Decoding Ideology: Machine learning-based Detection of Extremist Content

1st Shynar Mussiraliyeva
dept. of Information Systems
al-Farabi Kazakh National University
Almaty, Kazakhstan
mussiraliyevash@gmail.com

2nd Kymbat Baisylbayeva
dept. of Information Systems
al-Farabi Kazakh National University
Almaty, Kazakhstan
baisylbaeva.k@gmail.com

3rd Milana Bolatbek
dept. of Information Systems
al-Farabi Kazakh National University
Almaty, Kazakhstan
bolatbek.milana@gmail.com

4th Zhastay Yeltay
dept. of Information Systems
al-Farabi Kazakh National University
Almaty, Kazakhstan
jastayeltay@gmail.com

***Abstract*— This paper explores the use of machine learning techniques to classify texts with regard to extremist ideology, such as radicalization, propaganda, and recruitment. The relevance of this topic is the effective identification and analysis of content that contributes to the spread of extremist ideas on the Internet. This article discusses various approaches to preprocessing textual data and selecting machine learning models. Text materials on social networks, Internet forums, and other online resources were used as a data set. Experiments have been conducted using various classification algorithms, including Naive Bayes classifier, SVM and Logistic regression, etc. The results of the study confirm the possibility of effective use of machine learning methods for automatic classification of texts according to their extremist ideology, which can be a useful tool for detecting and countering the spread of extremist ideas on the Internet.**

Keywords*— *machine learning, radicalization, propaganda, recruitment, text classification, NLP

I. Introduction

The Internet has become an integral part of the daily lives of billions of people around the world. Social networks, forums, blogs and other online platforms provide unique opportunities for sharing ideas, information and access. Along with freedom of speech, destructive speech flourished. As the Internet becomes an increasingly important communication channel, it has also become a platform for various forms of negative communication, including bullying, threats, discrimination, and even cyberbullying [1-2]. This is an alarming situation, raising serious questions about free speech, responsibility and ethical behavior online. Determining destructive text is one of the most important activities. It helps create problematic patterns of behavior in online environments. Recognizing destructive speech helps prevent negative consequences such as interpersonal conflicts, the spread of hatred and violence, as well as psychological harm to the victims of such speech. In addition, destructive text detection allows online platforms to protect users from harmful or threatening content. Also, understanding destructive speech helps to build healthy relationships and has a great effect on strengthening the relationship between network users. Destructive text that encourages extremism can cause many dangerous problems. One of them is radicalization – when people start to adopt radical or violent ideologies, acts of terrorism, hate speech and can cause hatred and discrimination against certain groups of people because of their religion, race, political beliefs, and other characteristics. Disruption of social harmony and conflict between different groups can be attributed to another of the problems caused by the destructive text. The ideology of extremist texts is a system of beliefs, values, ideas, and concepts that are propagated and disseminated in the form of texts in order to attract people to extremist or radical views and actions. These texts may contain incitement to violence, discrimination, hatred against certain groups of people, as well as promotion of ideas aimed at destroying or destroying the existing values of society. It may include the following moments: hatred and discrimination, incitement to violence, falsification of concrete facts, manipulation of society and use of emotional methods to increase the effect of propaganda, rejection of democratic values. Determining the ideology of the text plays an important role in the fight against radicalization, propaganda and recruitment, it allows to identify, analyze and prevent actions that harm the society at the initial stage. The purpose of this work is to build machine learning models for classification by different classes such as Neutral texts, Propaganda, Recruitment and Radicalization. The goal is directly related to the detection of extremist texts on social networks.

As we wrote earlier, this work examines three directions of ideology, such as radicalization, propaganda, and recruitment. We decided to give a brief description of each of them below:

Radicalization is defined as the process of increasing the extremity of beliefs, feelings, and behaviors in support of political violence in the context of strong group identification and response to perceived threats to the in-group. Extremist propaganda can radicalize a target audience by strengthening group identification, fostering hatred toward other groups, and exaggerating external threats. The process of radicalization can occur through direct influence by extremist religious leaders and combat training, as well as through virtual terrorist radicalization, disseminated via the internet and social media.

