Data Protection in the Utilization of Natural Language Processors for Trend Analysis and Public Opinion: Cryptographic Aspect

Inna Rozlomii [1], Nataliia Yehorchenkova [2], Andrii Yarmilko [1], and Serhii Naumenko [1]

[1] *Bohdan Khmelnytsky National University of Cherkasy, 81, Shevchenko Blvd., Cherkasy, 18031, Ukraine*
[2] *Slovak University of Technology in Bratislava, 81, Vazovova 5, 812 43 Bratislava, Slovak Republic*

Abstract

In the digital age, the significant increase in information generation and processing is accompanied by a growing threat of unauthorized access, illegal distribution, and use. One of the most promising strategies for protecting information from various cyber threats and malicious attacks is the use of Natural Language Processing (NLP) processors. This article focuses on the methodology of data protection in the context of utilizing Natural Language Processing for sentiment analysis and trend detection. Emphasis is placed on the relevance of using NLP to address tasks related to text content analysis for identifying suspicious or dangerous information. The article covers the stages of text data collection and processing, including data gathering from various sources such as social media, news portals, forums, and blogs. Subsequently, preliminary processing is performed, involving noise removal, tokenization, stemming, and lemmatization of the text to prepare the data for further analysis. The application of NLP allows for the identification of keywords, topics, sentiment, and text structure, facilitating categorization and trend identification in public opinion. Additionally, a mathematical model for detecting phishing indicators is presented, along with an example of identifying suspicious text features. It is noted that the use of cryptographic methods can effectively secure processed data, reducing the risk of unauthorized access or misuse. The article provides a detailed description of data protection methods in the process of sentiment analysis using NLP and underscores the necessity of employing cryptographic techniques to ensure the security of processed text data.

Keywords

Natural language processing, natural language processing technologies, information security, analysis of global trends, cybersecurity, disinformation, phishing, automatic text analysis, text classification, threat detection, digital security, cyber threats.

1. Introduction

In today's information society, against the backdrop of rapid technological advancements and dynamic changes in the global information space, information security gains increasing importance and relevance. The growing volume of information circulating on the Internet, along with the rapid development of social networks, digital platforms, and online services, creates new opportunities for communication, collaboration, and knowledge access. However, this also increases the risk of unauthorized access to personal data, the spread of disinformation, phishing attacks, and other threats that jeopardize the security and resilience of information processes.

[1]SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, November 9, 2023, Lviv, Ukraine
EMAIL: inna-roz@ukr.net (I. Rozlomii); nataliia.yehorchenkova@stuba.sk (N. Yehorchenkova); a-ja@ukr.net (A. Yarmilko); naumenko.serhii1122@vu.cdu.edu.ua (S. Naumenko)
ORCID: 0000-0001-5065-9004 (I. Rozlomii); 0000-0001-5970-0958 (N. Yehorchenkova); 0000-0003-2062-2694 (A. Yarmilko); 0000-0002-6337-1605 (S. Naumenko)

CEUR Workshop Proceedings (CEUR-WS.org)

In this context, it is crucial not only to identify specific threats and react to them but also to anticipate their emergence, understand the dynamics of global trends, and adapt security measures in a timely manner. One way to achieve this goal is by utilizing Natural Language Processing (NLP) for the analysis of public opinion and textual content [1]. NLP encompasses a set of technologies based on natural language processing and machine learning, enabling the automatic analysis and understanding of linguistic context [2].

The aim of this article is to explore the relevance and importance of applying NLP in the context of analyzing global trends and public opinion, as well as their role in ensuring the security of information processes. To achieve this goal, a comprehensive approach is used, which includes data collection and preparation, identification of key topics and terms, sentiment analysis, and the application of classification and clustering methods. By investigating the capabilities of these technologies, the article aims to highlight their potential in detecting and countering cyber threats, including phishing attacks, the dissemination of disinformation, and other forms of attacks on information security. Additionally, the article emphasizes the importance of analyzing global trends and public sentiment as tools for prevention and response to potential threats. This contributes to a deeper understanding of the role of NLP in the modern information environment and helps develop new approaches to ensuring the security of information processes, providing more effective protection in the evolving digital landscape.

2. Related works

Analysis of trends and public opinion is a key tool for business, politics, science, and social research in the modern information society. The use of Natural Language Processors (NLP) allows for the automation of the analysis of a large amount of textual information, enabling the detection of topics, sentiments, and sentiment [3]. However, this approach faces significant challenges in terms of confidentiality, integrity, and security of processed information.

NLP has long been used for the analysis of public opinion and trend identification in textual sources [4]. Previous research has focused on sentiment analysis, emotion classification, as well as identifying keywords and phrases to understand public sentiments [5].

Recently, researchers have been paying attention to the application of cryptographic methods to protect information processed using natural language processors [6]. This is important due to the risks to the confidentiality and integrity of data during text processing by third parties.

Previous research has focused on the development of cryptographic methods to protect information transmitted and processed when using natural language processors [7]. Some approaches include the use of encryption, message signing, and other cryptographic protocols to ensure the confidentiality and authenticity of data during processing [8, 9].

Additionally, the interest in text processors is evidenced by publications related to the analysis of various languages, such as Indonesian [10], Bengali [11], Arabic [12], and others.

3. Research methodology

The methodology of the research discussed in this article is based on the combination of NLP analysis with the analysis of global trends and public opinion to ensure information (data) protection in the digital environment. In the context of the article, data protection is regarded as the application of cryptographic methods and strategies to guarantee the confidentiality, integrity, and availability of data being processed and stored while using Natural Language Processing for trend analysis and public sentiment evaluation. This encompasses protection against unauthorized data access, ensuring the confidentiality of personal information, and guaranteeing data unavailability to unauthorized parties. Such protection may involve encryption, authentication, digital signatures, and other cryptographic methods to secure data during processing.

In turn, the analysis of global trends is considered as the process of studying and identifying common changes or patterns in data that reflect a particular evolution or movement in public opinion or consumer behavior based on the analysis of a large volume of textual information, including social media, news, blogs, and other virtual sources. This may include identifying popular topics, opinions, sentiments, reactions, or thoughts that circulate online, as well as identifying changes in consumer habits, trends in

public opinion, or reactions to specific events. Such analysis can help in understanding public sentiment towards specific issues, identifying risks, determining popular opinions, and forecasting potential directions of development.

The concept of "public opinion" is used to refer to the collective beliefs, views, and sentiments of the public, which can be expressed through various sources such as social media, surveys, expert opinions, and other communication channels. This encompasses a wide range of views, beliefs, reactions, and sentiments that exist in society regarding specific issues, events, individuals, or processes. Public opinion is important for determining trends and sentiments in society, as well as for measuring the level of support or rejection of certain ideas, political decisions, goods, or services. The analysis of public opinion can help in understanding the needs and expectations of society, as well as in forming communication and influence strategies.

To achieve the stated research goal, a systematic methodology has been developed, which includes the following steps:

1. **Data Collection and Preparation.** The initial stage involves gathering various textual data from different sources, such as social media, news portals, forums, etc. [13-14]. The sample should be representative and cover current topics and trends. The collected data undergo preliminary processing, such as tokenization, noise removal, and so on.
2. **Analysis of Global Trends and Public Opinion.** The application of natural language processing allows for the identification of key topics, popularity, and sentiments in textual data [15-16]. Using classification and clustering methods, connections between terms are established, and patterns in global trends and public opinion are identified.
3. **Detection of Threats and Anomalies.** The use of NLP enables the detection of textual indicators that may point to security threats, such as phishing attempts, the spread of disinformation, insults, and more [17]. An automated analysis system can highlight suspicious information and classify it based on predefined criteria.
4. **Development of Forecasting Models.** By utilizing data on global trends and public opinion, predictive models can be created to help anticipate potential risks and threats in the future [18]. These models may be based on the analysis of past events and dependencies between various factors.
5. **Validation and Evaluation of Results.** Assessing the effectiveness of developed models and methods requires validation on real data or simulated scenarios. This stage involves comparing the analysis results with actual events and evaluating the accuracy of forecasts.
6. **Analysis of Innovative Approaches.** Innovative approaches to the application of natural language processors in ensuring information security and trend analysis include the use of deep learning, neural networks, and other modern methods [19-20].

This methodology enables the detection, analysis, and prediction of security threats and real-time responses, relying on the analysis of textual content and global sentiments. The research findings can be a valuable contribution to enhancing information security and risk management in the modern digital environment.

