform Feature Engineering with different pre-existing contextual/non-textual features and build new relevant contextual/non-textual features; ii) improve present textual features; iii) use Feature Selection to select the best features by comparing different feature combinations to see which one works the best; and iv) use contextual/non-textual and textual features in a multimodal/combined feature set, never in isolation.

Concerning the Classification of Cyberbullying, the two most important findings are the context-dependent effect on selecting both ML classifiers and the subsequent Evaluation Metrics. Traditional ML approaches appear to outshine the more complex DNN/DL models for modestly-sized datasets. Their training requires large amounts of data, the absence of which will result in overfitting and unrealistically high performance, which is undesirable. This shows that in considering which ML classifiers to deploy in one’s system, one should always decide based on the context. As observed in the case of datasets that are not large, complex solutions are not necessarily better. Sometimes it is worth looking at more straightforward approaches before contemplating using more complex ones.

In summary, when performing Classification, selecting ML classifiers and performance metrics best suited for the context is recommended instead of going for what is popular or commonly used. Keeping an open mind and experimenting with different ML classifiers and performance metrics will allow researchers to determine the best classifiers for their specific data context and have metrics that can represent how well their classifiers are performing in that particular context. Under the proper context, DNN/DL approaches outperform Traditional ML classifiers. Therefore, researchers should explore other DNN/DL approaches.

6 Conclusion

This study has demonstrated a deep dive into the state of the art of papers on Cyberbullying detection in social media using ML classifiers through a systematic literature review to provide insights into the three pillars: Conceptualization, Characterization, and Classification of Cyberbullying. Our results show that: 1) Cyberbullying is distinct from Traditional Bullying though they share some commonalities. 2) The combined usage of contextual and textual features in a multimodal feature set can improve Classification accuracy. 3) The selection of ML classifiers and performance metrics is context-dependent. In isolation, these results have been presented in prior works multiple times, so they are not unique to this study. However, this study offers a condensed view of all the results in a continuous narrative from one pillar to another; when observed in separation, the whys and hows may not be adequate for a holistic understanding of the subject matter.

A. Limitations

Suppose there should be one constraint in this study. In that case, it is the fact that the inclusion and exclusion criteria set in the SLR are far too limiting to retrieve the breadth of studies that are essential for making up state of the art on papers related to Cyberbullying detection using ML in its complete totality. For instance, we only considered papers either using Traditional ML classifiers, DNN/DL approaches, or a mix of the two. Furthermore, we excluded those papers that used other soft computing techniques such as Fuzzy Systems, Evolutionary Computing, and Swarm Intelligence. This exclusion potentially hides critical takes on feature engineering and evaluation metrics used in those studies, creating a distorted and narrow worldview for readers.
B. SUGGESTIONS FOR FUTURE STUDY

Hence, future iterations of this study should take an all-inclusive approach, generalizing the inclusion criteria to allow for more studies to be screened through the SLR. Additionally, we believe that another direction for future studies is to consider using the term Cyberaggression instead of Cyberbullying as an inclusion criterion in the SLR and the title piece of research. Potentially, Cyberaggression might be a more suitable and all-encompassing term than Cyberbullying. It is because it suggests a digital equivalent of Traditional Bullying, which in turn means that they should share similar core criteria, which in the case of Cyberbullying is not so clear cut at times.

ACKNOWLEDGEMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES


