THE ASIAN BULLETIN OF BIG DATA MANAGEMENT
Vol.5. Issue1 (2025)
https://doi.org/ 10.62019/abbdm.v5i1.1.292

A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach

Iqra Aslam*, Muhammad Furqan Khawaja, Adnan Ahmad, Wajeeha Tariq, Muhammad Sheraz Nawaz, Fawad Nasim, Hamayun Khan

Chronicle

Article history

Received: Jan 3, 2024
Received in the revised format: Jan 27, 2024
Accepted: Jan 8, 2025
Available online: Feb 9, 2025

Iqra Aslam, Wajeeha Tariq, Fawad Nasim and Hamayun Khan Are currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan.
Email: iqraranjha449@gmail.com
Email: wajeehatariq02@gmail.com
Email: fawad.nasim@superior.edu.pk
Email: hamayun.khan@superior.edu.pk

Muhammad Furqan Khawaja is currently affiliated with the Department of Computer Science, as a Senior Data Scientist and AI Consultant in Pakistan.
Email: furqankhawaja1@gmail.com

Adnan Ahmad is currently affiliated with the Department of Riphah International University School of computing, Lahore Pakistan.
Email: adnan.ahmad@riphah.edu.pk

Muhammad Sheraz Nawaz is currently affiliated with the department University of Management and Technology (UMT), Lahore, 54000, Pakistan
Email: msheraz135@outlook.com

Corresponding Author*

Abstract

In this contemporary era, the internet has become the mode of communication and has changed the lifestyle of individuals with advancements in technology. Social media networks are becoming an essential part of life for most of the world's population. Social networking platforms give users countless opportunities to share information collaborate, cyberbullying and communicate positively. Cyberbullying is the use of technology as a medium to bully someone. Although it has been an issue for many years, the recognition of its impact on young people has recently increased. Detecting cyberbullying using Machine learning and natural language processing algorithms is getting the attention of researchers. The same platform can be extended to a fabricated and poisonous atmosphere that gives an impersonal, harmful platform for online misuse and assault. Yet it also poses significant challenges, including blackmailing and cyberbullying. These malicious activities can have severe psychological, emotional, and social consequences. These unsolicited activities have an impact on increasing the vulnerability of crime against women and among younger age groups children including adolescents. This paper provides a comprehensive analysis of the phenomenon of social media blackmailing and cyberbullying. It examines their prevalence, psychological impacts, and countermeasures. The framework considering all possible actors in the cyberbullying event must be designed, including various aspects of cyberbullying and its effect on the participating actors. A synthesis of findings from recent studies is presented to highlight the trends and effectiveness of current mitigation strategies. The paper also outlines methodologies employed in recent research, discusses results, and provides conclusions on future directions. Furthermore, Future developments of the work could include handling multimedia data of various sizes and the ability to categorize the material neural network-based algorithms and future challenges are also discussed.

Keywords: Cyberbullying, Internet bullying, electronic bullying, higher institutes of learning, personal factors, psychological factors.

INTRODUCTION

Emotion Bullying is defined as targeting an individual or a group of individuals and exposing them to ridicule and negative actions both physical and mental deliberately.

This is a common but serious and demoralizing experience that every individual encounters at least once in his or her lifetime. Social networking sites are great tools for connecting with people. However, as social networking has become widespread, people are finding illegal and unethical ways to use these communities. We see that people, especially teens and young adults, are finding new ways to bully one another over the Internet [1]. Close to 25% of parents in a study conducted by Symantec reported that, to their knowledge, their child has been involved in a cyberbullying incident. Social media platforms have revolutionized communication, offering users an opportunity to connect globally. However, the anonymity and broad reach of these platforms have led to the rise of detrimental activities such as blackmailing and cyberbullying [2, 3]. This section delves into the scope, mechanisms, and impact of these activities, offering a structured overview. As an alternative to conventional process-based and empirical models, applying different machine learning (ML) algorithms as data-driven models has proven tremendously successful because of the powerful computational efficiency [4, 5]. However, protecting IT systems from threats and criminal network behavior is still very difficult because cyber-attacks are always changing. Due to regular network intrusions and harmful actions, effective defenses and security concerns were given key importance for developing trustworthy solutions [6].

