Cyberbullying in Digital Era: History, Trends, Limitations, Recommended Solutions for Future

Amit Kumar Tyagi [0000-0003-2657-8700]
Department of Fashion Technology, National Institute of Fashion Technology, New Delhi, Delhi, India
amitkrtyagi025@gmail.com

Terrance Frederick Fernandez
Department of Information Security, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, TN,
frederick@pec.edu

Meghna Manoj Nair
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
mnairmeghna@gmail.com

Abstract. The digital and virtual world has taken a toll on the lives of the vast majority of the population across the globe. Even though it has resulted in numerous technological advancements and has enhanced the scope of socialising and staying connected with people from different parts of the earth, it has a variety of drawbacks and negative aspects which seem to dwindle the affected person both physically and mentally. One such adversity is the reality of cyberbullying, which millions of people who extensively use digital platforms and social media are exposed to. Cyberbullying is a very broad field of adversity and pressing concern in the twenty-first century, especially since it's the digital era. Cyberbullying occurs in varied forms and affects people in numerous ways with different intensities. It includes cracking into an individual's profile, posting unnecessary comments to defame people, malicious use of social media platforms, etc. Techniques and algorithms to bring a halt to cyberbullying are one of the primary areas researchers and programmers need to focus on. In the earlier stages of the digital era, cyberbullying was considered to be an event of the occurrence of a mishap due to peer pressure. As virtual platforms evolved massively, cyberbullying has taken the spotlight resulting in the harassment of naïve individuals. The fact that there's an absence of face-to-face confrontation has complemented the cruel aims and deeds of cyberbullies. Cyberbullies have initiated the use of technology in the disguise of a weapon to humiliate and hamper the growth and success of people out there. Another trend that has been closely observed is the conversion transition and huge jump from physical bullying to cyberbullying wherein, social media and similar digital tenets which were meant to play a positive role in the lives of people started amplifying the negativities of virtual bullying. This chapter talks about how cyberbullying has evolved over the decades, the limitations and drawbacks of cyberbullying, and solutions and methodologies to prevent this mishap.

Keywords: Cyberbullying, Threat, Impacts of Social Networking, Digital and Virtual World.

I. INTRODUCTION

Bullying has been an issue that has lasted for long and in the majority of places, it isn't seen as a problem or mode of suppression which actually requires major attention, especially in the earlier stages. However, things have taken a turn and society has recognized bullying as an issue that requires and warrants attention. Over the years, different types ad forms of bullying have taken roots and with technological and scientific advancements, people are being bullied in the virtual world today. This is called Cyber Bullying wherein, bullying is carried out by a diverse range of technological gadgets available [1].

Based on numerous surveys and research conducted on students across different countries, it has been observed that nearly 91% of the kids aged between 12 to 15 years use the internet majorly and the 57% of these children were treated with disheartening and angry comments [2].

979-8-3503-4821-7/23/$31.00 ©2023 IEEE

Cyberbullying takes place through mobile phones, PCs, tablets and other tech gizmos. It may happen through text messages, apps, forums, and social media. In other words, cyberbullying is bullying with the use of technological advancements. Some of the common examples of cyberbullying include spreading false accusations, posting illicit pictures of others on social media platforms, sending threats and absurd comments, making use of fake accounts to impersonate another person, etc. The key point to be noted here is that cyberbullying leaves a digital footprint, i.e., a record that can be tracked and decoded to provide evidence against uncanny abuse [3].

The word "bully" can be traced back to the 1530s which in its simplest sense refers to aggressive interaction between two people – the intimidator and the victim. Some of the researches have stipulated that the competition of survival and inner feelings of egoism are some of the driving factors for bullying. Though bullying and cyberbullying can take similar roots from the perspective of the intention, they do have major differences too. In broader terms, with the evolution of technology bullying has taken stronger and deeper roots in society [4]. Analyses and studies have been conducted in the field of cyberbullying and traditional bullying and it was observed that the repeated trend in negative action was majorly found in those youngsters and adults who had disturbed family structure and functioning. It was also noticed that the victims were mainly those who can't defend themselves in a strong and opposing manner [5]. In the modern world, where the new-fangled and golden agers spend a majority of their time on virtual platforms, social media and discussion forums, cyberbullying has taken a strong stand throughout and it's the need of the hour to reduce and eliminate its presence for a healthy virtual living. This chapter gives insights into the evolution and history of cyberbullying along with detailed descriptions of its trends, limitations and scope of reducing this illicit component.

1.1 Cyberbullying

Cyberbullying refers to the action of bullying and harassing individuals or groups over digital platforms through gadgets like mobile phones, computers, tablets, etc. This has been one of the highly diminishing factors with regards to all those platforms and applications prevalent on the internet. After the outbreak of the pandemic, people across the world have taken up digital solutions for their sustenance and profession and this rapid increase in the use of cyber solutions has further aggravated the cyberbullying crises. The term cyberbullying was prominently used in 1998 initially. In those days, the term was used to reference actions that involve posting mean and aggressive comments and messages about an individual through anonymous means. However, with the evolution of the internet, the definition and roots of cyberbullying have evolved. In the current scenario, cyberbullying can be described as the intended and repetitive harm and aggression inflicted on the targeted individual through digital and tech gizmos [6]. There are a couple of parts of cyberbullying that separate it from conventional tormenting, which makes it an exceptional worry for guardians and educators. A portion of these distinctions include:

- Secrecy: While casualties generally know who their harasser is, online domineering jerks might have the option to conceal their characters on the web. The obscurity of the web can prompt crueller or harsher maltreatments from the domineering jerk, all while the casualty has no methods for finding who their harasser is.
- Persevering: Bullying ordinarily closes once the casualty is taken out from the negative social circumstance. Be that as it may, cell phones, workstations, and different gadgets have caused it feasible for individuals to speak with one another during the entire hours and from almost any area. Cyberbullies might have the option to torture their casualty 24 hours of the day, seven days of the week, making it hard for the casualty to get away from it by returning home or in any event, evolving schools.
- Public: With customary harassing, frequently just individuals that connect with those elaborate will know about the maltreatment. Nonetheless, when a substance is posted or shared on the web, it's conceivable that anybody may see it. This opens up the casualty to more expected disparagement or agony from outsiders. This is compounded by the obscurity managed by virtual spaces: while tormenting face to face might be done clandestinely or out of view to maintain a strategic distance from discipline, cyberbullies need not dread being seen in the demonstration if their characters are not known.
- Perpetual: Because the online substance is difficult to erase, cyberbullying may harm the victim's, or perhaps the bully's, notoriety forever. Regardless of whether the substance is taken out or erased from the first site, somebody may think that it is posted somewhere else later. This may adversely affect future work, school confirmations, or connections for casualty and menace the same.
- Not entirely obvious: Cyberbullying might be more earnestly for instructors, managers, and guardians to find since they might not approach understudies' online exercises. They will be unable to catch or see the maltreatment occurring. Except if somebody approaches, guardians and educators may never realize that harassment is occurring.

1.2 Examples of Cyberbullying

As innovation has been created in the course of the most recent twenty years, cyberbullying has become an undeniably bigger issue. The gigantic fame of cell phones, different texting applications, and the ascent of web-based media have opened up an ever-developing number of ways for cyberbullies to hurt their objectives.

- Badgering: Much like disconnected provocation, online badgering includes sending harsh or hostile messages to an individual or gathering. Provocation requires incredible exertion concerning the domineering jerk to hurt the person in question. Further, it is purposeful, rehashed, and consistent. The casualty will frequently have no respite from the harasser. Particularly throughout some stretch of time, these messages can negatively affect the casualty's confidence or certainty.
- Cyberstalking: Cyberstalking is a type of badgering. These messages are frequently not, at this point simply hostile or impolite, however additionally undermining in nature. Messages may heighten to undermine the casualty's actual security. Cyberstalking can rapidly prompt face to face provocation or following.
- Rejection: Avoidance includes intentionally segregating the person in question. This may include forgetting about them from web-based media gatherings, talk rooms, messages, occasions, or exercises. It might mean deliberately having discussions via web-based media stages or applications that the casualty does not approach, or that they see, but can't join. The gathering may then proceed to express savage or discourteous things about the prohibited individual despite their good faith.
- Excursion: Excursion is the point at which the harasser openly shares private messages, pictures, or other data about the casualty on the web. This is managed without the casualty's information or assent, and is intended to humiliate, disgrace, or mortify them. The data might be unimportant or more private and genuine, yet in any case, it is a type of excursion.
- Disguising: Disguising happens when the domineering jerk, or conceivably even domineering jerks, expects another character to namelessly bother the person in question. They may either imitate another person, utilize a genuine individual's record or telephone number, or make a totally phoney personality. Regularly, the domineering jerk will know the casualty well in the event that they want to conceal their personality. The harasser may disturb or cyberstalk with a casualty. This is commonly done trying to interest themselves or mortify the person in question.
- This puts forward an overview of the cognitive theory from social aspects along with the online disinhibition effect and their impact on cyberbullying:
- Bibliometric Analysis: It is made use of quantitative and qualitative methods with statistical information to analyse and study the contextual matter put forward by a publication.
- Bullying: Refers to immature and hostile behaviour against humans leading to drastic physical and mental impacts on the victims.
- Cyberbullying: Confers to an unethical attitude to adversely affect and harm other humans through means of gadgets, gizmos, and social platforms.
- Moral Disengagement: The process which refers to oneself being unable to recognize and identify the ethical and moral norms and regulations which one

must follow and these individuals lack empathy, sensitivity and pity.

- Power Imbalance: It is the line of differentiation between bullying and cyberbullying which goes around the fact of a malicious activity that is continuously dispersed with time and is exposed to many users who may turn out to be active/passive bullies.
- Artificial Intelligence: It's a technically advanced and enhanced field of engineering that analyses and focuses on the behavioural functionalities which can be stipulated from a variety of machines and devices.
- Bullying: An agitating and disruptive behaviour of people who wish to suppress their fellow beings by physical and mental abuse. It's very often found in juvenile contexts.
- Digital Psychology: It refers to a multi-faceted and interdisciplinary tactic towards psychology along with which the study of humans and their interaction with research on nascent technologies take place.
- Embodied Conversational Agent: They consist of characters that are created by informatic tools and portray features that are solely dedicated to the physical and face to face interactions between humans.
- Machine Learning: This is a technique and concept of analysing and studying data with features related to self and automatic learning experience to identify complex details and data.
- Peer Support: It's a situational and scenario-based approach wherein respect and pertaining features classify relationships among humans and people with similar experiences.
- Virtual Reality: A digital environment that is capable of emulating reality through which humans can indulge in and connect with each other with the help of gadgets, visors, etc.
- Psychosomatic Problems: It is a disease evicted among humans which involves a physical/mental disability.
- Social Media: They consist of internet-related means of communication and interaction and include blogs, social networking, etc.
- When comparing cyberbullying to traditional bullying (refer table 1), there are a number of differences that stand out, and they include:
- Anonymity: In traditional bullying, anonymity is a factor that can't be achieved easily by the bully; however, it has made it easier for cyberbullies to mask themselves in the anonymity provided by the virtual world. This is one of the main reasons why cyberbullies relish and proliferate at a rapid rate. All the while, the victim has hardly any chance of identifying the harasser in a virtual environment.
- Relentless: Traditional bullying often comes to an end once the victim steps out of the negative social impression. On the contrary, cyberbullying often attack and harass the victim relentlessly and are able to trace and track their activities leading to a very petrifying situation.
- Easily overlooked: Cyberbullying can be quite difficult to trace and track especially among students. Unless and until a concerned elderly or authority figures it out, many of the individuals of the society might not even be aware of the fact that they're being cyberbullied.
- Reach and Publicity: Traditional bullying is very often done in private and doesn't really harm the public image of the victim. However, in the case of cyberbullying, the rampant spread of the issue and the news would cover all the social media platforms, diminishing the personality and reputation due to the impact.

For the above-mentioned pointers, cyberbullying seems to have flourished over the years and is increasing at a rapid rate due to the complementary support of virtual connections and platforms. The point to be highlighted here is that despite the support and upliftment provided by the Internet, there are a number of people who make use of it for spiteful purposes. The diagram has been explained in Fig 1. Explains the repetitive cycle of how the bullying process takes place and how it affects and impacts people.

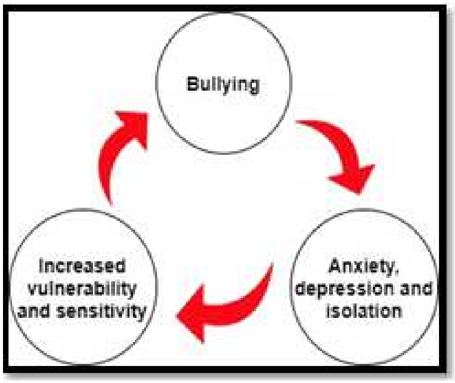
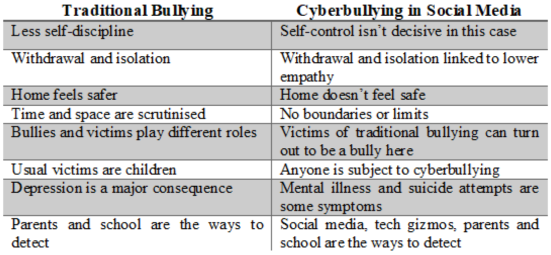

Bullying
Anxiety, depression and isolation
Increased vulnerability and sensitivity

Figure 1: Bullying Cycle

Table 1 explains the differences between the two types of bullying which have evolved with time due to advanced technologies and social networks.



Traditional Bullying	Cyberbullying in Social Media
Less self-discipline	Self-control isn't decisive in this case
Withdrawal and isolation	Withdrawal and isolation linked to lower empathy
Home feels safer	Home doesn't feel safe
Time and space are scrutinised	No boundaries or limits
Bullies and victims play different roles	Victims of traditional bullying can turn out to be a bully here
Usual victims are children	Anyone is subject to cyberbullying
Depression is a major consequence	Mental illness and suicide attempts are some symptoms
Parents and school are the ways to detect	Social media, tech gizmos, parents and school are the ways to detect

Table 1. Traditional Bullying vs Cyberbullying

1.3 Organisation of the Work

This work can be organised as: Section 2 discusses history or background and type of Cyberbullying. A few theoretical aspects of Cyberbullying is explained in section 3. Further, a few points for cyberbullying and Targets at Workplace are explained in section 4. Further, various solutions and Recommendations are explained for Cyberbullying in section 5. Then, Artificial Intelligence to Combat Cyberbullying is explained in Section 6. Section 7 discusses the theoretical framework for cyberbullying. Then, several implications of Cyberbullying at Work in this Smart Era with Future Research Directions are discussed in section 8. In last, section 9 concludes this work in brief.

II. HISTORY/ BACKGROUND AND TYPE OF CYBERBULLYING

The origin of the word bully dates back to the 1530s and the very essence of the term bullying consists of both a bully and a victim/target. The bully indulges in practices to harass the victim physically/mentally. These practices may be direct, verbal or indirect. One of the major reasons for the spark of origin and evolution of bullying at an exponential rate is mainly due to the desire to survive and bring down their competitors in life [4]. Various researches and studies have shown that four out of five teenagers have been subject to cyberbullying and teen life being one of the most crucial stages in life, can adversely impact the youngsters [8]. A multinational study conducted across a few countries in 2005 has revealed how consistent and concurrent commonplace bullying is and how adverse its effects are. Results showed that the number of bullying youngsters have been exposed to in the 28 countries had several variations from different perspectives and parameters. Fig. 1 displays the trend in the cycle observed in bullying cases. In the early days, bullying being physical in nature had a number of disadvantages and impacts on the victim. However, in the modern era, cyberbullying through social media and other virtual platforms seem to have a wider reach and even more drastic impact.

The very definition of cyberbullying contains a plethora of mannerisms and behaviours which are carried out and perpetuated using electronic gadgets and gizmos and this has been an issue of extreme concern due to the rapid rate at which people are taking undue advantage of harassing and torturing others because of the anonymity factor involved. There are many different forms of cyberbullying tactics used by perpetrators. Some of the most common forms are as follows:

- Cyberstalking is one of those techniques and methods through which the harasser consistently threatens and sends inapt content which is offensive and suppressive. Many times, this manifests from virtual to physical bullying.
- The practice of posting and sharing flares (inappropriate messages and content) which often follows virtual fights and debates, popularly called 'flaming' often falls under cyberbullying. The victim is attacked through different means of communication including those emails, social media platforms etc.
- Another approach for cyberbullies is to ignore and leave out the targeted people from chats, online groups and discussions, singling them out and this can take shape in workplaces, social media groups, among friends, etc.
- One of the other common practices observed in cyberbullying is 'outing', wherein the bully leaks out personal and private data and information of the targeted to defame and humiliate the victim.
- Some cyberbullies often take fake identities of others, called Masquerading, with the aim of bullying and hurting the sentiments of the targeted people and forwarding inapt messages to them, while maintaining his/her anonymity.

Denigration is the act where an individual is criticized in a derogatory manner by the cyberbully.

Types of Cyberbullying

Cyberbullies have devised numerous ways to confront and suppress the targeted victims through cyberbullying, although the intention remains to be the constant parameter. The techniques used by the bullies are aimed to hurt the sentiments, emotions and image of the victim on social media platforms either for fun and satisfaction or on the note of revenge. The different types of cyberbullying are as follows [7]:

- Exclusion: In this type of cyberbullying, the victim is left out deliberately and on purpose from joining conversations, chats or group calls on social media platforms. This mainly creates a sense of loneliness desolation and the victim develops weird emotions to himself/herself and those around him/her in extreme conditions.
- Harassment: This type forms the base root for any sort of bullying and is a broad category and concept. It usually infers to a consistent and ongoing pattern of hurting or threatening the victim through texts, messages, etc. to harm/hurt them.
- Outing: Also known as doxing, this form of cyberbullying caters to revealing personal details and other sensitive information of the victim without their consent with the sole purpose of embarrassing/humiliating them. It can range from publicizing personal photos or other essential documents online.
- Trickery: This form of cyberbullying is extremely similar to that of an outing but it has an added element of deception here. The bully is likely to trick the victim into believing that they're close friends and would lull the victim into a wrong sense of security. This would allow the victim to initially take over the victim's trust and then abuse the victim on similar grounds.

Cyberstalking: This is a serious and quite dangerous instance of cyberbullying wherein the bully would closely track and monitor the victim through different virtual means leading to false accusations, threats, etc. This is often considered a criminal offence leading to jail cases for the bully.

Draping: In this form of cyberbullying, the bully would hack the victim's account and take control over it to post unnecessary posts, comments, etc. and has the potential to be quite harmful as it can diminish the victim's image to a great extent.

Trolling: This usually takes place when the bully wishes to upset the victim or a group of victims by circulating inflammatory and viral contents circling the victim. Though this may not always be considered a cyberbullying attempt, it can get serious when done with malicious and disrespectful content.

Flaming: It involves publicising or directly sending out insults and mean comments to the victim with a more directed approach to provoke the victim.

The above-mentioned types of cyberbullying are the most common and majorly present types of virtual bullying. It can be noted that in the above-mentioned types, the main motive or intent of the bully revolves around the harsh fact of cruelty and abnormality against the victim which needs to be brought to a halt and must be penalised. Figure 2 shown below elucidates the different ways in which a bully is likely to harass a victim through online means.

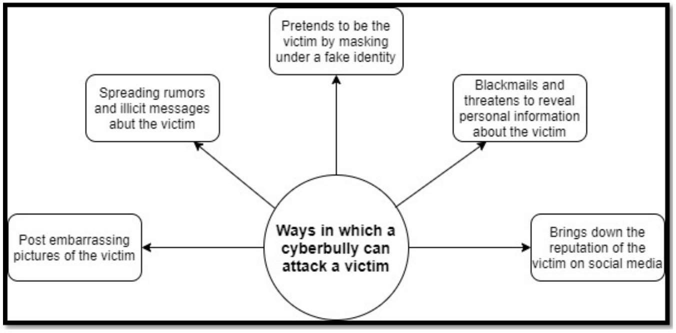

Pretends to be the victim by masking under a fake identity
Spreading rumors and illicit messages abut the victim
Blackmails and threatens to reveal personal information about the victim
Post embarrassing pictures of the victim
Ways in which a cyberbully can attack a victim
Brings down the reputation of the victim on social media

Figure 2: Different ways a cyberbully attacks a victim

III. THEORETICAL BACKGROUND FOR CYBERBULLYING

Important, essential and sensitive topics like cyberbullying call for a thorough background study and background check on the same. It's necessary to consider the different parameters and influential factors from various perspectives to assess the intensity and assign suitable measures to eradicate the problem. Studies carried out among adolescents across different countries have estimated that the frequency of cyber victimization is 9% and that of cyber aggression is 5%. Around 29% of teenagers have admitted to being treated in a hurtful and vulgar way in the virtual world. Recent studies and analyses on cyberbullying in Latin America have shown a steep rise in the number of cyberbullying cases. Around 39% of the population in Argentina reported having been exposed to virtual victimization, of which 13% were frequently prone to the same. While in Spain, the numbers are still higher, reaching a peak of around 44% of cyberbullies/aggressors. The common trend and pattern which has been observed are that as adolescents and teenagers grow, they feel more suppressed and only 1 in 10 victims of cyberbullies are likely to report this issue. A few other reviews and studies have shown a heterogeneous and inconsistent response to cyberbullying based on gender. Over the decade, research in this sensitive field have shown that over the decades with rapid advancement in technology that promotes social media usage and the internet, cases have proliferated and cyberbullying has rooted its foundation based on socio-ethnic cultures in a few regions too [10]. However, one must know that cyberbullying can occur to people from different age groups belonging to different regions. Studying and analysing cyberbullying among adults is a gruelling task. In fact, the very definition of cyberbullying possesses a number of different mannerisms and behaviours which are carried forward through tech gadgets and gizmos. It has been observed that cyberbullies make use of different ways and techniques to threaten and harass bullies. Cyberstalking is very commonly used along with the unhealthy practice of sharing and forwarding flares. Another approach for cyberbullies is to completely ignore and isolate the person of the target (outing) or to fake the identities of others through masquerading.

IV. CYBERBULLYING AND TARGETS AT WORKPLACE

There used to be a time when technology and science were revolutionising the workplaces in different fields. Though there are several advantages with regards to information and communication technologies, cyberbullying and other technologically illicit practices are prevalent in work atmospheres across the globe. Public interest in cyberbullying has majorly been stimulated by media publicity which is often linked with teenagers, suicide, etc. However, cyberbullying is an issue that affects and impacts a much broader proportion of society. Findings have stated that around 52% of women in New Zealand have been harassed virtually and studies conducted in the United States of America have exposed that people have been experiencing cyberbullying gravely during their adulthood. It has been recently noticed that more than 1.3 billion people have been working virtually and due to lack of guidance and proper support, the available communication technologies are being used for cyberbullying and other unhealthy practices [11]. Very often, people consider that cyberbullying is an issue faced by teenagers and children who aren't well aware of their social media responsibilities, but in the twenty-first century, the workplace is highly immune to cyberbullying. It has been observed that cyber incivility at the workplace is mainly used for intimidating co-workers and for controlling their environment. However, if the victim knows how to advance and take control of this environment, then they can easily get through the situation. Employees or workers who are being harassed/bullied virtually can follow the below-mentioned steps to overcome the trouble they're facing:

- Respond to messages carefully: When a co-worker says something inflammatory or tries to attack you through virtual means, understand the whole situation and get a hold of your thoughts irrespective of how harsh the post could have hit you. Only if the situation calls for a response, a response is required, else ignore the messages.
- Keep responses rationale: Although the co-worker taking up the role of a bully would try to provoke the victim in many ways, it's always advisable to keep a calm response to the messages rationally to keep the situation under control.
- Convey a clear picture of expectation: Though the victim must respond to the messages only when required, it is always important to note that the victim must put it forward to the bully, that they don't encourage this behaviour and would take necessary actions to condemn it.
- Consolidate pieces of evidence: The victim must always gather pictures, copies, posts and comments as evidence to get proof of the bullying the worker has gone through.
- Report to the authorities: If the situation gets out of control and the bully doesn't show a sign of bringing an end to the harassment, it is advisable to report it to the concerned department or team of the victim's workplace.

As innovation has been created in the course of the most recent twenty years, cyberbullying has become an undeniably bigger issue. The gigantic fame of cell phones, different texting applications, and the ascent of web-based media have opened up an ever-developing number of ways for cyberbullies to hurt their objectives. The dreadful consequence of cyberbullying is the impact it can have on the victim leading to self-harm, destroyed relationships, depression, low self-esteem, and so on. Some of the symptoms and implications which convey that a person has been cyberbullied either at the workplace or any other platform is:

- Extremely low self-esteem for a person
- Self-isolation and withdrawal from family and friend circles
- Reluctance to allow peers to check out their phone
- Emotions of rejection and willingness to stay at home often
- Weight loss and other physical symptoms
- Causing self-harm through different means
- Change in personality from several perspectives

V. SOLUTIONS AND RECOMMENDATIONS FOR CYBERBULLYING

Cyberbullying is one of the prime concerns in today's age, especially because of its impact and steep increase over the years. However, one of the major shortcomings and limitations in Cyberbullying is the absence and dearth of sufficient theoretical foundations which would provide a stable base for developing technologies to put a stop to cyberbullying. After obtaining a detailed analysis on how every online user is vulnerable to cyberbullying, its prevention is a matter of both awareness and response because cyberbullying is turning out to be a burning issue for people of all age groups in society. Though it can get extremely tedious and nearly impossible to eradicate cyberbullying altogether, there are several strategies that one can adopt to reduce the frequency of occurrence and the impact of cyberbullying. Some daily life strategies which one can adopt to prevent cyberbullying are:

- Develop a healthy climate of communication with peers: It's always better to be heard when in situations of trouble and stress. The victim should act wisely and open up about such grave issues to a peer of theirs be it a trustworthy friend or a loyal family member. This would develop and instil a sense of support in the victim and give them the confidence that they're not alone in this race against cyberbullying.
- Protect social media accounts and passwords: Safeguarding passwords and using unguessable passwords are extremely important to avoid any sort of data leakage and cyberattacks. This would reduce the chance of provoking the cyberbully from posting or morphing illicit details obtained from the victim's account.
- Never open unknown messages or links: It's important to note that online users must never click on links or open up messages which they have received from unknown accounts. Very often such messages are likely to contain viruses and other malware which could extract all information from the victim device and send it to the bully. The cyberbully will then be able to harass and destroy the image of the victim in the virtual world.
- Log out of accounts on public devices: Apart from safeguarding passwords, it is equally important to keep accounts safe by logging out of social media accounts after use on public devices and computers to reduce the chance of allowing anyone to extract details from the account and use it for malicious needs.
- Counselling: All institutes and organizations must have a well-trained department dedicated to counselling services for supporting and providing a helping hand to those employees who have been exposed to severe circumstances of cyberbullying.
- Training: Frequent and full-fledged training sessions and workshops at the school, institute and community level must be carried out to create awareness on this prime issue. The structure and framework of the session must be such that it provides a proactive measure to all attendees on how to combat cyberbullying.