Terrorist recruitment can be defined as the process of attracting young individuals to participate in terrorist activities and support the Islamic jihad war. This process can involve direct influence by extremist religious leaders as well as the use of social media and the internet to spread propaganda and recruit new members. With the growth of internet and social media penetration, terrorist networks exploit platforms like Twitter, YouTube, and Facebook to recruit new members, particularly among the youth, and to promote violent ideologies.

Propaganda is defined as information, particularly biased or misleading, used to promote a political cause or viewpoint. In the context of terrorist networks, propaganda plays a critical

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

role and is employed to achieve tactical objectives on both global and local levels. Terrorist propaganda involves the use of violent actions to spread fear, intimidate public opinion, legitimize violence, and engage broader audiences with terrorist ideologies. Additionally, it is aimed at establishing an emotional connection with the target audience, and fostering a collective identity that motivates violent actions. Propaganda plays a key role in ISIS's operations, and the terrorist organization's success is largely due to its ability to use data and manipulative means to shape its fascination and persuasion in the open. [3-7]

Focusing on the Kazakh language in this article is a significant and reasonable choice for several reasons, including the uniqueness and novelty of the study. It is important to note that in world practice there are very few such studies, and this work is the first aimed at determining the ideology of texts in the Kazakh language. This article represents the first attempt to determine the ideology of texts in the Kazakh language, which is an important step in the development of this area and opens up new prospects for future research.

II. RELATED WORKS

The used dataset in [8] consists of two parts. The first dataset includes 400 examples, and the second one is compiled from 40,000 tweets. The second dataset itself is divided into two groups: the first group is based on ISIS ideology, and the second group is a collection of anti-white messages. It is used in automatic short description of extremist oriented texts with the help of primary data set. The data set in the second part was used to train the classifier and to determine the area where extremism occurred. Algorithms such as naïve Bayes, support vector machine, random forest and XGBoost were applied to the collected database [9]. The best performance was achieved using the support vector machine algorithm.

In the work [10] about three thousand tweets published by one user recognized as a whistleblower. One of the main questions addressed in this study is how extremists use social media, including Twitter, to spread extremist ideology, specifically radicalization, propaganda, and recruitment. The study aims to understand how IS members and supporters use social media for terrorism.

In the work [11], a news dataset was considered as a dataset, and the BERT model with and without additional tuning was used as a model. Makes significant contributions to the study of political ideology and polarization by introducing a multidimensional approach. This approach improves understanding of ideological content in media and its evolution over time, offering a valuable resource for future research in political science and computational linguistics. The study's innovative methodology and rigorous analysis provide a strong foundation for further exploration of the complexities of political ideology.

The research work [12] provides specific descriptions of extremism and radicalization and also mentions ways of identifying texts in the direction of extremism and radicalization in social networks. The study highlights the importance of an interdisciplinary approach and the use of various NLP techniques to create more effective systems for detecting extremist content.

The paper [13] used about ninety thousand data sets collected from Twitter and separated them into extremist/non-extremist groups. Various classification algorithms were applied to the dataset. A high rate of classification accuracy is achieved using the BERT model.

III. MATERIALS AND METHODS

This article deals with the classification of texts into radicalization, propaganda, recruitment and neutral classes using machine learning. To implement machine learning, we needed advanced knowledge of datasets and machine learning algorithms.

The dataset was compiled using open data sources, including social networks. The platforms used include Telegram, VK, Youtube. The total volume is about eight thousand. The dataset was compiled into four different classes: neutral, radicalization, propaganda, and recruitment. The dataset consists of about 8000 texts, approximately for each class: texts in the direction of radicalization - 2200, texts in the direction of propaganda - 1800, texts in the direction of recruitment - 1700, texts in a neutral direction - 1700.

