Sentiment and Emotion Analysis with Large Language Models for Political Security Prediction Framework

Liyana Safra Zaabar, Adriana Arul Yacob, Mohd Rizal Mohd Isa,
Muslihah Wook, Nor Asiakin Abdullah, Suzaimah Ramli, Noor Afiza Mat Razali*
Faculty of Defence Science & Technology, National Defence University of Malaysia, Kuala Lumpur

***Abstract*—The increasing spread of textual content on social media, driven by the rise of Large Language Models (LLMs), has highlighted the importance of sentiment analysis in detecting threats, racial abuse, violence, and implied warnings. The subtlety and ambiguity of language present challenges in developing effective frameworks for threat detection, particularly within the political security domain. While significant research has explored hate speech and offensive content, few studies focus on detecting threats using sentiment analysis in this context. Leveraging advancements in Natural Language Processing (NLP), this study employs the NRC Emotion Lexicon to label emotions in a political-domain social media dataset. *TextBlob* is used to extract sentiment polarity, identifying potential threats where anger and fear intensities exceed a threshold alongside negative sentiment. The Bidirectional Encoder Representations from Transformers (BERT) was applied to enhance threat detection accuracy. The proposed framework achieved an Area Under the ROC Curve (AUC) of 87%, with the BERT model achieving 91% accuracy, 90.5% precision, 81.3% recall and F1-score of 91%, outperforming baseline models. These findings demonstrate the effectiveness of sentiment and emotion-based features in improving threat detection accuracy, providing a robust framework for political security applications.**

***Keywords*—Political security; large language models; sentiment analysis; emotion analysis; BERT; threat prediction**

I. INTRODUCTION

Today, cyberspace has proven to be a very powerful tool and can impact national security. As new risks emerge, there is interest in developing more advanced defence strategies[1]. The current response to this problem is too limited, as it cannot capture the scale of information sharing that big data analyses. In this cyber arena, various platforms become addresses for various types of transactions including emotional transactions among the public [1]. These feelings can trigger great security concerns, such as the real-world example at the beginning of the Arab Spring, where the spread of false information online exacerbated negative attitudes and led to social instability that endangered national security[1], [2]. The events of the Arab Spring are one round of examples showing how emotions affect social and political stability. People are emotional creatures, and the emotion of anger or fear can mobilize people towards collective action, even disruptive to society. For example, anger has been demonstrated to lead more often to approach behaviour (increasing social movement participation), while fear leads most frequently to avoidance [2]. Indeed, these emotional responses to political will unravel even relatively stable societies as seen in the Arab Spring protests. The collapse of stability in the Middle East and North Africa region caught almost all Western policy makers off guarded, but perhaps a paralytic counselling should be devoted to emotional matters within political and social regulation [3].

Many platforms accommodate a wide variety of different types of data exchange in cyberspace, including a wide range of public emotional expressions. These emotions can pose security risks, as evidenced by events like the Arab Spring, where negative sentiments were fuelled by misinformation online, which eventually led to societal unrest that threatened national security. As such, promptly detecting disruptive sentiments like these is essential for authorities to effectively manage crises. However, existing methodologies for emotional evaluation regarding national security are inadequate [9]. While most researchers explore various techniques for classifying human emotions, there is insufficient attention given to connecting these emotions to security threats and developing appropriate measurement mechanisms. Despite the capability of sentiment analysis methods to ascertain word polarity, their application in predicting threats remains largely unexplored, particularly in the realm of political security[5], [9].

Existing research on sentiment analysis largely focuses on hate speech and offensive content, with limited attention to detecting political security threats. While sentiment analysis effectively monitors public sentiment, it often fails to connect emotions like anger and fear to security threats within dynamic environments such as social media. Furthermore, traditional models struggle to capture the contextual and sequential dependencies necessary for identifying evolving threats. This study addresses these gaps by leveraging a BERT-based framework enhanced with the NRC Emotion Lexicon to improve the accuracy of political threat detection. By integrating advanced sentiment and emotion analysis, this research provides a robust model for enhancing political security prediction and contributes to bridging critical gaps in existing literature.

This paper is organized as follows: Section II reviews related work, establishing the relevance of the study and highlighting the contributions of the proposed approach. Section III describes the methods and materials, including details on the dataset, data preprocessing, word embedding

*Corresponding Author.

techniques, and the proposed BERT-based model for detecting political security threats. Section IV presents the results, offering a comparative analysis of the model's performance relative to existing approaches. Section V discusses the comparative findings and explores infrastructure requirements and future directions for deploying large language models in secure and efficient environments. Finally, Section VI concludes with the key findings and their implications for advancing political security threat prediction frameworks.

II. Related Work

Authors in study [13] developed a global cyber-threat intelligence system using Conventional Neural Network and employed sentiment analysis techniques to detect global threats. In this study, the Bidirectional Encoder Representations from Transformers (BERT) model is used to address limitations inherent in traditional Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks when capturing long-term dependencies in sequential data.

Traditional RNNS suffer from a vanishing gradient problem, in which gradients will diminish exponentially over time, making it difficult for the network to learn long-range dependencies [14]. While LSTMs mitigate this issue by introducing a memory cell with a sophisticated structure [12], BERT outperforms both RNNs and LSTMs by leveraging a transformer-based architecture that effectively models contextual relationships across the entire sequence, eliminating the constraints of sequential processing [15].

Emotions are known to have an important impact on human cognitive processes and decision-making [4]. Intelligence has been influenced by emotion, as they contribute for several underlying cognitive skills such as salience detection, decision making and adaptation in a critical way [4]. An interesting discovery is that non-compliant behaviour against security procedures can be influenced by emotions, with four main emotional traits in the field of information security domain including rage, trust fear and stress. Fear has been recognised as a foundational principle for keeping people using security measures. The emotion-based security threat detection is not meant to completely replace the traditional measures but can act as a complement strategy by providing an additional layer of intelligence and adaptability [5].

Recent studies highlight those emotions detected through sentiment analysis, specifically from social media, play an important role in identifying potential security threats. For example, the massive use of sentiment analysis on user-generated content such as tweets or Facebook posts has proven useful in monitoring public sentiment that may signal social instability, the spread of disinformation, or other factors that could threaten national security [6]. Emotional sentiment can be an early indicator of chaos, allowing authorities to intervene early before tensions escalate, as is the case in events such as the Arab Spring [7], [8]. Advances in sentiment analysis have leveraged machine learning and artificial intelligence (AI) technologies to not only detect emotional changes in social media content but also predict potential security concerns. By applying natural language processing (NLP) techniques, the system can detect changes in emotional tone or intensity among a broad population, identifying issues such as anger, fear, or frustration that may lead to greater social threats [8].

Recent research has pointed out that emotions detected with sentiment analysis, especially those emanating from social media, become highly important in the process of identifying potential security threats. The high-volume applications of sentiment analysis on user-generated content such as tweets or Facebook posts have proven useful in the monitoring of public sentiments indicative of social instability, disinformation dissemination, and other factors that can threaten national security [6]. Therefore, it may be said that emotional sentiment can act as an early warning signal for chaos, and the authorities can intervene at an early stage before tensions escalate, as in events like the Arab Spring [7], [8]. Advanced sentiment analysis harnessed the power of machine learning and AI technologies to identify not only emotional changes in content on social media but also predict possible security concerns. Using the methods of NLP, it can observe changes in emotional tone or intensity of the greater population and pinpoint problems such as anger, fear, or frustration that might be a larger threat to society.

Negative emotions such as anger, fear, disgust and anxiety have been identified as potential indicators of security threats, especially when these emotions are widely expressed in public or digital spaces [9]. For example, anger is often associated with social discontent and can trigger collective actions such as protests or riots, especially in politically unstable contexts. According to studies, anger can be a trigger for aggressive behaviour when an individual or group feels marginalized or oppressed. This shift from emotion to action has been observed in many cases of social instability, where negative sentiment on social media is closely linked to violence or instability in the real world [8], [17].

Fear and related emotions such as extreme fear and anxiety also play an important role in predicting threats. While fear is not an immediate threat, it can cause destabilizing reactions, such as panic buying, mass evacuation, or rioting, especially when influenced by the spread of false information or rumours [18]. Studies in behavioural psychology and security frameworks emphasize that fear increases the perception of vulnerability, making it a useful tool for predicting crises and emergency response strategies [19]. Disgust, often fuelled by moral or ethical outrage, can also increase social division and instability, further contributing to security risks. Sentiment analysis tools, when used to monitor these emotions, have become increasingly accepted for predicting and mitigating threats before they escalate [5]. Author in [9] proposed that emotion is a key variable in determining an opinion or sentiment. Emotions such as anger, fear, disgust, fear, and anxiety can serve as emotional indicators in determining the existence of political security threats in text data. These emotions, as studies have determined, are closely related to the political security domain and have the potential to trigger political events such as riots, coups, terrorism, international wars, civil wars, and political elections, which can lead to negative sentiments or opinions. These opinions or sentiments can be analysed to predict threats in the political security domain [9], [20].

