A Digital Forensic Readiness Cybercrime Semantic Trigger Process

Stacey O. Baror[1(✉)], Hein S. Venter[1], and Richard Adeyemi Ikuesan[2]

[1] Department of Computer Science, University of Pretoria, Hillcrest, South Africa
{stacey.baror,hventer}@cs.up.ac.za
[2] IT Department Science and Technology Division, Community College, Doha, Qatar
richard.ikuesan@ccq.edu.qa

Abstract. The recent wave of the global Covid-19 pandemic has led to a surge in text-based non-technical cybercrime attacks within the cyber ecosystem. Information about such cyber-attacks is often in unstructured text data and metadata, a rich source of evidence in a digital forensic investigation. However, such information is usually unavailable during a digital forensic investigation when dealing with the public cloud post-incident. Furthermore, digital investigators are challenged with extracting meaningful semantic content from the raw syntactic and unstructured data. It is partly due to the lack of a structured process for forensic data pre-processing when or if such information is identified. Thus, this study seeks to address the lack of a procedure or technique to extract semantic meaning from text data of a cybercrime attack that could be used as a digital forensic readiness semantics trigger in a cybercrime detection process. For the methodology to address the proposed approach, data science modelling and unsupervised machine learning are used to design a strategy. This method process extracts tokens of cybercrime text data, which are further used to develop an intelligent DFR semantic tool extractor based on natural language patterns from cybercrime text data. The proposed DFR cybercrime semantic trigger process when implemented could be used to create a digital forensic cybercrime language API for all digital forensic investigation systems or tools.

Keywords: Digital forensics · Cyber attack · Cybercrime · Semantic · Trigger · Cloud computing

1 Introduction

Text-based cyber crimes have seen a significant rise due to the reliance on text and document-related communications in carrying out daily transactions. Sentences and semantics in text-based messaging, such as texts, emails, or instant

Supported by DigiForS Research Group.

Y. H. Sheikh et al. (Eds.): AFRICOMM 2021, LNICST 443, pp. 319–339, 2022.
https://doi.org/10.1007/978-3-031-06374-9_21

messages, are often based on natural human languages. Therefore, to use the natural human language of communication to detect cybercrime, one would need first to understand how the language semantics work. Semantics, in this regard, is the study of meaning in human language [12,25]. In natural language processing (NLP), its purpose is derived at the sentence level, making it a viable tool for cybercrime study.

The concept of cybercrime is defined as "a form of criminal activity that involves the gathering of individual data and applications such as banking details, e-commerce applications, personal identifier information, or information on credit cards through unauthorised access, intending to commit a crime" [15]. For example, four main approaches for spreading spam messages on social media networks include: (i) setting up a fake account used explicitly for spreading spam messages, (ii) setting up a bot, (iii) setting up a cyborg and (vi) compromising accounts of users. Meanwhile, a significant portion of these cybercrime is text-based [5,6].

However, the fundamental problem is that there is no means to identify valuable cybercrime markers that employ the natural human language of communication while the crime is in progress. This limitation provides unrestrained for a cybercriminal, especially in a cloud-computing platform. Thus, this study seeks to address the lack of a process or technique to identify and extract semantic features of a text-based cybercrime attack capable of alerting an imminent cybercrime in progress. Therefore, the study proposes an approach that uses text-data message and language patterns as a digital forensic readiness process that extracts valuable semantics from text data of reported cybercrime and artefacts generated during a digital forensic investigation and incidents report document.

The methodology used to address this problem is (i) firstly, the study looks at language and its evolution. (ii) Secondly, the study examines semantic analysis techniques that employ data science modelling and unsupervised machine learning tasks. (iii) Thirdly, the use of existing digital forensic readiness processes, neural network model that focuses on deep autoencoder neural networks, topic modelling classification algorithm and feature engineering approaches. (iv) Finally, adopting the techniques in (i), (ii) and (iii), this study proposes a process that extracts variables of cybercrime text data as a fundamental input to design an integrated intelligent semantic tool that could use cybercrime text data. It further extrapolates the functionality of both logical and lexical semantics, using cybercrime text data as an input to design the proposed process, such that these two components are the essential contribution of this paper. The proposed digital forensic readiness process is evaluated by aligning it to ISO/IEC 27043, that is, existing digital forensic processes [28].

The remainder of this paper is structured as follows: The background literature Sect. 2 consists of the following: an overview of digital forensics and cybercrime. This is followed by a brief presentation of natural language processing (semantics) and unsupervised machine learning techniques. Section 4 outlines the motivation for this study, which then leads to introducing the

high-level overview of the proposed digital forensic readiness (DFR) process. Section 5 presents the discussion and how the proposed approach was evaluated, while the conclusion of knowledge discussed in this manuscript, as well as the future studies, are given in Sect. 6.

2 Background

The background section presents an overview domain knowledge of this study. It includes digital forensics, cloud computing, and cybercrime. Digital forensics is a subdomain within the forensic science discipline, saddled to identify (potential) digital evidence using scientifically derived and proven methods for legal (and sometimes to enhance security) purposes.

Potential digital evidence is electronic data that could alter or determine the flow of a significant decision in a criminal or civil case under investigation [8]. Ani-Narh and Williams [3], stated that digital evidence must be protected from virus, mechanical, and any other form of attack, whether malicious or accidental. Furthermore, a forensic investigator must demonstrate that a piece of evidence is not altered before, during or after evidence acquisition to enable its admissibility in court. Casey, [8] defines digital evidence as any data stored or transmitted using electronic devices that could support or refute the theory of how an offence occurred and further addresses the critical elements of the crime in terms of the intent and alibi. Hargreaves [11] on the other hand, defined digital evidence as reliable objects that can uphold or refute a hypothesis in legal or civil proceedings. That means, for the admissibility of digital evidence, data integrity must be proven to an acceptable degree of reliability.

