A Novel Approach - Detecting Nefarious Activity On Social Media Network Using Rnn Algorithm

[1]Santhoshi R, [2]Vinish A, M.E
[1]*M.Sc Data Science and Business Analysis,* [2]*Assistant Professor, Department of Computer Science*
Rathinam College of Arts and Science,Coimbatore

Abstract - This research aims to enhance the security of social media networking websites by employing Recurrent Neural Networks (RNNs) for detecting malicious activities. With the increasing complexity of digital platforms, identifying and mitigating potential threats has become more challenging. The proposed system prioritizes the utilization of RNNs to capture the temporal dependencies within user behavior sequences, offering a dynamic and adaptive approach to identifying suspicious patterns indicative of malicious intent. By leveraging advanced techniques in data preprocessing, sequence encoding, and real-time analysis, the developed model aims to provide an effective and scalable solution to the evolving landscape of cybersecurity threats in social media. User data undergoes encoding into numerical sequences before being fed into the RNN-based model, enabling it to seize the temporal dynamics of user behavior. Real-time monitoring capabilities allow the system to analyze ongoing activities, promptly detecting deviations from normal patterns and triggering alerts for potential malicious activities. Emphasizing the adaptability of the RNN algorithm, the project ensures continuous learning and evolution in response to emerging threats, contributing not only to improved cybersecurity measures on social media platforms but also offering valuable insights into the development of sophisticated, context-aware detection models for malicious activities.
Keywords:RNN, Posting Patterns, Cyberbullyin, Content Semantic, Predictive Modeling, Context-aware Analysis.

1 Introduction

The rapid expansion of social media networking websites has indisputably transformed communication and connectivity, fundamentally altering the digital landscape. Yet, this surge in online interactions has also spawned a mounting threat landscape, where malicious activities pose significant risks to users and the platforms' integrity. Addressing these challenges, this research centers on the pivotal task of identifying malicious activities on social media networks. Through the utilization of advanced technologies like Recurrent Neural Networks (RNNs), the study seeks to offer a resilient and adaptable solution for real-time detection and mitigation of potential security threats. Social media platforms have evolved into intricate ecosystems where users engage in diverse activities, from content sharing to peer interaction. However, the sheer volume and complexity of daily user behavior data render traditional security measures inadequate in tackling the nuanced nature of contemporary cyber threats. Harnessing the capabilities of RNNs provides a promising avenue to unravel these complexities. RNNs, adept at capturing temporal dependencies in sequential data, present an opportunity to effectively model the dynamic nature of user interactions on social media. The prevalence of various malicious activities, spanning spam, fake accounts, phishing, and coordinated attacks, underscores the need for a proactive and adaptive security approach. While traditional rule-based and signature-based methods struggle to keep pace with evolving tactics, RNNs excel in learning and identifying patterns within sequences, making them well-suited for detecting subtle, context-dependent anomalies indicative of nefarious behavior. This research explores how leveraging the inherent temporal dependencies in user behavior sequences can establish a robust framework for detecting malicious activities.

This project aligns with the broader imperative of securing online spaces, not only to safeguard individual users but also to preserve the trust and integrity of social media platforms. As these platforms evolve, so do the tactics of malicious actors, demanding an intelligent and adaptive defense mechanism. RNNs, with their capacity to learn from historical user behavior data and adapt to emerging patterns, offer a solution transcending traditional methods. The overarching goal is to enhance the safety and resilience of social media networking websites, cultivating an environment where users can engage freely without the looming threat of malicious activities. In subsequent sections, we delve into the specifics of our research methodology, elucidating the steps encompassing data collection, preprocessing, and the design and implementation of the RNN-based detection model. The study accentuates real-time monitoring capabilities, adaptability to evolving threats, and the integration of educational initiatives to empower users. Through this research, we strive to contribute to the development of sophisticated and context-aware systems for detecting malicious activities on social media platforms, ultimately fostering a safer and more secure online experience for users.