VI. ARTIFICIAL INTELLIGENCE TO COMBAT CYBERBULLYING

In the 21st century era, the development of science and technology has resulted in the creation of certain fields with extreme potential like Artificial Intelligence (AI). AI refers to simulating human intelligence and behaviour through machines and other devices which can be obtained through programming and training the models accordingly. It also correlates to giving the programmed machines the capability to think, learn and solve problems. AI is currently being used in a plethora of fields including healthcare, education, robotics, image classification, etc. However, AI can also be incorporated to strategize techniques that would bring a halt to cyberbullying. Since cyberbullying mainly occurs through social media posts and comments, AI algorithms can be efficiently used to filter out abusive and abrasive threads on any virtual platform. The algorithm can be trained in such a way that each time a bully tries to send a comment or a post that is categorized as disrespectful or offensive, the bully will be blocked from sending the same. Further, the developers of the algorithm must note that the algorithm must be trained and curated in such a way that it scrutinizes each message, comment or post word by word so as to avoid any kind of mishap and reduce cyberbullying to a great extent. This algorithm, on being incorporated with all social media platforms would definitely help monitor and control the cases of cyberbullying [12].

However, the algorithm will have to support further extensions and added features to detect those messages and posts which may not necessarily include any abusive or vulgar content but intends to defame others or famous personalities [13]. In such cases, sentiment analysis plays an important role. Sentiment analysis, also known as opinion mining or emotion AI, is a classification under AI that has the capability to categorize emotional labels, positive or negative attributes along with the intensity from the comment or post. A technique called Natural Language Processing (NLP) is used here to identify the attitude within the text. Sentiment analysis is one of the best ways to detect scams, sarcasm and irony along with that of the target intention of the user [14]. Hence, we can conclude from the above-mentioned strategies that though bullying through online modes can't be eradicated, it can be controlled and reduced by detecting bullies and taking up necessary action against them. Figure 3 shown below describes the process of how online content can be filtered out to detect offensive comments on social media platforms using AI. As observed, the data posted by the user on any of the social media platforms are pre-moderated and scrutinized by necessary AI algorithms which have been trained using required datasets. The comments are then classified as harmful, not harmful and uncertain. Those which fall under the 'not harmful' category are posted directly while those which are found as harmful are blocked. The uncertain posts have further proceeded for manual moderation after which the corresponding decision is made [15].

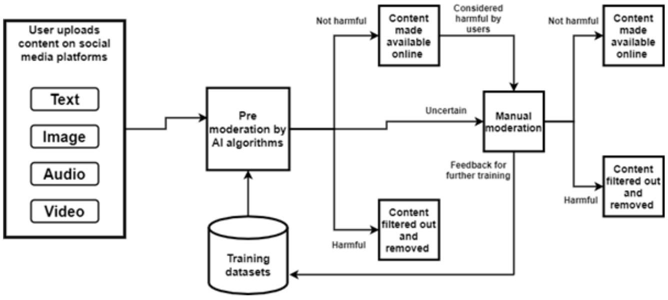

User uploads content on social media platforms
Text
Image
Audio
Video
Pre moderation by AI algorithms
Training datasets
Not harmful
Content made available online
Considered harmful by users
Uncertain
Harmful
Content filtered out and removed
Manual moderation
Feedback for further training
Not harmful
Content made available online
Harmful
Content filtered out and removed

Figure 3: The Role of Artificial Intelligence Protecting against Cyberbullying

VII. THEORETICAL FRAMEWORK

As discussed earlier, there are several different parameters and factors which influence youth and members of society to take up cyberbullying including financial stability, parental guidance, etc. Just like how AI can be incorporated to devise strategies to eradicate and reduce cyberbullying, there are a number of other technologies which can be used as well:

- **Human Intelligence:** It is one of the most essential and physical strategies for all human beings as it includes methodologies that facilitate learning from prior experience, acclimatizing to novel environments and conditions and making use of the gained knowledge and information to manipulate the surroundings to fit in accordingly [16].
- **Digital Intelligence:** One of the other profound strategies to combat cyberbullying is digital intelligence which is the sheer collection of social, emotional and cognitive abilities which are responsible for moulding individuals to tackle and overcome challenges in life in the digital world. This technique can provide great help in eliminating all those behaviours which would perpetuate cyberbullying traits.
- **Virtual Reality (VR):** VR refers to the computer technology and methodology which is used to develop a simulated environment. This is one of those fields which have been gaining a lot of technical attention in a plethora of fields because of its efficiency and this has surpassed some of the existing technologies. VR can easily be put to use for developing and creating a brief and summarised data visualization on posts and comments to prevent bullying among children and youngsters. VR is thus considered a futuristic tool to combat and suppress the issue of cyberbullying. The main reason for this is also because it proves to be one of the best components/tools for psychologists to extract and analyse the emotions of the victims. The fact that VR can be used to build an interactive three-dimensional interface by collecting large amounts of data and information with an increased chance of embedding real-time features. Note that the purpose of this study is to find out how big the problem is among adolescents, especially secondary students and teachers. The key goals are to find;
  - The recurrent incidence of bullying in school among students
  - Forms of school bullying
  - School intervention program
  - The consciousness of students to defend themselves from bullying.

Previous research examining cyberbullying has primarily focused on two categories of involvement, those who are victims and those who are perpetrators. These studies typically found prevalence rates of cyberbullying to range from approximately 10 to 35%.

VIII. THE IMPLICATIONS OF CYBERBULLYING AT WORK IN THE SMART ERA AND FUTURE RESEARCH DIRECTIONS

It can lead to extreme circumstances, self-harm, and damaged relationships if the situation goes undetected. Some common long-term effects of cyberbullying include depression, low self-esteem, unhealthy addictions, confidence problems, and poor mental health, according to Superintendent Alex Geordan.

