Proof of Concept of a Digital Forensic Readiness Cybercrime Language as a Service

Maryam Mohamad Al Mahdi and Stacey Baror
Department of Computer Science, University of Pretoria, South Africa

maryam.mohamadalmahdi@up.ac.za
stacey.baror@cs.up.ac.za

Abstract: Welcome to the 21st century, where more devices are connected to the Internet than people on this earth. Each device will be or has been a target of cybercrime. The popularity of text-based cybercrimes has become prevalent with the advancement of the Internet. The number of cybercrimes increases yearly, unlike the reports of such crimes. The major problem is the lack of awareness and protection from cybercrimes. These issues cascade into greater consequences, such as a shortfall of reports, deficiency of cybercrime data, etc. The DFClaaS system is proposed as a solution; it allows users to report text-based cybercrimes anonymously. Next, several NLP techniques are applied to such reports to comprehend text-based cybercrimes as a language, and once the usage of the language is detected, an investigation proceeds. Subscribed users are individuals or businesses that are in some regard connected to the Internet. The DFClaaS system aims to protect its users from text-based cybercrimes and provide digital forensic investigators resources to conduct a successful investigation, enriching digital forensics research. The system is a feature-rich digital forensics readiness tool that will track the aggressive advancements of text-based cybercrimes, thus serving and protecting its users.

Keywords: Digital forensics, Text-based cybercrime, Natural language processing, Phishing, cyberattacks, Digital forensics readiness

1. Introduction

In today's digital age, the Internet has ushered in unprecedented convenience and connectivity, but it has also brought forth a challenge: the proliferation of cybercrime. These illicit activities transcend geographical boundaries and linguistic barriers, posing a pervasive threat in our increasingly interconnected world. The extent and diversity of these cybercrimes are striking, encompassing a wide range of malicious activities, often exploiting the languages we use for communication. Digital forensics, the systematic process of collecting, analysing, and preserving electronic evidence to investigate and prevent cybercrime, plays a crucial role in combatting cybercrime. As we delve deeper into the challenges posed by the proliferation of cybercrime, it is essential to recognize how cybercrimes have evolved, especially in the context of the COVID-19 pandemic.

The COVID-19 pandemic and the widespread adoption of remote work have further exacerbated the cybercrime problem (Chigada and Madzinga, 2021). As society rapidly adapted to digital modes of operation, cybercriminals capitalized on the ensuing vulnerabilities.

The surge in cybercrimes has exposed a troubling trend: many individuals and businesses remain trapped in a reactive posture, scrambling to respond after attacks happen rather than proactively building defenses. This reactive stance breeds a host of critical issues that undermine our collective defense against cyber threats.

First, victims often remain silent, their voices muffled by a complex web of anxieties. Unawareness of reporting channels, fear of embarrassment or blame, concerns about anonymity, and even a lack of faith in law enforcement's ability to act – these factors collectively form a wall of silence that shields cybercriminals from consequences.

Second, businesses prioritize functionality over security, leaving gaping vulnerabilities within their services. This creates a digital landscape fraught with weak authentication protocols, unpatched software, and inadequate data encryption – a veritable buffet for skilled cybercriminals.

Third, the fight against cybercrime is hampered by a lack of robust data. Investigations flounder due to insufficient case information, and the development of crucial machine learning models for predictive analysis suffers from a dearth of training data. This data scarcity weakens our ability to anticipate and thwart future attacks.

Finally, the presence of incompetent third-party services only exacerbates the problem. Lacking the necessary knowledge, resources, and collaborative spirit, these entities delay the identification of cyberattacks and cast doubt on the accuracy of investigative findings. This muddies the waters and allows cybercriminals to operate with impunity.

The current reactive approach towards cybercrime simply is not sustainable. We must shift towards a proactive stance, actively strengthening defenses, fostering open communication, and bolstering our investigative capabilities.

Building upon the insights presented in the study titled "Functional Architectural Design of a Digital Forensic Readiness Cybercrime Language as a Service" (Baror et al., 2023), our research seeks to implement the proposed solution as a response to the surge in cybercrimes. Inspired by the functional architectural design presented in the mentioned paper, our study aims to revolutionize the approach to cybercrime by developing the Digital Forensic Cybercrime Language as a Service (DFClaaS) system. This innovative system, which forms the crux of our research, is designed to address the challenges posed by cybercrimes, particularly those of a text-based nature.

Our methodology involves constructing a high-level model based on the architectural design proposed by Baror et al. (2023), and subsequently implementing a proof-of-concept. Leveraging Natural Language Processing (NLP) models, including Large Language Models, sentiment analysis, and lexicon analysis, to create an efficient and effective tool for combating cybercrimes.

The key objectives include implementing microservices that address various challenges, proposing a system to enhance incident reporting and analysis, and providing valuable resources for investigators. Ultimately, the DFClaaS system aims to benefit many stakeholders, from individual users and organizations seeking a secure digital environment to digital forensic investigators striving to combat the ever-evolving landscape of cybercrime.

The next section follows the background literature on concepts key to understanding this research.

2. Background Literature

In our digitally connected world, text-based cybercrimes have become a pervasive threat, encompassing various illegal activities. As these cybercrimes evolve, digital forensics readiness (DFR) plays a crucial role in responding effectively. DFR involves preparing for digital incidents by developing policies and capabilities to collect and analyse digital evidence. To combat these evolving threats, the integration of cutting-edge technology, such as Natural Language Processing (NLP), is essential. NLP leverages human language understanding to help computers process, analyse, and generate text and speech data, making it valuable in combating text-based cybercrimes. Large Language Models (LLMs) are a significant development in NLP, transforming various fields with their deep understanding of language. This review explores the connections between text-based cybercrimes, DFR, NLP, and LLMs, emphasizing their importance in modern cybersecurity challenges. A review of text-based cybercrime is discussed next to address these emerging challenges.

2.1 Text-Based Cybercrimes

We live in a time of convenience; access to the Internet and devices to connect to it unveils the digital world where almost everyone and everything is accessible with a click of a button. However, this digital age also brings a new frontier of crime, text-based cybercrimes (Meifilina et al., 2019). These crimes encompass a wide range of illegal activities carried out through text communication on the Internet. Examples of such crimes are romance scams, identity theft, cyberbullying, and phishing (Stabek et al., 2010). When text-based cybercrimes are orchestrated, the intention is a win-lose situation. The attacker must gain something such as money or access to personal information, which is effectively what the victim loses (Aftab et al., 2022). Often, these scams appear genuine, making it challenging for individuals to distinguish between legitimate and fraudulent communication.

Text-based cybercrimes represent a significant concern that is often downplayed in terms of its gravity. The pressing need for awareness arises from the firm and the increasing emergence of these deceptive practices, highlighting the importance of recognizing and addressing the prominence of such crimes.

In the ever-evolving domain of cybercrime, where perpetrators exploit the ease of online communication to carry out malicious activities, digital forensics readiness plays a pivotal role in mitigating the impact of these offenses.

2.2 Digital Forensics Readiness

Digital forensics readiness (DFR) refers to the proactive measures taken to prepare for and effectively respond to digital incidents, cybercrimes, and data breaches. It involves the development and implementation of policies, procedures, and technical capabilities to ensure that digital evidence can be collected, preserved, and

analysed in a forensically sound manner (Harbawi and Varol, 2016). Digital forensics readiness is essential in today's technology-driven world to minimize the impact of cyberattacks, enhance incident response, and support legal investigations. Cybercrimes are forever advancing, and the need for digital forensics readiness is a growing concern worldwide. The importance of Digital Forensics Readiness (DFR) cannot be overstated. Its significance lies not just in responding to incidents but in proactively preparing individuals and organizations to safeguard against the pervasive and ever-advancing nature of cybercrimes (Holt et al., 2022).

In the domain of digital forensics readiness (DFR), it's essential to stay one step ahead in the constantly evolving landscape of cyberattacks (Harbawi and Varol, 2016). To achieve this, embracing cutting-edge technology becomes imperative, and Natural Language Processing (NLP) emerges as a pivotal ally.

2.3 Natural Language Processing

Natural Language Processing (NLP) is a field of computer science and artificial intelligence that draws inspiration from human language to enable computers to understand, interpret, and generate it. NLP involves the development of algorithms and models that allow computers to process, analyse, and generate text and speech data in a meaningful and useful way (Chowdhary and Chowdhary, 2020). It leverages lexical and morphological analysis, syntax analysis, semantic analysis, discourse integration, and pragmatic analysis (Chowdhary and Chowdhary, 2020). This multi-faceted approach allows NLP systems to break down the text into individual words, analyse grammatical structure, extract meaning, consider context, and understand implied intentions, facilitating applications like machine translation, sentiment analysis, chatbots, and speech recognition, thereby bridging the gap between human communication and computer understanding. As NLP algorithms continue to evolve, they pave the way for innovative applications. The continuous progress in NLP points towards a future where human-computer interaction is characterised by a deeper understanding and more nuanced interpretation of language (Berger and Packard, 2022).