2 Literature Survey

2.1 Online offensive behaviour in social media: Detection approaches, comprehensive review and future directions

The literature survey on online offensive behavior in social media presents a thorough examination of detection approaches, providing a comprehensive review of current methodologies and insights into future directions. The study encompasses a broad spectrum of offensive behaviors, including cyberbullying, hate speech, harassment, and misinformation. Detection approaches discussed range from rule-based methods to machine learning models, with an emphasis on context-aware strategies that consider user relationships, historical interactions, and platform-specific norms. Machine learning techniques, particularly natural language processing and deep learning, are explored for their efficacy in identifying offensive language and sentiment. The survey underscores the challenges associated with the dynamic nature of online language, cultural variations, and ethical considerations in content moderation. It also acknowledges the need for user-centric approaches, emphasizing the psychological impact on individuals affected by offensive content. Future directions highlighted include the exploration of explainable AI, improved cross-cultural models, and collaborative efforts between academia, industry, and social media platforms. The study recognizes privacy concerns and calls for a delicate balance between effective detection and respecting user privacy. Overall, the literature survey contributes valuable insights to guide further research, policy development, and industry practices aimed at addressing the complex issue of online offensive behavior.

2.2 Malicious URL Detection Based on Improved Multilayer Recurrent Convolutional Neural Network Model

This research addresses the critical challenge of malicious URL detection through the development of an innovative model based on an Improved Multilayer Recurrent Convolutional Neural Network (IML-RCNN). The escalating sophistication of cyber threats, particularly in the form of malicious URLs, poses a severe risk to users' cybersecurity. In response, this study explores an advanced neural network architecture that amalgamates the strengths of both recurrent and convolutional layers, enabling the model to effectively capture intricate patterns and temporal dependencies within URL sequences. The IML-RCNN model is designed to enhance the accuracy and efficiency of malicious URL detection, contributing to the ongoing efforts to fortify the cybersecurity landscape. Through meticulous preprocessing and feature extraction, the URL sequences are encoded and fed into the IML-RCNN model for training and evaluation. The model's effectiveness is assessed through rigorous testing, comparison with existing detection methods, and consideration of key performance metrics. By introducing an Improved Multilayer Recurrent Convolutional Neural Network for malicious URL detection, this research aims to provide a robust solution capable of adapting to the evolving tactics employed by cyber adversaries, thereby enhancing the overall resilience of cybersecurity measures.

2.3 Machine Learning Boosting Algorithms to Detect the Fake User Profiles on Instagram

In recent years, the proliferation of social media platforms like Instagram has given rise to a significant challenge in the form of fake user profiles, commonly employed for various malicious activities such as spreading misinformation, engaging in fraudulent activities, or manipulating online discourse. Detecting and mitigating the impact of these fake profiles has become a critical area of research, with machine learning (ML) techniques proving to be valuable tools in addressing this issue. One prominent set of ML algorithms that has shown promise in the context of fake user profile detection is boosting algorithms. Boosting algorithms, such as AdaBoost and Gradient Boosting, work by combining the predictive power of multiple weak learners to create a robust and accurate model. In the literature survey focused on Instagram fake profile detection, researchers have explored the application of boosting algorithms to effectively distinguish between genuine and fake profiles based on various features, including user behavior, content patterns, and network interactions.A comprehensive review of the literature reveals that boosting algorithms offer several advantages in the realm of Instagram fake user profile detection. These algorithms exhibit a strong ability to handle imbalanced datasets, a common characteristic in social media contexts where genuine profiles far outnumber fake ones. Furthermore, boosting algorithms are known for their adaptability to diverse feature sets and their ability to capture complex relationships within the data. Researchers have explored feature engineering techniques to extract relevant information from user profiles, posts, and network interactions, enhancing the performance of boosting models. The literature survey highlights the effectiveness of boosting algorithms in achieving high accuracy, precision, and recall rates, thereby contributing significantly to the ongoing efforts in developing robust solutions for detecting fake user profiles on Instagram and other social media platforms.

