Cambridge International

Professional Research Thesis

Titled

Cyber security and its relationship to public security, Emotion classification using AI

Researcher

Bahy Ibrahim El-sayed Mohammed

Supervisor signature

2025

Introduction

AI and cybersecurity are the two most important events in our present time because they have a clear and significant impact on all aspects of life.

For example, AI may be used properly in development and innovation or may be poorly used in forgery and threat to personal safety.

Cybersecurity may also be used properly to secure and defend or may be used as a loophole or to create loopholes for penetration and corruption.

Therefore, both AI and cybersecurity are the two most important events in today's tech world because of their impact on many aspects of life and on each other.

If the use of any AI or cybersecurity may be useful or may pose a threat to the public good and personal safety, how can the picture be if combined and used as a single entity.

This message reviews the concept and value of both artificial intelligence and cybersecurity and recognizes their value and impact on the public good and personal safety.

The usefulness and gravity of combining artificial intelligence with cybersecurity and the value of relying on them and being wary of them are also reviewed.

The most important problems facing both AI and cybersecurity are also reviewed as well as proposed solutions and future suggestions to advance the areas and provide ways of securing against tampering with them.

Let us therefore review the most important points on this subject and address them in detail for clear recognition.

Problem definition

Current Challenges in Emotion classification:

- Sentiment analysis and opinion mining have reached an advanced stage, but they still face some problems that prevent them from being fully generalized or relying on them mainly, especially in sensitive areas.
- These problems may be the weakness of some models or bad training and testing, but these problems are easy to overcome and these problems are temporary.
- The small number of expressions used in the classification is also a temporary problem.
- However, some problems are difficult to overcome and have temporary solutions, such as the weakness of the data set in terms of size or accuracy, and this is due to the continuous increase in data, which confirms the impossibility of manually classifying the data.
- The size and accuracy of data classification in the data set affect the accuracy of the results produced by the model positively or negatively, depending on the validity of the data set.
- The constant change of language, especially slang and also emojis.

Current Challenges in Cybersecurity:

- Advanced Persistent Threats (APTs): These attacks represent a long-term, persistent threat against critical systems.
- Attacks on critical infrastructure: Such as attacks on power grids or healthcare systems.
- Data privacy: Laws and regulations related to the protection of personal data and its safeguarding against leakage or misuse.
- Software vulnerabilities: New vulnerabilities continue to be discovered in the software and systems used by companies and individuals.

Motivation

- Some of the problems facing sentiment analysis prevent the continuation of many distinguished works.
- Sentiment analysis is required in many fields, but the problems it faces make it difficult to rely on it in the first place.
- Some data may carry multi- feeling content.
- Some data may carry very important or dangerous content
- Artificial intelligence may threaten cybersecurity and public security.
- Cybersecurity has some problems that prevent its absolute use.
- Developing cybersecurity to rely on in different situations and emergencies.
- Combining artificial intelligence with cybersecurity to use them for the common good.

Objectives

- Building a model that classifies data into 11 emotions accurately.
- Making sentiment analysis easier and more professional by overcoming some of the problems facing the idea.
- Giving former scholars an impetus to complete their stalled work and gives an impetus to upcoming scholars to delve into this field with confidence.
- Defines the different polarities of vocabulary and words.
- Design a dataset with a large size that tries to compensate for the weakness of the models to some extent, which makes training and testing models better.
- Include a lot of slang language and also deals with the novelties of the language.
- Understand the real meaning and basic purpose of using cybersecurity.

- Proper guidance for the use of cybersecurity from different situations and areas.

- Recognize the value and usefulness of combining artificial intelligence with cyber manna.

Study Hypotheses and Questions

Can artificial intelligence really be a double-edged sword?

What are the limitations of artificial intelligence?

Is there a relationship between artificial intelligence and cybersecurity?

To what extent do artificial intelligence and cybersecurity impact each other?

What is the relationship between cybersecurity and public safety?

What are the challenges facing artificial intelligence?

What are the challenges facing cybersecurity?

How can cybersecurity and artificial intelligence be combined to ensure public safety?

What are the challenges facing the idea of combining them?

Study Approach

The **Analytical descriptive methodology** was used to determine “Cyber security and its relationship to public security, Emotion classification using AI" .

The limits of study

Spatial Boundaries: all over the world.

Temporal Boundaries: 2019 - 2025.

Related Work

Emotion classification Related work.

- **Sentiment Analysis in Twitter Using Machine Learning:**
  - In ASRIC 2021 the researchers in the work [1] analyzed sentiment in 4, 8, and 11 sentiments using NB, SVM, LR, and KNN.
  - NB had the highest accuracy in all classifications, but the highest accuracy was in the range of 4 feelings due to the lack of sufficient data for training and testing.
  - The small size of the data set led to a deterioration in accuracy as the number of sentiments increased.

- **A lightweight sentiment analysis framework for a micro intelligent terminal:**
  - This work [2] seeks to solve the problem of colloquial language as it seeks to solve the problem of satirical language.
  - The researchers concluded that the strength, argument, and accuracy of the data set affect the success of the model.

- **Stock Emotions: Discover Investor Emotions for Financial Sentiment Analysis and Multivariate Time Series:**

  - In this work [3], the researchers used a dataset of 10,000 comments collected from a financial social media platform to search for emotion in the stock market.

  - This work was undertaken in an effort to solve the problem of the lack of textual data containing investor sentiments, and the existing datasets are small in size and limited in availability.

  - In the test, an average F1 score of 0.81 was achieved for the financial sentiment rating and 0.42 for the emotional rating.

- **Presence of informal language, such as emoticons, hashtags, and slang, impact the performance of sentiment analysis models on social media text:**

  - In this work [4] researchers seek to investigate the impact of the presence of informal language such as emoji and slang, as there is insufficient data or focus on mental health problems and suicidal ideation.

  - Finally, the researchers concluded that integrating sentiment data can improve the performance of sentiment analysis models.

  - The researchers also concluded that the presence of informal language affects the performance of sentiment

analysis models.

- **SemEval-2019 task 3: EmoContext Contextual Emotion Detection in Text:**

  - Through this work [5] the aim of the researchers was to discover the feelings in the texts and also to try to address the duality and mixing of feelings.
  - The driving force behind this work is that detecting emotions in texts is difficult due to the absence of facial expressions and tone of voice.
  - the highest evaluation was a micro-averaged F1 score of 79.59 and the best systems performance was for feelings of sadness and the worst was for feelings of happiness.

- **CARER: Contextualized Affect Representations for Emotion Recognition:**

- Traditional methods analyze data at the sentence level, which makes them less efficient compared to methods that represent the body as a complex network ,and methods based on rules and statistics cannot capture the evolving linguistic variation.

- Moreover, the short text is a difficult problem in emotion recognition and various natural language tasks, so this work [6] is based on representing the emotion group as a graph to reduce the usual problems facing emotion analysis, and the researchers seek in this work to facilitate the creation of

emotion recognition systems.

- The result showed good and promising results and paved the way for building more interpretable systems for emotion recognition.

- **Sentiment analysis and research based on two channel parallel hybrid neural network model with attention mechanism:**
  - This work [7] seeks to use BERT (Bi-directional Encoder Representations from Transformers) model to convert text into word vectors.
  - Proposing a Bi-directional Encoder Representations from Transformers (BERT)-based dual-channel parallel hybrid neural network model for text sentiment analysis.
  - The results of the hotel review data sets showed that the accuracy of proposed modeling sentiment classification reaches 92.35% and the F1 score reaches 91.59%.

- **Automated Sentiment and Hate Speech Analysis of Facebook Data by Employing Multilingual Transformer Models:**

  - The work [8] Analyzes the statistical distribution of the contents of hateful and negative emotions within a set of representative data on Facebook from 648 pages.
  - There was a weakness in the performance of the model and difficulty in identifying hate speech and negative feelings.
  - The Majority of non-hateful content is actually neutral in sentiment (38.07% of 88.29%). Within the non-hateful category, the amount of negative sentiment to the amount of positive amount (28.12% to 22.10%) – it seems counter-intuitive. XTC model has an F1-score of 37.7 for the non-hateful label.

- **ZYJ at SemEval-2021 Task 7: HaHackathon: Detecting and Rating Humor and Offense with ALBERT-Based Model:**

  - The work [9] stands on the Classification and discovery of humor and offense in the text using deep learning in tasks 1A, 1B, 1C, and task 2.
  - In Task 1A to discover humor, work is ranked No. 41 by F-Score = 0.9348. In TASK 1B for the average humor, work is ranked No. 43 by RMSE = 0.7214. In TASK 1C for the controversy of humor, the work is ranked No. 33 by F- Score = 0.4603.

- In TASK 2 for an average offensive, ranked work No. 31 by RMSE = 0.5204.The work needs to improve the performance, and also Using large and organized data groups may be useful to improve performance and compensate for some systems problems as the general performance is weak.

- **Automatic Detection of Hate Speech on Facebook Using Sentiment and Emotion Analysis:**

  - This work [10] Identifies hate speech and the pages which promote it on Facebook automatically. This work also uses graph, sentiment, and emotion analysis techniques to cluster and analyze posts on prominent Facebook pages. This work faced the problems of a Small data set and also the difficulty collecting modern comments and realizing new vocabulary.

Cybersecurity Related work.

- **Enhanced Intrusion Detection Systems Performance with UNSW-NB15 Data Analysis 2024**

  ➢ The paper presents a hybrid Intrusion Detection System (IDS) using CNN and LSTM for detecting security attacks, implemented on the UNSW-NB15 dataset. The proposed model significantly improves accuracy, achieving 91.86% on imbalanced and 92.10% on balanced datasets, compared to the basic CNN model and traditional classifiers. Data balancing and interpolation techniques were utilized for enhanced performance. The results highlight the proposed model's effectiveness in classifying network traffic as normal or attack [11].

- **Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cybersecurity 2023**

➢ Our research aims to improve automated intrusion detection by developing a highly accurate classifier with minimal false alarms. The motivation behind our work is to tackle the challenges of high dimensionality in intrusion detection and enhance the classification performance of classifiers, ultimately leading to more accurate and efficient detection of intrusions. To achieve this, we conduct experiments using the NSL-KDD data set, a widely used benchmark in this domain. This data set comprises approximately 126,000 samples of normal and abnormal network traffic for training and 23,000 samples for testing. Initially, we employ the entire feature set to train classifiers, and the outcomes are promising. Among the classifiers tested, the J48

tree achieves the highest reported accuracy of 79.1 percent. To enhance classifier performance, we explore two projection approaches: Random Projection and PCA. Random Projection yields notable improvements, with the PART algorithm achieving the best-reported accuracy of 82.0 %, outperforming the original feature set. Moreover, random projection proves to be more time-efficient than PCA across most classifiers. Our findings demonstrate the effectiveness of random projection in improving intrusion detection accuracy while reducing training time. This research contributes valuable insights to the cybersecurity field and fosters potential advancements in intrusion detection systems[12,13].

- **An Efficient Hyperparameter Control Method for a Network Intrusion Detection System Based on Proximal Policy Optimization 2021.**

  - Experiments were conducted to evaluate the system performance using the CICIDS2017 and UNSW-NB15 datasets. In the CICIDS2017 dataset, the model achieved an F1-score of 0.96552, while in the UNSW-NB15 dataset, it achieved an F1-score of 0.94268. To further test the robustness of the model, an experiment was conducted by merging the two datasets to create a more extensive and complex test environment. This merger resulted in a dataset with more diverse attack types and complex patterns, leading to an F1-score of 0.93567. This score indicates that the performance on the merged dataset was between 97% and 99% of the performance on the individual datasets (CICIDS2017 and UNSW-NB15). The results reveal that the proposed Intrusion Detection Hyperparameter Control System (IDHCS) improved the performance of the IDS by automating the learning of

new types of attacks. This was achieved by effectively managing intrusion detection features regardless of network environment changes through continuous learning [14].

- **Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset 2020**

➢ Computer networks intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are critical aspects that contribute to the success of an organization. Over the past years, IDSs and IPSs using different approaches have been developed and implemented to ensure that computer networks within enterprises are secure, reliable and available. In this paper, we focus on IDSs that are built using machine learning (ML) techniques. IDSs based on ML methods are effective and accurate in detecting networks attacks. However, the performance of these systems decreases for high dimensional data spaces. Therefore, it is crucial to implement an appropriate feature extraction method that can prune some of the features that do not possess a great impact in the classification process. Moreover, many of the ML based IDSs suffer from an increase in false positive rate and low detection accuracy when the models are trained on highly imbalanced datasets. In this paper, we present an analysis the UNSW-NB15 intrusion detection dataset that will be used for training and testing our models. Moreover, we apply a flter-based feature reduction technique using the XGBoost algorithm. We then implement the following ML approaches using the reduced feature space: Support Vector Machine (SVM), k-Nearest-Neighbour (kNN), Logistic Regression (LR), Artificial Neural Network (ANN) and Decision Tree (DT). In our experiments, we considered both the binary and multiclass classification configurations. The results demonstrated that the XGBoost-based feature selection method allows

for methods such as the DT to increase accuracy from 88.13 to 90.85% for the binary classification scheme [15, 16].