The selection of the proposed BERT-based framework is driven by its ability to overcome the key constraints of existing models, such as traditional RNNs and LSTMs, which face difficulties in addressing long-term dependencies and understanding of context. Unlike this approach, BERT uses a transformer architecture to effectively model data sequentially and capture more subtle relationships in text content. Additionally, while previous models primarily focused on general sentiment analysis or the detection of specific offensive content, they lacked the ability to link emotional intensity such as fear and anger to political security threats. By integrating Lexicon's NRC Emotion and sentiment polarity analysis, this proposed framework bridges the gap, providing better accuracy and adaptability for identifying threats. To prove the effectiveness of this framework, comprehensive verification measures and comparative analysis with existing methods were conducted, emphasizing its superiority in addressing the complexity of predicting political security threats.

III. Methods and Materials

In our research, we developed the BERT LLM Political Security Model to predict various threats from online platforms. Our model comprises several key stages, including data pre-processing and cleansing, word embedding and threat classification and detection. In this stage, BERT is used for threat detection by adopting sentiment analysis method. Fig. 1 illustrates the Workflow of BERT LLM Political Security Model.

A. Dataset

In this experimental design, we used the labelled dataset provided by [9]. This dataset was originally created by manually gathering various Malaysian online news sources, such as The Star, New Straits Times (NST), and Free Malaysia Today (FMT), and more. The dataset comprises 250 texts from online news sources. Out of these texts, 163 of them are categorized as positive, while the remaining 87 are categorized as negative. These positive and negative classifications serve as markers to ascertain the presence of threats within the sample texts.

B. Pre-processing

In Natural Language Processing (NLP), text pre-processing is a process that will enhance classifier performance and reduce feature complexity [10]. In this process, unnecessary elements such as punctuation, HTML codes, and symbols are removed, and the gathered text data is then transformed to lowercase and normalized. The normalization process consists of two main steps. First, the unstructured text dataset is converted into a structured word vector, and then, the feature vector's dimensionality is reduced by eliminating unwanted words and stemming them to their original forms. Stemming refers to reducing words to their roots, while lemmatization is the act of utilizing a lexical knowledge base to convert words to their base forms by rooting verbs. At the end of the process, words will be encoded into numerical formats [11].

C. Word-Embedding

Word embedding is a technique used in NLP and deep learning to represent words as dense vectors of real numbers [12]. It is a way to map words to vectors in a continuous vector space, where similar words are represented by similar vectors. This experimental layer carries max_words as an input dimension, with 50 as the output dimension (embedding size), and max_len as the input length. This layer creates a low dimensional vector that deals with each word in the input sequences and directly replaces them with their dense vector representation. These vectors are then multiplied from the embedding layer container and are then sent to the BERT layer for further processing.