Collected data must be pre-processed. Tokenization, deletion of stop words, deletion of punctuation marks can be attributed to those stages.

Text vectorization methods such as TF-IDF (Term Frequency-Inverse Document Frequency) and word embeddings (Word2Vec or GloVe) are used to extract features from text data.

Fig. 1 shows the ideology-defining architecture of extremist texts in the Kazakh language. The proposed architecture consists of several parts: data collection, integration into a single dataset, preprocessing part, model building using classification algorithms and evaluation of the best trained model using test data and evaluation metrics.

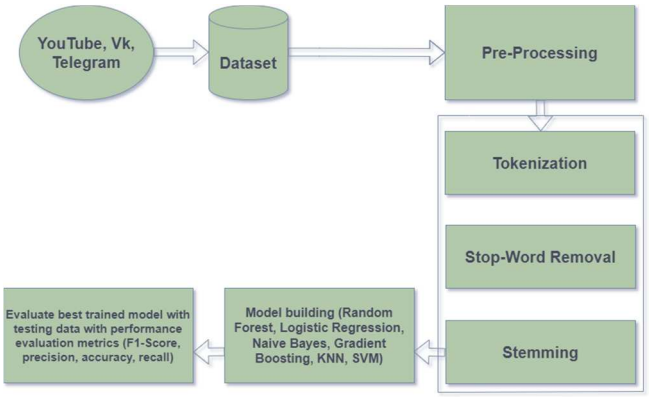

Fig. 1. Architecture that defines the ideology of extremist texts in the Kazakh language

Machine learning algorithms are mathematical models that are trained on data to perform various tasks, such as classification, regression, clustering, and more. At the core of machine learning lies the ability of algorithms to extract patterns from data and apply them for prediction or decision-making. Classification is one of the most common tasks in machine learning. In this task, algorithms are trained on labeled data to predict categorical labels for new, unseen data.

Working on machine learning algorithms has its own reasons. Below is a brief description of each and the reason for their selection:

Naive Bayes is one of the most popular algorithms for text classification problems. This algorithm is based on the application of Bayes' theorem with the assumption of independence of features, which makes it simple and fast to implement. Naive Bayes was chosen due to its efficiency when working with text data.

Logistic Regression is known for its interpretability and ability for binary classification, but can also be extended to multi-class classification. Logistic Regression was chosen for its ability to provide probabilistic estimates of class membership, which is useful for determining the degree of extremism of a text.

Random Forest is an ensemble method that builds many decision trees and averages their results to improve the accuracy and robustness of the model. Random Forest was chosen for its ability to handle large numbers of features and cope with the problem of overfitting.

Gradient Boosting is a powerful ensemble learning technique that improves predictions by iteratively correcting errors of previous models. Gradient Boosting was chosen for its ability to create more powerful models with high accuracy by correcting errors made by previous models.

Support Vector Machine (SVC) is widely used for classification problems, including problems with text data, due to its ability to operate efficiently on high-dimensional feature spaces. SVC was chosen for its ability to create clear boundaries between classes, which is important for accurately classifying extremist texts.

K-Nearest Neighbor (KNN) is a simple classification algorithm based on the distance between objects. KNN was chosen for its simplicity and intuitiveness.

IV. RESULTS

Our analysis is one of the most necessary and important operations, because the number of people spreading the ideology of extremist texts is increasing day by day. To determine them, it is necessary to experiment with the help of algorithms using machine learning and choose the optimal model (Table 1).