- **Enhancing the Sustainability of Deep-Learning-Based Network Intrusion Detection Classifiers against Adversarial Attacks 2023**

➢ An intrusion detection system (IDS) is an effective tool for securing networks and a dependable technique for improving a user's internet security. It informs the administration whenever strange conduct occurs. An IDS fundamentally depends on the classification of network packets as benign or attack. Moreover, IDSs can achieve better results when built with machine learning (ML)/deep learning (DL) techniques, such as convolutional neural networks (CNNs). However, there is a limitation when building reliable IDS using ML/DL techniques, which is their vulnerability to adversarial attacks. Such attacks are crafted by attackers to compromise the ML/DL models, which affects their accuracy. Thus, this paper describes the construction of a sustainable IDS based on the CNN technique, and it presents a method for defense against adversarial attacks that enhances the IDS's accuracy and ensures it is more reliable in performing classification. To achieve this goal, first, two IDS models with a convolutional neural network (CNN) were built to enhance the IDS accuracy. Second, seven adversarial attack scenarios were designed against the aforementioned CNN-based IDS models to test their reliability and efficiency. The experimental results show that the CNN-based IDS models achieved significant increases in the intrusion detection system accuracy of 97.51% and 95.43% compared with the scores before the adversarial scenarios were applied. Furthermore, it was revealed that the adversarial attacks caused the models' accuracy to significantly decrease from one attack scenario to another. The Auto-PGD and BIM attacks had the strongest effect

against the CNN-based IDS models, with accuracy drops of 2.92% and 3.46%, respectively. Third, this research applied the adversarial perturbation elimination with generative adversarial nets (APE_GAN++) defense method to enhance the accuracy of the CNN-based IDS models after they were affected by adversarial attacks, which was shown to increase after the adversarial attacks in an intelligible way, with accuracy scores ranging between 78.12% and 89.40% [17].

- **Enhancing Privacy-Preserving Intrusion Detection through Federated Learning 2023**

➢ Detecting anomalies, intrusions, and security threats in the network (including Internet of Things) traffic necessitates the processing of large volumes of sensitive data, which raises concerns about privacy and security. Federated learning, a distributed machine learning approach, enables multiple parties to collaboratively train a shared model while preserving data decentralization and privacy. In a federated learning environment, instead of training and evaluating the model on a single machine, each client learns a local model with the same structure but is trained on different local datasets. These local models are then communicated to an aggregation server that employs federated averaging to aggregate them and produce an optimized global model. This approach offers significant benefits for developing efficient and effective intrusion detection system (IDS) solutions. In this research, we investigated the effectiveness of federated learning for IDSs and compared it with that of traditional deep learning models. Our findings demonstrate that federated learning, by utilizing random client selection, achieved higher accuracy and lower loss compared to deep

learning, particularly in scenarios emphasizing data privacy and security. Our experiments highlight the capability of federated learning to create global models without sharing sensitive data, thereby mitigating the risks associated with data breaches or leakage. The results suggest that federated averaging in federated learning has the potential to revolutionize the development of IDS solutions, thus making them more secure, efficient, and effective[18, 19].

- **Hybrid Deep Learning Based Attack Detection for Imbalanced Data Classification 2022**

➢ Intrusion Detection Systems (IDSs) using machine learning and deep learning techniques can detect security attacks accurately. This paper develops an IDS architecture based on Convolutional Neural Network (CNN) and Long Short-term Memory (LSTM) deep learning algorithms. We implement our model on the UNSW-NB15 dataset which is a new network intrusion dataset that categorizes the network traffic into normal and attacks traffic. In this work, interpolation data preprocessing is used to compute the missing values. Also, the imbalanced data problem is solved using a synthetic data generation method. Extensive experiments have been implemented to compare the performance results of the proposed model (CNN+LSTM) with a basic model (CNN only) using both balanced and imbalanced dataset. Also, with some state-of-the-art machine learning classifiers (Decision Tree (DT) and Random Forest (RF)) using both balanced and imbalanced dataset. The results proved the impact of the balancing technique. The proposed hybrid model with the balance technique can classify the traffic into normal class and attack class with reasonable accuracy

(92.10%) compared with the basic CNN model (89.90%) and the machine learning (DT 88.57% and RF 90.85%) models. Moreover, comparing the proposed model results with the most related works shows that the proposed model gives good results compared with the related works that used the balance techniques [20].