The Rise of Social Media

Social media platforms like Facebook, Instagram, Twitter, and TikTok have seen exponential growth in users over the past decade. According to a 2022 report by Statista, there are over 4.2 billion active social media users globally. This widespread adoption has enabled unprecedented levels of connectivity but also introduced avenues for misuse [7, 8]. Most currently employed techniques for recognizing cyber attacks match potential attack characteristics by blocking harmful connections to assist defenders in attack scenario analysis. Among these platforms, Facebook stands out as the most popular platform for human connection, boasting approximately 2.27 billion active users. Through various features provided by Facebook, users engage in conversations, and debates, and share their thoughts with others and communities [9].

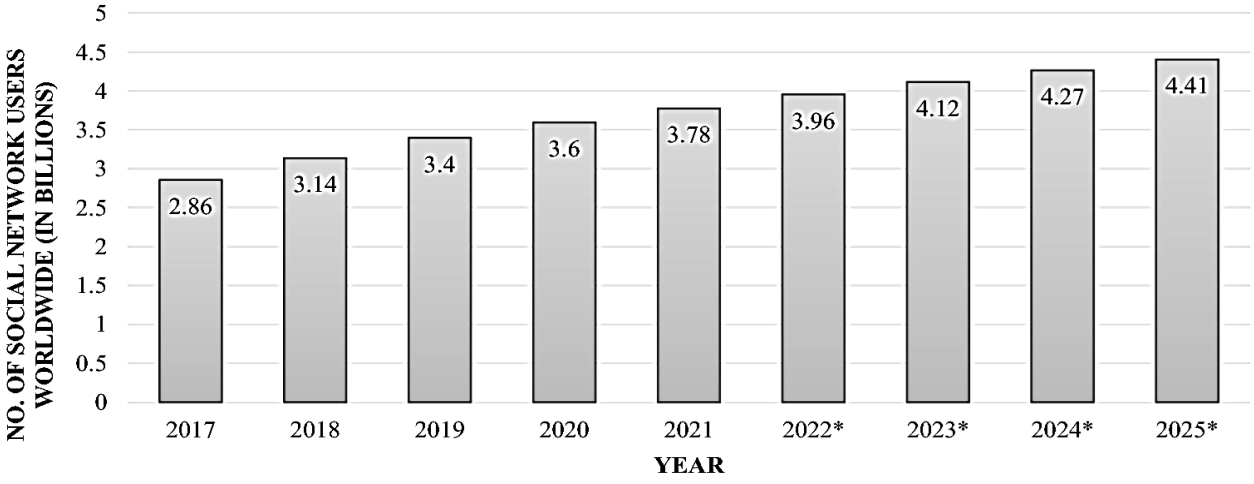

Figure 1:
Expansion of Social Netowk [10]

Role of Natural Language Processing (NLP) in Cyberbullying Detection

One direction in this field is to detect offensive content using Natural Language Processing (NLP). The most explanatory method for presenting what happens within a Natural Language Processing system is using the "levels of language" approach. These levels are used by people to extract meaning from text or spoken languages. This leveling refers to the reason that language processing relies mainly on formal models or representations of knowledge related to these levels [11]. For detection of cyberbullying System the accuracy and precision the below equations are used

$$\text{Accuracy} = TP+TN/TP+TN+FP+FN \quad \text{Eq (1)}$$

$$\text{Precision} = TP/TP+FP \quad \text{Eq (2)}$$

$$\text{Recall} = TP/TP+FN \quad \text{Eq (3)}$$

$$F - \text{Score} = 2\text{precisionrecall}/\text{precision}+\text{recall} \quad \text{Eq (4)}$$

Table 1:
Parameter Analaysis of Cyberbullying System [12]

Data Size	Features	Classifier	Performance
9484 tweets	Features (Personality, net- 10 (work, user	J48	Accuracy = 92.8% (Classes 4)
650000 posts and comments	Cyberbullying index + Losada ratio + sentiment analysis, social network analysis	Random Forest	F-Score = 0.80 (Classes 2)
103212 buzzes	Casual factors of cyberbullying	CRT	Accuracy = 74.5%
10,606 tweets	.Multiple types of Features	Random Forest	F-Score = 0.936 (Classes 2)
10,000 tweets	User, Text, Network features	Random Forest	Accuracy = 91% (Classes 3)
12,000 Posts FormSpring	-	CNN	F-Score = 0.93 (Classes 2)
2.1 Million tweets	User, Text, Network features	Random Forest	F-Score = 0.902 (Classes 3)
30,384 tweets	Content, user, network, sentiment features	ANN + DRL	Accuracy = 80.7% (Classes 2)
7,321 Tweets and 800 instances (MySpace)	-	SmSDA	Accuracy = 84%, 89% (Classes 2)

