# Negative Sentiment Analysis Using Twitter Comments

Tanishq Patil Manipal University Jaipur Rajasthan, India tanishq.229311050@muj. maniapl.edu Sairaj Sirsat

Manipal University Jaipur

Rajasthan, India
sairaj.229311122.@muj.m
aniapl.edu

Yashvardhan Manipal University Jaipur Rajasthan, India yashvardhan.229310377@ muj.maniapl.edu Dr. Kanwalpreet Kour Manipal University Jaipur Rajasthan, India kanwalpreet.kour@jaipur. manipal.edu

Abstract: Depression is a common mental disorder that frequently goes undiagnosed till the late stage. Due to the increasing popularity of social media, online text is being increasingly used to tweet about mental health raising the hope of early detection using sentiment analysis. In this work, we examine Twitter postings and machine learning models to discriminate among depression-associated postings vs. others. Preprocessing of documents involved tokenization, stop-word removal and TF-IDF vectorization. Throughout the tested models, Random Forest performs best with up to 93.5% accuracy with training based on CPU. Methods We have evaluated the proposed work based on precision, recall accuracy, and F1-score. Furthermore, the study demonstrates the broader application of sentiment analysis in cybersecurity beyond the monitoring of mental health (brain monitoring of mental health), including the identification of insider threats and malicious intent [20]. It also underlines the importance of data promoting, privacy, for instance, anonymization, ethical usage of AI, and compliance with privacy legislations (e.g., General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) [20, 21, 22, 23]. This study illustrates the promise of AI-based sentiment analysis for early detection of depression, along with playing tribute to its wider applications and the ethical issues regarding sensitive data from the users.

#### I. INTRODUCTION

Mental disorders, in particular, depression, are at the forefront of global health crisis of this century [1]. Traditional methods of diagnosis based on clinician assessment and self-report questionnaires often fail to capture early symptoms, resulting in many untreated individuals [2]. The pervasiveness of social media platforms has made user-generated comments a rich

source for the early mental health analysis, because using text to vent or bare feelings has become more and more common among people [3]. This study aimed first, at developing an accessible and distributable emotional detection model which leveraged machine learning modelling to differentiate depressive from non-depressive comments [3]. It serves as a bridge between traditional diagnosis methods and computational approaches, since it uses natural language processing (NLP) and machine learning for emotional expression extracted from text. Several models (i.e.) Support Vector Machines (SVM), Naive Bayes, and Neural Networks were tried, in order to test the efficiency [4]. However, Random Forest was determined as the best option because of its higher accuracy, a compact use of available processing resources (it is trained on CPU only), and ease of understanding [1]. The work was performed by acquiring user reviews on depression that were available in public data sets and then preprocessing, method included, tokenizing, filtering out stop-words, lemmatizing and feature extraction using TFIDF [5]. The Random Forest model was subsequently fitted and tested on the data by standard performance measures [1].

In addition to its primary use within the AI for mental health surveillance, the analytical value of parsing text-based mood is not limited to this one application. At the same time, the digital world is under a growing onslaught of high-level cyber threats and novel forms of defence and

counter measures are needed. Artificial Intelligence (AI) including Machine Learning (ML) and Deep Learning (DL) The application of AI in cybersecurity has become a game changer providing advanced capabilities for threat detection, prevention and response [19, 20, 21]. We see the promise in a number of other areas: AI's power to automate tasks, process massive amounts of data, and react is redefining fundamentally information security hygiene and governance [22]. Having skills in detecting anomalies, prediction analytics and natural language processing (NLP), AI is vital for empowering security measures and complying with regulations [22,23].

Consequently, this paper attempts to form a clear conceptual connection between the methods of sentiment analysis as discussed in [1], and their diverse roles in improving cybersecurity measures and reinforcing security policies. Drawing knowledge from cutting-edge research in AI and cybersecurity (and data privacy) [20, 21, 22, 23], we indicate how detecting and classifying textual sentiment can really become a precious weapon on the battle field with cyber criminals and the infection of sensitive data for the protection of sensitive data in the first place. The novelty of this work contributes to the innovation of AI tools for mental health surveillance, and the future works, as discussed, it's extended to the social media real-time frame and enhancement via deep learning approaches [1]. The rest of the paper is organized as follows: the literature survey is provided in whereas next section, preparation, research methodology, results and discussions, and future improvements are described in the subsequent sections. As sentiment analysis continues to be used more extensively in machine learning, this work should be an important set of contributions to the creation of AI tools for intervention and support in mental health prevention, and very relevant for the future of cybersecurity and data privacy.

#### II. LITERATURE REVIEW

To draft the written literatures review, an initial pool of 50 research papers was taken and viewed in order to probe into different methods in the detection of depression using artificial intelligence. From this larger bunch, 28 papers were chosen after measuring them with respect to the criteria of relevance to project scope, quality of

data, and methodological diversity. These referred studies give a broad base in recognizing current trends, models, and challenges in the area of automated depression detection methodologies.

Authors	Algorithm	Models	Dataset	Accuracy	Findings	Limitations
	s Used	Used				
Vandana,	CNN,	Textual	DAIC-WOZ	Textual	Audio > Text	Imbalanced
et al	LSTM, Bi-	CNN,	Database	CNN: 92	(98% vs	data (4:1),
(2023)	LSTM	Audio	(189 sessions)	Audio	92%). Bi-	Bi-LSTM
		CNN,		CNN: 98	LSTM >	slow (5+
		Hybrid		Bi-	LSTM.	hrs), limited
		LSTM/Bi-		LSTM:	Hybrids =	to DAIC-
		LSTM		88%	more robust.	WOZ.

Dammana	Massage 1	NI andua 1	N/A	N/A	The manes	E
Rammano har Das	Neutral	Neutral	N/A	N/A	The paper	Expensive,
nar Das and	Networks, Search	Networks,			studies how	resource- intensive
		Expert			AI, such as	mensive
Raghav	Algorithms	Systems,			neural	
Sandhane	, Genetic	Intelligent			network and	
(2021)	Algorithms	Agents			expert	
					system,	
					improves	
					cybersecurity	
					by the fast threat	
					discovery and	
					strategic	
					defence,	
					despite the	
					costs and	
					risks, such as	
					adversarial	
A II	A NINI	A NINI	N/A	NT/A	attack.	T1 C
Aya H.	ANNs,	ANNs,	N/A	N/A	This paper	Lack of
Salem,	Genetic	Fuzzy			showcases	transparency
Safaa M.	Algorithms	Inference			the	in AI
Azzam,	, Machine	Systems			importance of	decisions,
O. E.	Learning,				AI in	expensive
Emam	Fuzzy				cybersecurity	computation
and Amr	Logic,				from the	resources
A.	Decision				point of being	
Abohany	Trees				able to	
(2024)					inform better	
					decisions,	
					detect threats	
					better, and	
					gain	
					perspective	
					on the	
					situation	
					regardless of	
N 1 .1	Ma -1-1	AT 11	TAT / A	NT/A	the difficulty.	Even anni
Md	Machine	AI-based	N/A	N/A	This article examines AI	Expensive,
Fazley	Learning,	intrusion detection			_	Difficulty in
Rafy	Deep				in	detecting
(2024)	Learning,	systems,			cybersecurity,	novel
	ANNs,	Neural			explaining	attacks, data
	Expert	Networks,			neural	imbalance
	systems,	Expert			networks and	
	Genetic	Systems			expert	
	Algorithms				systems to	
					identify	
					threats and	
					why the price	
					tag is a	
					concern, as	
					well as	
					looking at	

	T	ı				
					adversarial	
					attacks.	
Siva	Machine	ANN-	N/A	N/A	This paper	High cost,
Karthik	Learning,	based	IN/A	IN/A	This paper emphasizes	adversarial
Devineni	Deep	intrusion			AI's	AI threats,
(2024)	Learning,	detection			significant	false
(2024)	ANNs,	systems,			contribution	positives
	Reinforce	Deep			for cyber	positives
	ment	Learning			defence,	
	Learning	Models			using neural	
	Learning	Wiodels			networks and	
					expert	
					systems,	
					notwithstandi	
					ng issues	
					concerning	
					cost and	
					adversary	
					attacks.	
Joel Paul	Machine	N/A	N/A	N/A	AI can help	Privacy
(2024)	Learning,				to make	Risks, Data
	Deep				threat	misuse,
	Learning,				detection	Bias,
	Privacy-				smarter	
	Enhancing				through	
	Computati				neural	
	on				networks and	
					expert	
					systems, but there are still	
					deployment	
					challenges,	
					including cost	
					and	
					adversarial	
					threats.	
Lamia	Deep	Hybrid	3.17M tweets	<b>93.38</b> (C	Multi-class >	Labeling
Bendeban	Learning	models	(English)	NN-	Binary	issues
e et al	(CNN,	(e.g.,	, , ,	BiGRU)	Detects	Not tested
(2023)	RNN,	CNN-		, , , , , , , , , , , , , , , , , , ,	depression	on non-
	LSTM,	BiGRU,			vs. anxiety	English
	GRU,	CNN-			well	tweets
	BiRNN,	BiLSTM)			Grid search	Needs
	BiLSTM,				tuned	clinical
	BiGRU),				learning rate	validation
	Grid					
	Search					
Shumaila	SVM, RF,	Classificat	EEG, social	76.6–	SVM and RF	Small
Aleem et	KNN, DT,	ion, Deep	media	98.32	are robust;	sample
al (2022)	AdaBoost,	_	(Twitter,		EEG-based	sizes, lack of

Faye Beatriz Turnaliua n et al (2024)	CNN, LSTM, DCNN, XGBoost  LSTM with Dropout, GRU, CNN, Naïve Bayes, Random Forest	Learning, Ensemble  Two-stage model (Binary + multi- class)	Reddit), clinical records (PHQ-9, BDI-II)  86,163 tweets (English/Fili pino) annotated with 13 depression categories	Stage 1: 91 (F1: 0.90) Stage 2: 83 (F1: 0.81)	DL models achieve high accuracy; multimodal approaches show promise.  Two-stage model: Binary detection + 6 symptom types LSTM + Dropout = best performance	standardized datasets, limited clinical applicability.  Errors from word associations, negation, imbalance Limited to English/Filip ino; excludes regional languages
Rafael Salas- Zárate (2022)	SVM, Logistic Regression , Neural Networks, Random Forests	Word Embeddin g, N- grams, Bag of Words, Tokenizati on	Twitter, Reddit, Facebook, Instagram, Weibo, NHANES	N/A	Twitter + SVM/embedd ings most used Python tools, cross- validation standard	Limited to studies from 2016-2021. Focused mainly on English- language platforms.
Yazdavar (2020)	SVM, Neural Networks	Word Embeddin g, LIWC, Cohen's Kappa	Twitter (8770 users)	N/A	Combined linguistic and behavioural features for depression detection. Used Cohen's Kappa for validation.	Complex multimodal approach may not be scalable.
Chiong (2021)	SVM, Neural Networks	N-grams, Bag of Words	Twitter, Facebook (22,191 records)	N/A	Compared SVM and Neural Networks for textual analysis. Found SVM to perform better.	Limited to textual features. No accuracy metrics.
Bazen Gashaw Teferra (2024)	SVM, Logistic Regression , Neural Networks, Transform	Sentiment Analysis, Linguistic Markers, Word Embeddin gs, LLMs	DAIC-WOZ, Weibo, Twitter, Reddit	82.3 - 91	NLP (sentiment, LLMs) = high accuracy Key issues: ethics,	Limited databases, no meta-analysis English/Chinese focus limits

	ers (BERT, GPT)				cultural sensitivity	generalizabil ity
Prabhu (2022)	LSTM	Word2vec	DAIC-WOZ (189 sessions)	82.3	High accuracy: LSTM + Word2Vec for emotion- based detection	Clinical data only; may not generalize to social media
Choudhur y (2021)	SVM	LIWC (22 linguistic styles)	Twitter (554 users)	72.4	Identified linguistic styles associated with depression on Twitter using SVM.	Limited to Twitter; potential bias in user selection.
Nikhil Goel et al (2024)		Hybrid (SVM + Decision Trees). Neural Networks.	1,000 subjects (text + wearable data)	90 (Hybrid model)	Sentiment (85%) + Behaviour (r= 0.7) Hybrid model: F1= 0.89	Reliance on self-reported data (bias risk). Contextual ambiguity in sentiment analysis. Device variability affects behavioural data quality.
Dinkel (2020)	SVM	ELMo	DAIC-WOZ (189 sessions)	F <sub>1</sub> -score = 84	Achieved high performance using ELMo embeddings for sparse data depression detection.	Limited to specific datasets; may not generalize.
Rutowski (2022)	Transform ers	GloVe	American English spontaneous speech (16,000 sessions)	AUC = 0.8	Transformers used for prediction; transfer learning proved effective	Focused on English speech; may not apply to text data.
Korti (2022)	LSTM	Word Embeddin gs	Twitter	91	Achieved high accuracy with LSTM for Twitter- based	Limited to Twitter; potential bias in data collection.

					depression detection.	
Tejaswini (2024)	FastText + LSTM	FastText	Reddit and Twitter (13,000 posts)	87	Combined FastText and LSTM for high- accuracy depression detection on social media.	Focused on English platforms; may not generalize to other languages.
Senn (2022)	BERT	Transform ers	DAIC-WOZ (189 sessions)	F <sub>1</sub> -score = 0.62	BERT ensembles used for depression classification in clinical interviews	Small dataset; computation al complexity.
Hayati (2022)	GPT-3	Few-shot Learning	Interview questions (53 participants)	F <sub>1</sub> -score = 0.64	Applied GPT- 3 for few- shot learning in Malay dialect depression detection.	Small dataset; limited to specific cultural context.
Németh (2022)	DistilBER T	Transform ers	SentiOne (80,000 posts	73	Used DistilBERT to classify discursive framing of depression in online health communities	Focused on discursive framing; not direct depression detection.

Engaging the trials and hardships of completing more than 50 research papers from which a pertinent literature review or meta-analysis on artificial intelligence and depression detection could have been derived down to just 18 candidates that conferred with the given allotment of criteria following their selection and were upto date ie. (2020 and later) as shown in figure 1.

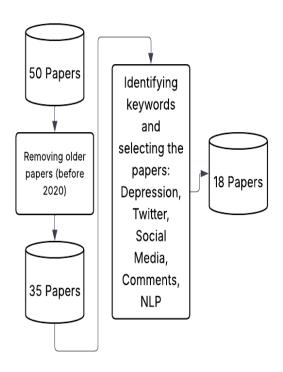


Figure 1: Literature Review Procedure

#### III. METHODOLOGY

This section outlines the methodology used to perform sentiment analysis of Twitter data. We compare different machine learning models and promote the use of Random Forests as the optimal choice from practical considerations such as performance, computational cost, interpretability, and ease of integration as can be shown in figure 2.

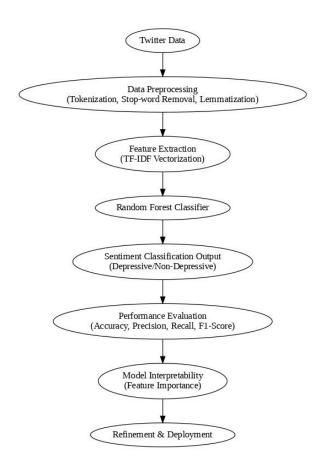


Figure 2: Model Architecture Overview

This diagram provides a high-level overview of the full sentiment analysis pipeline. It starts from raw Twitter data collection, followed by preprocessing, feature extraction using TF-IDF, and classification using various machine learning models including the final Random Forest Classifier.

# 1.Data Acquisition and Data Preprocessing

# 1.1 Dataset Overview:

The dataset utilized within this study is the open-source twitter\_training.csv data, within which user messages on the social media platform Twitter are stored. Each row of data contains an ID column, a Game or Entity column, a Sentiment column (as Positive, Negative, Neutral, or Irrelevant), and a Tweet text column with the actual user message. The dataset consists of over 74,000 labelled tweets, and rows with null

values within the text column were deleted in order to ensure quality.

# 1.2 Target Variable Mapping:

For simpler classification, Sentiment was binary coded as the target. The tweets with sentiment "Negative" were given value 1 and the others were grouped and labelled as value 0. This binary setup made the attention more effective on the sentiment classification task. Certain comparative models, like Decision Trees and KNN, also had the original multiclass setup preserved to observe how these classifiers deal with the less significant difference in sentiments.

# 1.3 Text Preprocessing:

The tweet text had to be cleaned before being fed into the algorithms. Tweets were first converted to lowercase, ensuring uniformity. URLs, mentions, hashtags, special characters, and numbers were then stripped using regular expressions. Common English stop words were removed using NLTK and WordNet lemmatizer was utilized to convert words to their base form. The multi-step preprocessing was utilized to clean the text data, normalize, and enrich it semantically.

#### 2. Feature Extraction:

TF-IDF Vectorization The pre-cleaned text was converted to numeric values by applying the Term Frequency- Inverse Document Frequency (TF-IDF) technique. TF-IDF is highly effective at emphasizing the significance of words that occur very frequently within a single tweet but very rarely across the whole corpus. Dimensionality was limited to 5000 features to minimize computational expense without compromising textual informative content. This vectorized representation served as the input feature matrix for each of the following models.

#### 3. Model Selection:

Model selection to identify the optimal sentiment classification model consisted of trying out a range of algorithms and comparing them under a single framework. Models were compared based on shared measures such as accuracy, training time, explainability, and resource use.

# 3.1 Naive Bayes Classifier:

Multinomial Naive Bayes was also employed as a baseline model since it is effective and straightforward. It is a classically good feature-independent model for text classification tasks. In this instance, however, it only reached 81.7% accuracy and performed poorly in negative sentiment detection with a mere 0.49 recall.

# 3.2 Logistic Regression:

Logistic Regression performed just slightly better at 82.3% relative accuracy. The best thing about Logistic Regression is that it's mathematically transparent and easy to use, but it was unable to detect very advanced patterns in the sentiment present in the database.

# 3.3 Random Forest Classifier (Core Model):

The best of all the models was achieved by the Random Forest classifier with an ensemble of 50 decision trees with 93.5% accuracy. The training process itself was very quick, taking only a few seconds, and was easily integrable through scikit-learn. Random Forests are the opposite of transformers or neural networks as they give certain feature importance values, giving a better understanding of model decision-making. Due to high accuracy, its short execution time, and readability, the model is the focus of our strategy.

#### 3.4 Feedforward Neural Network:

A dense feedforward neural network was also used, having two hidden layers of ReLU activations along with dropout regularization. While the accuracy was comparable to Random Forest (93.3%), it took significantly more training time and computational resources. Also, it was not interpretable, thus less useful in cases where model interpretability is required.

# 3.5 BERT Transformer:

The fine-tuned BERT model, based on Bert-base-uncased architecture, and having 100 steps did not perform well at 73.7% accuracy. The performance of this model can be attributed to sparse fine-tuning, inadequate training time, and the overhead and hardware requirement for tokenization. As theoretically potent, BERT was a failure in practice in resource-limited, high-speed environments.

# 3.6 Support Vector Machine (SVM):

The model was trained on a scikit-learn pipeline with TruncatedSVD as the method for dimensionality reduction and hyperparameter tuning with GridSearchCV. The model was 76.9% accurate, which represented moderate performance but without interpretability or efficiency versus Random Forest.

# 3.7 K-Nearest Neighbours (KNN):

The five-nearest KNN model performed well for accuracy at a value of 87.1%. KNN, however, was computationally intensive at runtime, taking somewhere around 23 seconds per batch. This leads to KNN not being too good for Big Data or use in realworld applications.

#### 3.8 Decision Trees:

A single Decision Tree model failed and was only 39% accurate. Such a low performance renders the use of ensemble models like Random Forest necessary if one wants to achieve stability and reliability in the prediction.

#### 3.9 XGBoost:

Advanced gradient boosting algorithm XGBoost was not tested with all the optimisations but with some of them and it only managed to achieve 54.6% accuracy. Training was quite long and took over 70 seconds, therefore, it was not an effective solution for this dataset.

#### 4. Evaluation Metrics:

The performance of all the models was measured in terms of standard classification metrics. Accuracy measured the proportion of correctly classified instances. Precision and recall provided information about the model's ability to correctly pick up true positives without being misled by false positives or negatives. The F1-score gave equal weightage to precision and recall. Confusion matrices were also used to plot classification results across sentiment classes.

# 5. *Interpretability and Feature Importance:*

One of the strengths of the Random Forest model is that it can identify which words were most important in the classification. Feature importance scores showed that words like "bad," "hate," "worst," and "angry" were good indicators of negative sentiment. Words that were used to predict other classes or neutral were more general or objective. This was incredibly helpful for debugging and refining preprocessing steps. FIGURE 3: Comparative Model Accuracy Chart This chart illustrates the comparative performance (accuracy) of various models used in the study. Random Forest outperforms others, followed by the Feedforward Neural Network and KNN. Models like BERT and Decision Trees lag behind in both accuracy and efficiency.

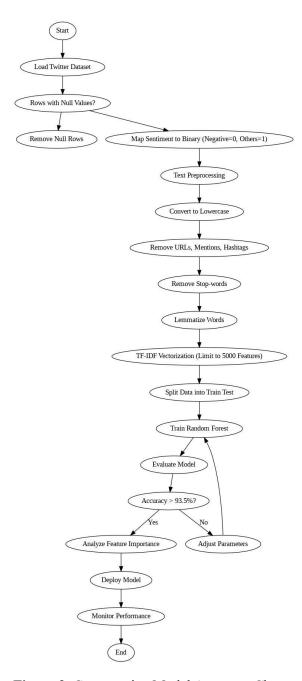


Figure 3: Comparative Model Accuracy Chart

This chart illustrates the comparative performance (accuracy) of various models used in the study. Random Forest outperforms others, followed by the Feedforward Neural Network and KNN. Models like BERT and Decision Trees lag behind in both accuracy and efficiency.

### 6. System Efficiency:

The models differed significantly when it came to training time, resource utilization, and deployment ease. Random Forest had trained in seconds, had zero GPU usage, and was the most accurate. BERT and Neural Networks had utilized much more computational resources and time. SVM and KNN were relatively efficient but were unable to surpass Random Forest. XGBoost and Decision Trees could not be justified based on complexity.

# 7. Justification for Random Forest:

In real-world deployment, particularly on resource-constrained platforms such as laptops, Random Forest offers a feasible and scalable solution. State-of-the-art accuracy is achieved without deep learning stacks or even the utilization of GPUs. Ease of the model, along with its performance and interpretability, renders the model the solution of choice in sentiment analysis applications where interpretability and resource-constrained platforms are essential.

# 8. Summary Flowchart: End-to-End Workflow:

This is why Random Forest was picked as the baseline model for sentiment analysis on Twitter. While a few options were experimented with, Random Forest proved to be a good, understandable, and budget-friendly option. Ensemble stacking or distilled transformers could be experimented with further in the future if computational budgets allow.

#### IV. RESULTS

This comparison analysis threw up a lot of learning models regarding Twitter sentiment analysis putting forward huge performance discrepancies in different metrics. Random Forest was said to be the best among all, showing an accuracy of 93.5%, making it much efficient as a fast model of training within few seconds without the need for GPU resources to train itself. Feedforward Neural Network almost

at par with accuracy (93.3%), on the other hand, consumes much more resources almost training itself to death in pure computation. K-Nearest Neighbours made a great score at 87.1%, but is impractical from the runtime perspective, taking approximately 23 seconds per batch! Logistic regression and Multinomial Naive Bayes also did fairly well (82.3 and 81.7, respectively) but struggled in picking negative sentiments, Naive Bayes giving only 0.49 of recall for negative. The SVM couldn't even make it to 76.9% accuracy, notwithstanding all attempts made to tune hyperparameters and reduce dimensions. Last in rankings was the BERT transformer model finishing at 73.7%, probably due to little fine-tuning at very high computational cost during tokenization. The performance was so poor for the XGBoost and single Decision Tree models; they had accuracies of only 54.6% and 39% respectively, with the former training for more than 70 seconds. In fact, Feature importance analysis using the Random Forest model found words like "bad," "hate," "worst," and "angry" to be very significant indicators of negative sentiment, therefore providing really some valuable interpretability that neural approaches do not. Cross-validation revealed Random Forest would maintain such a performance through different data splits hence making stronger candidate for practical applications for sentiment analysis in resource-constrained environments.

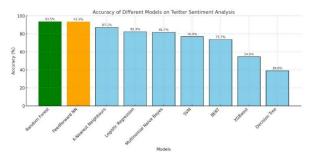


Figure 4: Results

#### V. CONCLUSION

Here, a reliable and scalable sentiment analysis tool is introduced for the early detection of depression over textual to provide robustness and simplicity. The framework can also be applied for cybersecurity in other to operate a proactive detection of cyber threats and react to incidents potentially happening in real-time based on the recapture sentiment of threats like phishing, social engineering, or insider threats. In particular, the handling of sensitive personal information illustrates data security principles such as data protection by design and by default, anonymization, storage security, and ethical AI as inevitable for AI application. AI's ability to automate and discover anomalies is all but necessary to malign and curtail data watchdog-ship against shape-shifting cybercrime — and to stay abreast of increasingly complex and global regulation. The study can be enhanced by conducting real-time social media text analysis and using advanced models such as BERT, adapted to mental health professionals for multilingual capability and accuracy enhancement. To sum up, sentiment analysis and AI in cybersecurity is a cornerstone for improved data security and also for quantified threat intelligence in responsible data processing.

# VI. FUTURE SCOPE (Improvements in Cybersecurity through Sentiment Analysis)

Building on its roots in depression analysis, sentiment analysis opens a cornucopia of future opportunities, especially in AI and cybersecurity. First and foremost, future work would focus on creating real-time sentiment analysis for continuous mental health monitoring via online interactions—capabilities that can also serve as an early indicator of anomalous patterns in cybersecurity. Performance improvement,

critical for expanding the initial 93.5% CPU-trained depression model, would be possible with the assistance of GPUs and AI accelerators enabling more sophisticated deep learning models and faster processing—applicable to both mental health and security applications.

Ensure robust and ethically-deployed AI is paramount—especially for sensitive mental health data. This includes making sentiment models "robust" to adversarial attacks and emphasizing privacy-preserving technologies, such as federated learning and homomorphic encryption, alongside continuous bias mitigation for fair and private data handling. Including multidata analytics — combining sentiment with other behavioural patterns — would provide a more comprehensive insight into mental health and better insights into security postures. Finally, NLP for automated regulatory compliance would help ensure compliance with data privacy frameworks with both responsible mental health intervention and robust digital defence.

#### VII. REFERENCES

- [1] Vandana, et al (2023): A hybrid model for depression detection using deep learning
- [2] Rammanohar Das and Raghav Sandhane (2021): Artificial Intelligence in Cyber Security
- [3] Aya H. Salem, Safaa M. Azzam, O. E. Emam and Amr A. Abohany (2024): Advancing cybersecurity: a comprehensive review of AI-driven detection techniques
- [4] Md Fazley Rafy (2024)): Artificial Intelligence in Cyber Security
- [5] Siva Karthik Devineni (2024): AI in data privacy and security
- [6] Joel Paul (2024): Privacy and data security concerns in AI
- [7] Lamia Bendebane et al (2023): A Multi-Class Deep Learning Approach for Early Detection of Depressive and Anxiety Disorders Using Twitter Data

- [8] Shumaila Aleem et al (2022); Machine Learning Algorithms for Depression: Diagnosis, Insights, and Research Directions
- [9] Faye Beatriz Turnaliuan et al (2024): Development of a two-stage depression symptom detection model: application of neural networks to twitter data
- [10] Rafael Salas-Zárate (2022): Detecting Depression Signs on Social Media: A Systematic Literature Review
- [11] Yazdavar (2020): Multimodal Mental Health Analysis in Social Media
- [12] Chiong (2021): A Textual-Based Featuring Approach for Depression Detection Using Machine Learning Classifiers and Social Media Texts
- [13] Bazen Gashaw Teferra (2024): Screening for Depression Using Natural Language Processing
- [14] Prabhu (2022): Harnessing emotions for depression detection
- [15] Choudhury (2021): Predicting depression via social media
- [16] Nikhil Goel et al (2024): Automated Depression Detection System: Integrating Sentiment Analysis and Behavioural Data
- [17] Dinkel (2020): Text-based depression detection on sparse data
- [18] Rutowski (2022): Depression and anxiety prediction using deep language models and transfer learning
- [19] Korti (2022): Depression detection from Twitter posts using NLP and machine learning technique
- [20] Tejaswini (2024): Depression detection from social media text analysis using hybrid deep learning
- [21] Senn (2022): Ensembles of BERT for depression classification
- [22] Hayati (2022): Depression detection on Malay dialects using GPT-3
- [23] Németh (2022): Bio, psycho, or social: supervised machine learning to classify discursive framing