TABLE I. COLLECTED DATASET'S TEXT EXAMPLES

	Message	Label	Translation to English
0	ИСИМ жауынгерлері Ирак пен Сирия арасындағы Танаф шекара бекетінде VSO жалдамалы сарбаздарына тойтарыс берді https://t.co/vxyLGZp KEF	propaganda	ISIS fighters repel VSO mercenaries at the Tanaf border crossing between Iraq and Syria https://t.co/vxyLGZp KEF
1	ИСИМ қырғи-қабақ соғысқа қосылды! Олар 7 ресейлік сарбазды Сирия мен Ирактағы АҚШ сарбазын өлтірді (әзірше) https://t.co…"	propaganda	ISIS joins the Cold War! They killed 7 Russian soldiers and a US soldier in Syria and Iraq (so far) https://t.co…"
2	Пальмира маңындағы Хомс қаласында ресейлік арнайы күштердің сарбазы ИМ содырлары қолынан қаза тапты	propaganda	A Russian special forces soldier was killed by IS militants in the city of Homs near Palmyra
3	ШұғылЖаңалықтар Ресей Қорғаныс министрлігі Хомс ауылында ресейлік сарбаздың қаза тапқанын хабарлады	propaganda	Urgent News The Ministry of Defense of Russia announced that a Russian soldier was killed in the village of Homs
4	ИСИМ содырлары жылда өлтірілді	propaganda	ISIS militants were killed in the year
…	…	…	
7786	Түсінгенім ең жақын достарың да ренжітуі мүмкін оларды кешіре білу керек	neutral	I understand that you should be able to forgive even your closest friends who may hurt you
7788	Бай болсаң да кедей болсаң да өз өміріңнің қадірін біл	neutral	Whether you are rich or poor, know the value of your life
7789	Көкке көтерілгенінде тәкаппарланып кетпе бұл мәңгілік емес	neutral	Don't be arrogant when you get to heaven it's not forever

To evaluate the performance of machine learning algorithms for classifying texts into extremist ideology, experiments were conducted using several algorithms, including Naive Bayes, Logistic Regression, Random Forest, Gradient Boosting, Support Vector Machine (SVC), and K-Nearest Neighbor (KNN).

Logistic Regression is a classification method that uses a logistic function to predict the probability of class membership. This method is well suited for binary classification and can be used to predict the probability of an object belonging to one of two classes [14].

Fig. 2 demonstrates the performance of the classification algorithm when using the Logistic regression algorithm on three different metrics. Overall accuracy shows a value of 0.93 for all three metrics.

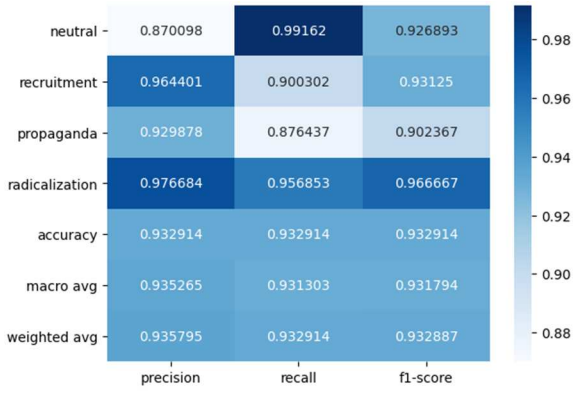

Fig. 2. Logistic Regression algorithm results

Naive Bayes is a probability classification method based on the Bayes theorem assumption of probability independence. It is often used for text classification, where each feature represents the frequency of occurrence of a word or term [14].

Fig. 3 shows the performance of the model under the Naive Bayesian algorithm.

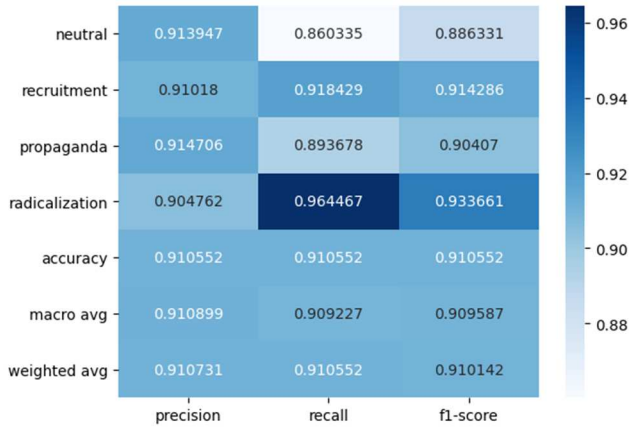

Fig. 3. Naive Bayes algorithm results

Random forest is an ensemble machine learning method based on building many decision trees during the training process and averaging their predictions to get more accurate and reliable results [15]. Fig. 4 shows the performance values of the sample using the Random Forest algorithm.