Study plan

Chapter one: AI (framework and concepts).

Section one: What's AI?

1. AI history.
2. AI pros and cons.
3. Examples of AI in real life.

Section two: Emotion classification.

1. What's Emotion classification?
2. Forms of Emotion classification.

Section three: Datasets.

1. What's datasets definition and use?

Chapter two: Emotion classification models building.

Section one: Background.

1. Stages of developing of emotions and classification workflow.
2. Dataset Details and emotions.

Section two: Models building.

1. Data preprocessing.
2. Feature extraction.
3. Algorithms.
4. Models training, testing and enhancing.

Chapter three: Cybersecurity.

Section one: Cybersecurity (history and concepts).

1. What's cybersecurity ?
2. Cybersecurity history.
3. Types of cyber threats and cybersecurity techniques used to combat them.
4. Current cybersecurity challenges and how to overcome them in the future.

Section two: Cyber security and its relationship to public security, Emotion classification using AI.

1. Cybersecurity and Public Security.
2. The Impact of Combining Artificial Intelligence (AI) and Cybersecurity on Public Security.

Conclusion

From previous studies it is clear to us that AI and especially the field of classification of emotions is a very important area and it enters into many and many fields in our daily and real life.

The classification of feelings has many ways and many disciplines but they all work for the same common goal but the classification of feelings through texts and the processing of natural language remains the most difficult due to constant changes in languages as well as multiple linguistic concepts.

It also reviewed the concept of cybersecurity and a glimpse of its history and various details and reflected its importance and value on public security and the security of organizations.

Finally, the link point was reached and a combination of the classification of emotions using artificial intelligence and cybersecurity and their significant impact on public security.

The topic was dealt with in many respects and examined its details for deeper understanding and understanding.

Challenges

Challenges of Integrating Artificial Intelligence (AI) with Cybersecurity for Public Security

While AI-powered cybersecurity enhances public security by improving threat detection, crime prevention, and digital protection, integrating AI into cybersecurity systems comes with several challenges. These challenges affect governments, law enforcement, businesses, and individuals who rely on AI for security.

1. AI Vulnerabilities & Adversarial Attacks

Problem: AI systems can be hacked, manipulated, or tricked by cybercriminals.

Adversarial Attacks: Hackers use deceptive inputs (e.g., altered images or data) to mislead AI security systems.

Data Poisoning: Attackers inject malicious data into AI training models, causing AI to make wrong security decisions.

AI Model Exploits: Cybercriminals study AI models to find weaknesses and bypass security measures.

Example: In 2019, researchers tricked AI-powered facial recognition systems into misidentifying people using slightly altered images.

Attackers can bypass AI spam filters by slightly changing words or structures in phishing emails.

2. AI Security Systems Require Huge Data & Computing Power

Problem: AI-powered cybersecurity relies on large datasets and massive computing resources.

AI needs continuous training on new cyber threats, requiring large amounts of high-quality data.

Small businesses and developing nations may struggle to afford high-performance AI cybersecurity systems.

AI-driven security systems consume a lot of computing power, leading to high operational costs.

Example: AI-based threat detection systems in large organizations generate huge amounts of security alerts, requiring expensive infrastructure to process them.

A government AI cybersecurity system may require millions of real-time data points, making it costly to maintain.

3. AI Can Be Used by Cybercriminals

Problem: Just as AI strengthens cybersecurity, cybercriminals also use AI to launch advanced attacks.

AI-powered malware can adapt, evolve, and evade detection.

Hackers use AI-driven deepfake technology to impersonate people and commit fraud.

AI automates cyberattacks, allowing hackers to launch millions of attacks at high speed.

Example: In 2019, cybercriminals used AI-powered deepfake voice cloning to impersonate a CEO and trick an employee into transferring $243,000.

AI-powered automated phishing attacks generate convincing fake emails that bypass traditional security filters.

4. Lack of Skilled AI & Cybersecurity Experts

Problem: There is a global shortage of AI and cybersecurity professionals, making it hard to implement AI security systems.

AI cybersecurity requires expertise in machine learning, cybersecurity, and threat intelligence, which is rare.

Many governments and organizations struggle to find skilled AI security experts.

The high cost of hiring AI specialists makes it difficult for smaller institutions to adopt AI cybersecurity solutions.

Example: The cybersecurity workforce gap is estimated at over 3.4 million unfilled positions worldwide.

Many organizations lack the technical knowledge to integrate AI into their cybersecurity operations.

5. Regulatory & Legal Challenges

Problem: AI in cybersecurity lacks clear regulations, leading to legal and ethical concerns.

Many countries don’t have laws governing AI-driven cybersecurity and surveillance.

Lack of global cybersecurity standards creates gaps in security enforcement.

AI-generated security decisions may conflict with human rights laws.

Example: GDPR (General Data Protection Regulation) in Europe limits how AI can process personal data, making it harder for AI security systems to track cybercriminals.

Some AI-powered predictive policing programs have been shut down due to privacy concerns.

Recommendations

1. Develop robust AI models that can detect and resist adversarial attacks, using constant updates and retraining.

2. Implement human oversight in AI decision-making for security-related applications.

3. Use privacy-preserving AI techniques, such as federated learning, to process data without compromising user privacy.

4. Use cloud-based AI cybersecurity solutions to reduce costs.

5. Develop AI-powered cybersecurity tools that can detect AI-generated attack in real-time.

6. Train cybersecurity professionals in AI threat defense techniques.

7. Invest in AI and cybersecurity education programs to train new experts.

8. Governments must create strong AI cybersecurity laws that protect both security and privacy.

9. Establish international cooperation on AI cybersecurity policies.

REFRENCES

1. Bahy Ibrahim, Mohamed Ahmed, Rasha Stohy, "Sentiment Analysis in Twitter Using Machine Learning", African scientific Research and Innovation Council(ASRIC), Sep 2021
2. Lin Wei, Zhenyuan Wang, Jing Xu, Yucheng Shi, Qingxian Wang, Lei Shi, Yongcai Tao, Yufei Gao "A Lightweight Sentiment Analysis Framework for a Micro-Intelligent Terminal" School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450001, China , 2023 Jan doi: 10.3390/s23020741.
3. Lin Wei, Zhenyuan Wang, Jing Xu, Yucheng Shi, Qingxian Wang, Lei Shi, Yongcai Tao, Yufei Gao "A Lightweight Sentiment Analysis Framework for a Micro-Intelligent Terminal" School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450001, China , 2023 Jandoi: 10.3390/s23020741
4. Jean Lee, Hoyoul Luis Youn, Josiah Poon, Soyeon Caren Han, "StockEmotions: Discover Investor Emotions for Financial Sentiment Analysis and Multivariate Time Series" The University of Sydney, 23 January 2023.
5. Aadil Gani Ganie, "Presence of informal language, such as emoticons, hashtags, and slang, impact the performance of sentiment analysis models on social media text", Department of Informatics, University of Miskolc, Hungary, Email: ganie.aadil.gani@student.uni-miskolc.hu, *28 Jan2023*

6. Ankush Chatterjee, Kedhar Nath Narahari, Meghana Joshi, Puneet Agrawal “SemEval- 2019 Task 3: EmoContext Contextual Emotion Detection in Text” 13th International Workshop on Semantic Evaluation, 6–7 June 2019.

7. Elvis Saravia, Hsien-Chi Toby Liu, Yen-Hao Huang, Junlin Wu, Yi-Shin Chen “CARER: Contextualized Affect Representations for Emotion Recognition” Conference on Empirical Methods in Natural Language Processing, 4 November 2018.

8. a Chen, Yanqiu Sun, Yan Yan “Sentiment analysis and research based on two- channel parallel hybrid neural network model with attention mechanism” IET Control Theory and Applications published , John Wiley and Sons, 5 April 2023.

9. R. Manuvie, S. Chatterjee, “Automated Sentiment and Hate Speech Analysis of Facebook Data by Employing Multilingual Transformer Models”, University College Groningen, University of Groningen,31 Jun 2023 .

10. ,” ZYJ at SemEval-2021 Task 7: HaHackathon: Detecting and Rating Humor and Offense with ALBERT-Based Model”, The 15th International Workshop on Semantic Evaluation (SemEval-2021), 2021.