Within the dynamic field of NLP, a transformative breakthrough has been the emergence of Large Language Models. Large Language Models present a transformative dimension to how we address digital forensics readiness in the context of text-based cybercrimes by offering advanced text analysis insights from textual evidence and improving the identification of cybercrime patterns, ultimately strengthening the readiness and responsiveness to text-based cybercrimes.

2.4 Large Language Models

Large Language Models (LLMs) represent a significant milestone in the field of NLP and artificial intelligence, revolutionizing NLP tasks and applications. These models are meticulously pre-trained on massive datasets containing diverse text from the Internet (Petroni et al., 2019), allowing them to grasp the intricacies of syntax, semantics, and contextual relationships in language. The breakthroughs leading to the emergence of modern LLMs can be primarily attributed to the deep learning revolution with the introduction of neural network architectures. In 2018, models like Bidirectional Encoder Representations from Transformers (BERT) and Generative Pre-trained Transformer 2 (GPT-2) marked a turning point, showcasing the potential of large-scale, pre-trained neural language models. These models have profoundly impacted a wide range of fields, from chatbots and language translation to text generation and content understanding (Pal et al., 2023), demonstrating their versatility and potential to reshape how humans and machines interact with language.

The following section will provide an exploration of relevant literature in the field of cybercrimes and digital forensics readiness (DFR).

3. Related Literature

Table 1: Related Literature

Referenced literature	Summary of Contents	Evaluation	Conclusion
Ch et al. (2020)	Proposed a generalized framework for classifying cybercrimes, including text-based cybercrimes. The dataset was collected from Kaggle and CERT-In. Achieved 99% accuracy, outperforming some models. The ”others” category lacks specificity. Limited applicability to text-based cybercrimes.	The framework demonstrated high accuracy and outperformed some models, but its limited specificity and focus on Indian cybercrimes may affect its generalization to other countries.	The framework’s generalization for text-based cybercrimes is limited, and future work should focus on more specific categories.
Dinakar et al. (2011)	Introduced a system to recognize textual cyberbullying by scraping YouTube comments. Different labels were used, and models achieved up to 72.96% accuracy. Recognizing sarcasm remained a challenge.	The models showed promising accuracy, especially with specific features, but the challenge of recognizing sarcasm was acknowledged.	The importance of understanding text-based cybercrimes as a language and handling nuances like sarcasm is highlighted.
Janet et al. (2020)	Proposed a system to detect phishing using a balanced dataset of URLs. Achieved 96% accuracy using an ensemble model of CNN and LSTM.	The model’s accuracy was excellent compared to heuristic and list-based methods. LSTM’s data persistence was intelligently utilized for understanding context.	The combination of CNN and LSTM for phishing detection proved highly effective and could be applied in real-world scenarios.
Mahbub and Pardede (2018)	Introduced a system to detect online recruitment fraud through advertisements using the EMSCAD dataset. JRip rule-based classifier achieved the highest accuracy of 96%.	The dataset was relatively small, which may have limited the model’s diversity.	Versatility in the dataset is crucial for developing reliable models for text-based cybercrimes, considering the frequent occurrence and various types of such crimes.

4. Case Study: DFClaaS in Action - Cybercrime Investigation

Characters:

- Alice: A diligent user of the Digital Forensic Readiness Cybercrime as a Service (DFClaaS) system, employed at Bank A.
- Bob: An anonymous cybercriminal attempting to extort Bank A.

Incident: Cyberattack at Bank A
Background:

Bank A, a leading financial institution, faces a severe cyberattack attempt orchestrated by an anonymous threat actor, Bob. Bob demands a substantial sum of money, threatening to release sensitive customer data if the bank fails to comply. Bank A, equipped with DFClaaS, swiftly responds to counter the threat and launch a comprehensive investigation.

DFClaaS Services in Action:

1. Detection and Alert Service:

- As soon as Alice visits the suspicious website associated with the cyberattack attempt, the DFClaaS system activates.

- The system conducts real-time scanning, detecting red flags such as false promises, similarities to known scam websites, etc.
- An alert is triggered, and a pop-up message warns Alice about the potential cybercrime attempt, advising her not to provide personal or financial information.

