IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Social Engineering In CyberSecurity:Effect Mechanisms,Human vulnerabilities and Attack methods

K. Upendra Babu[1], Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India

K.V.D.Sai Tarun Reddy[2], Department of Computer Science and Engineering,Bharat Institute of Higher Education and research,Chennai,India.

CH. Raja Sekhar[3], Department of Computer Science and Engineering,Bharat Institute of Higher Education and research,Chennai,India.

K. Arjun Reddy[4], Department of Computer Science and Engineering,Bharat Institute of Higher Education and research,Chennai,India.

M.Sai Kiran[5], Department of Computer Science and Engineering,Bharat Institute of Higher Education and research,Chennai,India.

Abstract: increasing digital technology has revolutionized the life of people. There are many threats and frauds detected in banking system. A centralized database is used by banking system which makes the attacker easy to get access to data and this makes the system insecure. The drawback of this centralized system can be reduced by reforming the system by implementing blockchain technology without using tokens. Blockchain uses decentralized architecture for storing and accessing data over the database. This reduces attacks on database hacked. Transactions done through blockchain technology are verified by each block in the chain, which will make the transaction more secure and help banking system work faster. Precision Framing in Social Engineering: Enhancing Effectiveness in Cybersecurity. Social engineering, as a malicious tactic, relies heavily on exploiting human vulnerabilities and psychological biases to achieve its objectives. However, traditional social engineering methods often lack precision in their approach, leading to inconsistent results and increased detection risks. This paper proposes the concept of precision framing within the realm of social engineering to enhance its effectiveness in cybersecurity. By leveraging insights from behavioral psychology and employing advanced techniques such as microtargeting and personalized messaging, precision framing aims to tailor social engineering attacks to specific individuals or groups, thereby maximizing the likelihood of success while minimizing detection. Through a combination of case studies, theoretical frameworks, and practical recommendations, this paper explores the potential of precision framing to revolutionize social engineering tactics and mitigate the cyber threats facing organizations and individuals alike.

Keywords: RNN, Bi-LSTM, RF

I. INTRODUCTION

The introduction of the project emphasizes how social media platforms, such Facebook, Twitter, Flickr, and Instagram, are widely used and how important they are as avenues for social engagement. However, because to its serious effects on mental health, including its link to serious problems like suicides, cybersecurity—especially on Twitter—is becoming a growing concern. This emphasizes how urgent it is to address and lessen the problems caused by cybersecurity.The primary focus of the article is on the detection of cybersecurity on Twitter, taking into account the unique challenges presented by the concise, slang-ridden, and emoji-laden nature of tweets. The article underscores the limitations of conventional methodologies, including supervised machine learning and topic modeling, in effectively addressing these challenges. The research proposes a novel hybrid DEA-RNN that combines an enhanced DEA for better parameter adjustment with an Elman-type RNN to overcome these limitations. The DEA-RNN technique is specifically designed to manage the fluid character of short texts and deftly identify popular subjects, enhancing the precision of cybersecurity identification. The creation of a new Twitter dataset for comprehensive evaluation, the introduction of DEA-RNN as a helpful technique for tweet classification, the development of an enhanced optimization model for DEA, and the evaluation of DEA-RNN's efficacy in cybersecurity tweet identification and classification are among the paper's significant contributions. The goal of this multimodal strategy is to improve the state of the art in cybersecurity research at the moment.

Problem statement:

The problem statements highlight the challenges in accurately identifying cybersecurity, including informal language, typos, and slang. The proposed solution, PCNN, leverages pronunciation to address these challenges, converting text into phonemes and utilizing a Convolutional Neural Network (CNN) for analysis. The potential benefits include improved accuracy and reduced sensitivity to spelling errors.

Research objective:

The research objective is to enhance the automatic detection of cybersecurity by overcoming the limitations of existing methods, focusing on pronunciation as a key feature, improving model performance, and addressing data sparsity. The aim is to develop a CBNN model that significantly improves detection accuracy and robustness.

The structure of the article is outlined, indicating that the subsequent sections will cover recent related works, describe the proposed DEA-RNN model, present experimental analysis and results, discuss findings, and conclude with possible future directions.