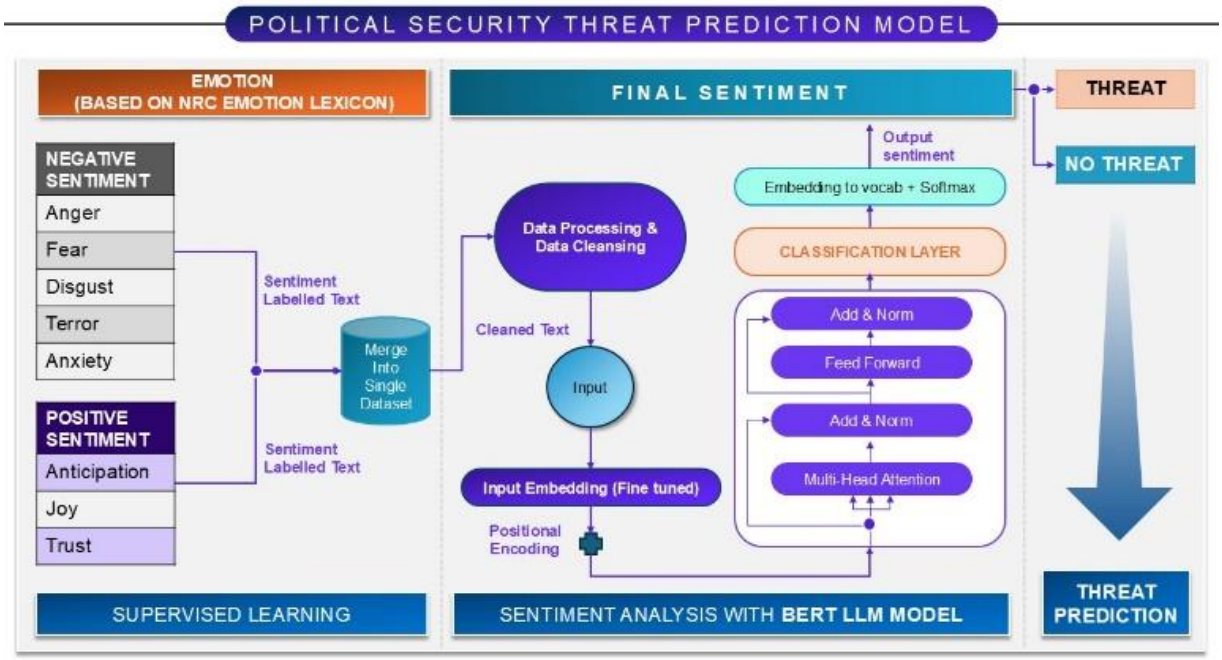

Fig. 1. Workflow of BERT LLM political security model.

D. Threat Prediction Using BERT

To validate our proposed model, an experimental analysis was conducted. The dataset for this research is constructed by collecting text data from various online news platforms, and the proposed model seeks to open new research avenues at the intersection of sentiment analysis and national security. The model will achieve this to enhance emotion measurement and threat prediction in cyberspace.

Fig. 2 illustrates the political security prediction model leveraging NRC Emotion Lexicon [15] and BERT [16]model for threat classification and prediction.

An experiment was conducted on a PC with an Intel® Core™ i7-8650U CPU @ 1.90GHz, 2.11 GHz, 8GB of RAM, a 64-bit OS, and an x64-based processor to test the developed model in Python 3.11.1 environment. 250 sentences from Malaysian online news sources were used as the main labelled dataset after the cleansing and data preparation process. To gauge the efficacy of our models, we compared them to the model developed by the researchers cited in reference [9]. We selected their model for comparison because it addresses the same task as our study, which is identifying threats in the political domain, and because it also utilizes the same dataset for evaluation, which is data that is derived from Malaysian online news.

The final phase of the research design is to validate the analyzed data. This study demonstrated a comparative performance evaluation to validate the proposed theoretical framework in this phase. The results of the evaluation test compare precision, recall, accuracy and F-measure [21]. The performance measure involves calculation of the accuracy, precision and recall value of the test dataset. The evaluation process commenced after the labelling of data into either positive or negative classes, or the imbalance between the class proportions was addressed. A random subset of sentences was selected, to train and test it with the BERT transformer-based model. The employment of confusion matrix and the computation of accuracy, precision, and recall are the strong indicators to evaluate the performance of the chosen model based on the training data. The formula for accuracy, as shown in Eq. (1), is the proportion of correctly predicted opinions out of all input opinions to the classifier. This proportion is determined by true positive (TP), true negative (TN), false positive (FP), and false negative (FN) values.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision is shown in Eq. (2) and is the percentage of true cases of an opinion (of an instance) among all the classified cases of the opinions (of all instances). To determine the accuracy, true positive rate (TP) was used, as shown in the formula below.

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall is defined as the proportion of properly categorized occurrences of a polarity over the total number of correct instances of the polarity. The formula to calculate the recall values using TP and FN is shown in Eq. (3):

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

The F-score is calculated by dividing the number of true positives by the sum of true positives and false positives, as shown in Eq. (4).