Some of the implications and signs which can be seen in the person who is cyberbullied are:

- Poor self-esteem for oneself
- Withdrawal from family and a lot of time spent alone
- Reluctance to enable parents or other members of the family anywhere near their phones, laptops etc.
- Seeking reasons for staying away from school or jobs, like a rejection of school
- Friends missing from social activities or being omitted
- Weight loss or appearance changes to try to blend in
- Fresh skin marks that could suggest self-harm and dressing differently, such as wearing long-sleeved clothing in the summer to conceal any marks.
- A personality change, i.e., anger, depression, crying, withdrawal.

Despite the endless possibilities in developing strategies and methodologies which can be curated to suppress the rising concern of cyberbullying, there are a few bottlenecks and limitations as well. Firstly, most of the analyses and studies have been conducted on some of the existing information and research papers due to which there are possibilities of missing out on a few crucial points. Secondly, this work revolves around some of the essential topics and words related to cyberbullying and social media platforms and this can slightly inhibit the expected response. Hence, it's highly encouraged to take this topic further for future research and exploration to step out of the factors of irrationality and cohesion to draw apt deductions. Along with this, it is also encouraged to conduct further studies in other major fields of education, ethics and humanities to conceptualise the effect of cyberbullying from a number of different perspectives. In the last, authors in [17, 18, 19, 20, 21, 22, 23, 26 and 27] have listed various uses of Blockchain in preserving privacy, analytics role for improving people life or increasing growth of many sectors, whereas articles [24, 25] summarize that how cyber-attacks are the essential attacks to counter/ overcome in this smart era with emerging technologies. Furter, articles [26-50] discuses about importance of several useful technologies in modern smart era, i.e., to provide efficient and convenient solutions to the modern society.

IX. CONCLUSION

To conclude, over the years, the cases of cyberbullying have been on a steep rise leading to the generation of a large amount of negativity in social media platforms. Analyses and studies in the current decade have portrayed that very often, negative intentions and cases of defaming are gaining much more attention and followers. Therefore, the development in advanced technologies and sciences must be utilised to provide comprehensive and effective strategies using AI, ML and VR for fighting against cyberbullying. Social Media platforms and applications can also make use of algorithms and embedded techniques to demote users who seem to have malicious intentions and cyberbullies.

REFERENCES

[1] Campbell, Marilyn A. "Cyber bullying: An old problem in a new guise?." Journal of Psychologists and Counsellors in Schools 15.1 (2005): 68-76.

[2] Website link: https://www.unicef.org/end-violence/how-to-stop-cyberbullying

[3] Gradinger, Petra, Dagmar Strohmeier, and Christiane Spiel. "Traditional bullying and cyberbullying: Identification of risk groups for adjustment problems." Zeitschrift für Psychologie/Journal of Psychology 217.4 (2009): 205-213.

[4] Zych, Izabela, Rosario Ortega-Ruiz, and Rosario Del Rey. "Scientific research on bullying and cyberbullying: Where have we been and where are we going." Aggression and violent behavior 24 (2015): 188-198.

[5] Website link: https://online.maryville.edu/blog/what-is-cyberbullying-an-overview-for-students-parents-and-teachers/

[6] Website link: https://blog.securly.com/2018/10/04/the-10-types-of-cyberbullying/

[7] Website link: https://www.kaspersky.com/about/press-releases/2015_the-evolution-of-bullying-from-schoolyard-to-smartphone-24-7

[8] Website link: https://blogs.scientificamerican.com/guest-blog/the-origins-of-bullying/

[9] Calmaestra, Juan, et al. "Cyberbullying in adolescents from Ecuador and Spain: Prevalence and differences in gender, school year and ethnic-cultural background." Sustainability 12.11 (2020): 4597.

[10] Farley, Samuel, Iain Coyne, and Premilla D'Cruz. "Cyberbullying at work: Understanding the influence of technology." Concepts, Approaches and Methods (2021): 233-263.

[11] Niall Firth, "AI systems could fight cyberbullying", New Scientist, Volume 214, Issue 2871, 2012.

[12] S. Ramezanian and V. Niemi, "Privacy Preserving Cyberbullying Prevention with AI Methods in 5G Networks", 25th Conference of Open Innovations Association (FRUCT), Helsinki, Finland, 2019.

[13] Shane Murnion, William J. Buchanan, Adrian Smales, Gordon Russell, "Machine learning and semantic analysis of in-game chat for cyberbullying, Computers & Security", Volume 76, 2018.

[14] Website link: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

[15] Website link: https://www.britannica.com/science/human-intelligence-psychology

[16] Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56.

[17] A. K. Tyagi, T. F. Fernandez and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2020, pp. 498-504, doi: 10.1109/ICECA49313.2020.9297655.

[18] Shasvi Mishra, Amit Kumar Tyagi, "The Role of Machine Learning Techniques in Internet of Things Based Cloud Applications", AI-IoT book, Springer, 2021.

[19] M. M. Nair, A. K. Tyagi and N. Sreenath, "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-7, doi: 10.1109/ICCCI50826.2021.9402498.

[20] Varsha R., Nair S.M., Tyagi A.K., Aswathy S.U., RadhaKrishnan R. (2021) The Future with Advanced Analytics: A Sequential Analysis of the Disruptive Technology's Scope. In: Abraham A., Hanne T., Castillo O., Gandhi N., Nogueira Rios T., Hong TP. (eds) Hybrid Intelligent Systems. HIS 2020. Advances in Intelligent Systems and Computing, vol 1375. Springer, Cham. https://doi.org/10.1007/978-3-030-73050-5_56

[21] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[22] Nair M.M., Kumari S., Tyagi A.K. (2021) Internet of Things, Cyber Physical System, and Data Analytics: Open Questions, Future Perspectives, and Research Areas. In: Goyal D., Gupta A.K., Piuri V., Ganzha M., Paprzycki M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_36

[23] Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

[24] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 72-81 (2020).