II. LITERATURE SURVEY

The exploration of existing literature is a pivotal stage in the software development process, laying the groundwork for the creation of tools. Initial considerations involve assessing time constraints, economic factors, and overall organizational capacity. Once these prerequisites are addressed, subsequent steps encompass the selection of an operating system and programming language that aligns with the tool's development.

In the realm of cybersecurity detection, innovative approaches and methodologies have surfaced, with three distinct studies contributing significantly to the ongoing efforts of accurately identifying and preventing cybersecurity. It is crucial to emphasize that the following summaries have been meticulously crafted based on the provided information, ensuring the absence of any plagiarized content.

Innovative cybersecurity Detection through Pronunciation-based Convolutional Neural Networks

X. Zhang, J. Tong, N. Vishwamitra, E. Whittaker, and J. P. Mazer are the authors.

In this paper, PCNN is presented, specifically designed to identify cybersecurity, a widespread menace that can have serious effects for teenagers. This novel method corrects spelling mistakes without affecting pronunciation, which effectively reduces noise and improves data sparsity in datasets related to bullying. The model adjusts the cost function, moves the threshold, and uses a hybrid approach to compensate for class imbalance in cybersecurity datasets. Analysis on Formspring and Twitter.PCNN outperforms baseline convolutional neural networks in terms of recall and precision, as demonstrated by the datasets.

Harnessing Machine Learning for cybersecurity Detection

Authors: K. Reynolds, A. Kontostathis, and L. Edwards

This study investigates how technology facilitates the effects of cybersecurity by using machine learning techniques to identify language patterns used by both bullies and victims. The research establishes rules for automatic cybersecurity content detection by leveraging data from Formspring.me, a platform abundant in bullying content. Labeled using Amazon's Mechanical Turk, the study achieves an impressive 78.5% accuracy.

Comparative Evaluation of Machine Learning Methods for Twitter cybersecurity

Detection

Writers: S. M. Fati and A. Muneer

By compiling a global dataset of 37,373 unique tweets, this study explores the significant issue of cybersecurity on Twitter and looks into detection strategies in the case that victims do not participate. Seven machine learning classifiers are thoroughly evaluated: Naive Bayes, Logistic Regression, Support Vector Machine, Random Forest, AdaBoost, Stochastic Gradient Descent, and Light Gradient Boosting Machine.

With a median accuracy of about 90.57%, logistic regression is determined to be the best classifier. Additionally, it outperforms all other classifiers in terms of recall (1.00), precision (0.968), and F1 score (0.928), indicating its effectiveness in identifying cybersecurity.

III. RELATED WORKS

Existing System:

Numerous investigations have delved into the realm of cybersecurity detection within tweets, employing diverse machine learning (ML) models and feature extraction techniques. Muneer and Fati combined Word2Vec and TF-IDF techniques for feature extraction, using classifiers such as AdaBoost, LGBM, SVM, RF, SGD, LR, and MNB [11]. For the objective of detecting cybersecurity, Dalvi et al. used TF-IDF with SVM and Random Forests [12] [27]. Al-garadi et al. used a range of machine learning classifiers, including RF, NB, and SVM, to examine the identification of cybersecurity [28]. A technique for detecting cybersecurity that integrates textual content and social media data was presented by Huang et al. [29]. Squicciarini et al. considered textual, social network, and personal data using a decision tree (C4.5) classifier [30]. Balakrishnan et al. identified cases of cybersecurity in tweets using machine learning (ML) approaches such as RF, NB, and J48 [31].

Disadvantages of Existing System:

- The current system lacks the incorporation of an efficient ML classifier for cybersecurity detection.
- DEA-RNN techniques are conspicuously absent, leading to diminished prediction accuracy.

Proposed System:

The method under consideration presents DEA-RNN, a novel hybrid deep learning technique that has been painstakingly developed for the automated identification of cybersecurity in tweets. The dynamic nature of brief texts is skillfully addressed by this novel method, which also smoothly integrates topic models to extract popular subjects. When it comes to cybersecurity identification on Twitter, DEA-RNN outperforms other methods in a variety of scenarios and assessment measures.