3 Existing System

Current systems for detecting malicious activities on social media networks often rely on a blend of rule-based heuristics, pattern recognition, and machine learning algorithms. Traditional methods, such as rule-based systems, utilize predefined rules to flag potential malicious activities like spam, phishing, or fake accounts. While somewhat effective, these approaches struggle to keep pace with the ever-changing tactics seen on social media platforms (Bouarara, H. A., 2021). Consequently, there's a growing demand for more sophisticated solutions capable of adapting to the continually shifting online threat landscape. Machine learning algorithms, notably Recurrent Neural Networks (RNNs), have gained prominence due to their ability to analyze sequential data and capture temporal dependencies in user behavior. Within existing systems, RNNs are utilized to model the sequential nature of social media interactions, aiding in the identification of anomalous patterns indicative of malicious activities. However, challenges persist regarding model interpretability, scalability, and the necessity for ongoing learning to effectively combat emerging threats. Current systems often struggle with large-scale datasets and real-time monitoring, prompting the exploration of advanced architectures and approaches to bolster the accuracy and responsiveness of malicious activity detection.
Integrating these attributes with RNNs enhances the contextual comprehension of user behavior, enabling the differentiation between normal and potentially harmful activities. Despite progress, there's still room for improvement in balancing false positives and false negatives, safeguarding user privacy, and effectively communicating the rationale behind identified threats to users. Continuous research and development in this domain strive to construct more resilient and adaptive systems for mitigating malicious activities on social media networks.

4 Proposed System

The proposed system involves comprehensive data preprocessing, sequence encoding, and the deployment of an RNN-based model to analyze user actions in real-time. By capturing intricate patterns and contextual nuances associated with both benign and malicious behaviors, the developed system aims to provide an advanced and adaptive solution for enhancing security measures on social media platforms Naik, D. B., Sri, S. N., Priya, G. M., & Priya, P. S. (2023, September). The integration of RNN algorithms offers a promising approach to addressing the evolving nature of online threats and contributes to the broader objective of fostering a safer and more secure online environment for users. In contrast to traditional systems, our approach focuses on the inherent temporal dependencies in user behavior sequences, acknowledging the dynamic nature of online interactions. The system integrates advanced machine learning techniques, utilizing RNNs to analyze patterns and anomalies in user actions, which can be indicative of various malicious activities, including but not limited to spam, phishing, and coordinated attacks. RNNs inherently capture temporal aspects, allowing the model to evolve and learn from emerging threats over time Jafari Sadr, M., Mirtaheri, S. L., Greco, S., & Borna, K. (2023). The system will be designed to dynamically update its understanding of normal and malicious behavior based on real-time data, ensuring it remains effective in identifying novel and sophisticated threats. This adaptability is crucial for staying ahead of malicious actors who constantly modify their tactics to evade detection. To address concerns related to data privacy on social media platforms, the model will be designed with privacy-preserving measures, ensuring that user data is handled responsibly. Additionally, a transparent reporting mechanism will be integrated, providing users with insights into the detected threats and empowering them with information on how to protect themselves. By combining advanced machine learning techniques with a user-centric approach, the proposed system aims to provide a robust, privacy-respecting, and transparent solution for malicious activity detection on social media networking websites.

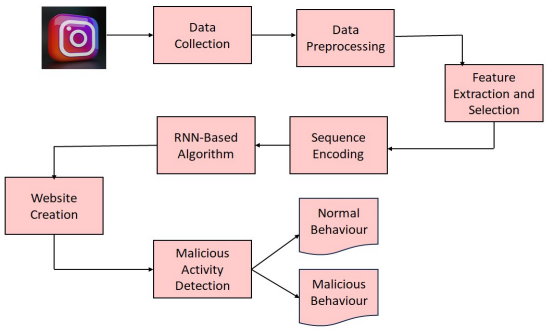

Fig.No.4.1 System Design

5 Modules Specification

5.1 Data Collection Module:

Gather comprehensive user activity data from the social media platform. API Integration is Connect to the social media platform's API to collect data. Web Scraping is Employ scraping techniques for collecting additional information. Timestamps and Metadata is Capture timestamps and relevant metadata for temporal analysis Cao, C., & Caverlee, J. (2015). The model specification involves a systematic approach to gather diverse and representative data. This includes designing a web scraping mechanism to extract relevant information from social media platforms, capturing textual content, user interactions, and temporal patterns. The collected data should encompass a variety of user behaviors and potential malicious activities. Special attention is given to the temporal aspect to capture evolving patterns over time. Additionally, features such as user engagement metrics, post content, and network relationships are curated for comprehensive representation. The dataset is preprocessed to handle noise, imbalances, and ensure compatibility with RNN architecture. The model specification also involves defining input sequences, configuring the RNN layers, and fine-tuning hyperparameters to optimize the network for detecting malicious activities. The goal is to create a robust data collection pipeline that facilitates the training and evaluation of the RNN model for accurate detection of malicious behavior on social media platforms.