$$F - score = \frac{2TP}{2TP+FP+FN} \quad (4)$$

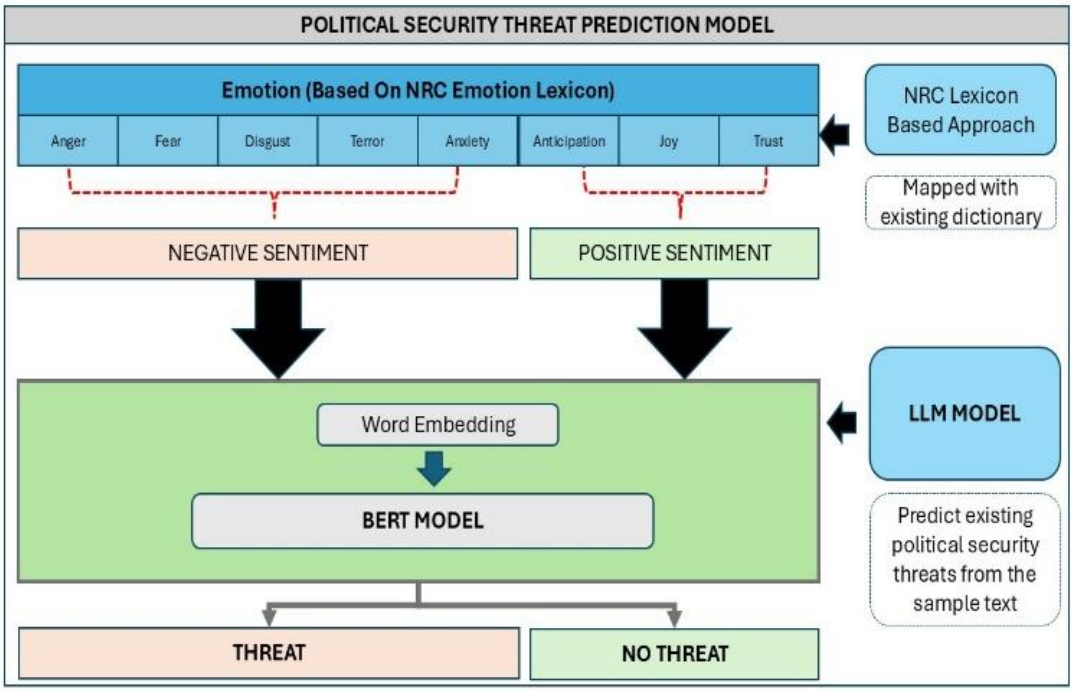

Fig. 2. Political security threat prediction model.

IV. RESULTS

A. Comparative Output and Benchmarking

The performance of the current model, BERT LLM, proposed model in political security domain, was benchmarked against the baseline hybrid model (Lexicon + Decision tree) by [9] as well as LSTM model. In Table I and Fig. 3, the BERT LLM model is compared to other currently existing approaches across key metrics: accuracy, precision, recall and F-score [22]. The findings indicate that the BERT LLM model surpasses the hybrid methods in performance, and that the LSTM model yields the least favorable results.

TABLE I. COMPARATIVE OUTPUT OF THE BERT LLM MODEL WITH OTHER METHODS

Methods	*Accuracy*	*Precision*	*Recall*	*F-Score*
Baseline Model (Lexicon + Decision Tree)	66.14%	98.86%	40.65%	57.62%
LSTM	81.30%	94.00%	71.80%	81.30%
BERT	91.00%	90.50%	81.30%	91.00%

Table I compares the performance of the BERT model with the Baseline Model (Lexicon + Decision Tree) and LSTM in terms of accuracy, precision, recall, and F-score. The BERT model outperforms both alternatives, achieving the highest accuracy (91.00%) and F-score (91.00%), demonstrating its superior ability to understand and classify threat effectively. While the Baseline Model shows high precision (98.86%), its low recall (40.65%) leads to a significantly lower F-score (57.62%), indicating limited generalizability. The LSTM model balances performance better, achieving 81.30% accuracy and F-score with substantial improvements in recall (71.80%) over the Baseline. However, BERT surpasses LSTM in all metrics, particularly in accuracy and F-score, highlighting its robustness in capturing contextual dependencies and delivering precise and balanced predictions.

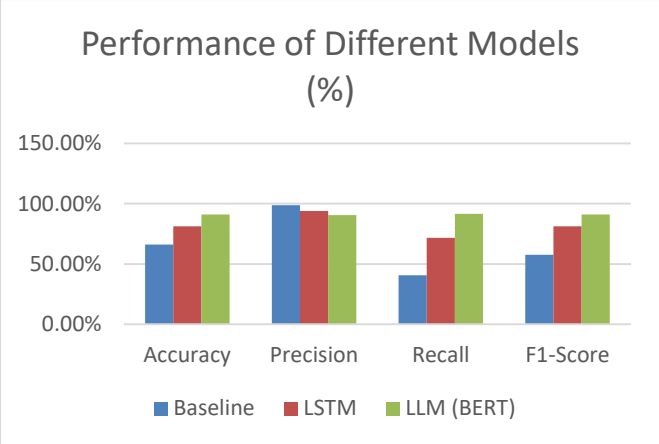

Fig. 3. Comparative performance of BERT LLM model and other methods.

V. DISCUSSION

A. Units Area Under Precision Recall (AUC-PR)

In Fig. 4, an AUC-PR of 0.87 indicates that there is high precision being recalled at different thresholds, suggesting that the model performs well in separating positive classes from negative classes. The curve demonstrates a high area under the curve (AUC-PR = 0.87), which reflects BERT's ability to maintain a strong balance between precision (90.50%) and recall (91.50%). This high value indicates that BERT effectively minimizes false positives while accurately capturing true positives, even in scenarios with imbalanced datasets. The gradual decline in precision with increasing recall emphasizes the model's robustness in handling trade-offs between these metrics. The shaded region under the curve quantifies the AUC-PR, underscoring the superior contextual understanding and classification efficiency of the BERT model compared to the Baseline and LSTM methods. This result further highlights BERT's utility in tasks requiring precise and consistent predictions.