3.1. Data collection

The first stage of the research involves collecting a large volume of textual data from various sources such as social networks, news portals, forums, and blogs [21]. It is important to consider the diversity of sources and linguistic variety to ensure the representativeness of the sample. At this stage, a substantial amount of textual data is gathered from different sources for further analysis and processing. Since information sources can be diverse, ensuring the representativeness of the sample, including linguistic and cultural diversity, is crucial [22].

Steps of data collection:

1. **Source Determination.** The selection of information sources depends on the specific objectives of the research. Social networks (Twitter, Facebook, Reddit), news portals (BBC, CNN), forums, and blogs can provide diverse insights into global trends and public opinion [21].

2. **Data Collection.** The use of APIs and web scraping assists in automatically gathering textual data from selected sources. For example, Twitter API can be used to collect tweets on a specific topic.
3. **Linguistic Diversity.** Ensuring representativeness involves choosing data from different languages and cultures. For instance, if the research pertains to global trends in sustainable technologies, it's important to consider data from various countries and linguistic communities [10-12].

Figure 1 provides a scheme of the process of collecting textual data from various sources. This scheme illustrates how, after data collection, analysis and processing of information occur to identify key aspects, sentiment analysis, and semantic analysis. It also involves analyzing textual relationships between words and concepts. All these stages help in understanding global trends and public opinion based on an extensive selection of textual data.

Thanks to the integration of NLP in this process, researchers and specialists receive additional tools for understanding social and informational phenomena, which are becoming more and more complex. The results of such research can be used to develop more effective risk management strategies, ensure cyber security and create more objective information environments. Thus, the use of NLP in the collection and analysis of textual data has great potential for improving the quality and security of the information space.

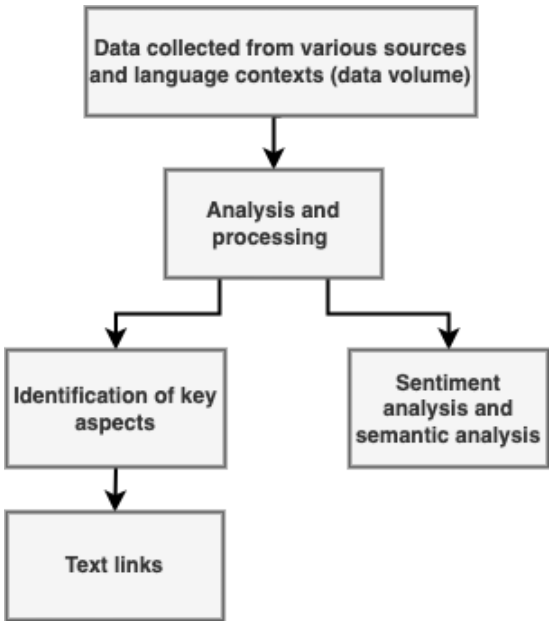

Figure 1: Data collection scheme from information sources

3.2. Preprocessing

The obtained data undergo preprocessing, which includes noise removal, tokenization, stemming, and lemmatization of texts. This stage helps prepare the data for further analysis, reduce dimensionality, and ensure normalization [23, 24].

Data preprocessing is an important stage in preparing information for further analysis and research [25]. Here are the steps typically involved in data preprocessing:

1. **Noise removal:** First, it's necessary to eliminate redundant or irrelevant information, such as special characters, advertisements, URLs, punctuation marks, etc. This helps make the data cleaner and facilitates more accurate analysis.
2. **Tokenization.** Text is divided into individual words or tokens. This can be done by splitting the text using spaces or other delimiters. Consequently, each word becomes a separate element to work with.
3. **Stemming and Lemmatization.** Stemming and lemmatization help reduce words to their base forms. Stemming involves removing affixes (prefixes and suffixes), while lemmatization

involves reducing words to their lemma (base form). For example, the word "running" can become "run" after stemming or "run" after lemmatization.

4. **Stopword Removal.** Words that are extremely common and carry little meaningful information (e.g., "and," "the," "in," "with") can be removed from the text. This helps reduce noise and focus on keywords.
5. **Normalization.** To ensure uniformity, data may be transformed to lowercase, which helps avoid duplicate words due to different letter casing.

After performing these steps, the data is ready for further analysis. It's important to note that data preprocessing may vary depending on the specific task and data type, but the general principle involves cleaning, normalizing, and structuring the information before its subsequent use.

Specialized software tools and libraries for text processing can be used for these stages, such as Natural Language Toolkit (NLTK) or spaCy for the Python programming language.

Following preprocessing, the data becomes more structured and prepared for further analysis. Below is an example of real results after data preprocessing.

Original text: "Global climate changes affect the economy and natural resources. Innovative technologies contribute to sustainable economic development".

Result of data preprocessing: ["global", "climate", "changes", "affect", "the", "economy", "and", "natural", "resources", "innovative", "technologies", "contribute", "to", "sustainable", "economic", "development"].

This preprocessing ensures the uniformity of textual data and prepares them for further analysis, making it easier to recognize key words, identify themes, and other aspects of global trends and public opinion.

3.3. Analysis of global trends

After the preprocessing, the data undergo analysis using natural language processors [27]. Various algorithms and models are employed to identify key words, topics, sentiment, and to determine the structure of texts. NLP helps to extract and categorize data, enabling the detection of common trends and differences in public opinion [28]. The application of NLP analysis opens up possibilities for a detailed understanding of global trends and public sentiment. This section elaborates on the methods and approaches that allow the identification of key topics, assessment of popularity, and determination of sentiments in textual data using natural language analysis. Classification and clustering methods are also used to find connections between terms and patterns in global trends and public opinion.

In this section, we will conduct a detailed analysis of the process of identifying key topics, assessing popularity and sentiments, as well as the application of classification and clustering methods for analyzing global trends and public opinion.

3.3.1. Identification of key topics and terms

When analyzing textual data, we use text processing techniques to identify key themes and terms. For example, let's consider a virtual dataset of text discussions on cybersecurity. We determine the frequency of each key term's mentions and its importance using Term Frequency-Inverse Document Frequency (TF-IDF).

TF-IDF is a statistical measure that indicates the importance of a term within a text relative to the entire corpus of texts [29]. It consists of two components: Term Frequency (TF), which shows how often the term appears in a specific text, and Inverse Document Frequency (IDF), which indicates the rarity of the term across the entire dataset of texts.

Let's apply the TF-IDF method to this set of texts:

Text 1: "The cyberattack on a major bank was an explicit threat!"

Text 2: "How to protect your data from hackers?"

Text 3: "Top 5 most common cyber threats this year."

Based on these texts, we calculate the TF-IDF values for key terms (Table 1).

Table 1
TF-IDF values for key terms in the text dataset

Key term	Number of mentions	Importance (TF-IDF)
Cyberattack	2	0.602
Threat	1	0.301
Protection	1	0.301
Hackers	1	0.301

3.3.2. Assessment of popularity and sentiments

For each key term, we also conduct sentiment analysis to assess popularity and sentiments. Sentiment analysis evaluates the emotional tone of the text and determines whether it is positive, negative, or neutral. Table 2 provides an example of sentiment values for the analyzed text dataset.

Table 2
Sentiment values for key terms in the text dataset

Key term	Positive sentiment	Negative sentiment
Cyberattack	0.6	- 0.8
Threat	- 0.3	- 0.7
Protection	0.7	0.1
Hackers	- 0.7	- 0.9

3.3.3. Classification and Clustering

Classification and clustering methods help organize and group key terms and topics based on certain characteristics. Applying classification and clustering methods in the analysis of textual data collected from various sources allows for the systematic organization of a large amount of information and the identification of connections that may be imperceptible during superficial analysis. For example, through clustering, it is possible to identify groups of similar themes or viewpoints that form in public opinion regarding information security (Figure 2).

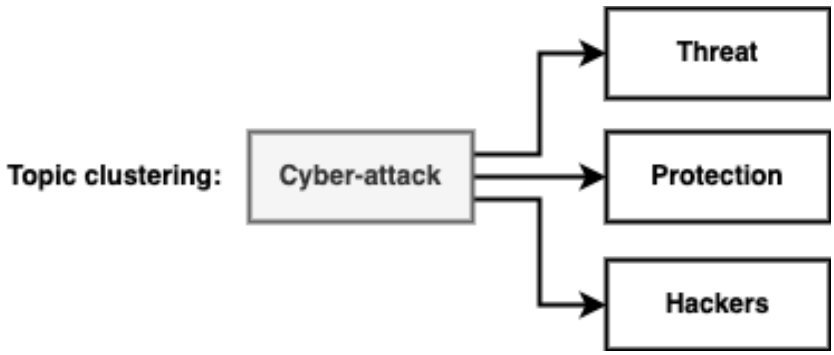

Figure 2: Clustering of the "Cyberattack" topic

Using natural language processing and classification and clustering methods, we can delve deeper into the relationships and patterns within textual data and gain a better understanding of global trends in information security.

4. Detection of threats and anomalies

The increasing volume of data processed by Natural Language Processing (NLP) processors for trend analysis and public sentiment gives rise to an important challenge of detecting threats and anomalies in the raw data. Researchers are actively working on the development and enhancement of cryptographic methods and algorithms that efficiently identify potential vulnerabilities in natural language processing systems.

One key aspect of data protection involves securing natural language processing models from potential attacks by malicious actors. To achieve this, it's necessary to implement monitoring systems capable of timely detecting deviations in the models' performance, which may indicate hacking attempts or the introduction of malicious algorithms. Special attention should be paid to the detection of abnormal patterns and data in the input streams fed into natural language processors. This can be achieved through methods analyzing data structure and comparing it to reference templates, as well as the application of machine learning algorithms for automatic anomaly detection.

For effective protection against malicious attacks on data obtained during public sentiment analysis, it is essential to implement comprehensive cryptographic methods such as encryption, digital signatures, user authentication, and more. Additionally, it is recommended to regularly update cryptographic protocols to address modern threats and vulnerabilities.

In this section, we will explore the application of NLP for identifying textual features that may indicate security threats, such as phishing attempts, disinformation, and abuse. We will also examine an automated analysis system that allows the identification of suspicious information and classifies it based on various criteria. It's worth noting that after NLP analysis, an expert analysis is conducted, involving a deep examination of the sample, the identification of nuances and context that may be lost during automated analysis. The expert approach helps ensure the accuracy and reliability of the results.

Natural language processors can analyze text and identify key features that indicate potential security threats. For example, phrases containing suspicious URLs or queries related to personal data can be indicators of phishing attempts. Additionally, detecting intense negative language and insults can point to potential instances of harm or offensive behavior.

Let's consider an automated analysis system capable of identifying suspicious information and classifying it based on various criteria. This system is used to enhance security and identify potential threats in textual data.

4.1. Operation of the automatic analysis system

The automatic analysis system is based on trained machine learning models that recognize patterns and differences in text (Figure 3).

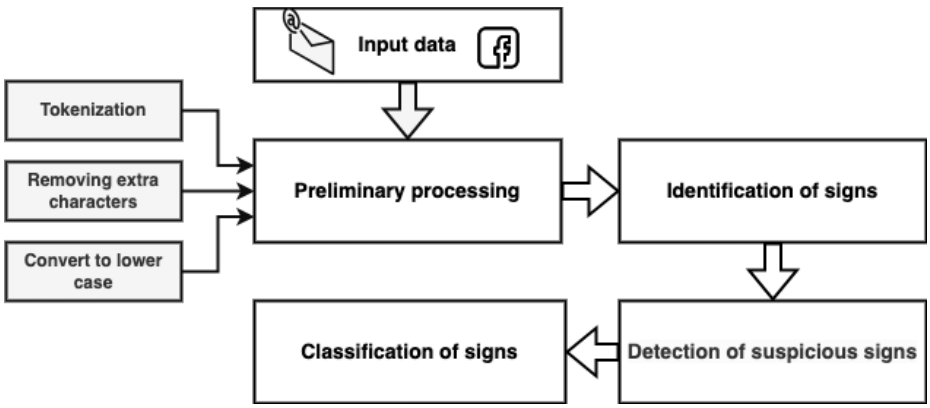

Figure 3: The process of processing text data to detect potential threats or anomalies

The analysis process consists of the following stages:

1. **Text Retrieval.** The system initially obtains text data for analysis, which can come from various sources such as social media, emails, news, etc.

2. **Preprocessing.** Text data undergo preprocessing, including tokenization (splitting into individual words or tokens), removing unnecessary characters, converting to lowercase, etc.
3. **Feature Extraction.** Natural Language Processing (NLP) tools are used to extract features from the processed text. These features may include words, phrases, collocations, lexical and grammatical features, word frequencies, sentiment analysis, the use of linguistic devices (metaphors, comparisons), the use of special symbols and emojis, links and URLs, word repetition counts, and other aspects.
4. **Detection of Suspicious Features.** The system analyzes the extracted features and looks for those that may indicate potential threats or anomalies. These could include unusual queries, suspicious URL links, negative tone, rapid tone changes, specific information requests, business proposals from unknown sources, calls for immediate action, unexpected identity changes, excessive use of special symbols and mixed-case letters, attempts at psychological influence, etc.
5. **Classification.** Trained classifier models are applied to assign class labels to the text data. This classification can be based on the level of suspicion, the type of threat (phishing, disinformation, etc.), and other criteria (Table 3).

Table 3
Classification of Suspicious Textual Features

Criterion	Variants of manifestation
Degree of suspicion	Low, medium, high
Types of threats	Phishing, social engineering, malware, disinformation, spam, espionage, cyberbullying, financial fraud, identity theft, infrastructure cyberattacks, skimming, data theft
Target audience	Individuals, corporations, government entities, financial institutions, media, social networks
Industry sectors	Financial, medical, technological, energy, transportation, educational, public
Threat scale	Individual, group, mass
Sphere of influence	Cybersecurity, information security, economic security, political security, personal security
Attack methods	Email phishing, social engineering, use of trojans, SQL injections (database attacks), DDoS attacks (server overload), identity theft

4.2. A mathematical model for detecting phishing indicators

To detect phishing indicators in text, machine learning models such as a binary classifier (e.g., logistic regression or naive Bayes classifier) can be used.

Let T be a feature vector of the text, which includes important parameters of the analyzed text. Also, let C represent the class label for the given text, where C can take values "phishing" or "non-phishing". Thus, we have a training dataset D:

$$D = \{(T_1^2, C_1^2), (T_2^2, C_2^2), \dots, (T_n^2, C_n^2)\}, \quad (1)$$

where n – is the number of training examples.

The model can be represented as follows:

$$h_\theta(x) = \frac{1}{1 + e^{-\theta^T x}}, \quad (2)$$

where θ – represents the model parameters that are learned during training.

During the training process, our goal is to reduce the value of a loss function (e.g., logarithmic loss function) using the gradient descent method. This method allows us to find optimal parameter values θ, that help the classifier determine whether the text is suspicious phishing or not.

4.3. Example of detecting phishing signs

Let's consider a real example of how the automatic analysis system works. Suppose we have the following text with a phishing attempt: "Welcome! Your account has been blocked. Please click on the link and enter your credentials to unlock."

To analyze this text sample, we can use a previously trained model designed to detect phishing features. After applying natural language processing to the text, we obtain a feature vector, which we'll denote as T. Plugging this vector T into the model already supported by parameters θ, we can obtain the probability that the given text is phishing.

To illustrate the process, let's assume that after processing the text, we obtained the following feature vector: $T = [0.2, -0.5, 0.8]$, and the model parameters $\theta = [0.1, 0.4, -0.7]$. The probability can be calculated using the hypothesis function h according to the following formula:

$$h_\theta(T) = \frac{1}{1 + e^{-\theta^T}} \quad (3)$$

Substituting the values of the feature vector T and the parameters θ into this formula, we obtain the calculated probability, which indicates how likely it is that this text is phishing.

In our example:

$$h_\theta(T) = \frac{1}{1 + e^{-0.2*0.1-0.5*0.4+0.8*(-0.7)}} \approx 0.72 \quad (4)$$

This number, approximately 0.72, indicates the probability that the given text is phishing.

Thus, by examining a specific example of phishing feature detection, you can understand how text analysis automation systems work in practice. They use NLP to extract features from text, and then apply trained models to determine the likelihood of a specific threat. The significance and importance of each feature can be determined by the model parameters, allowing systems to accurately detect potential threats and anomalies in textual data. These approaches are an important tool for ensuring cybersecurity and effectively identifying malicious actions in the modern digital environment.

5. Discussions

The presented research opens up prospects for further development in the field of information security and public sentiment analysis using NLP. The research focuses on the use of NLP for detecting cybersecurity threats as well as analyzing trends in the cryptographic aspect. The main results of the article can serve as an important starting point for further research and practical applications.

The research underscores the importance of using NLP for threat detection and global trend analysis. Future research could focus on improving methods for anomaly detection and malicious activity identification, as well as developing new algorithms for implementing intelligent cybersecurity systems.

In the future, it may be possible to enhance the performance of sentiment analysis using NLP by refining emotion classification algorithms and determining the importance of trends for different aspects of society.

Future research could also focus on analyzing real-world examples of NLP usage for information security and trend analysis. This may include assessing the impact of such systems on practical aspects of information security.

6. Conclusion

The article discusses the role of natural language processors (NLP) in detecting security threats such as phishing attacks, misinformation, insults, and spam. The research focuses on the capabilities of NLP in analyzing global trends and public sentiment that indicate potential risks and vulnerabilities in the information space.

The research conducted underscores the evident fact that the use of NLP for public sentiment analysis and trend detection is an integral part of the modern research process. The collection and processing of textual data from various sources, including social media, news portals, forums, and blogs, demonstrate the significant role of NLP in identifying key words, sentiment, and themes that reflect public opinion. It is shown that effective preliminary processing of textual data, such as noise

removal, tokenization, stemming, and lemmatization, is a critical step in preparing data for further analysis, ensuring the accuracy and completeness of the obtained results.

The application of cryptographic methods to protect processed data is a key aspect that guarantees the security and confidentiality of information, especially when dealing with sensitive data. The developed mathematical model for phishing detection and the examples of identifying suspicious textual features highlight the importance of employing cryptographic methods to protect processed data.

It's also worth noting that expert analysis plays a crucial role in understanding context and nuances that may be lost in the process of automated analysis. This emphasizes the need to consider the human factor when processing information with NLP to ensure the accuracy and reliability of the results.

Therefore, the use of NLP in identifying security threats in the information space opens up opportunities for timely threat detection and effective response. The proposed research methodology allows for the use of natural language processors to analyze and understand global trends and public sentiment, taking into account cultural and linguistic peculiarities. Combining technical analysis with an expert approach ensures objective and reliable results that can be used for forecasting and making strategic decisions in various fields of activity.

7. References

[1] K. Chowdhary, K. R. Chowdhary, Natural Language Processing. In: Fundamentals of Artificial Intelligence. Springer, New Delhi, 2020, pp. 603-649. doi: https://doi.org/10.1007/978-81-322-3972-7_19.

[2] D. Khurana, A. Koli, K. Khatter, S. Singh, Natural language processing: State of the art, current trends and challenges, Multimedia tools and applications 82(3) (2023) 3713-3744.

[3] V. Raina, S. Krishnamurthy, Natural Language Processing, in: V. Raina, S. Krishnamurthy (Eds.), Building an Effective Data Science Practice: A Framework to Bootstrap and Manage a Successful Data Science Practice, Apress, Berkeley, CA, 2022, pp. 63–73. doi: https://doi.org/10.1007/978-1-4842-7419-4_6.

[4] R. Oshikawa, J. Qian, W. Y. Wang, A survey on natural language processing for fake news detection, arXiv:1811.00770 [cs.CL] (2018). doi: https://doi.org/10.48550/arXiv.1811.00770.

[5] D. Khurana, A. Koli, K. Khatter, S. Singh, Natural language processing: State of the art, current trends and challenges, Multimedia tools and applications 82(3) (2023) 3713-3744.

[6] D. H. Maulud, S. R. Zeebaree, K. Jacksi, M. A. M. Sadeeq, K. H. Sharif, State of art for semantic analysis of natural language processing, Qubahan academic journal 1(2) (2021) 21-28.

[7] J. H. Li, Cyber security meets artificial intelligence: a survey, Frontiers of Information Technology & Electronic Engineering 19(12) (2018) 1462-1474.

[8] R. May, K. Denecke, Security, privacy, and healthcare-related conversational agents: a scoping review. Informatics for Health and Social Care 47(2) (2022) 194-210. doi: 10.1080/17538157.2021.1983578.

[9] R. K. Jha, Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing, Journal of Trends in Computer Science and Smart Technology 5(3) (2023) 284-301.

[10] A. W. Pradana, M. Hayaty, The effect of stemming and removal of stopwords on the accuracy of sentiment analysis on indonesian-language texts, Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control 4(4) (2019) 375-380.

[11] N. Banik, M. H. H. Rahman, S. Chakraborty, H. Seddiqui, M. A. Azim, Survey on text-based sentiment analysis of bengali language, in: 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/ICASERT.2019.8934481.

[12] M. O. Hegazi, Y. Al-Dossari, A. Al-Yahy, A. Al-Sumari, A. Hilal, Preprocessing Arabic text on social media, Heliyon 7(2) (2021). doi: 10.1016/j.heliyon.2021.e06191.

[13] E. Hossain, R. Rana, N. Higgins, J. Soar, P. D. Barua, A. R. Pisani, Natural language processing in electronic health records in relation to healthcare decision-making: a systematic review, Computers in Biology and Medicine 155 (2023). doi: https://doi.org/10.1016/j.compbiomed.2023.106649.

[14] Z. Jiang, L. Liu, Research on sentiment analysis of online public opinion based on semantic, in: Geo-Spatial Knowledge and Intelligence, in: H. Yuan, J. Geng, C. Liu, F. Bian, T. Surapunt (Eds.), Geo-Spatial Knowledge and Intelligence, GSKI 2017, volume 849 of Communications in Computer and Information Science, Springer, Singapore, 2017, pp. 313–32.1 https://doi.org/10.1007/978-981-13-0896-3_31.
[15] S. Salloum, T. Gaber, S. Vadera, K. Shaalan, A systematic literature review on phishing email detection using natural language processing techniques, IEEE Access 10 (2022) 65703-65727. doi: 10.1109/ACCESS.2022.3183083.
[16] X. Chen, R. Ding, K. Xu, S. Wang, T. Hao, Y. Zhou, A bibliometric review of natural language processing empowered mobile computing, Wireless Communications and Mobile Computing (2018). https://doi.org/10.1155/2018/1827074.
[17] T. Peng, I. Harris, Y. Sawa, Detecting phishing attacks using natural language processing and machine learning, in: 2018 IEEE 12th International Conference on Semantic Computing (ICSC), Laguna Hills, CA, USA, 2018, pp. 300-301. doi: 10.1109/ICSC.2018.00056.
[18] Y. Zhu, X. Li, J. Wang, Analysis and research of Weibo public opinion based on text, Journal of Physics: Conference Series 1769(1) (2021). doi: 10.1088/1742-6596/1769/1/012018.
[19] W. E. Zhang, Q. Z. Sheng, A. Alhazmi, C. Li, Adversarial attacks on deep-learning models in natural language processing: A survey, ACM Transactions on Intelligent Systems and Technology (TIST) 11(3) (2020) 1-41.
[20] H. Gan, Research on data mining method based on privacy protection, in: 020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), Shenzhen, China, 2020, pp. 502-506. doi: 10.1109/AEMCSE50948.2020.00114.
[21] N. Garg, K. Sharma, Text pre-processing of multilingual for sentiment analysis based on social network data, International Journal of Electrical & Computer Engineering 12(1) (2022) 2088-8708.
[22] C. Qian, N. Mathur, N. H. Zakaria, R. Arora, V. Gupta, M. Ali, Understanding public opinions on social media for financial sentiment analysis using AI-based techniques, Information Processing & Management 59(6) (2022). doi: https://doi.org/10.1016/j.ipm.2022.103098.
[23] M. Anandarajan, C. Hill, T. Nolan, Text Preprocessing, in: Practical Text Analytics. Advances in Analytics and Data Science, Springer, Cham, 2019. doi: https://doi.org/10.1007/978-3-319-95663-3_4 45-59.
[24] A. Tabassum, R. R. Patil, A survey on text pre-processing & feature extraction techniques in natural language processing, International Research Journal of Engineering and Technology (IRJET) 7(06) (2020) 4864-4867.
[25] A. Kurniasih, L. P. Manik, On the Role of Text Preprocessing in BERT Embedding-based DNNs for Classifying Informal Texts, Neuron 1024(512) (2022) 927-934.
[26] J. Potočnik, E. Thomas, R. Killeen, S. Foley, A. Lawlor, J. Stowe, Automated vetting of radiology referrals: exploring natural language processing and traditional machine learning approaches, Insights into Imaging 13(1) (2022) 1-8.
[27] H. Brown, K. Lee, F. Mireshghallah, R. Shokri, F. Tramèr, What does it mean for a language model to preserve privacy? in: 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), ACM, Seoul, Republic of Korea, New York, NY, USA, pp. 2280-2292. doi: https://doi.org/10.1145/3531146.3534642.
[28] H. Yang, Q. He, Z. Liu, Q. Zhang, Malicious encryption traffic detection based on NLP. Security and Communication Networks (2021). doi: https://doi.org/10.1155/2021/9960822.
[29] M. I. Alfarizi, L. Syafaah, M. Lestandy, Emotional Text Classification Using TF-IDF (Term Frequency-Inverse Document Frequency) And LSTM (Long Short-Term Memory). JUITA: Jurnal Informatika 10(2) (2022) 225-232.