Literature Review

2.1. Sentiment Analysis

2.1.1. Introduction

Sentiment Analysis is an evolving field within natural language processing. It has generated significant attention due to the surge in opinionated texts in the digital age. Often referred to as 'opinion mining', it plays a vital role in influencing decision-making across various sectors. The primary objective is to identify the emotional tone or polarity of a text, categorizing it as positive, negative, or neutral. Over time, methodologies have varied from machine-learning-based approaches to vocabulary-based methods. For instance, machine learning techniques utilize labelled data for training classifiers, whereas vocabulary-based methods, though not dependent on labelled data, face challenges in adapting to different contexts, especially when interpreting slang or concise messages (Gonçalves et al., 2013).

2.1.2. Sentiment Analysis Methods

The field of Sentiment Analysis has seen the development of diverse methods to identify and categorize sentiments . Early techniques involved the use of emoticons, correlating specific emoticons with sentiments (Mejova, 2009). Vocabulary-based methods, such as LIWC (Linguistic Inquiry and Word Count) and SentiWordNet, employ predefined dictionaries for classification. In contrast, machine learning techniques leverage algorithms like Naïve Bayes and Support Vector Machine to detect patterns (Mejova, 2009). Each method presents its own set of advantages and challenges, which will be explored further in this review.

2.1.3. Sentiment Analysis Levels

Understanding the levels of sentiment analysis is crucial. The Word Level, focusing on individual words, is foundational for creating sentiment dictionaries (Gonçalves et al., 2013). The Sentence Level examines entire sentences, useful in contexts with mixed sentiments. The Document Level assesses the overall sentiment of a document. Document Level sentiment analysis is also ideal for singular-topic reviews (Gonçalves et al., 2013). Lastly, Feature Level sentiment analysis looks into specific features of a topic or product. Based on the desired task, these levels individually produce pleasing results. However, combining these levels can yield more detailed sentiment results (Gonçalves et al., 2013).

2.1.4. Challenges in Sentiment Analysis

Despite its potential, sentiment analysis faces a few challenges. Polarity shift, where a sentence's sentiment can be misidentified due to specific words, is a primary concern (Kumar and Sebastian, 2012). Another limitation is the binary classification approach, which may oversimplify the vast diversity of human emotions. Additionally, terminological ambiguities, such as the interchangeable use of "opinion mining" and "sentiment analysis," can lead to confusion (Kumar and Sebastian, 2012). The diverse nature of user-generated content and open subjectivity of sentiments further complicate the analysis (Kumar and Sebastian, 2012).

2.1.5. Gaps and Observations

While scholars like Mejova (2009) and Gonçalves et al. (2013) have provided comprehensive overviews, gaps persist. Notably, advancements in deep learning techniques for sentiment analysis, such as RNNs and transformers, are underrepresented (Mejova, 2009). Additionally, sentiment analysis in non-English languages remains largely unexplored. A deeper exploration into method evaluation and benchmarking would offer clearer insights into their effectiveness (Gonçalves et al., 2013).

2.1.6. Conclusion

Sentiment analysis remains a cornerstone in natural language processing. Its significance is highlighted by various scholars, each highlighting its unique factors. As the digital age progresses, the insights from sentiment analysis will undoubtedly remain important for both researchers and practitioners.

2.2. Threat Detection

2.2.1. Introduction

In the rapidly evolving field of cybersecurity, insider threats have emerged as a primary concern. The digital age, while presenting numerous advantages, also unveils significant security vulnerabilities. Notably, these vulnerabilities stem not just from external adversaries but increasingly from within organizations. Al-Mhiqani et al. (2020) highlighted the impact of insider threats on an organization's reputation, financial health, and intellectual assets. The gravity of the situation is further emphasized by the statistics presented: a significant 53% of threats in 2018 were internal, a number that has risen alarmingly since then.

2.2.2. Classification of Insider Threats

As the concern over insider threats increases, researchers have looked into their classification. Al-Mhiqani et al. (2020) made a significant contribution by proposing a comprehensive two-fold classification system. The first category focuses on the insiders themselves, examining their access, types, motivations, profiling, and methodologies. The second category looks into the technological dimension, examining behaviors, techniques, datasets, detection methodologies, and evaluation matrices associated with insider threats.

2.2.3. Techniques for Insider Threat Detection

Transitioning from classification, it's crucial to address the techniques employed for insider threat detection. Traditional methods, such as rule-based systems, have shown limitations, especially against sophisticated insider threats. Consequently, machine learning has surfaced as a promising contender (Al-Mhiqani et al., 2020). The Deep Feature Synthesis algorithm, for instance, stands out for its prowess in characterizing user behaviours (Al-Mhiqani et al., 2020). The ongoing debate comparing anomaly-based detection methods to classification-based detection methods further motivates the discussion (Bin Sarhan & Altwaijry, 2023). Deep learning, a machine learning subset, also offers potential with techniques like Recurrent Neural Networks (RNNs) being explored for their efficacy (Bin Sarhan & Altwaijry, 2023). However, the spotlight isn't solely on machine learning. Meng et al. supported the integration of blockchain technology in Intrusion Detection Systems (IDS). Additionally, the Coburg Utility Framework (CUF) by Ring et al. is noteworthy for its innovative use of network data streams.

2.2.4. Sentiment Analysis in Threat Detection

A particularly fascinating avenue is the exploration of Sentiment Analysis for Threat Detection. With the growth of social media and sentiment-sharing platforms, coupled with the increasing tendency of individuals to express their views and biases, this method has gained major attention. Research indicates its potential in pinpointing insider threats. This article aims to dive deeper into the application of sentiment analysis, seeking ways to harness its techniques for identifying and countering insider threats.

2.2.5. Findings and Challenges

The trajectory of insider threat detection research has been upward, especially since the turn of the century. Significant peaks in research, as observed by Gheyas & Abdallah (2016), interestingly coincide with major real-world insider threat incidents that took place between 2009 and 2013, with a rapid

increase in these occurrences over the years (Gheyas & Abdallah, 2016). A noticeable finding is the common reliance on simulated data and game-theoretic approaches (Gheyas & Abdallah, 2016). However, the path to efficient threat detection is riddled with challenges. Data imbalance, for instance, seems to be a formidable obstacle. The potential of formal verification to boost the robustness of detection systems is a topic worth exploring further.

2.2.5. Conclusion

Insider threats have become a noticeable topic in the cybersecurity landscape. The studies reviewed offer a broad view of the challenges and methodologies associated with their detection. The insights from Al-Mhiqani et al. (2020) and Bin Sarhan and Altwaijry (2023) are particularly enlightening, pointing towards a future where machine learning and deep learning techniques dominate the threat detection arena.

2.3. Sentiment Analysis in Threat Detection

2.3.1. Introduction

In the rapidly evolving digital era, the production of online services has been escorted by an upsurge in security threats. As the cybersecurity landscape adapts to these challenges, the integration of sentiment analysis into threat detection has emerged as a crucial area of research. While sentiment analysis traditionally finds its application in detecting opinions in social media or product reviews, recent studies have expanded its effectiveness in detecting anomalies in operating system logs. Studiawan et al. (2021) introduced sentiment analysis to detect these anomalies, deviating from the conventional usage. Furthermore, the rising risk of insider threats has been highlighted by Nasir et al. (2021) and Jiang et al. (2018), both of whom proposed deep learning-based solutions. Jiang et al. (2018) particularly emphasized the significance of detecting previously undetected threats by referencing real-life incidents. Moreover, the role of sentiment analysis in measuring public sentiment through social networks has been highlighted by Hernández et al. (2023) and Parimala et al. (2021), particularly focusing on its use during natural disasters. Additionally, the challenge of identifying extremist content on platforms like Twitter has been addressed by Al-shaibani & Al-augby (2022), who stress the necessity for modern technological solutions due to the massive online content generation. Collectively, these studies highlight the potential of sentiment analysis in the field of cybersecurity and threat detection.

2.3.2. Existing Methods and Their Limitations

Various techniques have been developed for insider threat detection, offering different perspectives on identifying potential malicious activities originating from within an organization. Notably, a significant portion of these methods revolves around user behaviour-centric approaches. These techniques categorize user actions as normal or malicious based on behavioural patterns. Noteworthy contributions include supervised time series solutions utilizing a two-layer deep auto-encoder (Jiang et al., 2018), the implementation of an LSTM-CNN algorithm to extract temporal features for discerning user anomalous behaviour (Jiang et al., 2018), and the utilization of the XGBoost detection algorithm to extract behaviour characteristics from audit logs (Jiang et al., 2018). The Improved Hidden Markov Model (IHMM) has also been introduced as a method to detect malicious behaviour through feature extraction from user behaviour logs (Jiang et al., 2018).

Graph-based techniques introduce an innovative approach to insider threat detection, addressing user data details within structural and varied data. These approaches include techniques such as Gaussian Mixture models based on non-technical indicators (Jiang et al., 2018) and hybrid frameworks that combine "Graphical Processing Unit" (GPU) and "Anomaly Detection Unit" (ADU) components (Jiang

et al., 2018). Additionally, the use of recognized graphs gains importance for insider threat detection, providing a representation for high-dimensional and diverse data (Jiang et al., 2018).

Complementary to these strategies are methods arising from user behaviour and graph-based paradigms. For instance, the "Gargoyle" approach assesses the context of access requests for trustworthiness through Network Context Attribute (NCA) analysis (Jiang et al., 2018). Additionally, network packet inspection (Jiang et al., 2018) and the deployment of honeypot sensors within local networks (Jiang et al., 2018) offer individual strategies for insider threat detection. A noteworthy model integrates rules and regulations into complex events to facilitate the analysis of employee conduct (Jiang et al., 2018). Furthermore, psychological patterns within electronic communications have been analysed to anticipate and identify insider threats (Jiang et al., 2018).

However, a critical assessment of these techniques reveals limitations. While many models analyse user behaviours, they often overlook the content of communications, potentially leading to the exclusion of crucial context (Jiang et al., 2018, p.1). Emerging approaches attempting to include psychological aspects encounter challenges in acquiring appropriate user data. A comparative study by Nasir et al. (2021) highlights the widespread use of techniques such as LSTM and Deep AutoEncoders, which, despite their efficiency, present shortages concerning complexity, performance metrics, and evaluation datasets. The study highlights the need for fresh hybrid deep learning methodologies that balance efficiency, memory utilization, low false positive rates, and heightened accuracy (Nasir et al., 2021).

2.3.3. Conclusion

In summary, the reviewed articles collectively underline the growing significance of sentiment analysis across diverse fields. Parimala et al. (2021) showcase the efficacy of sentiment analysis, demonstrating its application in contexts as diverse as natural disasters. These studies contribute to a comprehensive understanding of sentiment analysis's roles and potentials, laying the groundwork for future research. Hernández et al. (2023) present an innovative approach to cybersecurity defence through sentiment analysis, utilizing user sentiments on Twitter to predict web security attacks. This groundbreaking methodology, along with Jiang et al.'s (2018) inventive insider threat detection technique, further underlines the transformative impact of sentiment analysis on cybersecurity. Nasir et al.'s (2021) deep learning-based approach also stands out within this landscape, offering a promising solution to the complex challenges posed by insider threats. Finally, the work by Studiawan et al. (2021) introduces a innovative technique for anomaly detection in Operating System logs through sentiment analysis, supported by deep learning strategies and addressing class imbalance concerns. Collectively, these findings highlight the potential, versatility, and strength of sentiment analysis, making substantial contributions to their respective fields and inspiring new avenues for exploration. The convergence of these findings explains the multi-layered role of sentiment analysis in addressing ongoing challenges across diverse domains, and that of insider threat detection included.

References

Al-Mhiqani, M.N., Ahmad, R., Abidin, Z.Z., Yassin, W., Hassan, A., Abdulkareem, K.H., Ali, N.S. and Yunos, Z., 2020. 'A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations', Applied Sciences, 10(15), pp.5208.

Al--shaibani, H.A., Alshaibani, H.A. and Al--augby, S., 2022. 'Terrorist Tweets Detection using Sentiment Analysis: Techniques and Approaches', Proceedings of the 5th International Conference on Engineering Technology and its Applications.

Bin Sarhan, B. and Altwaijry, N., 2023. 'Insider Threat Detection Using Machine Learning Approach', Applied Sciences, 13(1), pp.259. Available at: https://doi.org/10.3390/app13010259.

Gheyas, I.A. and Abdallah, A.E., 2016. 'Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis', Big Data Analytics, 1(6). Available at: [Link](https://www.researchgate.net/publication/283474435_Detection_and_prediction_of_insider_threats_to_cyber_security_a_systematic_literature_review_and_meta-analysis).

Gonçalves, P., Araújo, M., Benevenuto, F. and Cha, M., 2013. 'Comparing and Combining Sentiment Analysis Methods'.

Hernández, A., Sanchez, V., Sánchez, G., Pérez, H., Olivares, J., Toscano, K., Nakano, M. and Martinez, V., 2023. 'Security Attack Prediction Based on User Sentiment Analysis of Twitter Data'.

Jiang, J. et al., 2018. 'Prediction and Detection of Malicious Insiders' Motivation based on Sentiment Profile on Webpages and Emails'.

Kumar, A. and Sebastian, T.M., 2012. 'Sentiment Analysis: A Perspective on its Past, Present and Future', I.J. Intelligent Systems and Applications, 10, pp.1-14.

Mejova, Y., 2009. 'Sentiment Analysis: An Overview', Computer Science Department, University of Iowa. Available at: [Actual URL] [Accessed: Actual Date].

Ms.V.Gayathri and Ms.A.M.Abirami, 2016. 'A Survey on Sentiment Analysis Methods and Approach', 2016 IEEE Eighth International Conference on Advanced Computing (ICoAC). Available at: [Actual URL].

Nasir et al., 2021.

Oladimeji, T.O., Ayo, C.K. and Adewumi, S.E., 2019. 'Review on Insider Threat Detection Techniques', Journal of Physics: Conference Series.

Parimala, M. et al., 2021. 'Spatiotemporal-based sentiment analysis on tweets for risk assessment of an event using a deep learning approach'.

Studiawan, H., Sohel, F. and Payne, C., 2021. 'Anomaly Detection in Operating System Logs with Deep Learning-Based Sentiment Analysis', *IEEE Transactions on Dependable and Secure Computing*, 18(5).