[25] Tyagi, Amit Kumar and M, Shamila, Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019,

[26] Tyagi, Amit Kumar, Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019,

[27] Amit Kumar Tyagi (2022), Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World. IGI Global. DOI: 10.4018/978-1-6684-5250-9

[28] Khushboo Tripathi, Manjusha Pandey, and Shekhar Verma. 2011. Comparison of reactive and proactive routing protocols for different mobility conditions in WSN. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA, 156–161. https://doi.org/10.1145/1947940.1947974

[29] Jajula, S.K., Tripathi, K., Bajaj, S.B. (2023). Review of Detection of Packets Inspection and Attacks in Network Security. In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol 491. Springer, Singapore. https://doi.org/10.1007/978-981-19-4193-1_58

[30] Ranchhodbhai P.N, Tripathi K., "Identifying and Improving the Malicious Behavior of Rushing and Blackhole Attacks using Proposed IDSAODV Protocol", International Journal of Recent Technology and Engineering, vlo. 8(3), pp.6554-6562, 2019

[31] Midha S, Tripathi K, Sharma MK. Practical Implications of Using Dockers on Virtualized SDN. Webology. 2021 Apr; 18,pp.312-30.

[32] D. Agarwal and K. Tripathi, "A Framework for Structural Damage detection system in automobiles for flexible Insurance claim using IOT and Machine Learning," 2022 International Mobile and Embedded

Technology Conference (MECON), 2022, pp. 5-8, doi: 10.1109/MECON53876.2022.9751889.

[33] K. Somisetti, K. Tripathi and J. K. Verma, "Design, Implementation, and Controlling of a Humanoid Robot," *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 831-836, doi: 10.1109/ComPE49325.2020.9200020.

[34] Sai, G.H., Tripathi, K., Tyagi, A.K. (2023). Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_37

[35] S. Midha, G. Kaur and K. Tripathi, "Cloud deep down — SWOT analysis," *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, 2017, pp. 1-5, doi: 10.1109/TEL-NET.2017.8343560.

[36] S. Subasree, N.K. Sakthivel, Khushboo Tripathi, Deepshikha Agarwal, Amit Kumar Tyagi, Combining the advantages of radiomic features based feature extraction and hyper parameters tuned RERNN using LOA for breast cancer classification, Biomedical Signal Processing and Control, Volume 72, Part A, 2022, 103354, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2021.103354.

[37] Kumari, S. & Muthulakshmi, P. (2022). Transformative Effects of Big Data on Advanced Data Analytics: Open Issues and Critical Challenges. Journal of Computer Science, 18(6), 463-479. https://doi.org/10.3844/jcssp.2022.463.479

[38] S. Midha and K. Triptahi, "Extended TLS security and Defensive Algorithm in OpenFlow SDN," *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2019, pp. 141-146, doi: 10.1109/CONFLUENCE.2019.8776607.

[39] Midha, S., Tripathi, K. (2021). Extended Security in Heterogeneous Distributed SDN Architecture. In: Hura, G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_75

[40] Midha, S., Tripathi, K. (2020). Remotely Triggered Blackhole Routing in SDN for Handling DoS. In: Dutta, M., Krishna, C., Kumar, R., Kalra, M. (eds) Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India. Lecture Notes in Networks and Systems, vol 116. Springer, Singapore. https://doi.org/10.1007/978-981-15-3020-3_1

[41] Mapanga, V. Kumar, W. Makondo, T. Kushboo, P. Kadebu and W. Chanda, "Design and implementation of an intrusion detection system using MLP-NN for MANET," *2017 IST-Africa Week Conference (IST-Africa)*, 2017, pp. 1-12, doi: 10.23919/ISTAFRICA.2017.8102374.

[42] Tyagi, A.K. (Ed.). (2021). Data Science and Data Analytics: Opportunities and Challenges (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003111290

[43] Tyagi, A.K., & Abraham, A. (Eds.). (2022). Recurrent Neural Networks (1st ed.). CRC Press. https://doi.org/10.1201/9781003307822

[44] Tyagi, A.K., & Abraham, A. (Eds.). (2021). Recent Trends in Blockchain for Information Systems Security and Privacy (1st ed.). CRC Press. https://doi.org/10.1201/9781003139737

[45] Tyagi, A. K., Rekha, G., & Sreenath, N. (Eds.). (2021). Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. IGI Global. http://doi:10.4018/978-1-7998-3295-9

[46] Akshita Tyagi, Swetta Kukreja, Meghna Manoj Nair, Amit Kumar Tyagi, Machine Learning: Past, Present and Future, Neuroquantology, Volume 20, No 8 (2022), DOI: 10.14704/nq.2022.20.8.NQ44468

[47] Malik, S., Bansal, R., & Tyagi, A. K. (Eds.). (2022). Impact and Role of Digital Technologies in Adolescent Lives. IGI Global. http://doi:10.4018/978-1-7998-8318-0

[48] Kumar Tyagi, A., Abraham, A., Kaklauskas, A., Sreenath, N., Rekha, G., & Malik, S. (Eds.). (2022). Security and Privacy-Preserving Techniques in Wireless Robotics (1st ed.). CRC Press. https://doi.org/10.1201/9781003156406

[49] Amit Kumar Tyagi, G. Aghila, “A Wide Scale Survey on Botnet”, International Journal of Computer Applications (ISSN: 0975-8887), Volume 34, No.9, pp. 9-22, November 2011.

[50] Jayaprakash, V., Tyagi, A.K. (2022). Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, vol 481. Springer, Singapore. https://doi.org/10.1007/978-981-19-3182-6_18