International Journal of Information Technology
https://doi.org/10.1007/s41870-024-02077-5

ORIGINAL RESEARCH

LSTM and BERT based transformers models for cyber threat intelligence for intent identification of social media platforms exploitation from darknet forums

Kanti Singh Sangher[1] · Archana Singh[1] · Hari Mohan Pandey[2]

Received: 22 April 2024 / Accepted: 9 July 2024

Abstract

Cybercriminals, terrorists, political activists, whistleblowers, and others are drawn to the darknet market and its use for illicit purposes. Various methods are employed to identify the people who are behind these identities and websites. Since DNMs are more recent than other platforms, there are more unexplored research possibilities in this field. Research has been done to identify the buying and selling of products connected to hacking from Darknet Marketplaces, the promotion of cyber threats in hacker's forums and DNMs, and the supply chain elements of content related to cyber threats. The proposed research covers one of the most promising research areas: darknet markets and social media platforms exploitation tools and strategies. The research uses 6 DNMs publicly available data and then identified the most popular social media platform and intent of discussion based on the interaction available in form of the user remarks and comments. The research caters the social media platform and cybercrimes or threats associated to them, by help of the machine learning algorithms Logistic Regression, RandomForestClassifier, GradientBoostingClassifier, KNeighborsClassifier, XGBClassifier, Voting Classifier and Deep Learning based model LSTM and Transformer based Model used. In existing research, natural language processing techniques were employed to identify the kinds of commodities exchanged in these markets, while machine learning approaches were utilized to classify product descriptions.In proposed research work advanced and lighter version of BERT and LSTM model used yielding accuracy of 90.12% and 91.35% respectively. LSTM performed best to extract multiclass classification of actual intension of social media usage by intelligent analysis on hackers' discussions. Strategies on social media platforms such as Facebook, twitter, Instagram, Snapchat to exploit them using darknet platforms also explored. This paper contributes on cyber threat intelligence that leverages social media applications to work proactively to save their assets based on the threats identified in the Darknet.

Keywords Social media crimes · CTI · BERT · LSTM · Machine learning · Transformer based model

1 Introduction

Research work in the area of forum monitoring on the Dark Web and data retrieval for cyber threat intelligence is one of the prominent areas in the cyber threat intelligent. The cyber threat intelligence may benefit from certain important discoveries that are made through monitoring these forums. To mine and monitor the Dark Web forum data, many techniques and analyses have been used. One of the best techniques is to perform the focused crawling for collecting the data of these darkweb forums. The creation of an application-specific technique for surreptitious crawling of web was proposed in [1]. The research work proposed a task-configurable hidden web crawler that might potentially automate the process of extracting content from hidden webs. In contrast to other methods, they contend that crawling the hidden Web with human assistance is practical and allows for content access. The study that created a targeted crawler to gather dark web forums employed this forum access method [2]. 109 dark Web forums from three

✉ Kanti Singh Sangher
kantisingh19@gmail.com

[1] Amity School of Engineering and Technology (ASET), Amity University, Noida, India

[2] Department of Computing and Informatics, Bournemouth University, Fern Barrow, Poole BH12 5BB, UK

Published online: 14 August 2024

areas were successfully gathered in a variety of languages. But with the forums expanding so quickly, human-assisted crawling might not be as successful. To locate terrorist organizations on the TOR network, a dark Web crawler and network analysis were suggested [3]. An approach to web crawling was used to find the latent subjects from terrorist or extremist communities on the dark Web [4]. Markets on the dark web usually act as a conduit for illegal commerce. A study on forums marketplace talks was done in order to detect suppliers and doping agents on online marketplaces [5]. The analysis is restricted to the surface web, even though the method is effective in discovering drugging associated instance discussions. They could have used a faulty popularity metric in dark web. Numerous studies [6, 7] have looked into the effects of dark net forums and online chat rooms serving as a marketplace for the purchase of illicit narcotics. They found that the drug markets are stimulated by discussion forums because users from all over the world may interact and exchange information about drug usage, purchases, laws, and drug manufacturing and cultivation while remaining completely anonymous [8, 9]. In order to give a thorough examination of the illegal drug buying method with the items chemical profiling, investigation of one of the well-known marketplaces in dark web progression was conducted [10].

It might be challenging and time-consuming to select pertinent terms from a large volume of data. To extract latent topics from text corpora, generative probabilistic models like Latent Dirichlet Allocation (LDA) are used [11]. The Dark Net Markets subreddit was analyzed using Streaming Latent Dirichlet Allocation (SLDA), an unsupervised topic modeling technique [12] to determine the latent terms and topics. The subjects stayed the same during the duration of the research year, according to their analysis of the data. Conversely, during the exercises, a few topics related to real-life occurrences emerged. Cyber threat intelligence is now required to identify the different cybercrimes that originate from these darknet market forums and to analyze it within [13]. The Dark Web forum data was characterized and understood through the application of cluster characteristics analysis on the Black Market Reloaded (BMR) forum dataset. Network analysis and topic-model-based text mining techniques have been combined in research and surveillance on Dark Web forum portals to uncover overlapping communities in Dark Web portals [14]. Because it will offer a mechanism to prevent different types of cybercrimes, the research work that focuses on social media platforms, their utilization, and the context of their usage in the darknet forums needs to be investigated. A few of these include identity theft, financial fraud, hacking, data breaches, and illegal content distribution. The research work presented in this paper primarily caters the most popular worldwide social media applications and exchanges done by the darknet forum users that consist these applications. The dataset utilized in this study was obtained from Kilos' owner [15]. This is the greatest collection of Dark Web Market Forum data available, as it incorporates information from six different Darknet forums. As such, it can facilitate a plethora of innovative and worthwhile proactive Cyber Threat Intelligence (CTI) research questions. This paper is divided into the following sections. Firstly, the research examines previous research on cyber threat intelligence using the Darknet Forum datasets, talk about their CTI usefulness, and mention additional data gathering methods that are currently in use. Existing research in Darknet forums and cyber threat intelligence discussed in Sect. 2, research gaps identified were presented in Sect. 3, proposed research design alongwith the dataset analysis covered in Sect. 4. The findings of the conducted experiments and an assessment of their performance are included in Sect. 5. The research work is concluded in Sect. 6, and the future scope of the research covered under the Sect. 7.

2 Literature review

Darknet has made accessible for many illegal activities, including drug sales, child labor, and contract murders, to be conducted anonymously. International and federal authorities have long tried to regulate these operations, even if most of the procedures are laborious and manual. Several more recent approaches [16], such as Doc2Vec and Bidirectional Encoder Representation from Transformers (BERT), which haven't been thoroughly examined yet, are employed in this work. By contrasting the state of the art with tried-and-true methods that rely on conventional methods, such as Term Frequency-Inverse Document Frequency (TF-IDF), the study aims to classify illicit advertisements that are uploaded on the Darknet. Use different data balancing techniques as well as experiment with data using conventional procedures such as TF-IDF. The product classification or content classification using machine learning is popular research work. Research [17] conducted an eight-month crawl of the Silk Road Marketplace in 2012 and reported that a significant proportion of the adverts on the darknet are linked to narcotics. Content on Tor hidden services was classified in research paper [18] in 2014 and was divided into 18 themes. The Agora darknet dataset, was utilized in [19] between June 6, 2014, and July 7, 2015. In this work feature dimensions were reduced using Principal Component Analysis (PCA) and created vectors from description features using TF-IDF. Ultimately, a 79% accuracy rate was obtained while using a trained Support Vector Machine (SVM) to classify a product into 12 classifications. Tor hidden services were created in