11. Ieracitano, C.; Adeel, A.; Gogate, M.; Dashtipour, K.;Morabito, C.F.; Larijani, H.; Raza, A.; Hussain, A. Statistical analysis driven optimized deep learning system for intrusion detection. In Advances in Brain Inspired Cognitive Systems; Springer Nature: Cham, Switzerland, 2018; Volume 10989, pp. 759–769. [CrossRef]

12. Rodríguez, M.; Alesanco, Á.; Mehavilla, L.; García, J. Evaluation of Machine Learning Techniques for Traffic Flow-Based Intrusion Detection. Sensors 2022, 22, 9326. [CrossRef] [PubMed]

13. Markevych, M.; Dawson, M. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In Proceedings of the International Conference Knowledge-Based Organization, Sibiu, Romania, 19 July 2023; Volume 29, pp. 30–37.

14. Dini, P.; Elhanashi, A.; Begni, A.; Saponara, S.; Zheng, Q.; Gasmi, K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. Appl. Sci. 2023, 13, 7507. [CrossRef]

15. Vigneswaran, R.K.; Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security. In Proceedings of the 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 10–12 July 2020.

16. Nour, M.; Slay, J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. Inf. Secur. J. A Glob. Perspect. 2016, 25, 18–31. Nour, M.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the

Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 10–12 November 2015.

17. X. Wang, Y. Zhao and F. Pourpanah, “Recent advances in deep learning,” International Journal of Machine Learning and Cybernetics, vol. 11, no. 4, pp. 747–750, 2020.

18. S. Moyer, “IoT sensors and actuators,” IEEE Internet of Things Magazine, vol. 2, no. 3, pp. 10, 2019.

19. A. Hasan and V.K. Patle, “Security threats in perception and network layer of Internet of Things (IoT): A review,” International Journal of Technology, vol. 10, no. 2, pp. 143–152, 2020.

20. H. Khattak, M. Bouhlal, R. Aitabdelouah, S. Elfilali and E. Benlahmar, “Perception layer security in Internet of Things,” Future Generation Computer Systems, vol. 100, no. 7, pp. 144–164, 2019.

21. Bowen Baker, Ingmar Kanitscheider, Todor Markov, Yi Wu, EMERGENT TOOL USE FROM MULTI-AGENT AUTOCURRICULA, conference ICLR 2020, 11 Feb 2020.

22. Aadil Gani Ganie, Presence of informal language, such as emoticons, hashtags, and slang, impact the performance of sentiment analysis models on social media text?, Department of Informatics, University of Miskolc, Hungar, 28 Jan 2023, URL https://doi.org/10.48550/arXiv.2301.12303

23. Wei, W., Xiang, Y., Chen, Q.: Survey on Chinese text sentiment analysis. J.Comput. Appl. 31(12), 3321–3323 (2011)

24. M. Bansal, S. Verma, K. Vig, K. Kakran, Opinion mining from student feedback data using supervised learning algorithms, in: Third International Conference on Image Processing and Capsule Networks, Springer International Publishing, 2022, pp. 411–418. doi:10.1007/ 978-3-031-12413-6_32. URL https://doi.org/10.1007/978-3-031-12413-6_32
25. "Guide To Data Cleaning: Definition, Benefits, Components, And How To Clean Your Data". Tableau. Retrieved 17-10-2021.
26. Sarangi, Susanta; Sahidullah, Md; Saha, Goutam (September 2020). "Optimization of data-driven filterbank for automatic speaker verification".
27. Jurafsky, Daniel; H. James, Martin (2000). Speech and language processing : an introduction to natural language processing, computational linguistics, and speech recognition. Upper Saddle River, N.J.: Prentice Hall. ISBN 978-0-13-095069-7
28. James, Gareth (2013). An Introduction to Statistical Learning: with Applications in R. Springer. p. 176. ISBN 978-1461471370
29. Jump up to:a b Ripley, Brian (1996). Pattern Recognition and Neural Networks. Cambridge University Press. p. 354. ISBN 978-0521717700
30. "Deep Learning". Coursera. Retrieved 2021-05-18
31. Jump up to:a b c d e f Brownlee, Jason (2017-07-13). "What is the Difference Between Test and Validation Datasets?". Retrieved 2017-10-12.
32. Axel Rodríguez, Carlos Argueta, Yi-Ling Chen, "Automatic Detection of Hate Speech on Facebook Using Sentiment and Emotion Analysis", international conference on artificial intelligence in information and communication(ICAIIC), 01

February 2019.
https://www.researchgate.net/publication/33195347 0.

33. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

34. Computer security at the Encyclopædia Britannica.


THANKS