2. Anonymous Cybercrime Reporting Service:

- Alice, a cybersecurity analyst at Bank A, utilises the anonymous reporting service to report the extortion incident without compromising her identity.
- The reported incident contributes valuable string data to build the DFClaaS database.

3. Reporting Cybercrime Service:

- The system collects reported data about the attempted attack.
- Natural Language Processing (NLP) and machine learning components parse, clean, and analyse the data to identify potential cybercrime patterns as well as generating an analysis report.

4. Cybercrime Text Scraping Service:

- To augment the cybercrime dataset, the system employs web data extraction, scraping relevant string data from external sources.

5. User Management Service:

- Bank A's cybersecurity team, including Alice, interacts with the DFClaaS system.
- The user management service facilitates secure actions, such as logging in, updating profiles, and accessing the DFClaaS system.

6. Visualisation Service:

- Authorised users, including cybersecurity analysts, visualise raw data to identify patterns and potential threats.
- The system's visualisation service enhances usability, enabling a comprehensive analysis of historical string data related to cybercrime language patterns.

7. Cybercrime Text-Data Training Service:

- Deep learning techniques, process the collected cybercrime text data.
- Feature extraction ensures an accurate representation, narrowing down potential cybercrime language triggers.

8. Cybercrime Semantic Builder Service:

- Utilising generated semantic string data, the system builds a cybercrime semantic database.
- Lexical-semantic analysis validates the cybercrime string, creating unique semantics crucial for forensic investigators.

Outcome:

Proactive Cyber Defense:

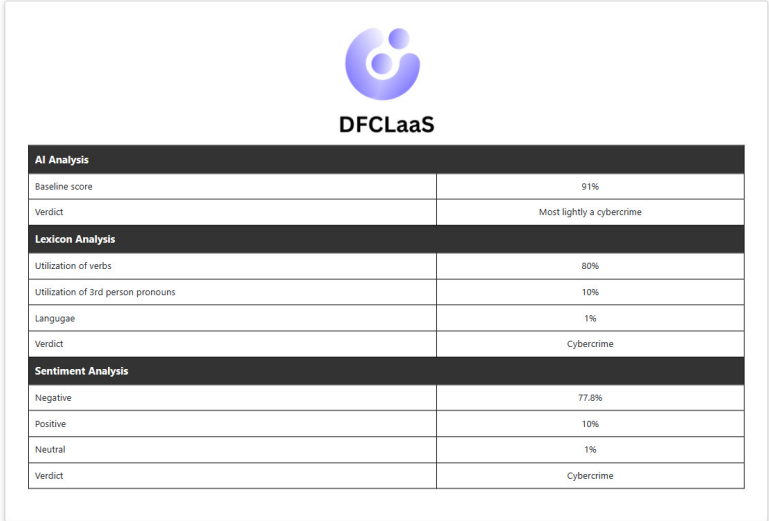
- Bank A's utilisation of DFClaaS ensures a proactive defence against cybercrime attempts.
- The collective services of the system contribute to the early detection, analysis, and prevention of cyber threats.

Secure Digital Forensics:

- DFClaaS provides Bank A with advanced tools for secure digital forensics.
- The system's integration of NLP and deep learning techniques enhances the investigation process, allowing for accurate threat assessment.

Collaborative Cybersecurity:

- The case exemplifies the collaborative nature of DFClaaS, where various services work in harmony to protect against cyber threats.
- Collaboration with a digital forensics investigator ensures a comprehensive analysis and potential legal action against the cybercriminal, Bob.



DFCLaaS

AI Analysis	
Baseline score	91%
Verdict	Most lightly a cybercrime
Lexicon Analysis	
Utilization of verbs	80%
Utilization of 3rd person pronouns	10%
Langugae	1%
Verdict	Cybercrime
Sentiment Analysis	
Negative	77.8%
Positive	10%
Neutral	1%
Verdict	Cybercrime

Figure 1: DFClaaS Analysis Report

In this incident, the DFClaaS system's Detection and Alert Service plays a crucial role in fortifyingBank A's cyber defences by providing real-time warnings and advice to users like Alice, ensuring a proactive response to potential cyber threats.

The next section will offer a proof of concept elaborating on the system's fundamental components and functionality.