Deep Learning Classifiers and Types of Blackmailing and Cyberbullying

Traditionally, features are designed by a human to train the machine learning algorithms, which require a lot of expertise and domain knowledge. Deep learning architectures exploit powerful neural networks containing multiple layers without the burden of feature engineering. Several useful deep learning architectures are successfully used in natural language processing image, and video processing. These deep learning architectures include Convolutional neural networks. Social media blackmailing involves coercing individuals through threats of revealing private information or images. Cyberbullying, in contrast, encompasses harassment, insults, and public shaming, often targeted at

specific individuals or groups. Both behaviors thrive on anonymity and the virality of digital content, making them challenging to control [14]. Cyberstalking and cyberbullying have both physical and mental impacts on individuals. Abusers take advantage of the anonymity provided by social media platforms, allowing their cruel behavior to go unchecked. Furthermore, as harassment becomes more frequent over time, the situation worsens [15].

Table 2:
Comparative Analysis [16]

Feature	Classifier	Accuracy	Dataset used
N/A	N/A	They did not evaluate their proposed model	Twitter and Ask.fm datasets
Bag of Words (BoW)	Sequential Minimal Optimization (SMO), IBK, JRip, J48	The model was capable of recognizing 78.5% posts in Formspring dataset	Formspring Link: www.Formspring.me
TF-IDF unigrams	Ensemble	NA	MySpace, Slashdot, Kongregate, Twitter
TF-IDF	SVM	Kongregate (0.289) Slashdot (0.273) MySpace (0.351)	MySpace, Slashdot, Kongregate
Second p Insult word erson pronouns, Swear word,	NA	Correctly identify 85.3% as cyberbully ing posts and 51.91% as innocent posts of MySpace dataset	MySpace
Negative comments, Total negative words, Unigrams	AdaBoost, LR	NA	Datasets of Vine
		- SMO (68.47%) - J48 (65.81)	

Feature Extraction

Features for cyberbullying detection can be broadly classified into Content features, Network features, Activity features, User profile features, and sentiment features. Table I summarizes a list of features used in cyberbullying detection in the literature [17]. Word embedding featuresare the most common features used for cyberbullying detection in the literature.

LITERATURE REVIEW

The emergence of social media has provided fertile ground for the proliferation of cyberbullying and blackmailing. Studies conducted over the past decade reveal that these issues are not confined to any particular demographic but span across age groups, genders, and cultural backgrounds. Research, such as the work by [18] has documented the rising prevalence of cyberbullying, with adolescents being particularly vulnerable. Technological advancements, while providing tools for connection, have also enabled malicious actors to exploit features like anonymity and wide-reaching communication channels. Historical perspectives show that online harassment has evolved from isolated incidents on forums to sophisticated operations involving hacking and phishing [19]. The

psychological impacts of these activities have been well-documented, with victims reporting symptoms ranging from acute stress to chronic mental health issues. Despite these insights, gaps remain in understanding the mechanisms behind perpetrator behavior and the long-term efficacy of intervention strategies [20].