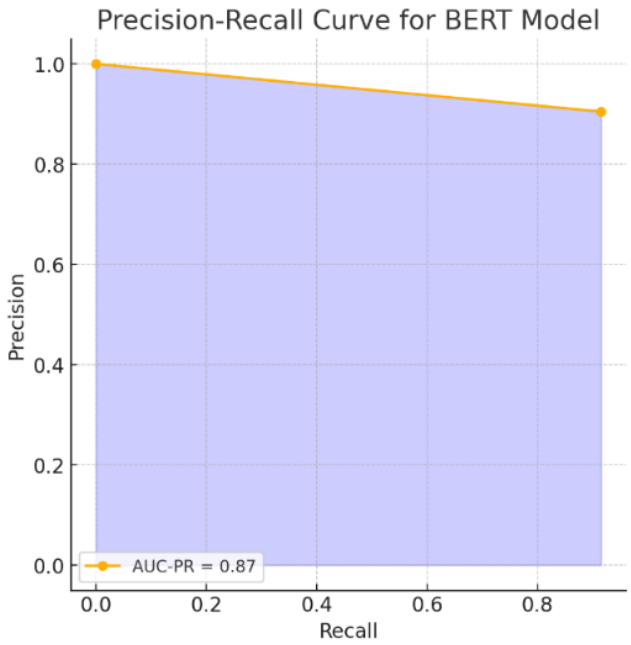

Fig. 4. Precision-recall curve of BERT-LLM model.

B. Training and Validation Loss Curve

The curves in Fig. 5 show the training and validation loss of the model. Validation Loss and Accuracy are calculated on a separate validation dataset and serve as indicators of how well the model generalizes unseen data [15]. The graph shown shows the train loss (red line) and validation loss (green line) over 100 epochs, which illustrates the model learning process.

The red line, which represents losses during training, decreases consistently, signifying that the model is getting better at understanding the patterns and characteristics present in the training data. This continued decline also indicates that the model is successfully reducing prediction errors on the training data, which is a sign that the model is learning well and becoming more efficient at performing predictions.

In addition, validation loss (green line) also shows a steady decline throughout the exercise. This decrease which is almost parallel to the train loss shows that the model not only learns well on the training data but also has good generalization capabilities on the validation data, which has never been seen

during training. The fact that these two losses are almost parallel indicates that the model does not suffer from overfitting, where it manages to avoid overlearning on training data alone, instead works well on the new data being tested.

Both lines show a good downward trend, and there is no significant difference between training loss and confirmation loss. This suggests that the model learns well without relying too much on training data alone. These results show that the model can be effectively used to make accurate predictions on new data. The model shows good generalizations, where it not only gives good results on the training data, but also on the validation data, which is important to ensure that the model does not fit too well with the training data alone.

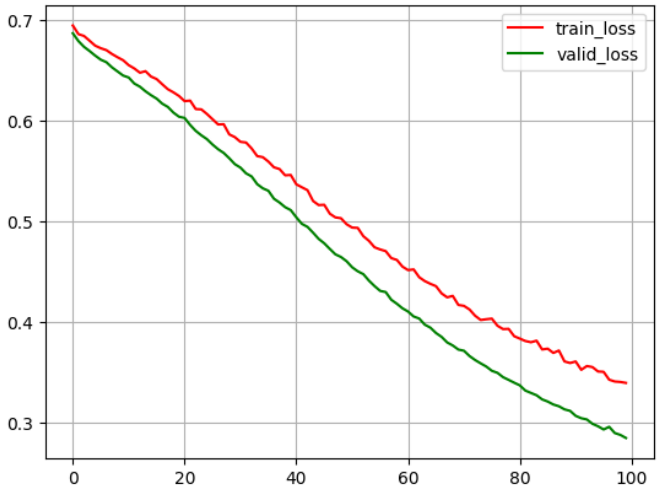

Fig. 5. BERT LLM model loss curves.

C. Future Environment and Infrastructure to Support Large Language Models

This research was conducted in a low-performance environment, utilizing a labeled dataset containing only 250 texts. Given the high computational demands of large language models, it is recommended to leverage high-performance cloud infrastructure in the future.