5. Proof of Concept

The Proof-of-Concept section delves into the core elements of DFClaaS, shedding light on the crucial components that underpin its functionality. At its heart, DFClaaS is designed to understand and identify text-based cybercrimes. It employs advanced AI and Natural Language Processing (NLP) techniques to assess and analyze the language, lexicon, and sentiment associated with these crimes. In the following subtopics, we will explore the Cybercrime Data Training Service, Lexicon Analysis, and Sentiment Analysis, all of which work in synergy to strengthen DFClaaS's ability to detect and interpret cyber threats in textual content. These integral components are pivotal in digital forensics and cybersecurity, offering a multi-faceted approach to safeguarding users and aiding investigators in their mission.

5.1 Cybercrime Data Training Service

The core of DFClaaS lies in understanding text-based cybercrime in terms of identifying the crime and analyzing the lexicon and sentiment that make up such crimes, essentially the services that implement the various NLP techniques.

The Cybercrime Data Training Service plays a pivotal role in digital forensics and cybercrime detection. This service leverages advanced AI and NLP (Natural Language Processing) techniques to estimate the likelihood of a reported text being a cybercrime. This section delves into the core functionalities and construction of the Cybercrime Data Training Service.

The heart of this service is a meticulously constructed AI model that utilizes the Google BERT model and TensorFlow. The model is designed to process user-submitted reports and assess the probability of the text containing elements of a potential cybercrime. The model construction involves the following essential layers:

- **Input Layer:** The model begins with an input layer that accepts text data.
- **Preprocessing Layer:** The preprocessing layer is responsible for preparing and preprocessing the text data.
- **BERT Encoder:** We utilized the BERT (Bidirectional Encoder Representations from Transformers) model from TensorFlow Hub, a pre-trained language model designed for various natural language understanding tasks.
- **Output Layer:** The model outputs a probability indicating the likelihood of a potential cybercrime.

The Cybercrime Data Training Service serves as the initial line of defense in cybercrime detection. At the same time, Lexicon Analysis further bolsters DFClaaS by enabling the system to comprehend and identify the intricate language associated with cybercrimes within textual content.

5.2 Lexicon Analysis

Lexicon analysis is a critical pillar of the DFClaaS system, serving as a robust tool for identifying and comprehending language related to cybercrimes within textual content. At its core, this analysis hinges on a meticulously constructed lexicon, encompassing a broad spectrum of terms and their corresponding meanings associated with cybercrimes. This lexicon acts as a valuable resource, equipping DFClaaS with the knowledge necessary to detect and interpret the intricate language of cybercrimes.

When a user submits a report, the system initiates lexicon analysis. The attack text within the report transforms into numerical representations through word embeddings, utilizing the GloVe model. This numerical conversion empowers the system to handle the text data in a structured and quantifiable manner. Subsequently, the system employs similarity analysis, specifically using cosine similarity scores, to assess the likeness between the terms in the input text and those present in the lexicon. Higher similarity scores indicate a greater likelihood of cybercrime language in the report.

By recognizing and understanding the nuances of cybercrime language, the system enhances its ability to fulfill its role in the digital forensics and cybersecurity domains. This in-depth analysis equips DFClaaS with the tools required to protect users from cyber threats and offer valuable insights to investigators.

Building on this foundation, Lexicon Analysis equips DFClaaS with the knowledge to detect cybercrime language. Sentiment Analysis enhances the system's detection capabilities by assessing the emotional tone and context within reported content.

5.3 Sentiment Analysis

The DFClaaS system incorporates sentiment analysis to enhance the detection of text-based cybercrimes. Sentiment analysis assesses the emotional tone of reported content, focusing on identifying negativity, neutrality, and positivity. When a user submits a report, this feature comes into play, particularly in evaluating the possibility of a hate crime. DFClaaS combines a profanity checker with a sentiment analyser from the Natural Language Toolkit (NLTK) to achieve this.

The analysis process commences by screening the text for profanity or offensive language, recognizing these as potential indicators of malicious intent. However, the presence of profanity alone is not sufficient to conclude a hate crime. Context plays a crucial role in determining intent. Therefore, the sentiment analyser measures the emotional context within the content, examining negativity, neutrality, and positivity.

The DFClaaS system generates an aggregated score by combining these analyses, providing an indicator of the potential of a hate crime. For instance, high negativity and the presence of profanity lead to an increased likelihood of a hate crime, while a moderate score indicates a moderate likelihood. This approach offers a nuanced assessment that considers both the presence of concerning language and the context in which it is used. Sentiment analysis, thus, contributes to a more accurate and comprehensive detection of potential threats in digital crime.