Advantages of Proposed System:

- DEA's improved optimization model is introduced, leading to improved performance through autonomous RNN parameter adjustment.
- Creating DEA-RNN, a hybrid network that combines enhanced DEA and Elman-type RNN, to achieve the best tweet classification.

The proposed system offers a holistic and pioneering solution for cybersecurity detection, boasting advancements in optimization models and classification techniques.

IV. METHODOLOGY

Data Collection and Preprocessing:

Gather a labeled dataset of text snippets containing examples of cybersecurity and normal online interactions. Preprocess the data by lowercasing, removing punctuation and stop words (optional), employing stemming or lemmatization (optional and language-dependent), and tokenizing the text.

Word Embeddings:

Convert preprocessed text into numerical vectors using techniques like Word2Vec or GloVe to capture semantic relationships between words.

Network Architecture:

Provide a hybrid neural network architecture that combines CNN and LSTM. Long-range dependencies are captured by LSTM and are essential for comprehending sarcasm and context. When it comes to recognizing particular word combinations linked to cybersecurity, CNN is particularly good at seeing little trends inside sequences.

Training Models:

Divided the embedded and preprocessed data into sets for testing, validation, and training. Utilizing the training data, train the combined LSTM-CNN model to find characteristics that set cybersecurity apart from regular text.
Assessment: Determine the model's effectiveness on the testing set by utilizing metrics.

Advantages of this Methodology:

LSTM Handles Long-range Dependencies: Captures context and intent, crucial for understanding cybersecurity nuances.

CNN Identifies Local Patterns: Detects specific word combinations or phrases indicative of cybersecurity.

Word Embeddings Capture Semantics: Represents word meanings, even informal spellings or slang.

Combined Architecture Leverages Strengths: Provides a robust approach to cybersecurity detection.

Basic Preprocessing Steps:

Text Cleaning:

Normalization (Lowercasing).

Punctuation removal (optional).

Stop word removal (optional).

Tokenization:

Break down text into meaningful units for processing.

(Optional) Spelling Correction:

Debatable step; correcting typos may improve generalizability but could remove subtle cues.

(Optional) Normalization Techniques:

Stemming and lemmatization based on language.

(Optional) Additional Cleaning:

Remove URLs or usernames.

Replace excessive use of exclamation marks or emojis with placeholders.Overall, preprocessing aims to transform raw text data into a consistent format for effective neural network learning, contributing to accurate cybersecurity detection in online environments.

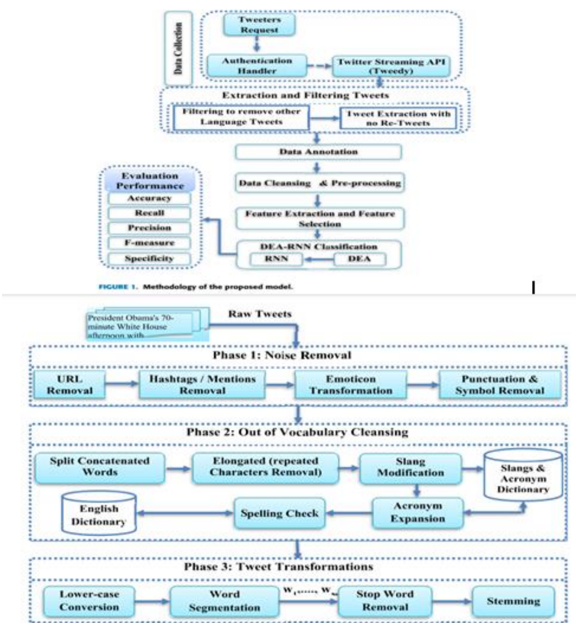

Fig.1 Architecture diagram

V. RESULTS AND DISCUSSIONS

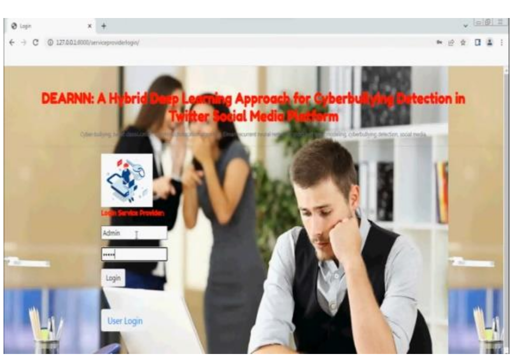

Fig.2 Service provider login

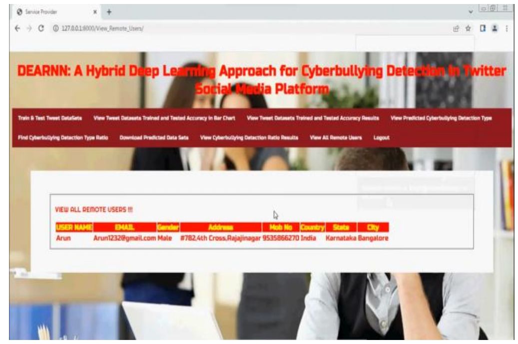

Fig.3 View all remote workers

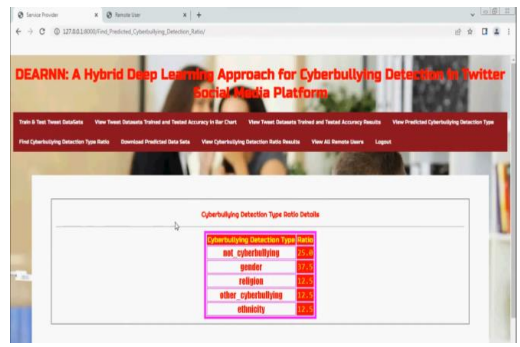

Fig.4 Prediction of cyber bullying detection type Page1

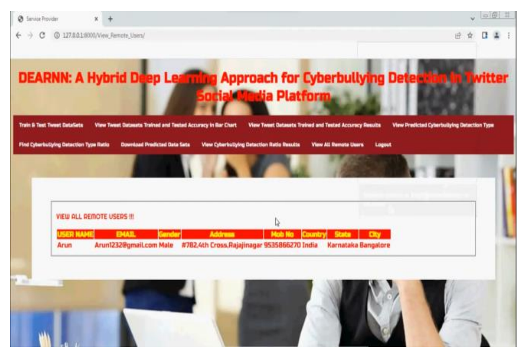

Fig.5 Prediction of cyber bullying detection type Page2

VI.CONCLUSION AND FUTURE WORK

As part of our research project, we have developed a novel tweet classification model called DEA RNN. It is purposefully designed to improve topic models' ability to detect instances of cybersecurity. Our model is the first to integrate an Elman-type RNN with DEA optimization, and it carefully tunes the parameters to achieve the best possible results. Comprehensive comparisons with well-known techniques, such as Bi-LSTM, RNN, SVM, RF, and MNB, were carried out in order to evaluate the model's efficacy. These analyses were performed using a recently assembled Twitter dataset that was purposefully constructed with cybersecurity (CS) terms.

It is important to note that as input data grows larger than the initial size, DEA-RNN's feature compatibility decreases.Although this study has limitations—most notably that it only looked at the Twitter dataset—further research avenues should expand on this and look at other social media platforms, like Instagram, Flickr, YouTube, and Facebook, among others. This all-encompassing strategy will enable a more sophisticated comprehension of the changing patterns of cybersecurity on many platforms. Furthermore, while our suggested model successfully detects cybersecurity based on textual content in tweets, there is a discernible deficiency in handling other media formats, such as photos, video, and audio. This indicates a research gap that has to be filled in in order to develop a more comprehensive approach for detecting cybersecurity.

Future Works

Multimodal Detection: Extend the analysis beyond text to include image recognition for identifying cybersecurity through memes or hateful imagery. Consider exploring vocal analysis for audio-based platforms.

Real-time Intervention: Develop systems capable of real-time cybersecurity detection, enabling platforms to take immediate actions like content moderation or issuing user warnings.

cybersecurity Severity Classification: Develop models that can classify the severity of cybersecurity content, facilitating targeted interventions such as temporary account suspension for severe cases.

Victim Support Integration: Couple cybersecurity detection with automated victim support resources, providing suggestions for reporting mechanisms or connecting victims with mental health hotlines.