However, in the uncertain time of Covid-19, document and text-data messages are among the primary sources used by cyber attackers to lure unsuspecting victims. Deception could be detected in any form of communication by analysing the textual messages using linguistic patterns, especially in a cloud computing platform or service. This type of investigation is known as cloud forensics. Zawoad [29] shows how clouds are not forensic friendly. When the virtual instance (virtual machine by extension) in a cloud environment terminates, data residing in it is lost because it is volatile [29]. Cloud service providers do not provide persistent storage to virtual machines. When the virtual machine is shut down, a rebooting occurs, or instances are deleted. All the information contained may be lost. For a post-incident investigation, such volatile data must be stored in persistent databases so that in the event of malicious activity or a user terminates the virtual machine, evidence of the activity could still be gathered. However, attempts to store all cloud instances for investigation purpose is practically infeasible as a storage size and potential network overhead could be voluminous. Furthermore, such logic would contradict the fundamental tenets of a cloud platform.

The current study, thus, proposes the use of forensic readiness and natural language processing (NLP) technique to provide a viable alternative to addressing some of these cloud forensics challenges. An NLP is “a theoretically motivated range of computational techniques for analysing and representing naturally

occurring texts at one or more levels of linguistic analysis to achieve human-like language processing for a range of tasks or applications" [27]. The overall purpose of NLP is to teach computers to understand human communication. Furthermore, using NLP techniques and defined digital forensic criteria for cybercrime reporting could contribute to the development of computer programs that can analyse human written language based on two primary roles, information retrieval and storage [27]. Furthermore, an NLP can be used to detect cybercrime by structuring large datasets. Using the NLP techniques, defined digital forensic criteria for cybercrime reporting was proposed by Baror et al. [5]. The proposed approach to address this fundamental cloud-forensics challenge is presented in the next section.

To ascertain the implementation feasibility of the process, tests with various devices and in various environments have been conducted [19]. For example, in mobile devices [22], the ISO/IEC27043 as shown in Fig. 1 was found to be effective, especially at the application of the concurrent processes. This process model is equally effective for digital forensic investigations carried out in a cloud environment, live forensics, and the postmortem type of digital forensic investigation.

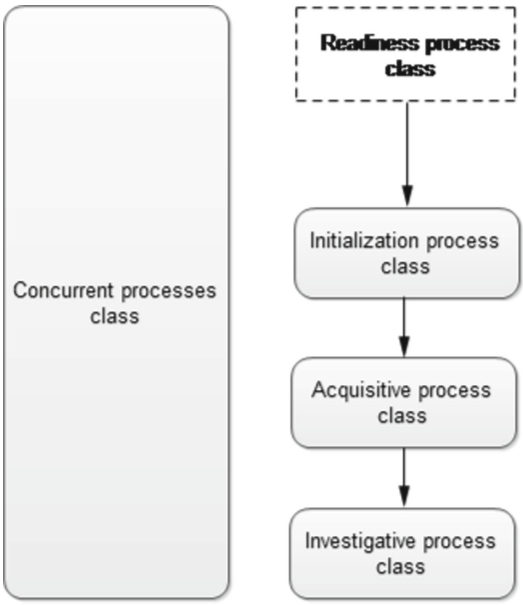

Fig. 1. ISO/IEC 27043 - the harmonised digital forensic process [28]

3 Previous Work

The current paper is a continuation of a series of papers focused on developing a digital forensic readiness (DFR) framework for public cloud computing based on natural human language capable of detecting and connecting cybercrime expediently to the offenders in a near-real-time approach in the public cloud.

This paper is a continuation of other previous work that is a series of research with its main objectives focusing on the speedy connection of cybercrime to a criminal in a near real-time manner. Firstly the authors looked at the current trajectory of cybercrime attack researches to identify that several solutions have been proposed or developed for cybercrime that is technical-based *(crimes requiring the attacker(s) possess)*. In line with their findings, the authors dived to highlight the need to also pay attention to cybercrime that requires little-to-no tech-savvy for the exploit to occur. To further bolster their argument, the authors developed a taxonomy of the most common cybercrime attacks in public cloud computing [6]. The paper's finding showed that cybercrime that is non-technical is much more on the rise, therefore the need to propose a digital forensic readiness approach to address this needs.

Following the paper [6] the authors further proposed and developed A natural human language framework for digital forensic readiness in the public cloud [4]. The paper leveraged natural human language as an identifier to develop a novel digital forensic readiness.

The last paper published on the series proposed a process platform that allows victims of cyber-attacks to report cybercrime incidents anonymously using a defined digital forensic cybercrime reporting process [5]. The process also added a secure, forensically sound storage process to store cybercrime data in a storage repository. The stored data serves as one of the data inputs used at the analysis phase of intelligent text-based cybercrime pattern identifier and trigger-based framework.

The following section presents the high-level view of the proposed digital forensic readiness cybercrime semantic trigger process, showing the components' relationships.

4 The Proposed Digital Forensic Readiness Cybercrime Semantic Trigger Process

Cybercrime text data collected from previously reported cybercrime incidents and text-data artefacts of reports from digital forensic investigation cases could be used as a baseline to identify, extract, and create a semantic trigger that could be used as knowledge-based for potential incident identification in a cloud platform and service environment. This paper, therefore, proposed a process that could achieve a cybercrime semantic digital forensic incident trigger using such a knowledge base. The proposed digital forensic readiness cybercrime semantic

trigger process is designed to continuously monitor, update, and recycle frequently used cybercrime text data in text-based cyberattacks, such as phishing, social engineering, and other non-technical cyber-attack ecosystems.

Cybercrime text data in the context of this research is a collective term used to describe text that might be involved with cybercrime activities coming from unstructured data sources, such as emails, SMSs, comments, customer feedback, a document of reported cyberattacks and document and other contents of the cybercrime-related text.

Firstly, a look at the high-level view of the proposition, which consists of six (6) steps—followed by a detailed discussion of each component of the six steps.

4.1 High-Level View of Digital Forensic Readiness Cybercrime Semantic Trigger Process

The proposed DFR cybercrime semantic trigger consists of the various components grouped into phases as shown in Fig. 2.

These include incident identifications and discovery, followed by exploring aspects of semantic analysis and how they can be used to design a digital forensic readiness process that uses existing cybercrime report test data, digital forensic investigations, text-data reports and artefacts as depicted in Fig. 2.

Phase I - Initialisations: The initialisation phase of the proposed process focuses on requesting the necessary authorisation required for data acquisition, application, and usage. This component of the DFR cybercrime semantic trigger process is likened to the initialisation process class of the ISO/IEC 27043 [28] as well as the requirements therein. The components of the initialisation phase consist of the following (i) Request cybercrime text-data use authorisation (ii) Employ obscurity of cybercrime text-data (iii) Apply named entity recognition to cybercrime text data obscurity. Each of these components are discussed in Sect. 4.2.