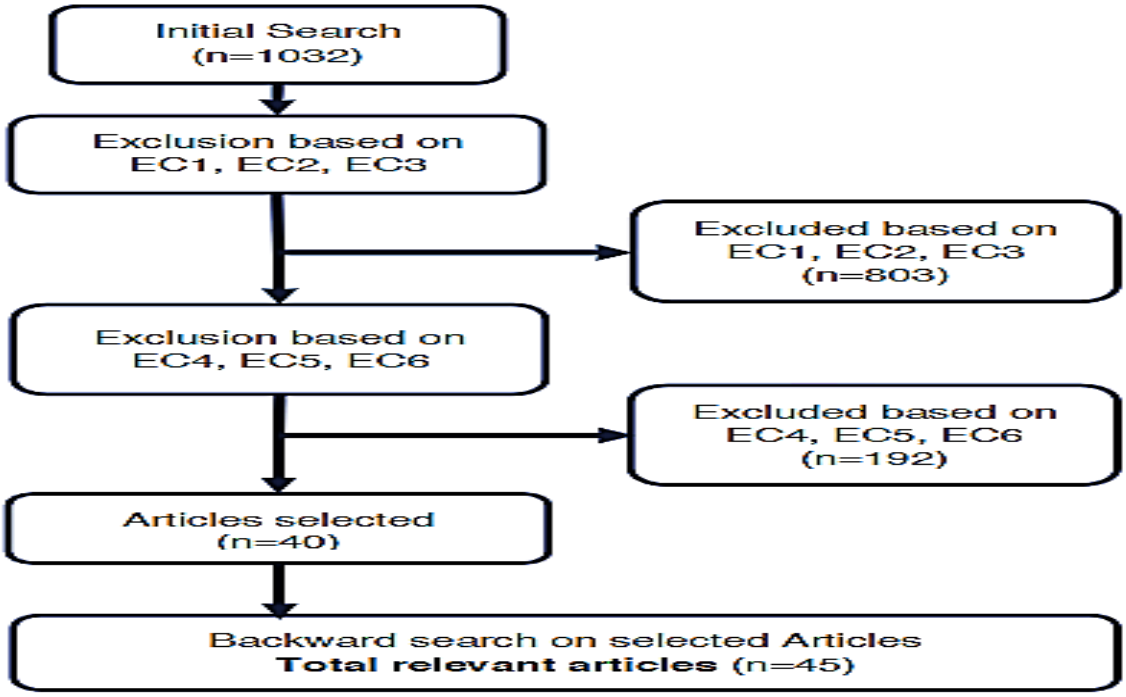

Figure 2:
Systematic Procedure for Literature

Role of Machine Learning Social Impact on Cyber Bullying

People connect on social media through various platforms. Every platform has certain limitations on shared content. Social media content can be text, images, video, or infographics. Monitoring cyberbullying on social media requires understanding the content, the social network of the connecting people, user activities, connection behavior on social media, and users' profiles [21]. The consequences of blackmailing and cyberbullying extend beyond the digital realm. Victims often experience anxiety, depression, and post-traumatic stress disorder. Cyberbullying victims are twice as likely to develop long-term mental health issues compared to their peers. Social impacts include strained relationships, loss of trust in online platforms, and, in severe cases, withdrawal from digital spaces entirely [22]. Anonymity is a double-edged sword on social media. While it allows users to express themselves freely, it also empowers perpetrators to engage in malicious activities without fear of accountability that over 60% of cyberbullying incidents are perpetrated by anonymous users, complicating identification and enforcement efforts [23, 24].

Influence of Technological Advancements

Technological advancements have inadvertently facilitated these issues. Features like disappearing messages, end-to-end encryption, and fake profiles create opportunities

for abuse. While these tools offer legitimate privacy benefits, they also hinder monitoring and intervention efforts [25].

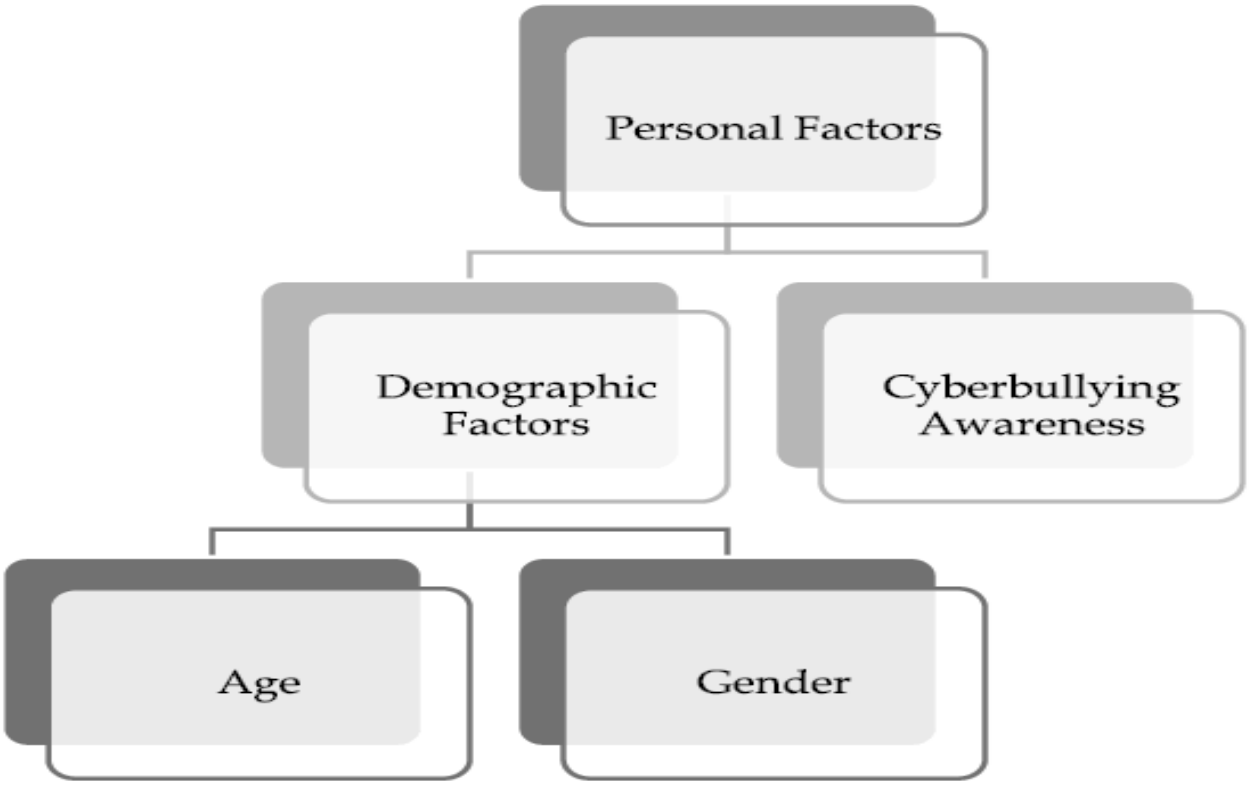

Figure 3:
Conceptual Framework of factors related with cyberbullying[26]

Legal and Ethical Challenges

The legal landscape surrounding social media abuse is fragmented. Different countries have varying definitions and penalties for online harassment and blackmail. Ethical concerns, such as balancing privacy rights with the need for monitoring, further complicate enforcement. Arguing that a unified international legal framework is essential for addressing these issues effectively [27]. Given the multifaceted nature of social media blackmailing and cyberbullying, a comprehensive approach is required. This includes technological interventions, educational programs, and robust legal frameworks. Collaboration among stakeholders, including governments, tech companies, educators, and mental health professionals, is crucial to creating a safer digital environment [28, 29].

DATA SEARCH STRATEGY & MATERIALS

This review employs a systematic approach to analyze recent literature on social media blackmailing and cyberbullying. The methodology comprises the following steps: Relevant studies were identified using a systematic search strategy. Databases such as IEEE Xplore, PubMed, Scopus, and Google Scholar were queried with a combination of keywords, including "social media blackmailing," "cyberbullying," "digital harassment," "online abuse," and "psychological impacts." The search was limited to articles published between 2020 and 2025 to ensure the inclusion of recent findings.

Inclusion and Exclusion Criteria

To ensure the relevance and quality of the selected studies, specific inclusion and exclusion criteria were applied:

Inclusion Criteria: Articles published in peer-reviewed journals or conference proceedings that focus on empirical research, case studies, or technological and policy solutions for combating social media blackmailing and cyberbullying.

Exclusion Criteria: Opinion pieces, non-peer-reviewed content, and studies focusing on general online behavior without addressing blackmail or cyberbullying specifically were excluded.

Table 3:
Comparative Analysis [30]

Year	Feature	Classifier	Accuracy	Dataset used
2015	Unigram 3-g	SVM, NB	- Naïve Bayes (71%) - SVM (78%)	Twitter
2020	TI-IDF	LR, NB, SVM, XGBoost	-LR (76.8%) - NB (60.6%) -SVM (64.8%) - XGBoost (77.4%)	A total of 197,566 comments from fo platforms: YouTube, Reddit, Wikiped and Twitter,
2012	Profanity, BoW, TF-IDF, Weighted unigrams	J48, SVM, NB -based learner, Rule-based Jrip	-NB (63%) - J48 (61%) -SVM (72%) - Rule-based Jrp (70.39%)	Formspring, Youtube
2013	Emoticons, Message length, N-gram, Bully keywords, Pronouns	SVM	NA	YouTube
2018	Character n-gram BoW, Word n-gram BoW	LSVM	F1 score of 64% and 61% for English and Dutch respectively	Posts of ASKfm in Dutch and English
2019	NA	LR, LSVM, RF	NA	Vine, Instagram
			- LR (90.57%) - LGBM (90.55%)	

Data Extraction and Categorization

Data extraction was conducted using a standardized template to ensure consistency. Information related to the prevalence, psychological impacts, mitigation strategies, and

research gaps was categorized. Thematic analysis was used to identify recurring patterns and insights.

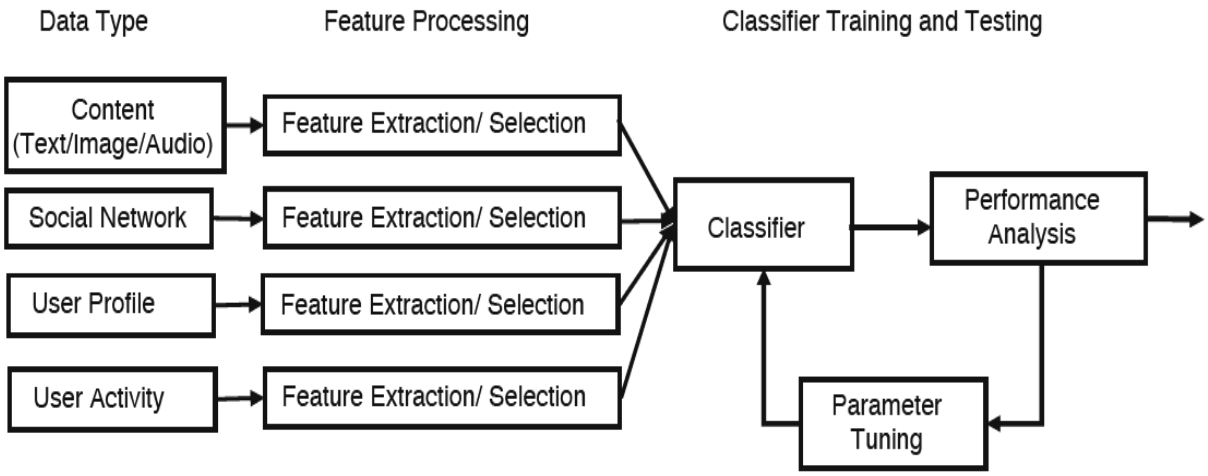

Figure 4:
Systematic Framework for Cyber Bullying [26]

Qualitative and Quantitative SynthSesis

The extracted data were synthesized both qualitatively and quantitatively. Qualitative synthesis involves thematic analysis of narrative data to identify common themes and trends. The quantitative synthesis involved statistical aggregation where data were available, such as percentages of affected individuals or effectiveness rates of interventions. To ensure the reliability and validity of findings, cross-referencing was performed across multiple sources. Independent reviewers validated the inclusion of articles and the categorization of data. Any discrepancies were resolved through discussion. While the methodology employed was rigorous, certain limitations must be acknowledged. The focus on studies published in English and within a specific time frame may have excluded valuable insights from other regions or earlier research. Additionally, reliance on self-reported data in some studies may introduce biases. This rigorous methodology ensured that the review encapsulates diverse perspectives and the latest advancements in the field.

Recent studies highlight the alarming prevalence of social media blackmailing and cyberbullying. For instance [31] reported that 34% of teenagers aged 13-18 experienced cyberbullying in 2023. Additionally, [32] observed a 20% increase in incidents of social media blackmailing during the COVID-19 pandemic. These findings reflect a growing trend of online abuse, particularly affecting adolescents and young adults. Moreover, research highlights that specific platforms, like Instagram and Snapchat, are often cited as common spaces for such activities [33]. Research by [34] indicates that 34% of teenagers aged 13-18 reported experiencing cyberbullying in 2023. Another study by shows in [35] found a 20% increase in social media blackmailing incidents during the COVID-19 pandemic. These findings underscore the growing vulnerability of users, particularly adolescents and young adults, to online abuse.

Psychological Impacts & Factors

The psychological toll of cyberbullying and blackmailing is significant. Victims often report feelings of helplessness, fear, and humiliation. Longitudinal studies reveal that victims are at a higher risk of developing anxiety disorders, depression, and post-traumatic stress disorder (PTSD). Additionally, the public nature of social media platforms amplifies the humiliation, causing long-lasting emotional scars.