The results of the different experimental models employed in identifying text-based cybercrimes are discussed in the following section.

6. Results

Before implementing the cybercrime data training service, we conducted experiments with four different models, LSTM autoencoder, Google Palm, Google BERT, and gzip text classification, to determine the most suitable model for identifying text-based cybercrime.

6.1 LSTM Autoencoder

The LSTM autoencoder was initially explored for the task. It was trained on a dataset that included cybercrime and non-cybercrime texts, focusing on anomaly detection. The model's ability to reconstruct input data was used to calculate averaged similarity scores on test data, leading to the determination of a threshold value for identifying anomalies in new attack texts. Unfortunately, the calculated threshold was a value of 269854234.8986, which turned out to be extremely high, considering the closer the value is to zero, the better the accuracy to be observed. This, therefore, indicates a low similarity between input and output texts.

Achieving better results would require a larger dataset and substantial computational resources (GPU and RAM), which were not readily available at the time of this study.

Google Palm was used to try to improve the performance of LSTM. However, this model struggled to process inputs containing inappropriate language, a significant characteristic of text-based cybercrime content. This limitation made the Google Palm model less suitable to achieve the set goals.

6.2 Google BERT

We explored the Google BERT model, known for its pre-training on a vast corpus of internet text data, allowing it to understand language structure and semantics. We fine-tuned the BERT model for the task of classifying attack text, generating a decimal value representing the likelihood of a cybercrime. Validation of the BERT model revealed promising results, with an accuracy rate of 93% and a minimal loss of 28%.

6.3 Gzip Text Classification

A further investigation of gzip text classification involves categorizing compressed text data into predefined classes based on content. The classifier was trained on a dedicated dataset and demonstrated an accuracy rate of 91% and a low loss of 9% when tested.

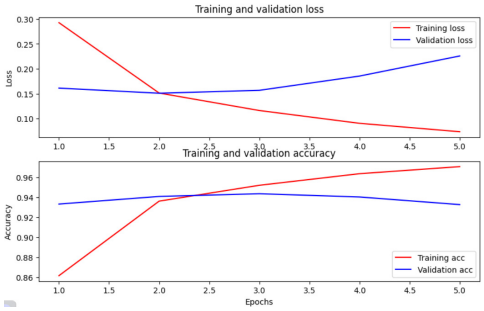


Figure 2: Plot of loss and accuracy during training and validation

These experiments informed the integration of the cybercrime data training service into the DFClaaS system, with the Google BERT model emerging as a key component in our efforts.

The following section will delve into the evaluation of the DFClaaS system.

7. Evaluation

This section delves into evaluating the different models considered for the DFClaaS system. While exploring and evaluating different models, the DFClaaS system ultimately adopted the Google BERT model. While the selection may seem influenced by the model's high accuracy, several key factors contributed to this decision.

Initially, the LSTM autoencoder appeared to be a promising choice. This model, designed for sequential data like text, boasts LSTM memory cells that can effectively store and retrieve information. This ability to remember and forget information is invaluable in capturing anomalous patterns, making it well-suited for identifying unusual events. Moreover, the model excels at automatically learning and extracting meaningful features from text sequences, enabling it to detect complex patterns and deviations. However, as experimentation proceeded, limitations became apparent. The model struggled when processing long text sequences, performed sequential processing leading to slow training, and demanded significant computational resources. In the evaluation process, the LSTM Autoencoder showed promise for capturing anomalous patterns and extracting meaningful features from text sequences but faced limitations in handling long sequences, leading to the choice of the Google BERT model with its bidirectional context understanding and computational efficiency within the DFClaaS system. The Google BERT model, built on the transformer architecture, emerged as a strong contender. This model offers parallel processing and incorporates attention mechanisms for efficient text analysis. It is characterised by its bidirectional context understanding, extensive pre-trained knowledge, fine-tuning capabilities, and computational efficiency. However, it's worth mentioning that the specific model developed exhibited a slight increase in loss and a slight decrease in accuracy during validation.

Transitioning from the Google BERT model, another noteworthy approach worth recognizing is the gzip text classification algorithm, which achieved high accuracy by directly analysing text content and optimizing text representation using efficient data compression techniques.

The gzip text classification algorithm deserves recognition for its ability to achieve high accuracy by directly analysing text content, bypassing the need for complex neural network architectures. This approach leverages efficient data compression techniques to optimize text representation, allowing the classifier to work efficiently with compressed data. While the gzip approach showcases the potential for high accuracy, it is essential to acknowledge the significance of understanding language, context, and semantics, particularly in the context of text-based cybercrimes. Ultimately, the decision to employ the Google BERT model in the DFClaaS system aligns with the pursuit of a balance between accuracy, computational efficiency, and contextual understanding.

The subsequent section will bring our discussion to a close, summarizing the key findings and insights.

8. Conclusion

In the face of rapidly evolving digital threats, particularly those perpetrated through textual means, the DFClaaS system emerges as a beacon of hope. Taking a meticulous and multifaceted approach, it delved into diverse text-based cybercrime identification models, wielding the potent tools of Natural Language Processing (NLP) for both lexicon and sentiment analysis. This comprehensive expedition paved the way for a robust system capable of parsing the insidious language of cybercrime with high accuracy.

However, the journey, while fruitful, is far from over. As we forge ahead, refinement beckons the opportunity to improve the chosen model, optimizing its precision and minimizing potential shortcomings. In doing so, DFClaaS will cement its position as a crucial bridge between efficient language processing and robust cybersecurity, safeguarding users in the face of cybercrime's omnipresent shadow. By deciphering the intricate nuances of this clandestine language, DFClaaS offers invaluable insights into the dark underbelly of digital crime, illuminating a path toward a safer digital domain for all.

References

Stacey Omeleze Baror, Richard Adeyemi Ikuesan, and Hein S Venter. Functional architectural design of a digital forensic readiness cybercrime language as a service. In *ECCWS 2023 22nd European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, 2023.

Rupa Ch, Thippa Reddy Gadekallu, Mustufa Haider Abidi, and Abdulrahman Al-Ahmari. Computational system to classify cyber crime offenses using machine learning. *Sustainability*, 12(10):4087, 2020.

Joel Chigada and Rujeko Madzinga. Cyberattacks and threats during covid-19: A systematic literature review. *South African Journal of Information Management*, 23(1):1–11, 2021.

KR1442 Chowdhary and KR Chowdhary. Natural language processing. *Fundamentals of artificial intelligence*, pages 603–649, 2020.

Karthik Dinakar, Roi Reichart, and Henry Lieberman. Modeling the detection of textual cyberbullying. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 5, pages 11–17, 2011.

Malek Harbawi and Asaf Varol. The role of digital forensics in combating cybercrimes. In *2016 4th International Symposium on Digital Forensic and Security (ISDFS)*, pages 138–142. IEEE, 2016.

B Janet, Srinivasulu Reddy, et al. Anti-phishing system using lstm and cnn. In *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pages 1–5. IEEE, 2020.

Syed Mahbub and Eric Pardede. Using contextual features for online recruitment fraud detection. 2018.

Andiwi Meifilina, M Umanailo, and Imam Fachruddin. Cybercrime cases impact the development of communication technology that is troubling society. *SCOPUS–Q3*, 8(9):1224–1228, 2019.

Fabio Petroni, Tim Rocktaschel, Patrick Lewis, Anton Bakhtin, Yuxiang Wu, Alexander H Miller, and Sebastian Riedel. ¨ Language models as knowledge bases? *arXiv preprint arXiv:1909.01066*, 2019.

Amber Stabek, Paul Watters, and Robert Layton. The seven scam types: mapping the terrain of cybercrime. In *2010 Second Cybercrime and Trustworthy Computing Workshop*, pages 41–51. IEEE, 2010.

Rana Mohtasham Aftab, Mariam Ijaz, Faisal Rehman, Ahmad Ashfaq, Hanan Sharif, Naveed Riaz, Shabbir Hussain, Muhammad Arslan, and Hadia Maqsood. A systematic review of the motivations of cyber-criminals and their attacking policies. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS), pages 1–6. IEEE, 2022.

Soumen Pal, Manojit Bhattacharya, Sang-Soo Lee, and Chiranjib Chakraborty. A domain-specific next-generation large language model (llm) or chatgpt is required for biomedical engineering and research. Annals of Biomedical Engineering, pages 1–4, 2023.

Jonah Berger and Grant Packard. Using natural language processing to understand people and culture. American Psychologist 77(4):525, 2022.

Thomas J Holt, Adam M Bossler, and Kathryn C Seigfried-Spellar. Cybercrime and digital forensics: An introduction. Routledge, 2022.