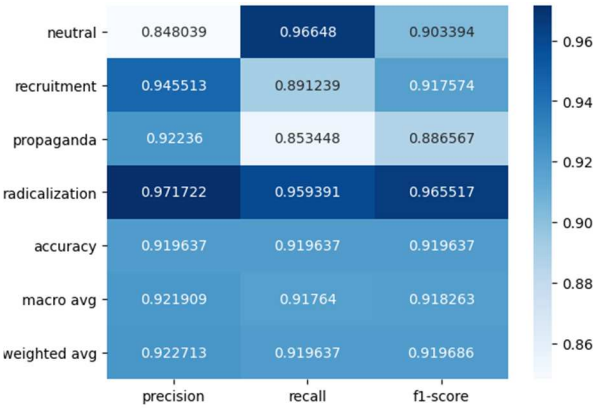

Fig. 4. Random Forest algorithm results

Gradient Boosting is an ensemble machine learning technique that sequentially builds an ensemble of weak models (often decision trees) where each new model tries to correct the errors of the previous ones. This makes it possible to create a more powerful model that can achieve high accuracy of forecasting [16]. Fig. 5 demonstrates the performance evaluation for the Gradient Boosting method.

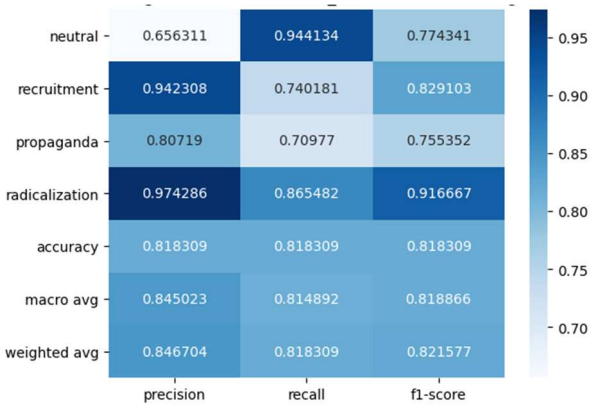

Fig. 5. Gradient Boosting algorithm results

SVC is a machine learning technique used for classification tasks. This method belongs to the group of support vector machines (SVM – Support Vector Machines), widely used in the field of data processing and machine learning. Fig. 6 shows the performance evaluation when using the SVC algorithm for classification.

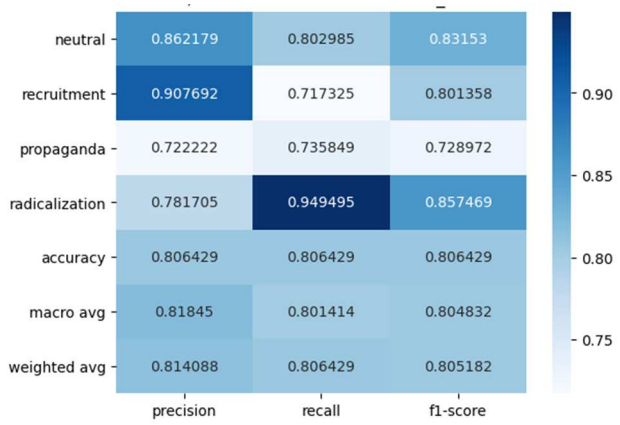

Fig. 6. SVC algorithm results

The K-Nearest neighbor method is a simple classification algorithm based on the principle of proximity of objects in the object space. To classify a new object, the algorithm finds the closest K objects from the training data set and assigns it the most frequent class among these neighbors [14]. Fig. 7 presents the performance evaluation when using the K Nearest Neighbors algorithm for classification

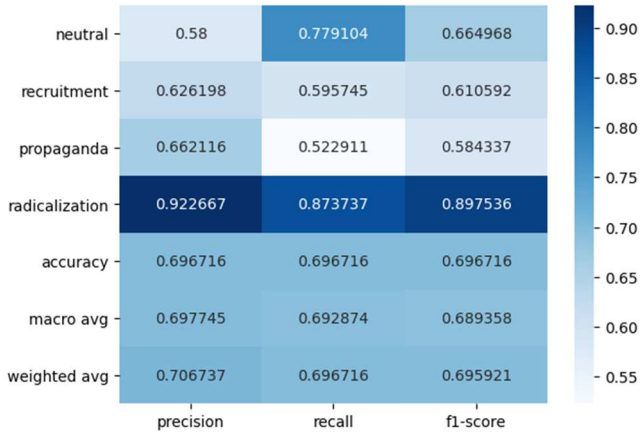

Fig. 7. The result when using the K Nearest Neighbors algorithm

In machine learning, metrics like Precision, Recall, F1-score, and Accuracy are used to evaluate the performance of classification models. They help in understanding how well a model performs in classifying data and allow for comparisons between different models or approaches.

The main metrics used to evaluate the models include Precision (1), Recall (2), F1-Score (3), and Accuracy (4).

- Precision: The percentage of correct positive predictions among all positive predictions.

$$\text{Precision}= \frac{TP}{TP+FP} \quad (1)$$

- Recall: Proportion of correct positive predictions among all actual positive examples.

$$\text{Recall}=\frac{TP}{TP+FN} \quad (2)$$

- F1-Score: Harmonic mean between precision and recall.

$$\text{F1}= 2\times \frac{Precison\times Recall}{Precision+Recall} \quad (3)$$

- Accuracy: Proportion of correct predictions among all predictions.

$$\text{Accuracy}= \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Where:

- TP (True Positive) — the number of correct predictions for the positive class.
- TN (True Negative) — the number of correct predictions for the negative class.
- FP (False Positive) — the number of incorrect predictions where the model mistakenly classified a negative instance as positive.
- FN (False Negative) — the number of incorrect predictions where the model failed to identify a positive instance (i.e., it was classified as negative).

Table 2 summarizes the performance of various machine learning methods (Logistic Regression, Naive Bayes, Random Forest, Gradient Boosting, Support Vector Classifier (SVC), and K-Nearest Neighbors) in classifying text into four different categories: Radicalization, Propaganda, Recruitment, and Neutral. The performance of these methods is evaluated using four key metrics: Precision, Recall, F1-score, and Accuracy.

TABLE II. COMPARISON OF MACHINE LEARNING METHODS

Comparison of machine learning methods	Ideology	Precision	Recall	F1-score	Accuracy
Logistic regression	Radicalization	0.97	0.95	0.96	0.93
	Propaganda	0.92	0.87	0.9	
	Recruitment	0.96	0.9	0.93	
	Neutral	0.87	0.99	0.92	
Naive Bayes	Radicalization	0.9	0.96	0.93	0.91
	Propaganda	0.91	0.89	0.9	
	Recruitment	0.91	0.91	0.91	
	Neutral	0.91	0.86	0.88	
Random Forest	Radicalization	0.97	0.95	0.96	0.91
	Propaganda	0.92	0.85	0.88	
	Recruitment	0.94	0.89	0.91	
	Neutral	0.84	0.96	0.9	
Gradient Boosting	Radicalization	0.97	0.86	0.91	0.81
	Propaganda	0.8	0.7	0.75	
	Recruitment	0.94	0.74	0.82	
	Neutral	0.65	0.94	0.77	
SVC	Radicalization	0.78	0.94	0.85	0.8
	Propaganda	0.72	0.73	0.72	
	Recruitment	0.9	0.71	0.8	
	Neutral	0.86	0.8	0.83	
K-Nearest Neighbors	Radicalization	0.92	0.87	0.89	0.69
	Propaganda	0.66	0.52	0.58	
	Recruitment	0.62	0.59	0.61	
	Neutral	0.58	0.77	0.66	

This comparison highlights the strengths and weaknesses of each machine learning method in classifying different types of ideological texts, helping to identify the most effective models for the task at hand.

To determine which method is better for the given results, we will need to analyze the performance indicators of each method. For this, we consider the Accuracy metric, as it shows the overall accuracy of the model classification across all categories. Based on the given data, the best overall accuracy is shown by the random forest and logistic regression models.

Other studies show that the use of F1 scores, accuracy, recall and precision is important when categorizing texts, especially when detecting extremist ideology. When false positives are costly, such as when neutral information is mistakenly classified as radical, accuracy is crucial. It is important to remember that failure to recognize real extremist texts can have serious consequences. Although accuracy is often used, other indicators are also used in unbalanced datasets. The F1 value is often used in studies to obtain a more reliable measure of effectiveness. These indicators allow the models to make accurate predictions and correctly identify various groups, such as radicalization, propaganda and recruitment.

To get as many real examples of extremist content as possible, recall should be a priority. This is especially important in situations where even one instance can have a big impact. If you focus on recall, you might get more false positives – when neutral information is marked as radical. This is an opportunity to improve the model and make sure only extreme content is marked. This could lead to censorship, limit acceptable speech and damage the reputation of the platform.

Precision-focused filtering reduces false positives and increases the likelihood that extremist content is identified, but it may also miss harmful content. Therefore, although a high recall helps ensure thorough detection, it must be carefully weighed against precision to prevent unintentional harmful effects. This highlights the difficulty of creating responsible and successful models for such sensitive tasks

Based on these results, which are shown in Table 1, the following conclusions can be drawn:

Best Performance: Logistic Regression and Random Forest showed the best results in all metrics (precision, recall, F1-Score and accuracy). These algorithms provide high classification accuracy for all classes of extremist texts (neutral, Radicalization, Propaganda, Recruitment).

Gradient Boosting and SVC: These algorithms showed good results, but are inferior to Logistic Regression and Random Forest. Gradient Boosting shows high accuracy for the "Radicalization" class, but has problems with the "Propaganda" class.

Naive Bayes and KNN: These algorithms have satisfactory performance, but generally perform poorly compared to other methods.

The results show that traditional algorithms such as Logistic Regression and Random Forest can be very effective for extremist text classification tasks. However, for more complex problems and large volumes of data, more advanced methods such as BERT and LSTM, which are able to take into account context and complex dependencies in the data, may be required.

At the moment, it is not possible to compare our results with other studies or baseline models due to the lack of similar work that would use the Kazakh language in the context of defining ideology. We hope that our research will become the basis for subsequent work and will contribute to the development of text processing technologies in the Kazakh language. This, in turn, will allow future comparative analyses and assessments of progress in this area.

The developed models can be used in the automatic detection of extremist content. Social networks can use these models to monitor and remove extremist content, thereby creating a safe environment for users. Forum and blog administrators can use these models to automatically moderate content and prevent the spread of radical ideas.

In the field of big data analytics, law enforcement agencies can use models to analyze large volumes of data, which helps in identifying and preventing terrorist threats. Academic and research institutions can apply these findings to study trends and patterns in the spread of extremist ideology.

Despite the significant practical importance of machine learning methods for classifying extremist texts, their implementation is associated with a number of challenges and limitations. Successful application of these methods requires a comprehensive approach that includes high data quality, regular model updates, ethical and legal considerations, and sufficient computing resources and infrastructure.

V. Conclusion

In conclusion, this work was focused on developing and evaluating machine learning models for classifying texts into categories such as neutral, recruitment, propaganda, and radicalization. Throughout the study, the performance of several methods, including K-Nearest Neighbor, Random Forest, Naive Bayes, and Logistic Regression, was analyzed. The results indicate that the Random Forest and Logistic Regression models achieved the highest classification accuracy. These findings suggest that the developed models can be effectively utilized to create automatic text content analysis systems, which have significant applications in fields such as social sciences, information security, and media analytics.

Funding statement. This research was carried out within the framework of the project funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No.AP19676342, supervisor of the project is Shynar Mussiraliyeva,e-mail:mussiraliyevash@gmail.com).

References

[1] Helen Cowie, Cyberbullying and its impact on young people's emotional health and well-being, Published online by Cambridge University Press: 02 January 2018

[2] Joshua R. Polanin, Dorothy L. Espelage, Jennifer K. Grotpeter, Katherine Ingram, Laura Michaelson, Elizabeth Spinney, Alberto Valido, America El Sheikh, Cagil Torgal, Luz Robinson, A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization, Published online: 22 June 2021, Prevention Science (2022) 23:439–454

[3] Akemi Takeoka Chatfield, Christopher G. Reddick, Uuf Brajawidagda, Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks, Faculty of Engineering and Information Sciences - Papers: Part A, 1-1-2015

[4] Noemi M. Rocca, Mobilization and Radicalization Through Persuasion: Manipulative Techniques in ISIS' Propaganda, International Relations and Diplomacy, November 2017, Vol. 5, No. 11, 660-670

[5] Irfan Tanoli, Sebasti˜ao Pais, Jo˜ao Cordeiro, Muhammad Luqman Jamil, Detection of Radicalisation and ExtremismOnline: A Survey, Preprint (it has not been peer reviewed by a journal)

[6] Mayur Gaikwad, Swati Ahirrao, Ketan Kotecha, Ajith Abraham, Multi-Ideology Multi-Class ExtremismClassification Using DeepLearning Techniques, IEEE Access, 104829 – 104843, 12 September 2022

[7] Younes Karimi, Anna Squicciarini, Peter Kent Forster, A longitudinal dataset and analysis of Twitter ISIS users and propaganda, Social Network Analysis and Mining, 03 January 2024

[8] Mayur Gaikwad, Swati Ahirrao, Shraddha Phansalkar, Ketan Kotecha, "Multi-Ideology ISIS/Jihadist White Supremacist (MIWS) Dataset for Multi-Class Extremism Text Classification", 2021, 6(11), 117;

[9] Mayur Gaikwad, Swati Ahirrao, Shraddha Phansalkar, Ketan Kotecha, Shalli, "Multi-Ideology, Multiclass Online Extremism Dataset, and Its Evaluation Using Machine Learning. Mayur Gaikwad" 01 March 2023, Computational Intelligence and Neuroscience

[10] Akemi Takeoka Chatfield, Christopher G. Reddick, Uuf Brajawidagda, "Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks supporters multi-sided Twitter networks", Proceedings of the 16th Annual International Conference on Digital Government Research, May 27 - 30, 2015, Pages 239 - 249

[11] Barea Sinno1, Bernardo Oviedo2, Katherine Atwell3, Malihe Alikhani3, Junyi Jessy Li, "Political Ideology and Polarization: A Multi-dimensional Approach", Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pages 231 - 243 July 10-15, 2022

[12] Irfan Tanoli, Sebastião Pais, João Cordeiro, Muhammad Luqman Jamil, Detection of Radicalisation and Extremism Online: A Survey, January 5th, 2022, unpublished

[13] Saja Aldera, Ahmed Emam, Muhammad Al-Qurishi, Majed Alrubaian, Abdulrahman Alothaim, Exploratory Data Analysis and Classificationof a New Arabic Online Extremism Dataset, IEEE Access, 03 December 2021, Page(s): 161613 - 161626

[14] https://towardsdatascience.com/comparative-study-on-classic-machine-learning-algorithms-24f9ff6ab222

[15] https://medium.com/@mrmaster907/introduction-random-forest-classification-by-example-6983d95c7b91

[16] https://medium.com/@hemashreekilari9/understanding-gradient-boosting-632939b98764