The success of future Large Language Models approaches relies on a robust cloud infrastructure and stringent security measures to safeguard sensitive data. Consequently, Transformer-based model training, equipped with advanced optimizers, must be performed within high-performance cloud infrastructure. Ensuring the security of the cloud infrastructure, including the underlying bare-metal, firmware, and software technologies, is critical to maintain the overall integrity and resilience of the training environment [23]. A thorough understanding of cloud computing security implications is essential to safeguard data and systems and to ensure the accuracy and reliability of the training data [24], [25].

Cloud security challenges, such as access control issues and the integration of blockchain technologies, including decentralized access control frameworks, must be addressed [26]. The recent adoption of advanced technologies like blockchain for cloud access control through smart contracts also necessitates careful consideration [27].Additionally, human factors, such as the acceptance of cloud computing, should be considered to mitigate security risks and enhance the delivery of training and predictive analyses [28], [29]. Additionally, consideration should be given to the human perspective, including the acceptance and trust in cloud computing, to mitigate security risk factors that could affect the delivery of training and predictive analysis of threat [30].

VI. Conclusion

This research study shows that combining the transformer-based BERT model significantly enhances deep learning models' abilities to predict political threats. This model is not only capable of reshaping the political security threat prediction landscape but can also support researchers' future studies within the national security field. The synergy between the sentiment analysis, word embedding and BERT networks offers enhanced accuracy and robustness in national security scenarios by adaptively adjusting learning rates, while also capturing long dependencies that are essential in detecting evolving threats. To summarize, the transformer-based BERT model introduces new and effective ways to enhance the accuracy, efficiency, and versatility of political threat prediction, making it a significant advancement in the domain of national security.

Acknowledgment

The authors fully acknowledge Ministry of Higher Education Malaysia (MOHE) and National Defence University of Malaysia (NDUM) which makes this important research viable and effective.

References

[1] P. Datta, N. Lodinger, A. S. Namin, and K. S. Jones, “Predicting Consequences of Cyber-Attacks,” in Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 2073–2078. doi: 10.1109/BigData50022.2020.9377825.

[2] S. Hatab, “Threat perception and democratic support in Post-arab spring Egypt,” Comp Polit, vol. 53, no. 1, pp. 69–91, 2020, doi: 10.5129/001041520X15822914282706.

[3] G. Wolfsfeld, E. Segev, and T. Sheafer, “Social Media and the Arab Spring: Politics Comes First,” International Journal of Press/Politics, vol. 18, no. 2, pp. 115–137, Apr. 2013, doi: 10.1177/1940161212471716.

[4] H. Strömfelt, Y. Zhang, and B. W. Schuller, “Emotion-Augmented Machine Learning: Overview of an Emerging Domain,” 2017.

[5] N. A. M. Razali et al., “Opinion mining for national security: techniques, domain applications, challenges and research opportunities,” J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00536-5.

[6] M. Suhairi et al., “Social Media Sentiment Analysis and Opinion Mining in Public Security: Taxonomy, Trend Analysis, Issues and Future Directions.”

[7] G. Wolfsfeld, E. Segev, and T. Sheafer, “Social Media and the Arab Spring: Politics Comes First,” International Journal of Press/Politics, vol. 18, no. 2, pp. 115–137, Apr. 2013, doi: 10.1177/1940161212471716.

[8] A. Arora, A. Arora, and J. McIntyre, “Developing Chatbots for Cyber Security: Assessing Threats through Sentiment Analysis on Social Media,” Sustainability (Switzerland), vol. 15, no. 17, Sep. 2023, doi: 10.3390/su151713178.

[9] N. A. M. Razali et al., “Political Security Threat Prediction Framework Using Hybrid Lexicon-Based Approach and Machine Learning Technique,” IEEE Access, vol. 11, pp. 17151–17164, 2023, doi: 10.1109/ACCESS.2023.3246162.

[10] L. Safra Zaabar, M. R. Yaakub, M. Iqbal, and A. Latiffi, "Combination of Lexicon Based and Machine Learning Techniques in the Development of Political Tweet Sentiment Analysis Model."

[11] M. Ridzwan Yaakub, M. Iqbal Abu Latiffi, and L. Safra Zaabar, "A Review on Sentiment Analysis Techniques and Applications," in IOP Conference Series: Materials Science and Engineering, Institute of Physics Publishing, Aug. 2019. doi: 10.1088/1757-899X/551/1/012070.

[12] K. Ohtomo, R. Harakawa, M. Iisaka, and M. Iwahashi, "AM-Bi-LSTM: Adaptive multi-modal Bi-LSTM for sequential recommendation," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3355548.

[13] F. Sufi, "A global cyber-threat intelligence system with artificial intelligence and convolutional neural network," Decision Analytics Journal, vol. 9, Dec. 2023, doi: 10.1016/j.dajour.2023.100364.

