Individual Report

Member name: Gautham Vijayaraj
Project Title: Detection Process of Suspicious Activities on Social Media Using Data Mining and Machine Learning
Date: 11/18/2023

Overview:
This project analyzes data mining and machine learning techniques applied for identifying suspicious activities on various social media platforms, with a focus on mitigating risks such as spams, fake profiles, criminal activities like extortion, and terrorism. The analysis spans text, images, and videos on platforms like Twitter, Facebook, and Instagram. There are many risks with social media and security, such as hacking, fake bots, account cloning, and more. The need to solve important problems quickly in data security, data mining, different social media platforms, and machine learning is what drove this project.

This research explores secure data collection and privacy preservation techniques, including distortion, encryption, and anonymity. It employs secure multiparty computation for limited data access, focusing on tweet polarity values. Privacy-preserving data mining techniques, such as outlier detection with visual explanation, user risk score assignment, and the 3LP+ approach, are discussed for safeguarding individual privacy.

During data pre-processing, diverse Natural Language Processing (NLP) techniques, including tokenization, stemming, stop word removal, translation, and vectorization, are employed to handle the complexities of social media data. The project also explores advanced feature extraction methods, such as TFIDF, Word2Vec, lexicon-based, and bi-functionality embeddings.

Various data mining techniques are explored, encompassing similarity metrics, comparative analysis of word embedding models and classifiers, sentiment analysis, emotional and domain-specific lexicons, and TFIDF embedding, with the goal of improving the detection of suspicious activities.

The project implements and assesses multiple machine learning algorithms, including deep neural networks like CNN, LSTM, and BiLSTM, as well as traditional models like Random Forest, Support Vector Machines, Naive Bayes, k-Nearest Neighbor, Decision Trees, and Logistic Regression. These models demonstrate effective threat detection with high precision, recall, and F1-scores in most studies.

In the domain of robust model evaluation, collective papers focus on advancing online security and trust. They introduce inventive methods to cultivate trust in social networks, enhancing content filtering and prioritization.

Additionally, the project suggests adaptive learning methods such as online and transfer learning for dynamic adaptation to new or sophisticated suspicious activities. They delve into the Decision Tree model's superior accuracy and training time for intrusion detection and advocate for the SPC model's effectiveness in cloud computing security. The research underscores the importance of algorithms and models to combat suspicious activities in social networks, proposing a deep learning-based approach for enhanced anomaly detection in multimedia applications.

Contributions:

I played a crucial role in various facets of our project, making substantial contributions to its success. To begin, I held the position of Deputy Leader of this project. I consistently assessed and approved our weekly reports, ensuring they adhered to our quality standards. Furthermore, I was responsible for creating and maintaining the GANTT chart on three occasions. Concurrently, I collaborated with the group leader in task assignment among group members and diligently followed up on tasks to optimize efficiency.

I wrote seven in-depth reports summarizing insights from seven reference papers and conducted extensive research on privacy-preserving data mining techniques, with a specific focus on methodologies tailored for social media datasets. This research significantly enriched our project's data processing strategy. All of my in-depth reports can be accessed from the following:

Gautham_Vijayaraj_Individual_In-depth_Report_1

Gautham_Vijayaraj_Individual_In-depth_Report_2

Gautham_Vijayaraj_Individual_In-depth_Report_3

Gautham_Vijayaraj_Individual_In-depth_Report_4

Gautham_Vijayaraj_Individual_In-depth_Report_5

Gautham_Vijayaraj_Individual_In-depth_Report_6

Gautham_Vijayaraj_Individual_In-depth_Report_7

In addition, I took charge of maintaining the quality of our project deliverables, involving the thorough evaluation and approval of in-depth and progress reports for four team members: Krupaben Kothadia, Sangeeth Santhosh, Rahul Nayak and Yeshwanth Reddy Chennur, encompassing crucial documents such as the Final Report, Presentation, Midterm Report, GANTT chart, and Weekly Reports. My meticulous attention to detail and dedication to quality control played a pivotal role in ensuring that our work consistently met the highest standards.

I visited the writing center to get my in-depth reports to verify and got it approved by them. The confirmation for my visit can be found at Gautham_Writing_Center_Confirmation.png. Furthermore, I addressed deficiencies during the presentation along with my fellow team members.

I actively contributed to our research by identifying and approving reference papers, establishing a strong foundation for our project in research and literature. Maintaining a proactive approach, I promptly addressed challenges and supported teammates as needed.

In addition to these responsibilities, the group leader and I regularly organized weekly meetings. Actively participating in discussions, I provided valuable insights to our decision-making processes. Offering guidance and support to fellow team members, I helped them overcome challenges and improve contributions. My commitment and dedication played a vital role in ensuring the effective completion of project tasks and the cohesive operation of our team.

Lessons Learned:

Conclusions summarized from the seven research papers I studied were:

Paper [1]: This paper provides a comprehensive overview of privacy-preserving data mining, outlining the various methods and techniques used to protect sensitive information while allowing for valuable data analysis.

Paper [2]: The existing PPDM techniques are intensively reviewed and classified based upon their methods that used data modification approaches. The study addresses data provider concerns and explores methods like data modification, cryptographic techniques, and anonymization to ensure privacy throughout the data lifecycle.

Paper [3]: Results from this paper include an in-depth explanation of methods used in machine learning for classifying suspicious content, which are helpful and relevant to the goal of this project. It also provides an analysis between the randomization and secure multiparty computation (SMC) with results.

Paper [4]: The analysis is conducted on a Facebook dataset to assign risk scores to users, with the notion that greater behavioral divergence implies higher risk. Three data mining approaches are outlined: supervised, semi-supervised, and unsupervised methods. The paper also highlights the increasing threat of cyberattacks on social networking sites, such as Sybil attacks and malware propagation.

Paper [5]: This paper explores sentiment analysis of Indian political tweets using data mining classifiers. Rigorous experimentation and data mining techniques establish the k-nearest neighbor classifier's reliable high predictive accuracy of 99.6456% from the analyzed 2,102,52 tweets.

Paper [6]: This paper discusses the 3LP+ privacy-preserving technique for safeguarding multiple sensitive attributes in online social networks (OSNs). Results indicate that 3LP+ can provide better privacy while maintaining higher utility than an existing privacy preserving technique even if an attacker uses a different set of classifiers.

Paper [7]: This research presents a groundbreaking method for extracting and analyzing healthcare-related information from social media, with a particular emphasis on cancer treatments. Data collecting, text processing, behavior analysis, and symptom-medication identification are important elements. This strategy could be used for detecting suspicious behavior in social media too.

Lessons learned from the overall project on identifying suspicious activities on social media using data mining and machine learning include: understanding the diverse threats such as social spam, fake accounts, criminal content, and extremist postings, informing the development of robust detection systems.

Preserving user privacy through encryption, data anonymization, and privacy-preserving techniques is crucial. Employing advanced privacy-preserving data mining methods like k-anonymity is recommended. Sophisticated natural language processing and feature engineering are vital for handling diverse, unstructured social media data.

Customizing machine learning models, exploring transfer learning, and employing adaptive learning methods are necessary for accurate threat classification. Thorough evaluation using real-world datasets, focusing on suspended accounts, is essential, covering metrics like accuracy, precision, recall, F1 score, and ROC AUC.

Collaboration with social media platforms enhances threat intelligence and supports impactful policy changes. In summary, the key takeaways involve deepening threat knowledge, ethical data practices, algorithm customization, adaptive learning, rigorous evaluation, and fostering collaborations, contributing to advancements in this critical intersection of technology and society.

References:

[1] Xinjun Qi, Mingkui Zong, “An Overview of Privacy Preserving Data Mining,” in “International Conference on Environmental Science and Engineering (ICESE)”, Harbin, China, 2011, pp.1341-1347

[2] Mohammed Binjubeir, Abdulghani Ali Ahmed, Mohd Arfian Bin Ismail, Ali Safaa Sadiq, Muhammad Khurram Khan, “Comprehensive Survey on Big Data Privacy Protection,” in “IEEE Access, Vol 12”, Riyadh, Saudi Arabia, 2019, pp.20067-20079

[3] J. Vaidya, C. Clifton, “Privacy-preserving data mining: why, how, and when”, in “IEEE Security & Privacy, Vol 2, Issue 6”, USA, 2004, pp.19-27

[4] M. S. Sudha, K. A. Priya, A. K. Lakshmi, A. Kruthika, D. L. Priya and K. Valarmathi, "Data Mining Approach for Anomaly Detection in Social Network Analysis," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1862-1866, doi: 10.1109/ICICCT.2018.8472985.

[5] Anurag P. Jain, Vijay D. Katkar, “Sentiments analysis of Twitter data using data mining,” in “International Conference on Information Processing (ICIP)”, Pune, India, 2015, pp.807-810

[6] Khondker Jahid Reza, Md Zahidul Islam and Vladimir Estivill-Castro,”Privacy Preservation of Social Network Users Against Attribute Inference Attacks via Malicious Data Mining”, in Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), Barcelona, Spain, pp. 412-420, doi: 10.5220/0007390404120420

[7] Sopan Ganpat Sutar, "Intelligent data mining technique of social media for improving health care," in International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1356-1360, June 2017, doi: 10.1109/ICCONS.2017.8250690.