5.2 Data Preprocessing Module:

Prepare collected data for analysis by handling noise and ensuring data consistency.Missing Value Handling is Address missing values in the dataset.Noise Removal is Identify and filter out irrelevant or erroneous data.Data Normalization is Normalize numerical data for consistent scaling.Sequence Organization is Arrange user activities into chronological sequences. The focus is on transforming raw data into a format suitable for input into the RNN model. Initially, text data is cleaned and tokenized, removing irrelevant characters, stopwords, and performing stemming or lemmatization to standardize the text. User interactions, timestamps, and other relevant features are normalized to ensure consistency and enhance the model's ability to generalize Mumu, M. H., & Aishy, T. (2023). Handling imbalances in the dataset, including oversampling or undersampling, is a crucial step to prevent biased learning. Additionally, temporal sequences are structured to create input sequences for the RNN, allowing the model to capture dynamic patterns over time. To address the variable length of text sequences, padding or truncation is applied. Finally, the preprocessed data is split into training, validation, and testing sets to facilitate effective model training and evaluation. The Data Preprocessing Module plays a pivotal role in preparing the input data, ensuring that the RNN model can effectively learn and identify malicious activities on social media networking websites.

5.3 Sequence Encoding Module:

Encode sequential user activities into numerical representations for the RNN model.One-Hot Encoding is Convert categorical variables into binary vectors.Embedding Layers is Utilize embedding layers to represent categorical features.Temporal Encoding is Incorporate timestamps to capture temporal dynamics. The primary objective is to convert the preprocessed data into a numerical representation that can be effectively processed by the RNN. Textual content is encoded using techniques such as word embedding or one-hot encoding to convert words into numerical vectors, capturing semantic relationships between them. User interactions, timestamps, and other temporal features are encoded to ensure the model grasps the sequential nature of social media activities. The resulting numerical sequences are then fed into the RNN architecture, where the network can leverage its memory cells to analyze and understand patterns in the sequential data. The choice of encoding methods and the design of input representations play a critical role in enhancing the model's ability to detect malicious activities by preserving contextual information and temporal dependencies within the social media data Harris, P., Gojal, J., Chitra, R., & Anitha, S. (2021). The Sequence Encoding Module is essential for bridging the semantic and sequential aspects of the input data to empower the RNN in effectively identifying patterns indicative of malicious behavior.

5.4 Feature Extraction Module:

Extract relevant features to enhance the model's ability to identify malicious activities.Posting Frequency is Extract user posting frequency.Content Analysis is Analyze post and comment content for suspicious patterns.Engagement Metrics is Consider metrics like likes and shares. The focus lies on extracting meaningful patterns and representations from the preprocessed data to enhance the model's ability to discern malicious activities Sheikhi Saeid. (2020). This module involves the identification and extraction of relevant features such as user behavior metrics, post content characteristics, and network interactions. Techniques like TF-IDF (Term Frequency-Inverse Document Frequency) or word embeddings may be employed to capture the

semantic meaning of text, while user engagement metrics and temporal patterns are derived to provide valuable context. The extracted features are then structured into a format suitable for input into the RNN, ensuring that the model can effectively leverage this information to identify patterns indicative of malicious behavior on social media platforms. The Feature Extraction Module is pivotal in empowering the RNN algorithm with discriminative information, enabling it to make accurate predictions by capturing the nuanced characteristics associated with malicious activities.

5.5 RNN-Based Algorithm:

Develop and implement the RNN algorithm for malicious activity detection. Model Architecture is Design the RNN structure with layers such as LSTM or GRU.Training is Train the model on labeled datasets emphasizing various malicious activities.