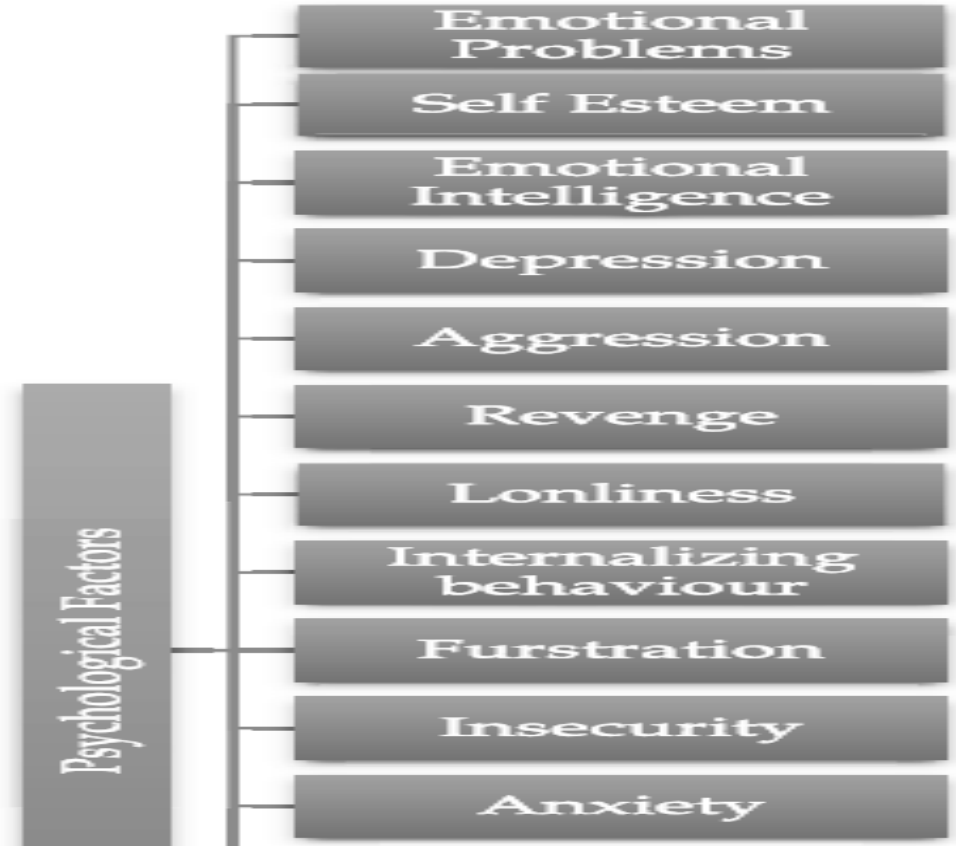

Figure 5:
Psychological Factors Assocaited with Cyberbulying [36]

Mitigation Strategies & Gaps

Technological interventions have gained traction as effective countermeasures. AI-driven tools for content moderation and abusive behavior detection are increasingly being deployed by platforms like Facebook and Twitter. Real-time monitoring systems have also demonstrated potential in flagging and removing harmful content before it spreads widely. Educational programs aimed at promoting digital literacy and awareness among users have shown promise in equipping individuals to recognize and report abusive behavior. Despite these advancements, significant challenges remain. The anonymity of perpetrators often shields them from accountability, and the lack of consistent legal frameworks across jurisdictions complicates enforcement. Moreover, the effectiveness of existing mitigation strategies in diverse cultural contexts remains underexplored.

Table 4:
Comparative Analysis Of Multi-Modal Cyberbullying Detection [37]

Data Size	Features	Classifier	Performance
3600 images with comments	Text features/ Image features	Random Forest	F-Score = 0.74
3000 images with comments	Text features/ Image features	SVM, Deep learning	Accuracy = 95%
10,000 comments, images	-	CNN	Accuracy = 97%
733 sessions with 15 posts or more	Textual, Visual, Audio features	LR	AUROC = 0.834 (Classes 2)
2100 images with comments	Image embedding, Text em- (bedding (TD-IDF	CNN	F-Score = 0.68 (Classes 2)
2218 sessions (Instagram)	LIWC, Word embedding	HANCD	F-Score = 0.778 (Classes 2)
969 video sessions with comments	-	Recurrent-CNN ResidualBiLSTM	F-Score = 0.75

Table 5:
Summary of Various Related Studies & Latest Gaps [38]

Publisher	Journal	Country	Methodology	Factors	Relationship
Scopus	Frontiers in Psychology	Spain	Questionnaire	Emotional Problems	Positive
				Cyberbully Awareness	Negative
Science Direct	Computers in Human Behaviour	Portugal	Interviews/ Questionnaire	Aggression	Positive
				Revenge	Positive
				Just For Fun	Positive
				Personality	Positive
Science Direct	Computers in Human Behaviour	Malaysia	Questionnaire	Technology exposure	Positive
				Easy Internet Access	Positive
Science Direct	Computers in Human Behaviour	USA	Survey	Disability	Positive
				Depression	Positive
				Self-esteem	Positive
				Parenting Style	Negative
				Emotional Problems	Positive
				Anonymity	Positive
Scopus	International Journal of Environmental Research and Public Health	Canada	Online Survey & Interview	Emotional Problems	Positive
				Self Esteem	Negative
				Depression	Positive
Scopus	Journal of the Egyptian Public Health Association	Egypt	Questionnaire	Aggression	Positive
				Depression	Positive
				Self Esteem	Negative
				Emotional Problems	Positive

DISCUSSION

The findings from this review highlight the multidimensional nature of social media blackmailing and cyberbullying. While technological solutions are making strides in detecting and preventing abusive behavior, their reliance on algorithms raises ethical and privacy concerns. The balance between user privacy and effective monitoring remains a contentious issue. Legal frameworks, though improving, often fail to address the transnational nature of online abuse. Collaborative efforts between governments, tech companies, and non-governmental organizations are crucial to developing comprehensive policies. Additionally, educational initiatives should not only focus on raising awareness but also on fostering resilience among potential victims. Digital ethics and empathy should be integral components of school curricula to instill responsible online behavior from a young age.

CONCLUSION

This study reviewed various aspects of machine learning-based cyberbullying detection. Most of the work is focused on classifying bullying or non-bullying events based on textual, user activity, and network information. Social media blackmailing and cyberbullying are pervasive and evolving challenges that require urgent attention. This review underscores the need for a holistic approach combining technological, educational, and policy-driven solutions. Future research should focus on enhancing AI algorithms for abuse detection, exploring the cultural nuances of online behavior, and developing robust international legal frameworks. Mental health support for victims should also be prioritized to mitigate the long-term impacts of these harmful activities.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author contributed equally to the creation of this work. However, Muhammad Ahmad Shahid took the lead in the research itself, as well as in its design, analysis, and manuscript preparation.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Aliyyah Rosyidah1 , Jumadi Mabe Parenreng, "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)" July, 06 2023

Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. Br. J. Criminol. 2017, 57, 704–722.

Alenezi, M.N.; Alabdulrazzaq, H.; Alshaher, A.A.; Alkharang, M.M. Evolution of malware threats and techniques: A review. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 326–337.

Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlationanalysis. Future Generation Computer Systems, 89, 349-359.

Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis ofdeep learning. IEEE Access, 8, 186125-186137.

Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.

Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers ofgreen growth and environment. Scientific Reports, 14(1), 28636.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mtmatical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering,Technology & Applied Science Research, 14(5), 16751-16756.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors"

,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

T. Vaillancourt, R. Faris, and F. Mishna, "Cyberbullying in children and youth: implications for health and clinical practice," Can. J. Psychiatry, vol. 62, no. 6, pp 368-373,2017.

C. Burger, D. Strohmeier, N. Spröber, S. Bauman, and K. Rigby, "How teachers respond to school bullying: An examination of self-reported intervention strategy use, moderator effects, and concurrent use of multiple strategies," Teach. Teach. Educ., vol. 51, pp. 191-202,Oct. 2015, doi: 10.1016/j.tate.2015.07.004.

Tahir, R. A study on malware and malware detection techniques. Int. J. Educ. Manag. Eng. , vol. 8, no. 20, 2018. M. Tomaiuolo, G. Lombardo, M. Mordonini, S. Cagnoni, and A. Poggi, "A survey on troll detection," Future Internet, vol. 12, no. 2, p. 31, 2020.

Z. Zsa Tajol Asanan, ``A study on cyberbullying: Its forms, awareness and moral reasoning among youth," Int. J. Inf. Commun. Sci., vol. 2, no. 5, p. 54, 2017, doi: 10.11648/j.ijics.20170205.11.