[20] to retrieve data from the darknet. They collected 5,000 samples from Tor onion pages and used SVM to categorize the products into 12 groups. In 2017, through research [21] automated keyword extraction performed for product categories. To build vectors, they recommended developing unique term-frequency forms for each product category. In [22], researchers created the Darknet Usage Text Addresses (DUTA) dataset and manually categorized products into primary categories and subcategories. Many scholars will use this very accurate dataset in their upcoming work. Using the same dataset that they had prepared, they trained machine learning models to categorize items [23]. 20% of the newly retrieved data was found to be illegal. Text mining was utilized in [24] to identify opioid products with a high impact. A dataset of product advertisements from Instagram was employed in the most recent study [25] on the classification of product commercials using Long Short-Term Memory (LSTM) neural networks. Few researchers attempted to find users who were comparable across two or more darknets. The theory put forth by [26] states that usernames belonging to the same person are probably going to be the same across marketplaces. Similar assumptions were also made by [27], after conducting image analysis, used profile photographs to find comparable members across several darknets.

Research on identifying threats within organizational data in the form of malware [28] can also have a significant impact, as most data breaches occur through Darkweb hacker forums. Cyber threat intelligence (CTI) makes handling organizational data easier and stores sensitive and personal information. Determining the patterns that are useful from the discussions amongst the Darkweb forums can therefore be very beneficial to the field of cyber threat intelligence [29]. Analyzing the text for patterns that are recognized and their correspondence can therefore aid in the design and implementation of a safe digital ecosystem. Virtualization is another area that can help with data theft, fraud, malware, hosting illicit operations, anonymity, and other issues on the dark web. Thus, one of the most critical actions an organization can take to protect virtual computers is to identify and address any vulnerabilities within them [30]. LSTM has been employed in [31] to optimize semantic for spam detection, and it can detect spam much more effectively than conventional machine learning techniques. The LSTM is employed for the classification task after the text has been converted into semantic word vectors using Word2vec, WordNet, and ConceptNet. The classification outcomes are contrasted with those of benchmark classifiers, including Random Forest, ANN, SVM, Naïve Bayes, and k-NN. Identifying communities within social networks is further vital, but most of them need significant user input parameters or take a long time to execute. Research work [32] proposes, Cohesion Index based Label Propagation (CILPA) technique, a new label propagation technique. Cohesion Similarity (CoSim) and Cohesion Index (CI) are two new functions introduced by the algorithm. The cohesiveness of a node is quantified by the cohesion index function, while cohesion similarity is used to measure similarity with neighboring nodes. Uncovering communities inside intricate social networks can be accomplished effectively with CILPA. Latest research in different aspects of darkweb based illicit activities has been explored and presented in Table 1.

As NLP uses Bidirectional Encoder Representation Transformer (BERT) for text processing with best results in proposed work has been used. Using unlabeled text, pre-train deep bidirectional word representations utilized. The advantage is one output layer can be added to that pre-trained model to tackle a variety of NLP issues, such as text classification.

3 Research gaps

The Dark Web is the online black market where hackers buy and sell stolen data for a profit. This is where most data breaches result in. Anybody can remain anonymous, private, and invisible by using the Dark Web, an encrypted portion of the Deep Web that can only be accessed with certain dark web browsers. Regulations and protections do not exist on the Dark Web. The Dark Web is not only being used by criminals, though; political dissidents and corporate whistleblowers have historically used it as a forum. On the Dark Web, bundles known as "fullz" that include a person's whole set of identifying information, including their SSN and birthdate, may be purchased for as little as $8. The quantity and potential long-term value of personally identifiable information (PII) determine its value to fraudsters, who may use it to sell stolen data to other criminals on the Dark Web in the future. After doing a literature review, two gaps were found. The analysis of cyber-threat assets and the communication surrounding them across numerous data sources has not been thoroughly investigated using analytical methodologies within the context of Dark-net research. The second identified gap pertained to the degree of pre- and post-availability of data after breaches and their victims, which is still not entirely understood.