Phase II - Pre-acquisition and Acquisition: Potential digital crime text data could be identified, acquired and preserved in this Phase, ensuring the validity and requirements of the evidence admissibility and forensic soundness are maintained. The components of the pre-acquisition and acquisition are as followed: (i) Identify potential cybercrime text-data (ii) Cybercrime text-data preservation. (iii) Collect and acquire potential cybercrime text data from various sources. (iv) Validate acquired cybercrime context type (v) Populate cybercrime text-data. Each of which is to be discussion in Sect. 4.2.

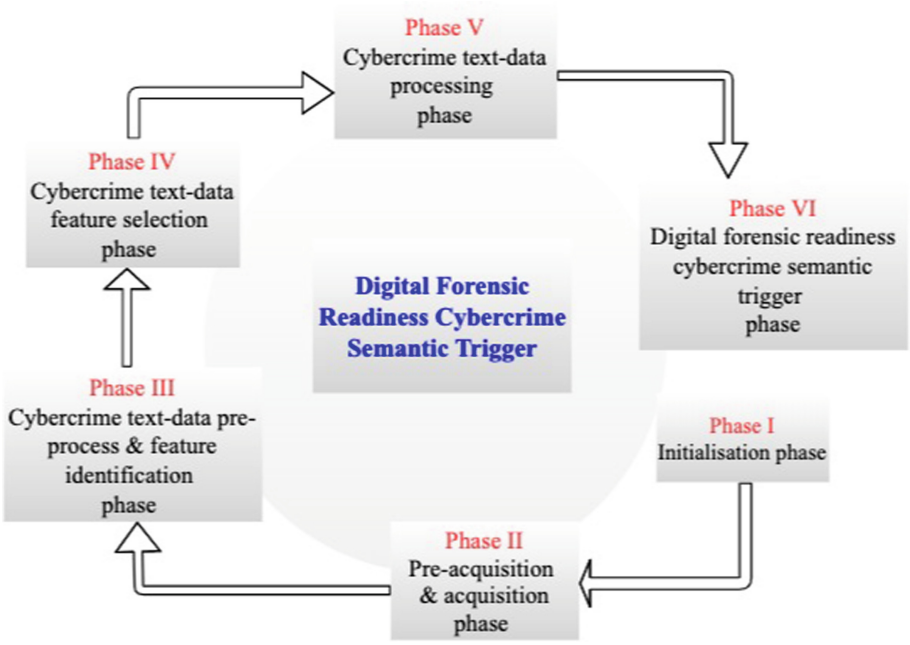

Fig. 2. The high level components of the proposed digital forensic readiness cybercrime semantics trigger process

Phase III - Cybercrime Text-Data Pre-Process and Feature Identification: The cybercrime text-data pre-process and feature identification takes a detailed look at the available text data and identifies the features with potentials. The process consists of eight (8) components as follows: (i) Cybercrime sentence segmentation (ii) Cybercrime text data dependency parsing (iii) Words tokenisation (iv) Predicting part of speech tagging (v) Cybercrime text data lemmatization (vi) Defined stop word filtration (vii) Cybercrime text-data named entity recognition tagging (viii) Co-reference text-data resolution mapping.

Phase IV - Cybercrime Text-Data Feature Selection: Phase IV of the DFR cybercrime semantic trigger process commences the process's basic feature and data analysis. The details of the components are to be discussed in Sect. 4.2 and are as follows: (i) Extract cybercrime text-data feature (ii) Clean extracted cybercrime text-data feature (iii) Capture text-data meaning (iv) Logical structure (v) Apply syntactic rule (grammar) (vi) Find context (vii) Identify relevant cybercrime semantic elements.

Phase V - Cybercrime Text-Data Processing: In data science text-data analysis is carried out during any text exploration [2,9]. The Phase V, that is, the cybercrime text-data process, applies the techniques used in data science to prepare text data to extract values and meaning that yield to a cybercrime (i)

Load cybercrime valid semantic elements (ii) training data set (iii) testing text data set. (iv) Embed ML model deep autoencoder (v) Learn extracted cybercrime semantic valid (vi) Compare and validate raw text-data set and testing text-data set.

Phase VI - Digital Forensic Readiness Semantic Trigger: The final Phase of the proposed cybercrime semantic trigger process is Phase IV. It takes input from all the other phases to create a cybercrime semantic API, such that when implemented, it could be called and be applied to any digital forensic environment, especially in the cloud domain. Phase VI consist of the following: (i) Search potential cybercrime contextual clue (ii) Cache DF potential cybercrime recurring semantic text (iii) Flag recurring cybercrime text (iv) Create DFR cybercrime semantics trigger (v) Call DFR semantic trigger API. The detailed discussions of each of these components is discussed in Sect. 4.2.

The next section discusses the details of each of the phases of the proposed DFR cybercrime semantic trigger process.

4.2 The Detailed Proposed Digital Forensic Readiness Cybercrime Semantic Trigger Process

This section will focus on describing in detail the various components of the DFR cybercrime semantic trigger as depicted in Fig. 3. First, the multiple features of the proposed process are displayed in a detailed view. Afterwards, the remainder of the section discusses Fig. 3. Each component is then described in detail and explains how the component contributes to the overall DFR semantic trigger process. Afterwards, the remainder of the section discusses Fig. 3. Each component is then described in detail and explains how the component contributes to the overall view of the DFR semantic trigger.

Phase I - Initialisations: In a digital forensic investigation, the initialisation phase consists of the various activities that must be carried out to prepare a digital data discovery process. For the proposed digital forensic readiness semantics trigger process as depicted in Fig. 3, the initialisation process starts the process that engineers the cybercrime data gathering and potential analysis process. The initialisation process comprises of the following (i) Request cybercrime data use authorisation, (ii) Employ obscurity to the cybercrime text-data, and (iii) Apply name entity recognition (NER) to the cybercrime text-data obscurity (see Fig. 3).

Request cybercrime text-data use authorisation. It is the process whereby data usage authorisation is requested and applied when such data is not readily available or in place to use the required cybercrime data. For example, the cybercrime data used for this study consists of cybercrime text data such as archived cybercrime data from government institutes and research centres. The content of the test data consists of email, fraud, phishing and miscellaneous, as given in **Here**.

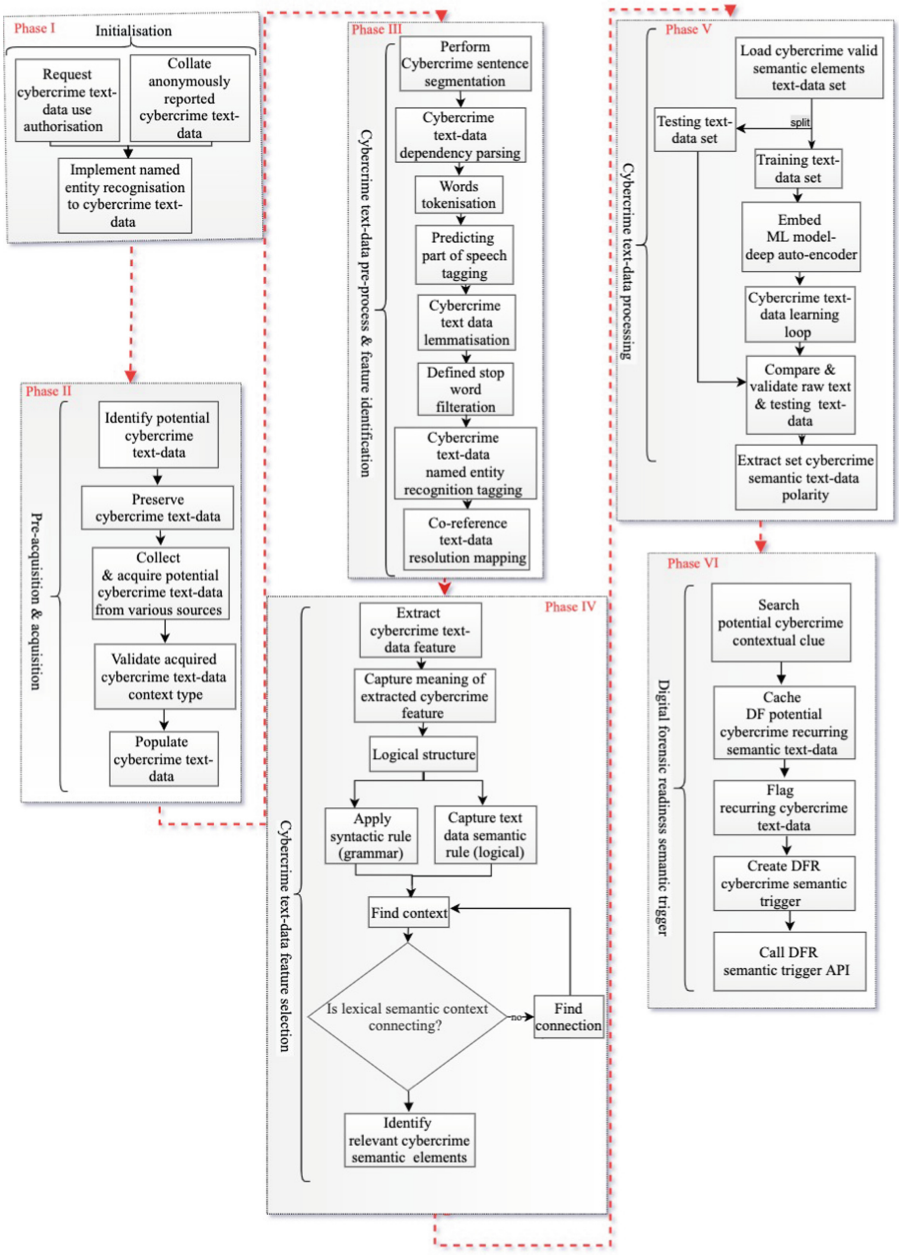

Fig. 3. The overview of the components of the proposed digital forensic readiness cybercrime semantics trigger process

Collate anonymously reported cybercrime text-data. The collate anonymously reported cybercrime text-data - makes use of available cybercrime text data and data generated by anonymous cybercrime reported by victim of cybercrime (as presented in a previous study [5]). This component is employed as input data to develop the proposed digital forensic readiness (DFR) semantics trigger process. Data inconspicuously must be ensured, and its anonymity to prevent a narrow output, thereby eliminating the challenges of potential false positives. The primary function of this component is to generate data, remove ambiguity, skewness of data, and provide clarity of the data set to satisfy the objectivity of the proposed tool.

Implement named entity recognition to cybercrime text-data. The implement named entity recognition (NER) to cybercrime text-data component at the initialisation level of the proposed process is a semi-application of extraction of predefined categories that sub-task the information text-data collected for the analysis. The named entity recognition otherwise locates and classifies unstructured data entities to describe the various types within the data set. The NER is a technique used to identify, tag, and extract representative information that can reveal relevant subjects/nouns within a text.

Phase II - Pre-acquisition & Acquisition: As depicted in Fig. 3, the pre-acquisition and acquisition phase of the digital forensic readiness semantic trigger process consists of four (4) components that collaborate to achieve the goal of text-data acquisition.

Identify potential cybercrime text-data. For the proposed DFR semantic trigger, the data is anticipated to originate from everyday users of the public cloud products, digital forensic investigator's or DF practitioner artefacts. The DF practitioner artefacts that are obtained from a digital forensic report could be in any of three ways - 'technical', 'investigative' or 'evaluative', reporting style, where each reporting type maintains a specific purpose and interpretative context, determined by the examination document [13]. Identifying potential cybercrime text data is the process of filtering the available cybercrime text data that could be useful for developing the proposed DFR semantic trigger. The identified text data must contain elements of past cybercrime or artefacts used to identify cybercrime, especially during a digital forensic investigation. For example, when an individual or a corporation report a cybercrime incident to an authority, during such reports, there are commonly peculiar 'words' and 'phrases' that predominantly occur in the input cybercrime document. These are predominantly words or phrases that focus on this section and are identified at this level of the DFR semantic process.

Cybercrime text-data preservation. The typical 'words' and 'phrases' that predominantly occur in such documents, as identified in the previous Subsect. 4.2, are preserved to be valid potential digital evidence. Although the document's

content is not in itself 'evidence' at this level, however, due to the several requirements of digital forensics, such as chain of evidence and forensic soundness, this preservation process is essential to retain the validity of the process. Forensic soundness must be ensured in the various components of the DFR semantic trigger process. In this Phase, header information about the identified words or phrases is used and preserved to ensure validity.

Collect & acquired potential cybercrime text-data from various sources. For this study, cybercrime text data utilised are collected and acquired from the following **Here**. The content of the cybercrime data include email, fraud, phishing and miscellaneous text data. Once the valuable content of the cybercrime text data has been identified and preserved, the Next Phase of the DFR semantic trigger process is collecting and acquiring the potential evidence that could be used in the process. The cybercrime text-data collection process of the DFR trigger process employs the rule of evidence [22,28], a chain of evidence and forensic soundness during this Phase.

Validate acquired cybercrime context type. The collected cybercrime text data are assembled for validation that ascertains that the collected text data can create valid semantics data capable of generating a digital forensic readiness cybercrime semantic trigger process. This process is essential to meet the requirements of digital evidence validity as presented by the ISO/IEC 27043 [22,28].

Populate cybercrime text-data. The next step for the DFR semantic trigger process is to populate the cybercrime data that must undergo the various functions of Phase I and II before commencing Phase III. At this stage, the cybercrime data has employed the default [22,28] phases of the digital forensic process of potential evidence validation, as well as the application of acceptable rules of evidence and chain of evidence process. Adding these processes ensures that the cybercrime text-data, while still in its raw state, satisfies the digital forensic investigations processes as prescribed in the ISO/IEC 27043 [22,28].

Phase III - Cybercrime Text-Data Pre-process & Feature Identification: As depicted in Fig. 3, the cybercrime text-data pre-process and pre-feature selection phase of the digital forensic semantic (DFR) semantic trigger process comprises several sub-processes. These are further explained.

Perform cybercrime sentence segmentation. Sentence segmentation is an NLP process that involves dividing and separating strings in a written sentence of a language into components. In English, for example, punctuation marks and spaces such as question marks, exclamation marks or the full stop/period character are some of the appropriate means to convey the emotion or tone of a sentence [24]. The cybercrime sentence segmentation tokenises the sentences by splitting the cybercrime text data using an appropriate separator.

Cybercrime text-data dependency parsing. The Cybercrime text-document dependency parsing is a syntactic structure consisting of relations between words illustrated using binary asymmetric to examine the relationship dependencies between the words in a sentence. This is to analyse the text document's grammatical structure fed into the proposed DFR semantic trigger process. Based on the identified relationship between the words, a sentence is then broken into several components of words. The dependency mechanism is then based on the concept that there is a direct link between every linguistic unit of a sentence.

Word tokenisation. Word tokenisation allows the splitting of a string, text into a list of tokens [24]. One can think of a token as parts like a word in a sentence, and a sentence is a token in a paragraph. The proposed DFR semantic trigger process converts the cybercrime text into a sentence token, then sentences into a words token using regular expressions tokenisation. The outputs from this process are further labelled to reflect the predefined classes.

Predicting part of speech tagging. This component of the DFR semantic trigger process enables the label assigned to the token (addressed in Sect. 4.2) of the cybercrime text corpus to indicate the part of speech and grammatical categories of tense, plural or singular. The part of speech tags is then used to search the corpus of the cybercrime text-data analysis.

Cybercrime text-data lemmatisation. The technique employed by the DFR cybercrime semantic trigger process to remove the suffix while returning the actual word of the language of a text document [16,23]. The purpose of lemmatisation is to obtain the exact valid words in the corpus of the cybercrime text data used to create the proposed digital forensic semantic trigger process. For example, plays, playing, played are all forms of the word 'play', such that play is the lemma common root.

Define stop word filtration. The defined stop words filtration applied to the proposed DFR cybercrime semantic trigger process is the process that riddles and sieves the collected cybercrime text data before the analysing commences. 'stop words' typically refer to the most common words used in the text any language in natural language processing. However, each NLP tool must define these 'stop words' because a universal list may create a false positive in case A and a different outcome in case B.

Tagging cybercrime text-data NER. This step tags and extracts information classified as a named entity mentioned in the cybercrime text-data document, inputting from previous steps. The cybercrime text-data tag focuses on extracting the specified predefined NER categories after the stop word filtration definitions. The NER categories entities, such as a person's name, an organisation, a place or location, time expressions, identity numbers, or monetary values, to be used for the DFR cybercrime semantic trigger process creation.

Co-reference text-data resolution mapping. Finally, this step attempts to apply coreference resolution of the tagged cybercrime text data. For Phase III: i.e., the cybercrime text-data pre-process and pre-feature selection shown in Fig. 3. In NLP, the goal of the coreference resolution system is to output all the coreference chains of a given text, which often relies on common sense reasoning [10,14]. Thus, for this study, the coreference cybercrime text-data resolution mapping helps the DFR semantic trigger process to understand and know who/what a particular text component is referring to in any given document [10,17]. This component of the DFR semantic trigger process must identify the 'referring expressions' and the discourse entity called the 'referent'.

Phase IV - Cybercrime Text-Data Feature Selection: As depicted in Fig. 3, the cybercrime text-data feature selection phase of the DFR semantic trigger process is focused on the feature selection process of the potential semantic text data that could be employed in the design of the proposed DFR process.

Extract cybercrime text-data feature. Feature engineering is where domain knowledge of used extract characteristics, properties, attributes from raw data is extracted [21]. As depicted in Fig. 3 extracting meaning features from a cybercrime text-data document is dependent on the language context, which gives clues as to the meaning of words and the relationship between the words in the text document to be analysed. The feature extraction of the DFR semantic trigger process further identifies the inferred meaning of the document content and uses this to logically create the semantic tokens that are then the basis for the proposed DFR semantic trigger design. For this study, the semantic feature extraction model employs both keyword and entity extraction rapped in the information security triad, which engineers the validity of any potential digital evidence that delivers forensic soundness.

Capture text-data meaning. This step is focused on the identification of the cybercrime text in a document. The text is processed into a normalised database suitable for analysis that could accept the machine learning techniques. As depicted in Fig. 3, the text-data feature selection should identify semantic meaning following the logical structure of NLP such that both the syntactic and semantic rule.

Logical structure. For the proposed DFR semantic trigger process, logically analysing the cybercrime text-data document is carried out in a hierarchical approach. It could determine the relationship between the various parts of the document. This step aid the cybercrime text-data document scan process create the required components for the next Phase of the process.

Apply syntactic rule (grammar). The syntactic rule (i.e., grammar rule) as employed in this process is a feature selection process focused on how a group of words are ordered to make sense, such that the sentence follows the excellent

rule of the language. For example, a sentence starts with a subject followed by a predicate (which could be a verb). There must also be an object to complement the subject and the predicate. This simple process is what makes any group of words communicate meaning. As depicted in Fig. 3, the application of a syntactic rule to the available text data is to minimise the false positives during semantic analysis. Once the syntactic ambiguities of the grammar are resolved, the meaning is then uniquely represented in logical form.

Capture text-data semantic rule (logical). The capture text-data semantic rule is focused on the logical meaning of a document. The agreeable rules of communications, whether abbreviation or in full details, the logical semantic rule plays a vital part in bringing the concepts of creating the DFR semantic trigger process. To capture the meaning of the extracted features of the cybercrime text-data collected from various sources as discussed in Sect. 4.2, the use of a lexicon and syntactic structures parse in a logical semantic meaning extraction is necessary, which is achieved in this component of the proposed process. As such, the meaning of objects, events, quantifiers, modifiers and determiners in the sense of a bag of words must be determined to enable us to build a valid semantic [4]. Using the first-order predicate that includes unary, binary, and n-ary predicates and the lambda calculus, the semantic information is transmitted in a case of grammar represented as a predicate.

Find context & connection. The various data sources extracted using the combination of data science approach and natural language processing that embeds the digital forensic triage [21], as presented in Sect. 4.2 has undergone the various stages of digital forensic soundness, chain of custody and rule of evidence. This fulfils the legal regulation of the interaction and implementation of fundamental rules in the national legislation of information extraction and exchange as discussed in Sect. 4.2. Therefore, the text data that has gone through the digital forensic Phase (forensic soundness check), analytic data phase (data mining, extraction, and cleaning) and the application of natural language processing technique (semantic and syntactic presentation). The next step is to use the available text data to find cybercrime contexts and connections of the document data, such that the context and relationships become the basis of validity to be used in a digital forensic readiness semantic trigger creation.

Identify relevant cybercrime semantic elements. Identifying the relevant content of the collected and cleaned text data is to assemble potential valid semantic input that could commence the cybercrime semantic building process. This process required the application of the semantic classification model, that is, (i) topic classification (ii) sentimental analysis and (iii) Intent classification to fully implement the semantic analysis that will generate the input data for the semantic builder, which in turn creates the digital forensic readiness semantic trigger process.

Phase V - Cybercrime Text-Data Processing: As depicted in Fig. 3, the cybercrime text-data processing phase of the digital forensic readiness (DFR) semantic trigger process is focused on the cybercrime data processing aspects, the various components of this phase as depicted in Fig. 3 are discussed next section

Load cybercrime valid semantic elements text-data set. In phase 4.2 (Fig. 3), the semantic feature selection and elements prepared the cybercrime text-data to be loaded in to commence the actual cybercrime data processing of the DFR semantic trigger process. The load cybercrime valid semantic elements text-data set is an input stage of the DFR process, the data at this Phase is split in two, that is, the training and testing data set and a subset to test the trained model.

Training and testing data-set. The task is to study cybercrime text data and feed the data to a created DFR semantic trigger process. The cleaned cybercrime text data is separated into training and testing datasets. The training dataset consists of unlabelled text data to be used to train the DFR semantic trigger process, and the testing dataset labels evaluates the performance of the process with the unseen data at Sect. 4.2. The entire DFR cybercrime semantic trigger process is to learn from the collected cybercrime data and make predictions on the data. To carry out data-driven predictions or decisions, it builds a mathematical model from input data. Data introduced into the model for training and prediction must be split into two—the training dataset and the testing dataset. Therefore, the testing data set is a subset to test the trained model and its original state. Its sole purpose is to compare the trained and the raw data to identify if changes in the output are noticeable.

Embed ML model - deep auto-encoder. The deep auto-encoder machine learning (ML) model is used in the experiment stage of the proposed DFR semantic trigger process. However, the proposed approach is designed as a generic model, such that any approach that uses word embedding word2vec and doc2vec could be employed to achieve this same goal [20]. To test the proposed DFR semantic trigger process, the Tensorflow and Keras Python library is employed. TensorFlow is an end-to-end open-source platform for machine learning to create large-scale neural networks with many layers, used for ML problems such as classification, perception, understanding, discovering, prediction and creation. Tensorflow provides workflows with high-level APIs. It is a comprehensive and flexible ecosystem of tools, libraries and other resources that give the workflows high-level APIs. It offers various concepts to be chosen when building and deploying machine learning models. On the other hand, Keras is a high-level neural networks library running on the top of TensorFlow, CNTK, and Theano. Using Keras in deep learning allows for easy and fast prototyping as well as running.

Data set learning. The learning of the text data inserted into the model is a continuous process to increase the accuracy. The extraction process is carried out

using the SQL Server integration services (SSIS) platform to create the extract-transform-load (ETL) package that extracts the text data. The data is stored in the NT Microsoft SQL Server database, and the SQL Server Management Studio is used to query the tables in the database. The cybercrime report text data from the victims and the artefact of digital forensic reports available on various cybercrime research data repositories are merged to get the desired dataset exported to a flat file. The flat file is then loaded into Python to analyse further, extract, and build the cybercrime semantic trigger.

Compare & validate raw text & testing text-data. The compare and validate raw and test text-data measures the predictive abilities of the deep auto-encoder machine-learning model as used in this case too is essential for establishing the practical usability of the proposed framework in a real-world scenario [7]. Therefore, one of the critical phases of the DFR semantic trigger process modelling process is the compare and validation phase. The trained model is evaluated using the raw cybercrime text data as received manual audit assessments. This testing data consisted of the cybercrime text data of victims reports and available final reports of digital forensic investigators in past cases. To validate the proposed process, the testing text dataset is compared to the training dataset, split before the training dataset is fed into the embed ML model, which reconstructs the output data.

Extract & set cybercrime semantic text-data polarity. The set cybercrime semantic text-data polarity is used to produce a reconstruction error for every potential cybercrime text fed into the model using a confusion matrix. The potential cybercrime value that resulted in reconstruction errors above the threshold were coded with '1' for a known text that has occurred in a previously reported crime or fraudulent activities, whilst the model returns a result in reconstruction errors below or equal to the threshold coded as '0' for unknown or new occurring semantic—using the confusion matrix to measure the recall, precision and accuracy. The confusion matrix is a performance classifier metric used to measure the performance of the classification models on the testing data [1].

Phase VI - Digital Forensic Readiness Semantic Trigger: The components of this phase is further explained in the following subsections.

Search potential cybercrime contextual clue. The search potential cybercrime contextual clue is when the DFR cybercrime semantic trigger process uses text to find clues about the crime content of a given text data. It derives a valid cybercrime ontology in line with the context of the surrounding bags of words with the help of both semantic clues and syntactic clues [26]. This takes input from Sect. 4.2. The component is focused on gathering the cybercrime semantics using context, ontology and taxonomy [4,18].

Cache DF potential cybercrime recurring semantic text. The cache digital forensic potential cybercrime recurring semantic text holds (i.e., temporal store) the searched and available semantic contextual clue, such that data request is faster when an API call in Sect. 4.2 is required. The purpose of the proposed DFR cybercrime semantic is to make available a flexible method for cybercrime text data to activate cybercrime incident detection. Having a cache location in-built as part of the process increases the speed of fetching and publishing architecture as in the software development context of the DFR cybercrime semantics trigger builder.

Flag recurring cybercrime text. The recurring flag text in a group of searched and cached cybercrime text. It is used to notify, as well as alert the DFR semantic trigger of available traces left by a previous attacker that has recurred in the present circumstances, and therefore the need to resume the semantic trigger process by either activating the identified new text to a semantic cache or adding or to store it as a recurring cybercrime text to a semantic database. (Semantic database and how it plays in the storage of cybercrime semantics was presented and discussed in a previous paper [5].)

Create DFR semantic trigger. The create DFR semantic trigger is the process that uses the input received by all the components to create an incident alert process that monitors and continuously provides comprehensive coverage of the cloud computing domain. The semantic trigger is designed to identify and differentiate between minor and major events and appropriately escalate these events to a state where the identified semantics are stored as input processes that generate the required text-data similarities and frequency check. This outcome of this component served as input to the next step and used all other outputs of the various components to create the semantic trigger.

Call DFR semantics trigger API. Generically in software development, programmable application interfaces (APIs) form protocols to develop software and models. The goal of designing and proposing the digital forensic readiness cybercrime semantic trigger is to eventually arrive at a situation where the cybercrime semantic is developed as an API call and implemented in any digital forensic tool or application or a cyber-attack incident detection system. The proposed concept is to make available APIs, such as local API for intrusion detection and a trigger component API, a web-based API that could be integrated by an organisation or in a private cloud scenario to identify potential threats in a near-real-time approach a possible program level API. In summary, the DFR semantics trigger API should be accessible and acceptable to any technology and implement a digital forensic machine learning model.

5 Discussion and Evaluation

In the era of COVID-19, there have been several cybercrime incidents when cyber attackers lured their victims via a text or document message into acting. The cyber attacker's usual modus operandi is to persuade an unsuspected user to unknowingly gives the cyber attacker access to the user's personal/private information that could lead to the intended cybercrime, such as information stealing impersonation or identity theft. Mitigate the consequences of cybercrime, enhancing cybersecurity, and an alert triggered based on semantics and the unique language identification formation of the users. The trigger is based on collecting and analysing data from reports of previous cybercrime (cybercrime historical data). Or corpus of data from a document of digital forensic investigator's report of various former incidents where expert witness's report was provided to a court of law (see detail cybercrime report process in [5] or other detection alerts when cybercrime is in progress (language being the main trigger). With the growth of cybercrime in the public cloud, the need has arisen for a streamlined method of processing historical attack data to create a means of identifying possible threats by semantic evaluation. The proposed solution is robust and available as an application programming interface (API) to process communications from multiple third parties and public cloud software as service users.

The study observed that a digital forensic readiness process (DFR) for cybercrime semantics identification could be further developed as a reliable DFR semantic trigger process when the proposed techniques are applied to a benchmarked cybercrime text-data repository. The extracted semantic data could identify cybercrime offenders based on their historical text data usage and real-time interaction with other users in the public cloud environment.

The proposed DFR cybercrime semantic trigger process consists of six (6) Phases that employs the domain knowledge of natural language processing, machine learning and cybercrime feature extractions to create a digital forensic readiness tool that addresses incident detection. Phase I is the initialisation part that deals with the administrative processes of adhering to authorities and data obscurity. Phase II addresses the pre-acquisition and acquisition aspects of the process. Both the initialisation (Phase I) and acquisition (Phase II) of the proposed DFR cybercrime semantic trigger process aligns with the digital forensic process [28], thereby abiding by the ISO/IEC 27043 international standard. Furthermore, Phase III and IV, that is, the cybercrime text-data pre-process and pre-feature selection and the cybercrime text-data feature selection phases, accepts the inputs of the digital forensic processes (see Fig. 3) that ascertain the forensic soundness of the cybercrime text-data to be used for the semantic analysis. Phase III and IV consist of 18 components that employ the context of natural language processing techniques, featuring extraction to develop this section of the proposed DFR cybercrime semantic process. Phase V then applies the machine learning techniques to the output of NLP as an input. The entire process then feeds to Phase VI, which shows the incident trigger part of the process. The study attempted to propose a digital forensic readiness cybercrime

semantic trigger process based on exploring and applying a corpus of data. The proposed system employs a methodology that combines data science modelling, recurrent neural networks, neural network language model (NNLM) and machine learning that also allows the use of feature engineering extraction as an agent to extract the variables of cybercrime. Furthermore, the presented DFR cybercrime semantic trigger with sufficient text data could analyse the data sets for accurate assumptions that account for context using the frequency of text appearance, the polarity of the sentences, and the semantic information provided. Cybercrime taxonomy, ontology, tags, and artefacts extract relevant and valuable information from large bodies of unstructured data and identify and remove the indicators that could negatively infect the content of the cybercrime data, for example, 'word stoppers' described in Phase III of the proposed process.

This paper is focused on proposing a digital forensic readiness process that employs digital forensic processing to create a semantic trigger using NLP and machine learning techniques. However, the drawback of this paper at its current state is that the testing is not present and not shown. Implementing a use case showing the proposed process output is part of future work that will focus on the machine learning precision and accuracy during its real-World testing.

6 Conclusion

In summary, the paper proposed a digital forensic readiness cybercrime semantic trigger process that pulled resources of the domain knowledge from natural language processing, data sciences and machine learning to embed in historical cybercrime text data to achieve a digital forensic readiness. The overall aim is to mitigate and identify cybercrime incidents in near real-time in the cloud computing environment by using text data extracted to formulate a natural language semantic patterns as an identifier and a trigger. The process addresses one of the underlying challenges of cybercrime incident detection while introducing a digital forensic methodology.

References

1. Kulkarni, A., Chong, D., Batarseh, F.A.: Foundations of data imbalance and solutions for a data democracy. In: Batarseh, F.A., Yang, R. (eds.) Data Democracy, pp. 83–106. Academic Press (2020). https://doi.org/10.1016/B978-0-12-818366-3.00005-8
2. Allen, T.T., Sui, Z., Akbari, K.: Exploratory text data analysis for quality hypothesis generation. Qual. Eng. **30**(4), 701–712 (2018)
3. Ami-Narh, J.T., Williams, P.A.: Digital forensics and the legal system: a dilemma of our times (2008)
4. Baror, S.O., Venter, H.S., Adeyemi, R.: A natural human language framework for digital forensic readiness in the public cloud. Aust. J. Forensic Sci. **53**(5), 566–591 (2021)
5. Baror, S.O., Ikuesan, R.A., Venter, H.S.: A defined digital forensic criteria for cybercrime reporting. In: International Conference on Cyber Warfare and Security, pp. 617–XVIII. Academic Conferences International Limited (2020)

6. Baror, S.O., Venter, H.: A taxonomy for cybercrime attack in the public cloud. In: International Conference on Cyber Warfare and Security, pp. 505–X. Academic Conferences International Limited (2019)
7. Bauder, R., Herland, M., Khoshgoftaar, T.: Evaluating model predictive performance: a medicare fraud detection case study, pp. 9–14 (2019). https://doi.org/10.1109/IRI.2019.00016
8. Casey, E.: Digital evidence and computer crime: forensic science, computers, and the internet. Academic Press (2011)
9. Cekik, R., Uysal, A.K.: A novel filter feature selection method using rough set for short text data. Expert Syst. Appl. **160**, 113691 (2020)
10. Ferreira Cruz, A., Rocha, G., Lopes Cardoso, H.: Coreference resolution: toward end-to-end and cross-lingual systems. Information **11**(2), 74 (2020)
11. Hargreaves, C.J., Solomon, S.H.: Assessing the reliability of digital evidence from live investigations involving encryption. Ph.D thesis, Deportment of Informatics and Sensors, Cranfield University, UK (2009)
12. Hofmann, T.: Realms of meaning: an introduction to semantics. Routledge (2015)
13. Horsman, G.: The different types of reports produced in digital forensic investigations. Sci. Justice **61**(5), 627–634 (2021). https://doi.org/10.1016/j.scijus.2021.06.009
14. Huoranszki, F.: Common sense and the theory of human behaviour. Philos. Q. **52**(209), 526–543 (2002)
15. Ivan, I., Milodin, D., Sbora, C.: Non security–premise of cybercrime. Theor. Appl. Econ. **19**(4), 59–78 (2012)
16. Jongejan, B., Dalianis, H.: Automatic training of lemmatization rules that handle morphological changes in pre-, in-and suffixes alike. In: Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP, pp. 145–153 (2009)
17. Jurafsky, D., Martin, J.H.: Speech and language processing (draft). Chapter A: Hidden Markov Models (Draft of 11 Sep. 2018). Retrieved 19 March 2019 (2018)
18. Kebande, V.R., Karie, N.M., Ikuesan, R.A., Venter, H.S.: Ontology-driven perspective of CFRaaS. Wiley Interdiscip. Rev. Forensic Sci. **2**(5), e1372 (2020)
19. Lagrasse, M., Singh, A., Munkhondya, H., Ikuesan, A., Venter, H.: Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism. In: Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS, pp. 296–305 (2020)
20. Ma, L., Zhang, Y.: Using word2vec to process big text data. In: 2015 IEEE International Conference on Big Data (Big Data), pp. 2895–2897. IEEE (2015)
21. McClelland, D., Marturana, F.: A digital forensics triage methodology based on feature manipulation techniques. In: 2014 IEEE International Conference on Communications Workshops (ICC), pp. 676–681. IEEE (2014)
22. Omeleze, S., Venter, H.S.: Testing the harmonised digital forensic investigation process model-using an android mobile phone. In: 2013 Information Security for South Africa, pp. 1–8. IEEE (2013)
23. Plisson, J., Lavrac, N., Mladenic, D., et al.: A rule based approach to word lemmatization. In: Proceedings of IS. vol. 3, pp. 83–86 (2004)
24. Popel, M., Žabokrtský, Z.: TectoMT: modular NLP framework. In: Loftsson, H., Rögnvaldsson, E., Helgadóttir, S. (eds.) NLP 2010. LNCS (LNAI), vol. 6233, pp. 293–304. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14770-8_33
25. Riemer, N.: Introducing Semantics. Cambridge University Press, Cambridge (2010)

26. Sinatra, R., Dowd, C.A.: Using syntactic and semantic clues to learn vocabulary. J. Read. **35**(3), 224–229 (1991)
27. Strawson, P.: Subject and Predicate in Logic and Grammar. Routledge (2017). https://doi.org/10.4324/9781315242132
28. Valjarević, A., Venter, H., Petrović, R.: ISO/IEC 27043:2015–role and application. In: 2016 24th Telecommunications Forum (TELFOR), pp. 1–4. IEEE (2016)
29. Zawoad, S., Dutta, A.K., Hasan, R.: Towards building forensics enabled cloud through secure logging-as-a-service. IEEE Trans. Dependable Secure Comput. **13**(2), 148–162 (2016). https://doi.org/10.1109/TDSC.2015.2482484