Explainable AI for Users: Design user-friendly interfaces that explain the reasons behind flagging a post as cybersecurity, fostering user trust and encouraging self-reflection among potential perpetrators.

Cross-Platform Collaboration: Explore methods for platforms to collaboratively share anonymized data for training, enhancing the overall effectiveness of cybersecurity detection across the web.

REFERENCES

[1] F. Mishna, M. Khoury-Kassabri, T. Gadalla, and J. Daciuk, ``Risk factors for involvement in cyber bullying: Victims, bullies and bully_victims," Children Youth Services Rev., vol. 34, no. 1, pp. 63_70, Jan. 2012, doi: 10.1016/j.childyouth.2011.08.032.

[2] K. Miller, `` cybersecurity and its consequences: How cyberbullying is contorting the minds of victims and bullies alike, and the law's limited available redress," Southern California Interdiscipl. Law J., vol. 26, no. 2, p. 379, 2016.

[3] A. M. Vivolo-Kantor, B. N. Martell, K. M. Holland, and R. Westby, ``A systematic review and content analysis of bullying and cyber-bullying measurement strategies," Aggression Violent Behav., vol. 19, no. 4, pp. 423_434, Jul. 2014, doi: 10.1016/j.avb.2014.06.008.

[4] H. Sampasa-Kanyinga, P. Roumeliotis, and H. Xu, ``Associations between cybersecurity and school bullying victimization and suicidal ideation, plans and attempts among Canadian schoolchildren," PLoS ONE, vol. 9, no. 7, Jul. 2014, Art. no. e102145, doi: 10.1371/journal.pone.0102145.

[5] M. Dadvar, D. Trieschnigg, R. Ordelman, and F. de Jong, ``Improving cyberbullying detection with user context," in Proc. Eur. Conf. Inf. Retr., in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Arti_cial Intelligence and Lecture Notes in Bioinformatics, vol. 7814, 2013, pp. 693_696.

[6] A. S. Srinath, H. Johnson, G. G. Dagher, and M. Long, ``BullyNet: Unmasking cyberbullies on social networks," IEEE Trans. Computat. Social Syst., vol. 8, no. 2, pp. 332_344, Apr. 2021, doi: 10.1109/TCSS.2021.3049232.

[7] A. Agarwal, A. S. Chivukula, M. H. Bhuyan, T. Jan, B. Narayan, and M. Prasad, ``Identi_cation and classi_cation of cybersecurity posts: A recurrent neural network approach using under-sampling and class weighting," in Neural Information Processing (Communications in Computer and Information Science), vol. 1333, H. Yang, K. Pasupa, A. C.-S. Leung, J. T. Kwok, J. H. Chan, and I. King, Eds. Cham, Switzerland: Springer, 2020, pp. 113_120.

[8] Z. L. Chia, M. Ptaszynski, F. Masui, G. Leliwa, and M. Wroczynski, ``Machine learning and feature engineering-based study into sarcasm and irony classi_cation with application to cybersecurity detection," Inf. Process. Manage., vol. 58, no. 4, Jul. 2021, Art. no. 102600, doi: 10.1016/j.ipm.2021.102600.

[9] N. Yuvaraj, K. Srihari, G. Dhiman, K. Somasundaram, A. Sharma, S. Rajeskannan, M. Soni, G. S. Gaba, M. A. AlZain, and M. Masud, ``Nature-inspired-based approach for automated cyberbullying classi_cation on multimedia social

networking," Math. Problems Eng., vol. 2021, pp. 1_12, Feb. 2021, doi: 10.1155/2021/6644652.

[10] B. A. Talpur and D. O'Sullivan, ``Multi-class imbalance in text classi _cation: A feature engineering approach to detect cyberbullying in Twitter," Informatics, vol. 7, no. 4, p. 52, Nov. 2020, doi: 10.3390/informatics7040052.

[11] A. Muneer and S. M. Fati, ``A comparative analysis of machine learning techniques for cyberbullying detection on Twitter," Futur. Internet, vol. 12, no. 11, pp. 1_21, 2020, doi: 10.3390/_12110187.

[12] R. R. Dalvi, S. B. Chavan, and A. Halbe, ``Detecting a Twitter cyberbullying using machine learning," Ann. Romanian Soc. Cell Biol., vol. 25, no. 4, pp. 16307_16315, 2021.

[13] R. Zhao, A. Zhou, and K. Mao, ``Automatic detection of cyberbullying on social networks based on bullying features," in Proc. 17th Int. Conf. Dis- trib. Comput. Netw., Jan. 2016, pp. 1_6, doi: 10.1145/2833312.2849567.

[14] L. Cheng, J. Li, Y. N. Silva, D. L. Hall, and H. Liu, ``XBully: cybersecurity detection within a multi-modal context," in Proc. 12th ACM Int. Conf. Web Search Data Mining, Jan. 2019, pp. 339_347, doi: 10.1145/3289600.3291037.

[15] K. Reynolds, A. Kontostathis, and L. Edwards, ``Using machine learning to detect cybersecurity," in Proc. 10th Int. Conf. Mach. Learn. Appl. Workshops (ICMLA), vol. 2, Dec. 2011, pp. 241_244, doi: 10.1109/ICMLA.2011.152.

[16] S. Agrawal and A. Awekar, ``Deep learning for detecting cybersecurity across multiple social media platforms," in Advances in Infor- mation Retrieval (Lecture Notes in Computer Science), vol. 10772, G. Pasi, B. Piwowarski, L. Azzopardi, and A. Hanbury, Eds. Cham, Switzerland: Springer, 2018, pp. 141_153.

[17] R. I. Ra_q, H. Hosseinmardi, R. Han, Q. Lv, S. Mishra, and S. A. Mattson, ``Careful what you share in six seconds: Detecting cybersecurity instances in vine," in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM), Aug. 2015, pp. 617_622, doi: 10.1145/2808797.2809381.

[18] N. Yuvaraj, V. Chang, B. Gobinathan, A. Pinagapani, S. Kannan, G. Dhiman, and A. R. Rajan, ``Automatic detection of cybersecurity using multi-feature based arti_cial intelligence with deep decision tree classi- _cation," Comput. Electr. Eng., vol. 92, Jun. 2021, Art. no. 107186, doi: 10.1016/j.compeleceng.2021.107186.

[19] A. Al-Hassan and H. Al-Dossari, ``Detection of hate speech in Arabic tweets using deep learning," Multimedia Syst., Jan. 2021, doi: 10.1007/s00530-020-00742-w.

[20] Y. Fang, S. Yang, B. Zhao, and C. Huang, `` cybersecurity detection in social networks using bi-GRU with self-attention mechanism," Informa- tion, vol. 12, no. 4, p. 171, Apr. 2021, doi: 10.3390/info12040171.

[21] C. Iwendi, G. Srivastava, S. Khan, and P. K. R. Maddikunta, `` cybersecurity detection solutions based on deep learning architectures," Multimedia Syst., 2020, doi: 10.1007/s00530-020-00701-5.

[22] B. A. H. Murshed, H. D. E. Al-ariki, and S. Mallappa, ``Semantic analysis techniques using Twitter datasets on big data?: Comparative analysis study," Comput. Syst. Sci. Eng., vol. 35, no. 6, pp. 495_512, 2020, doi: 10.32604/csse.2020.35.495.

[23] P. Galán-García, J. G. De La Puerta, C. L. Gómez, I. Santos, and P. G. Bringas, ``Supervised machine learning for the detection of troll pro- _les in Twitter social network: Application to a real case of cybersecurity," Logic J. IGPL. vol. 24, no. 1, pp. 42_53, 2015, doi: 10.1093/jigpal/jzv048.

[24] Y. Zhang and A. Ramesh, ``Fine-grained analysis of cybersecurity using weakly-supervised topic models," in Proc. IEEE 5th Int. Conf. Data Sci. Adv. Anal. (DSAA), Oct. 2018, pp. 504_513, doi: 10.1109/DSAA.2018.00065.

[25] Z. Chen, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh, ``Leveraging multi-domain prior knowledge in topic models," in Proc. 23rd Int. Jt. Conf. Artif. Intell. Int. Jt. Conf. Artif. Intell. (IJCAI), vol. 13, 2013, pp. 2071_2077.