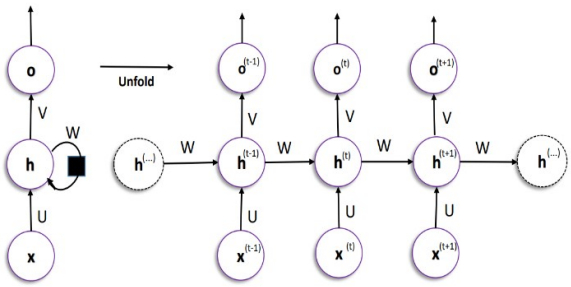

Fig.No.5.5.1 RNN Algorithm

The left side of the diagram illustrates the representation of an RNN using notation, while the right side demonstrates the process of unrolling (or unfolding) the RNN into a comprehensive network. Unrolling involves expanding the network to cover the entire sequence. For instance, if the sequence comprises three words, the network would be unfolded into a three-layer neural network, with each layer corresponding to a word in the sequence.

Input: x(t) is taken as the input to the network at time step t. For example, x1, could be a one-hot vector corresponding to a word of a sentence.

Hidden state: h(t) represents a hidden state at time t and acts as “memory” of the network. h(t) is calculated based on the current input and the previous time step’s hidden state: The function f is taken to be a non-linear transformation such as tanh, ReLU.

Weights: The RNN has input to hidden connections parameterized by a weight matrix U, hidden-to-hidden recurrent connections parameterized by a weight matrix W, and hidden-to-output connections parameterized by a weight matrix V and all these weights (U,V,W) are shared across time.

Output: o(t) illustrates the output of the network. In the figure I just put an arrow after o(t) which is also often subjected to non-linearity, especially when the network contains further layers downstream.

Hyper parameter Tuning is Fine-tune parameters for optimal performance. Real-time Adaptation is Implement mechanisms for the model to adapt to emerging threats. The RNN is designed to process sequential data, making it well-suited for capturing the temporal dependencies inherent in social media activities. The input layer of the RNN is fed with encoded sequences representing preprocessed data, encompassing user interactions, post content, and temporal patterns Saraswathi, K., Mohanraj, V., Suresh, Y., & Senthilkumar, J. (2023). Stacked recurrent layers with memory cells enable the model to retain information over time, while additional fully connected layers contribute to the extraction of high-level features. The output layer produces binary classification results, distinguishing between normal and malicious activities. Parameters such as learning rates, dropout rates, and the number of hidden units are fine-tuned during the training process to optimize the model's performance. The RNN-Based Algorithm is crafted to effectively leverage the sequential nature of social media data, making it proficient in detecting and mitigating malicious activities on these platforms.

5.6 Feature Selection Module:

Identify and retain the most informative features to optimize model performance.Correlation Analysis is Assess and eliminate redundant features.Information Gain is Evaluate the information gain of each

feature.Recursive Feature Elimination is Iteratively eliminate less significant features. The emphasis is on identifying and retaining the most relevant features to enhance the model's efficiency and performance. This module involves a strategic process of evaluating the importance of various input features and selecting a subset that contributes significantly to the detection of malicious activities Seo, S., Kim, Y., & Lee, C. (2018). Techniques such as recursive feature elimination or information gain analysis may be employed to assess the impact of each feature on the model's predictive accuracy. The selected features, which could include user behavior metrics, content characteristics, and temporal patterns, are then used as inputs for the RNN algorithm. This careful selection not only helps reduce computational complexity but also improves the model's interpretability and generalization to different scenarios. The Feature Selection Module plays a crucial role in optimizing the model's efficacy by focusing on the most informative aspects of social media data for accurate and efficient detection of malicious activities.

5.7 Malicious Activity Detection Module:

Deploy the trained model for real-time detection of malicious activities on the social media platform. Real-time Monitoring is Continuously monitor user activities.Threshold Setting is Define thresholds for classification. The model specification involves leveraging the capabilities of the Recurrent Neural Network (RNN) to effectively classify and detect harmful behaviors. The RNN is trained on carefully preprocessed and encoded data, encompassing user interactions, post content, and temporal patterns Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., & Razak, S. A. (2017). The model utilizes sequential information processing to capture the dynamic nature of social media activities, allowing it to discern patterns indicative of malicious behavior. The input features, selected through a feature selection process, are fed into the RNN, which consists of stacked recurrent layers with memory cells for contextual understanding and additional fully connected layers for feature extraction. The model is trained using labeled data, enabling it to learn and generalize patterns associated with both normal and malicious activities. The Malicious Activity Detection Module aims to provide an efficient and accurate means of identifying threats on social media platforms, contributing to the overall security and integrity of online communities.

5.8 Privacy and Ethics Module:

Ensure user privacy and ethical data handling throughout the system.Anonymization is Implement techniques to anonymize user data.Compliance is Adhere to data protection regulations and ethical standards.Transparency is Communicate clearly on data usage and system functionality. The model specification places a strong emphasis on safeguarding user privacy and adhering to ethical considerations. This module involves implementing measures to ensure that the detection algorithm operates within the boundaries of privacy regulations and guidelines Chinivar, S., Roopa, M. S., Arunalatha, J. S., & Venugopal, K. R. (2023). Privacy-preserving techniques, such as anonymization and encryption, are employed during data collection and preprocessing to mitigate the risk of unauthorized access or misuse. Ethical considerations encompass transparency in model deployment, providing clear information to users about the purpose and nature of malicious activity detection. Additionally, mechanisms for user consent and opt-out options are integrated into the model to respect individual privacy preferences. The Privacy and Ethics Module aims to strike a balance between effective malicious activity detection and preserving the rights and privacy of social media users, fostering a responsible and ethical approach to algorithmic deployment in online platforms.

6 Conclusion

In conclusion, the implementation of a Malicious Activity Detection system on social media networking websites using the Recurrent Neural Network (RNN) algorithm represents a significant stride towards fortifying online security. The utilization of RNNs, with their innate ability to model temporal dependencies in user behavior sequences, contributes to a more nuanced and adaptive approach to identifying malicious activities. This system holds the promise of effectively distinguishing subtle anomalies indicative of threats such as spam, phishing, and coordinated attacks. The integration of real-time monitoring, continuous learning mechanisms, and user-friendly interfaces enhances the system's responsiveness and user engagement. As social media platforms continue to evolve, the adoption of advanced technologies like RNNs becomes imperative in addressing the dynamic nature of online threats. This endeavor not only augments the resilience of these platforms but also underscores the commitment to fostering a safer and more secure online environment for users. Moving forward, ongoing research and development will be essential to refine and advance these detection systems in tandem with emerging cyber threats and evolving user behaviors.

7 Result

RNN-based malicious activity detection on Instagram has the potential to create a safer and more positive user experience. By proactively flagging harmful content like hate speech, cyberbullying or misleading

information, such systems can help mitigate the negative impacts of such activities on users wellbeing and mental health. This could foster a more inclusive and respectful online environment for everyone. Balancing the need for content moderation with upholding freedom of speech further complicates the ethical landscape. By reducing the prevalence of harmful content, such system can help promote positive social interactions and foster a healthier online platform. By training on massive datasets labeled for malicious content, RNNs can learn to identify patterns in text, user behavior, and post metadata. This allows them to analyze new content and assign probability scores indicating the likelihood of malicious activity. This approach can potentially improve detection accuracy, reduce false positives, and enable faster intervention. This approach offers promise for a safer online environment but challenges remain. The model's accuracy hinges on unbiased training data, and malicious actors can adapt their tactics. Ethical considerations regarding privacy, transparency, and free speech require careful navigation.

REFERENCES

[1] Jafari Sadr, M., Mirtaheri, S. L., Greco, S., & Borna, K. (2023). Popular Tag Recommendation by Neural Network in Social Media. Computational Intelligence and Neuroscience, 2023.

[2] Bouarara, H. A. (2021). Recurrent neural network (RNN) to analyse mental behaviour in social media. International Journal of Software Science and Computational Intelligence (IJSSCI), 13(3), 1-11.

[3] C., & Caverlee, J. (2015). Detecting spam urls in social media via behavioral analysis. In Advances in Information Retrieval: 37th European Conference on IR Research, ECIR 2015, Vienna, Austria, March 29-April 2, 2015. Proceedings 37 (pp. 703-714). Springer International Publishing.

[4] X. Wang, Y. Zhang, and T. Yamasaki, "Earn more social attention: user popularity based tag recommendation system," in Proceedings of the Companion Proceedings of the Web Conference 2020, New York, NY, USA, April 2020.

[5] Xue, Z., Li, Q., & Zeng, X. (2023). Social media user behavior analysis applied to the fashion and apparel industry in the big data era. Journal of Retailing and Consumer Services, 72, 103299.

[6] K., Mohanraj, V., Suresh, Y., & Senthilkumar, J. (2023). Deep Learning Enabled Social Media Recommendation Based on User Comments. Computer Systems Science & Engineering, 44(2).

[7] D. Yang, B. Qu and P. Cudré-Mauroux, "Privacy-preserving social media data publishing for personalized ranking-based recommendation," IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 3, pp. 507–520, 2019.

[8] W. Sun, G. Z. Dai, X. R. Zhang, X. Z. He and X. Chen, "TBE-Net: A three-branch embedding network with partaware ability and feature complementary learning for vehicle re-identification," IEEE Transactions on Intelligent Transportation Systems, pp. 1–13, 2021.

[9] Chinivar, S., Roopa, M. S., Arunalatha, J. S., & Venugopal, K. R. (2023). Online offensive behaviour in socialmedia: Detection approaches, comprehensive review and future directions. Entertainment Computing, 45, 100544.

[10] Seo, S., Kim, Y., & Lee, C. (2018). Instagram users behavior analysis in a digital forensic perspective. Journal of the Korea Institute of Information Security & Cryptology, 28(2), 407-416.

[11] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[12] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011

[13] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[14] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012

[15] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[16] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[17] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[18] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[19] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[20] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[21] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[22] P. Harris, J. Gojal, R. Chitra and S. Anitha, "Fake Instagram Profile Identification and Classification using Machine Learning", 2021 2nd Global Conference for Advancement in Technology (GCAT), pp. 1-5, 2021.

[23] Sheikhi Saeid, "An Efficient Method for Detection of Fake Accounts on the Instagram Platform", Revue d intelligence artificielle, vol. 34, pp. 429-436, 2020.

[24] Krutika Palav, Pranali Awari and Siddhi Jiman, "Instagram Fake Account Detection", International Research Journal of Modernization in Engineering Technology and Science, vol. 3, no. 5, pp. 455-460, 2021.

[25] Naik, D. B., Sri, S. N., Priya, G. M., & Priya, P. S. (2023, September). Machine Learning Boosting Algorithms to Detect the Fake User Profiles on Instagram. In 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS) (pp. 1-7). IEEE.

[26] M. Egele, G. Stringhini, C. Kruegel and G. Vigna, "Towards detecting compromised accounts on social networks", IEEE Trans. Dependable Secure Comput., vol. 14, no. 4, pp. 447-460, Jul./Aug. 2017.

[27] K. Chakraborty, S. Bhattacharyya and R. Bag, "A survey of sentiment analysis from social media data", IEEE Trans. Comput. Social Syst., vol. 7, no. 2, pp. 450-464, Apr. 2020.
[28] T. Ji, C. Luo, Y. Guo, Q. Wang, L. Yu and P. Li, "Community detection in online social networks: A differentially private and parsimonious approach", IEEE Trans. Comput. Social Syst., vol. 7, no. 1, pp. 151-163, Feb. 2020.
[29] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan and S. A. Razak, "Malicious accounts: Dark of the social networks", J. Netw. Comput. Appl., vol. 79, pp. 41-67, 2017.
[30] Mullah, N. S., & Zainon, W. M. N. W. (2021). Advances in machine learning algorithms for hate speech detection in social media: a review. IEEE Access, 9, 88364-88376.
[31] Mumu, M. H., & Aishy, T. (2023). Malicious URL Detection Using Machine Learning and Deep Learning Algorithms (Doctoral dissertation, East West University).