[14] Y. Touzani and K. Douzi, "An LSTM and GRU based trading strategy adapted to the Moroccan market," J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00512-z.

[15] A. Saeed and E. Al Solami, "Fake News Detection Using Machine Learning and Deep Learning Methods," Computers, Materials and Continua, vol. 77, pp. 2079–2096, 2023, doi: 10.32604/cmc.2023.030551.

[16] N. J. Prottasha et al., "Transfer Learning for Sentiment Analysis Using BERT Based Supervised Fine-Tuning," Sensors, vol. 22, no. 11, Jun. 2022, doi: 10.3390/s22114157.

[17] I. H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," Nov. 01, 2021, Springer. doi: 10.1007/s42979-021-00815-1.

[18] D. Wollebæk, R. Karlsen, K. Steen-Johnsen, and B. Enjolras, "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior," Social Media and Society, vol. 5, no. 2, 2019, doi: 10.1177/2056305119829859.

[19] J. Kruger, B. Chen, S. Heitfeld, L. Witbart, C. Bruce, and D. L. Pitts, "Attitudes, Motivators, and Barriers to Emergency Preparedness Using the 2016 Styles Survey," Health Promot Pract, vol. 21, no. 3, pp. 448–456, May 2020, doi: 10.1177/1524839918794940.

[20] T. G. Coan, J. L. Merolla, E. J. Zechmeister, and D. Zizumbo-Colunga, "Emotional Responses Shape the Substance of Information Seeking under Conditions of Threat," Polit Res Q, vol. 74, no. 4, pp. 941–954, Dec. 2021, doi: 10.1177/1065912920949320.

[21] Md. N. Y. Ali, Md. G. Sarowar, Md. L. Rahman, J. Chaki, N. Dey, and J. M. R. S. Tavares, "Adam Deep Learning With SOM for Human Sentiment Classification," International Journal of Ambient Computing and Intelligence, vol. 10, no. 3, pp. 92–116, Jul. 2019, doi: 10.4018/IJACI.2019070106.

[22] S. Nawaz, "A Comparative Study of Machine Learning Algorithms for Sentiment Analysis," 1999. [Online]. Available: www.ijrpr.com

[23] Proceedings, 2020 16th IEEE International Colloquium on Signal Processing & its Application (CSPA 2020) : 28th-29th February 2020 : conference venue, Hotel Langkawi, Lot 1852 Jalan Penarak, Kuah 07000 Langkawi, Kedah, Malaysia. IEEE, 2020.

[24] M. Noorafiza, H. Maeda, R. Uda, T. Kinoshita, and M. Shiratori, "Vulnerability analysis using network timestamps in full virtualization virtual machine," in ICISSP 2015 - 1st International Conference on Information Systems Security and Privacy, Proceedings, SciTePress, 2015, pp. 83–89. doi: 10.5220/0005242000830089.

[25] M. Noorafiza, H. Maeda, T. Kinoshita, and R. Uda, "Virtual machine remote detection method using network timestamp in cloud computing," in 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013, IEEE Computer Society, 2013, pp. 375–380. doi: 10.1109/ICITST.2013.6750225.

[26] W. N. Wan Muhamad et al., "Enhance multi-factor authentication model for intelligence community access to critical surveillance data," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer, 2019, pp. 560–569. doi: 10.1007/978-3-030-34032-2_49.

[27] N. M. Noor, N. A. M. Razali, S. N. S. A. Sham, K. K. Ishak, M. Wook, and N. A. Hasbullah, "Decentralised Access Control Framework using Blockchain: Smart Farming Case," International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, pp. 566–579, 2023, doi: 10.14569/IJACSA.2023.0140560.

[28] M. R. A. Bakar, N. A. M. Razali, M. Wook, M. N. Ismail, and T. M. T. Sembok, "Exploring and Developing an Industrial Automation Acceptance Model in the Manufacturing Sector Towards Adoption of Industry4.0," Manufacturing Technology, vol. 21, no. 4, pp. 434–446, 2021, doi: 10.21062/mft.2021.055.

[29] M. R. Abu Bakar, N. A. Mat Razali, M. Wook, M. N. Ismail, and T. M. Tengku Sembok, "The Mediating Role of Cloud Computing and Moderating Influence of Digital Organizational Culture Towards Enhancing SMEs Performance," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Science and Business Media Deutschland GmbH, 2021, pp. 447–458. doi: 10.1007/978-3-030-90235-3_39.

[30] K. Khalil Ishak et al., "Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions."