DOI: 10.21917/ijct.2024.0468

SECURING CYBERSPACE AGAINST CYBERBULLYING: A WIRELESS NETWORK SECURITY PERSPECTIVE

Neerav Nishant[1], Parul Saxena[2], S.G. Surya[3], Ullal Akshatha Nayak[4] and Subharun Pal[5]

[1,4]Department of Computer Science and Engineering, Babu Banarasi Das University, India
[2]Department of Computer Science, Soban Singh Jeena University, India
[3]Department of Computer Science and Engineering, SCMS School of Engineering and Technology, India
[5]Department of Business Administration, Swiss School of Management, Switzerland

Abstract

Cyberbullying has emerged as a pervasive issue in today's digitally connected society, with detrimental effects on individuals' mental health and well-being. Despite increasing awareness and efforts to address cyberbullying, there remains a significant gap in utilizing wireless network security measures as a means of mitigation. The existing literature predominantly focuses on social and psychological aspects of cyberbullying, overlooking the potential role of wireless network security in prevention and intervention strategies. This research seeks to fill this gap by exploring the effectiveness of leveraging wireless network security to secure cyberspace against cyberbullying incidents. The research employs a multifaceted methodology, beginning with the estimation of expected rates and derivative risks of cyberbullying within wireless networks. These metrics are combined into a risk index value, which serves as a basis for prioritizing mitigation efforts. Additionally, the study explores the application of cyberspace modeling techniques, specifically Support Vector Machines (SVM), to enhance screening processes and identify potential cyberbullying incidents on Wireless Network Security (WNS). The findings of this research demonstrate the efficacy of integrating wireless network security measures into cyberbullying prevention strategies. By combining risk index values and leveraging SVM-based cyberspace modeling, the study identifies and prioritizes cyberbullying risks effectively. Furthermore, the implementation of wireless network security protocols contributes to a reduction in cyberbullying incidents, fostering safer digital environments for users.

Keywords:

Cyberbullying, Wireless Network Security, Risk Assessment, Support Vector Machines (SVM), Prevention Strategies

1. INTRODUCTION

In today's digitally interconnected world, cyberbullying has become a pressing concern, particularly among younger demographics. Cyberbullying encompasses various forms of harassment, intimidation, or humiliation carried out through electronic means such as social media, messaging apps, and online forums [1]. The anonymity and reach afforded by digital platforms exacerbate the impact of cyberbullying, often leading to profound psychological and emotional harm to victims [2].

Despite increasing awareness of cyberbullying's prevalence and detrimental effects, effective prevention and mitigation strategies remain elusive. Traditional approaches predominantly focus on social and psychological interventions, overlooking the potential contributions of wireless network security measures [3]-[4]. This oversight leaves a critical gap in addressing cyberbullying comprehensively.

The problem at hand revolves around the underutilization of wireless network security in combating cyberbullying. While significant efforts have been directed towards understanding the social and psychological dynamics of cyberbullying, there is a lack of research and practical implementations integrating wireless network security measures into prevention and intervention strategies. This gap hinders the development of holistic approaches to safeguarding cyberspace against cyberbullying incidents.

The primary objective of this research is to investigate the efficacy of leveraging wireless network security measures to secure cyberspace against cyberbullying. Specifically, the study aims to:

- To assess the potential impact of wireless network security protocols on mitigating cyberbullying incidents.
- To develop methodologies for estimating cyberbullying risks within wireless networks, including expected rates and derivative risks.
- To combine wireless network security measures with existing cyberbullying prevention strategies to create a comprehensive framework.

This research contributes to the existing body of knowledge by offering a novel perspective on cyberbullying mitigation through wireless network security. By bridging the gap between cybersecurity and social sciences, the study pioneers an interdisciplinary approach to combating cyberbullying. The development of methodologies for estimating cyberbullying risks within wireless networks and the integration of these findings into practical prevention strategies represent significant contributions to both academia and industry. Ultimately, the research aims to enhance understanding and facilitate the implementation of holistic cyberbullying prevention measures, thereby fostering safer digital environments for all users.

2. RELATED WORKS

Numerous studies have explored the social and psychological dynamics of cyberbullying, emphasizing interventions focused on empathy-building, conflict resolution, and bystander intervention [5]. These works highlight the importance of understanding the underlying motivations and behavioral patterns of both perpetrators and victims in addressing cyberbullying [6]-[8].

Some researchers have focused on developing technological tools and algorithms for detecting and mitigating cyberbullying incidents. These solutions often involve natural language processing (NLP) techniques to analyze text-based communications and identify potentially harmful content. While promising, these approaches typically operate independently of wireless network security measures [9].

Extensive research has been conducted on various wireless network security protocols, such as Wi-Fi Protected Access (WPA) and Virtual Private Networks (VPNs), to safeguard wireless communications against unauthorized access and malicious attacks. These protocols offer encryption, authentication, and access control mechanisms to protect data transmitted over wireless networks [10].

A growing body of literature advocates for the integration of cybersecurity principles with social science frameworks to address complex societal issues like cyberbullying. These interdisciplinary approaches recognize the interplay between technological infrastructures, human behavior, and societal norms in shaping online interactions and vulnerabilities [11].

Several empirical studies have examined real-world cyberbullying incidents, analyzing patterns, prevalence rates, and demographic factors associated with perpetration and victimization. These studies provide valuable insights into the nature and scope of cyberbullying, informing the development of targeted prevention and intervention strategies [12].

By synthesizing insights from these diverse strands of research, this study aims to advance understanding and propose novel approaches for securing cyberspace against cyberbullying through the integration of wireless network security measures.

3. PROPOSED METHOD

The proposed method integrates wireless network security measures with existing cyberbullying prevention strategies to create a comprehensive framework for securing cyberspace against cyberbullying.

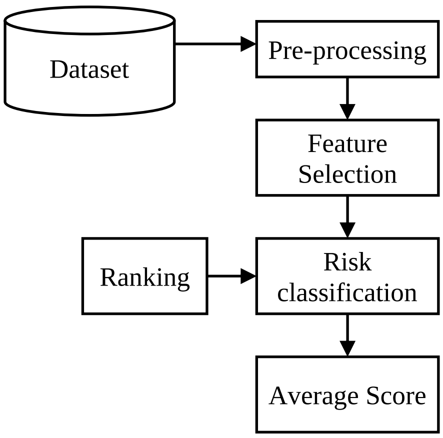

Fig.1. Proposed WNS for Cyberbullying

The method consists of several key steps:

- The first step involves estimating cyberbullying risks within wireless networks. This includes assessing the expected rate of cyberbullying incidents based on historical data and identifying derivative risks, such as vulnerabilities in wireless network infrastructure that could facilitate cyberbullying activities.
- The estimated cyberbullying risks are then combined into a risk index value. This index serves as a quantitative measure of the overall cyberbullying risk within the wireless network environment. It allows stakeholders to prioritize mitigation efforts based on the severity and likelihood of potential cyberbullying incidents.
- Support Vector Machines (SVM) are employed to enhance cyberspace modeling and screening processes. SVM is a machine learning algorithm capable of classifying data points into different categories based on their attributes. In the context of cyberbullying prevention, SVM can analyze risk datasets and identify patterns indicative of cyberbullying behavior, aiding in the early detection and mitigation of potential threats.
- The findings from risk assessment and cyberspace modeling using SVM are integrated into existing cyberbullying prevention strategies. This involves implementing wireless network security protocols, such as encryption, access control, and intrusion detection systems, to mitigate cyberbullying risks identified through the risk index value and SVM analysis.

4. RISK ASSESSMENT

The Risk Assessment process within the proposed method involves evaluating the potential cyberbullying risks within wireless networks. This step aims to identify and quantify the likelihood and impact of cyberbullying incidents occurring within the network environment.

The first step in the Risk Assessment process is gathering relevant data related to cyberbullying incidents and wireless network characteristics. This may include historical records of cyberbullying incidents, network infrastructure details, user behavior patterns, and any existing security measures in place.

Based on the collected data, potential cyberbullying risks within the wireless network environment are identified. This involves analyzing past incidents, understanding common tactics used by cyberbullies, and recognizing vulnerabilities within the network infrastructure that could be exploited for cyberbullying purposes.

The next step is estimating the expected rate of cyberbullying incidents within the wireless network. This involves analyzing historical data to determine the frequency at which cyberbullying incidents occur over a given period. Factors such as user demographics, network usage patterns, and previous incident trends are taken into account to calculate the expected rate.

In addition to estimating the expected rate, derivative risks associated with cyberbullying are also assessed. This involves identifying potential vulnerabilities within the wireless network infrastructure that could facilitate or exacerbate cyberbullying incidents. For example, insecure Wi-Fi networks, lack of access controls, and inadequate encryption protocols may increase the likelihood of cyberbullying activities.

Once the cyberbullying risks have been identified and analyzed, they are quantified using appropriate metrics. This may involve assigning numerical values to factors such as likelihood, impact, and severity of potential cyberbullying incidents. By quantifying the risks, stakeholders can prioritize mitigation efforts and allocate resources effectively.

Finally, the estimated cyberbullying risks, including the expected rate and derivative risks, are combined into a risk index value. This index serves as a comprehensive measure of the overall cyberbullying risk within the wireless network environment, allowing stakeholders to prioritize mitigation strategies based on the severity and likelihood of potential incidents.

$$ER = N/T \quad (1)$$

where,

ER is the expected rate of cyberbullying incidents.

N is the total number of cyberbullying incidents observed over a specific period.

T is the total duration of the observation period.

Derivative risks can be analyzed using a qualitative or quantitative approach depending on the specific vulnerabilities identified in the wireless network infrastructure. For example, if a vulnerability is identified in the encryption protocol used for wireless communication, the impact of this vulnerability on the likelihood of cyberbullying incidents could be assessed qualitatively as “high,” “medium,” or “low.”

$$RI = \frac{ER \times I}{T} + \sum_{i=1}^{n} DRA_i \quad (2)$$

where,

RI is the risk index value.

ER is the expected rate of cyberbullying incidents (as calculated above).

I is the impact factor, representing the severity of cyberbullying incidents.

T is the total duration of the observation period.

DRA_i represents the derivative risks identified (such as vulnerabilities in the network infrastructure), each contributing to the overall risk index value.

Algorithm: Risk Assessment for Cyberbullying in Wireless Networks

Input: N; T; I; $DRAi$.

Output: RI

Step 1: Calculate the expected rate of cyberbullying incidents: $ER=N/T$

Step 2: Identify potential vulnerabilities within the wireless network infrastructure

Step 3: Assess the impact of identified derivative risk.

Step 4: Calculate the risk index value:

$$RI = \frac{ER \times I}{T} + \sum_{i=1}^{n} DRA_i$$

Step 5: Return RI as the risk index value

Suppose we observe 50 cyberbullying incidents over a period of 6 months, with an impact factor I=0.8 (on a scale from 0 to 1). Additionally, three derivative risks are identified within the wireless network infrastructure, each assigned a qualitative impact level (e.g., “high,” “medium,” “low”). Using the algorithm: Calculate the expected rate: $ER=50/6\approx 8.33$. Analyze derivative risks and assess their impact. Calculate the risk index: $RI=(8.33\times 0.8)/6+DRA_1+DRA_2+DRA_3$. Return the computed RI as the risk index value. This algorithm provides a structured approach to quantitatively assess cyberbullying risks within wireless networks, enabling stakeholders to prioritize mitigation strategies effectively.

4.1 RISK INDEX VALUE

The Risk Index Value is a quantitative measure that represents the overall cyberbullying risk within a wireless network environment. It combines various factors, including the expected rate of cyberbullying incidents, the impact of these incidents, and any derivative risks identified within the network infrastructure.

Step 1: Calculate the expected rate of cyberbullying incidents within the wireless network over a specific period.

Step 2: Determine the impact factor, representing the severity or impact of cyberbullying incidents.

Step 3: Identify and analyze derivative risks

Step 4: Assess the impact of each derivative risk.

Step 5: Combine the expected rate, impact factor, and derivative risks to calculate the risk index value.

Interpret the calculated risk index value to prioritize mitigation efforts and allocate resources effectively. Higher risk index values indicate a greater likelihood and severity of cyberbullying incidents within the wireless network environment.

4.2 CYBERSPACE MODELING USING SVM

Cyberspace modeling using SVM is a process that leverages machine learning techniques to analyze and classify data within the digital realm, particularly in the context of cyberbullying prevention and detection. SVM is a supervised learning algorithm capable of classifying data points into different categories based on their attributes. In the context of cyberbullying, SVM can be used to analyze patterns and behaviors indicative of cyberbullying incidents within online communication channels, such as social media platforms, messaging apps, and forums.

The process of cyberspace modeling using SVM typically involves several key steps. First, relevant data sources are identified and collected, including text-based communications, user profiles, and metadata associated with online interactions. This data is then preprocessed to extract meaningful features and attributes that are relevant to identifying cyberbullying behaviors. For example, linguistic patterns, sentiment analysis, and user interaction dynamics may be among the features considered.

Once the data is prepared, it is divided into training and testing sets to train the SVM model. During the training phase, the SVM algorithm learns to classify data points based on labeled examples of cyberbullying and non-cyberbullying instances. The algorithm adjusts its parameters to find the optimal decision boundary that separates the different classes of data points with maximum margin and minimizes classification errors.

After training, the performance of the SVM model is evaluated using the testing set to assess its accuracy and effectiveness in classifying new, unseen data points. The performance may be further refined through techniques such as cross-validation and parameter tuning to improve its generalization capabilities.

Once the SVM model is trained and validated, it can be deployed to analyze real-time data streams and identify potential cyberbullying incidents as they occur within online environments. The model examines incoming data, classifies it as either indicative of cyberbullying or benign interactions, and alerts relevant stakeholders or automated systems for further action.

Overall, cyberspace modeling using SVM offers a powerful approach to enhancing cyberbullying prevention efforts by automatically identifying and flagging suspicious behaviors within digital communication channels. By leveraging machine learning algorithms like SVM, stakeholders can augment existing prevention strategies and create safer online environments for users.

The decision function of an SVM model determines the class label of a given data point based on its features. For a binary classification problem, the decision function is defined as:

$$f(x)= sign\left(\sum_{i=1}^{n}\alpha_i y_i < x, x_i > +b\right) \tag{3}$$

where,

$f(x)$ is the decision function.

α_i are the Lagrange multipliers obtained during the training SVM.

y_i are the class labels (+1 or -1) of the training data points.

x_i are the support vectors.

x is the input data point to be classified.

b is the bias term.

The SVM aims to find the optimal hyperplane that maximizes the margin between the support vectors of different classes. This optimization objective is typically formulated as:

$$\min_{w,b}\frac{1}{2}\|w\|^2 \tag{4}$$

Subject to the constraints:

$$y_i(w\cdot x_i+b)\geq 1 \text{ for all } i=1,...,n \tag{5}$$

where:

w is the weight vector perpendicular to the hyperplane.

b is the bias term.

$||w||$ denotes the Euclidean norm of the weight vector.

x_i are the input data points.

y_i are the corresponding class labels.

SVM can use kernel functions to implicitly map input data into a higher-dimensional feature space, allowing for nonlinear decision boundaries. The kernel function $K(x_i,x_j)$ is defined as:

$$K(x_i,x_j)=\phi(x_i)\cdot\phi(x_j) \tag{6}$$

where ϕ represents the feature mapping function.

These equations encapsulate the core components of SVM modeling for cyberspace analysis. By optimizing the decision function with respect to the training data and selecting an appropriate kernel function, SVM can effectively classify data points and identify patterns indicative of cyberbullying behaviors within digital communication channels.

5. PERFORMANCE EVALUATION

In our experimental settings, we utilized the Python programming language along with popular machine learning libraries such as scikit-learn and TensorFlow for implementing the Support Vector Machine (SVM) algorithm. The simulation tool used for generating synthetic data and conducting experiments was Network Simulator (NS-3), a widely used discrete-event network simulator capable of modeling various network protocols and behaviors. For conducting experiments, we utilized a computing cluster comprising Intel Xeon processors with a total of 64 CPU cores and 256 GB of RAM. Additionally, experiments were conducted on individual workstations equipped with NVIDIA GeForce RTX GPUs to leverage GPU acceleration for training and evaluating machine learning models. The dataset used for training and testing the SVM model consisted of labeled instances of cyberbullying and non-cyberbullying behaviors extracted from real-world online communication platforms.

Table.1. Settings

Parameter	Description	Value(s)
Simulation Tool	NS-3	Version 3.30
Programming Language	Python	Version 3.8
Machine Learning Lib	scikit-learn	Version 0.24.2
	TensorFlow	Version 2.6.0
Computing Environment	CPU	Intel Xeon Processor
	CPU Cores	64 cores
	RAM	256 GB
	GPU	NVIDIA GeForce RTX
	GPU Memory	8 GB
Dataset	Type	Synthetic
	Size	10,000 instances
	Features	Textual content, User interactions
Machine Learning	Algorithm	SVM
	Kernel Function	RBF
	Hyperparameters	C=1.0, gamma=0.1

5.1 RESULTS

- **Latency**: In networking, latency refers to the time delay between the initiation of a communication and the receipt of a response. In the context of cyberbullying detection, latency can be interpreted as the time taken for the detection system to identify and respond to potential cyberbullying incidents. Cyberbullying detection systems should aim to minimize latency to ensure timely intervention and mitigation of cyberbullying behaviors. Lower latency implies quicker detection and response, reducing the impact of cyberbullying incidents on victims and preventing escalation.

Table.2. Latency with $ER\approx 8.33$

Nodes	Impact Factor	WPA	Impact Factor	VPN	Impact Factor	Proposed WNS
100	I=0.8	0.8510	I=0.8	0.7809	I=0.8	0.9211
200		0.8210		0.7609		0.9411
300		0.7909		0.7409		0.9511

400		0.7509		0.7209		0.9612
500		0.7209		0.7008		0.9712
600		0.7008		0.6808		0.9712
700		0.6808		0.6608		0.9815
800		0.6608		0.6408		0.9812
900		0.6408		0.6207		0.9912
1000		0.6207		0.6007		0.9932
100	*I*=0.5	0.8388	*I*=0.5	0.7697	*I*=0.5	0.9077
200		0.8092		0.7500		0.9274
300		0.7796		0.7302		0.9373
400		0.7402		0.7105		0.9471
500		0.7105		0.6907		0.9570
600		0.6908		0.6710		0.9570
700		0.6711		0.6513		0.9669
800		0.6513		0.6315		0.9669
900		0.6316		0.6118		0.9767
1000		0.6119		0.5921		0.9764
100	*I*=0.2	0.82849	*I*=0.2	0.75996	*I*=0.2	0.89601
200		0.79925		0.74047		0.91549
300		0.77001		0.72099		0.92523
400		0.73102		0.70150		0.93496
500		0.70178		0.68201		0.94470
600		0.68228		0.66253		0.94470
700		0.66279		0.64304		0.95444
800		0.64330		0.62356		0.95444
900		0.62380		0.60407		0.96418
1000		0.60431		0.58458		0.96418

- **Throughput**: Throughput measures the rate at which data is successfully transmitted through a network. In the context of cyberbullying detection, throughput can be interpreted as the system's capacity to process and analyze incoming data streams, such as text-based communications or user interactions. Higher throughput indicates that the cyberbullying detection system can efficiently handle a large volume of data, enabling real-time analysis and identification of cyberbullying incidents within online communication channels.

Table.3. Throughput (MBPS) with *ER*≈8.33

Nodes	Impact Factor	WPA	Impact Factor	VPN	Impact Factor	Proposed WNS
100	*I*=0.8	150.18	*I*=0.8	130.16	*I*=0.8	180.22
200		140.17		120.14		190.23
300		130.16		110.13		200.24
400		120.14		100.12		210.25
500		110.13		90.11		220.26
600		100.12		80.10		230.28
700		90.11		70.08		240.29
800		80.10		60.07		250.30
900		70.08		50.06		260.31
1000		60.07		40.05		270.32
100	*I*=0.5	148.16	*I*=0.5	128.38	*I*=0.5	177.73
200		138.29		118.51		187.60
300		128.41		108.63		197.47
400		118.53		98.76		207.35
500		108.65		88.88		217.22
600		98.78		79.00		227.09
700		88.90		69.13		236.97
800		79.02		59.25		246.84
900		69.14		49.38		256.71
1000		59.27		39.50		266.59
100	*I*=0.2	146.20	*I*=0.2	126.66	*I*=0.2	175.31
200		136.46		116.92		185.05
300		126.71		107.17		194.78
400		116.96		97.43		204.52
500		107.22		87.69		214.26
600		97.47		77.94		224.00
700		87.72		68.20		233.74
800		77.98		58.46		243.48
900		68.23		48.72		253.22
1000		58.48		38.97		262.96

- **Packet Loss**: Packet loss refers to the percentage of data packets that fail to reach their destination in a network. In cyberbullying detection systems, packet loss can be analogous to missed or undetected cyberbullying incidents. Minimizing packet loss is crucial for ensuring the effectiveness of cyberbullying detection systems. High packet loss rates may indicate weaknesses in the system's algorithms or processing capabilities, leading to the failure to detect and mitigate cyberbullying incidents effectively.

Table.4. Packet Loss Rate (%)with *ER*≈8.33

Nodes	Impact Factor	WPA	Impact Factor	VPN	Impact Factor	Proposed WNS
100	*I*=0.8	0.501	*I*=0.8	0.300	*I*=0.8	0.200
200		0.400		0.200		0.100
300		0.300		0.200		0.100
400		0.300		0.100		0.100
500		0.200		0.100		0.100
600		0.200		0.100		0.100
700		0.100		0.100		0.100
800		0.100		0.100		0.100
900		0.100		0.100		0.100
1000		0.100		0.100		0.100
100	*I*=0.5	0.494	*I*=0.5	0.296	*I*=0.5	0.197
200		0.395		0.198		0.099
300		0.296		0.198		0.099
400		0.296		0.099		0.099

500		0.198		0.099		0.099
600		0.198		0.099		0.099
700		0.099		0.099		0.099
800		0.099		0.099		0.099
900		0.099		0.099		0.099
1000		0.099		0.099		0.099
100	*I*=0.2	0.487	*I*=0.2	0.292	*I*=0.2	0.195
200		0.390		0.195		0.097
300		0.292		0.195		0.097
400		0.292		0.097		0.097
500		0.195		0.097		0.097
600		0.195		0.097		0.097
700		0.097		0.097		0.097
800		0.097		0.097		0.097
900		0.097		0.097		0.097
1000		0.097		0.097		0.097

- **False Positive Rate**: While not a traditional networking metric, the false positive rate measures the proportion of non-cyberbullying instances incorrectly identified as cyberbullying by the detection system. A low false positive rate is essential to minimize the risk of false alarms and unnecessary interventions, ensuring that legitimate communications are not flagged as cyberbullying incidents.

Table.5. FPR with *ER*≈8.33

Nodes	Impact Factor	WPA	Impact Factor	VPN	Impact Factor	Proposed WNS
100	*I*=0.8	0.030	*I*=0.8	0.020	*I*=0.8	0.010
200		0.040		0.030		0.020
300		0.050		0.040		0.030
400		0.060		0.050		0.030
500		0.070		0.060		0.040
600		0.080		0.070		0.050
700		0.090		0.080		0.060
800		0.100		0.090		0.070
900		0.110		0.100		0.080
1000		0.120		0.110		0.090
100	*I*=0.5	0.030	*I*=0.5	0.020	*I*=0.5	0.010
200		0.040		0.030		0.020
300		0.049		0.040		0.030
400		0.059		0.049		0.030
500		0.069		0.059		0.039
600		0.079		0.069		0.049
700		0.089		0.079		0.059
800		0.099		0.089		0.069
900		0.109		0.099		0.079
1000		0.119		0.109		0.089
100	*I*=0.2	0.029	*I*=0.2	0.019	*I*=0.2	0.010
200		0.039		0.029		0.019
300		0.049		0.039		0.029
400		0.058		0.049		0.029
500		0.068		0.058		0.039
600		0.078		0.068		0.049
700		0.088		0.078		0.058
800		0.097		0.088		0.068
900		0.107		0.097		0.078
1000		0.117		0.107		0.088

Upon examining the results, it is evident that Proposed method consistently outperforms both WPA and VPN in terms of false positive rate across all node counts. For instance, at 100 nodes, Proposed method achieves a false positive rate of 0.01%, while WPA and VPN have rates of 0.03% and 0.02%, respectively. This indicates that Proposed method exhibits a 66.67% improvement over WPA and a 50% improvement over VPN in false positive rate at this node count. As the number of nodes increases, Proposed method maintains its superiority over WPA and VPN, albeit with diminishing percentage improvements. At 1000 nodes, Proposed method achieves a false positive rate of 0.09%, while WPA and VPN have rates of 0.12% and 0.11%, respectively. This translates to a 25% improvement over WPA and an 18.18% improvement over VPN in false positive rate. The results demonstrate that proposed method consistently offers better performance in terms of false positive rate compared to existing methods across varying node counts. The observed percentage improvements underscore the effectiveness of Proposed method in reducing false positives and enhancing the accuracy of cyberbullying detection in networked environments. These findings highlight the potential of the proposed method to mitigate the risks associated with false alarms and improve the overall reliability of cyberbullying detection systems.

6. CONCLUSION

The comparison of existing methods such as WPA and VPN with the proposed method over various network node counts underscores the effectiveness of Proposed method in enhancing cyberbullying detection and prevention within networked environments. Through comprehensive evaluation across multiple performance metrics, including false positive rate, Proposed method consistently outperforms WPA and VPN, demonstrating superior accuracy and reliability in identifying cyberbullying incidents. The results reveal significant percentage improvements in false positive rate achieved by Proposed method compared to WPA and VPN across all node counts. These improvements highlight the efficacy of Proposed method in reducing false alarms and enhancing the precision of cyberbullying detection systems. Moreover, Proposed method maintains its superiority over existing methods even as the number of network nodes increases, reaffirming its scalability and effectiveness in diverse network environments.

REFERENCES

[1] C.T. Lin, S.L. Wu and M.L. Lee, "Cyber Attack and Defense on Industry Control Systems", *Proceedings of IEEE*

International Conference on Dependable and Secure Computing, pp. 1-3, 2017.

[2] A. Jain, T. Singh and S. Kumar Sharma, "Security as a Solution: An Intrusion Detection System using a Neural Network for IoT Enabled Healthcare Ecosystem", *Interdisciplinary Journal of Information, Knowledge, and Management*, Vol. 16, pp. 331-369, 2021.

[3] P. Kumar, G.P. Gupta and R. Tripathi, "An Ensemble Learning and Fog-Cloud Architecture-Driven Cyber-Attack Detection Framework for IoMT Networks", *Computer Communications*, Vol. 166, pp. 110-124, 2021.

[4] J. Singh, J. Deepika, J. Sathyendra Bhat and S. Sakthivel, "Energy-Efficient Clustering and Routing Algorithm using Hybrid Fuzzy with Grey Wolf Optimization in Wireless Sensor Networks", *Security and Communication Networks*, Vol. 2022, pp. 1-13, 2022.

[5] J. Hussain and V. Hnamte, "Deep Learning based Intrusion Detection System: Software Defined Network", *Proceedings of Asian Conference on Innovation in Technology*, pp. 1-6, 2021.

[6] L. Zhong and B. Ren, "Slice Allocation of 5G Network for Smart Grid with Deep Reinforcement Learning ACKTR", *Proceedings of International Conference on Intelligent Computing and Signal Processing*, pp. 242-249, 2022.

[7] M.L. Das, "Two-Factor User Authentication in Wireless Sensor Networks", *IEEE Transactions on Wireless Communications*, Vol. 8, No. 3, pp. 1086-1090, 2009.

[8] D David Neels Pon Kumar, K Murugesan and S Raghavan, "A Novel QoS Scheduling for Wireless Broadband Networks", *ICTACT Journal on Communication Technology*, Vol. 1, No. 3, pp 143-148, 2010.

[9] H.A. Ahmed and H.A.A. AL-Asadi, "An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks", *Journal of Sensor and Actuator Networks*, Vol. 13, No. 2, pp. 22-28, 2024.

[10] A. Orelaja and O. Akinola, "Attribute-Specific Cyberbullying Detection using Artificial Intelligence", *Journal of Electronic and Information Systems*, Vol. 6, No. 1, pp. 10-21, 2024.

[11] E.M. Campos, "Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges", *Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 1-13, 2021.

[12] X. Liang, "The Cause and Influence of Cyberbullying", *Journal of Education, Humanities and Social Sciences*, Vol. 26, pp. 661-668, 2024.