The following queries are put forth considering these gaps:

A. How widespread are cyberthreats and communication among hacker communities?
B. What kinds of assets that pose a cyber threat is the Dark-net ecosystem gravitating toward?

Table 1 Latest research work explored and presented categorically based on the outcome

S. No.	Year	Focus of the paper	Techniques & parameters used	Outcome
1.	2017	Human trafficking	Without regard to the subjects' age or genre, a research report in Spanish is presented in [33]. analysis to find trends connected to human trafficking using data from a variety of sources, including social media, the dark web, and online newspapers.	Since darkweb-based data is the most prominent, the result gives useful suggestions that future work on this topic should focus more on it.
2.	2017	Drug Transactions	Impact study of crackdowns on Cryptomarkets is the main focus of this research work [34].	It was discovered that the duration and extent of the impact of crackdowns were restricted.
3.	2019	Pornography Industry	A significant amount of onion domain name data was examined in [35] utilizing the "Fresh Onions" open source Tor tool and the "Ichidan" search engine.	Simplified the process of implementing a directed graph simulator made from the discovered hyperlinks and connection statuses to the dark web. Using the graphed categorization results as a guide, It was also tried to identify the features and connections between each instance of Dark Web content.
4.	2021	Terrorism	Cybersecurity flaws are used by terrorists as weapons of mass destruction. In real time, the dark web provides a safe sanctuary for illegal behavior because of its robust transparency and difficult-to-track protocols. Text mining from the darkweb dataset was the goal in [36] in order to obtain supporting results.	Using TF-IDF function extraction and an AdaBoost classifier implementation, research produced an accuracy of 0.942. By using the work, researchers and System authoritarian agencies can confirm whether or not their darkweb corpus contains such illegal conduct based on the relevant regulations of the unlawful categories.
5.	2020	Markets for Cybercrime Tools and Stolen Data	Honeypot-based evidence collection of any malicious behavior seen on the dark web [37].	honeypots built using the malicious material found as evidence and the darkweb vulnerabilities.
6.	2022	Dark Net currency exchange using Bitcoin	Identifying the illicit drug trade can help us better understand the elements driving DNM customers' decisions [38]. To investigate the behavior of DNM new drug users over time, temporal topic models and sentiment analysis were used to the ClearNet forum data.	The apparent dynamics of significant events in the cryptocurrency realm, such as the switch from Bitcoin to Monero, were effectively reflected by the extracted temporal topic models.
7.	2020	Cyber hacking techniques P7 [38]	A systematic method for automatically extracting "topics of interests (ToIs)" from hackers' websites and using them as inputs for actionable security measures or Indicators of Compromise (IOS) collectors was proposed in the research paper [39].	Created a crawler for the dark web and assessed the extraction of ToIs.
8.	2021	Drug selling	A large-scale [40], longitudinal measuring study on posts and listings in anonymous marketplaces was used to create profiles for the opioid supply chain in these forums and anonymous markets.	Described providers in anonymous forums and marketplaces (e.g., activeness and cross-market activities), commodities (e.g., popular items and their evolution), and transactions (e.g., origins and shipment destination).
9.	2024	Hacking-Cyber Crime	Producing word vectors with a limited feature set to improve the differentiation across Dark Web classes [41].	TextCNN with topic modeling weights integrated. The proposed method proved to be more successful in classifying content from the Dark Web than existing text classification algorithms when two datasets were used for validation.
10.	2019	Vending	Utilizing Linear Discriminant Analysis (LDA) to identify conversation topics, describe the evolution of themes across forums using a non-parametric HMM [42].	It was possible to find hidden patterns in several forums and identify unusual occurrences in a wealth of diverse, rich material.
11.	2021	Hash Value Analysis	A workaround for worms, dos attacks, backdoors, DDoS attacks, RDoS attacks, spam, and malicious materials has been proposed [43].	Darknet traffic was analyzed using the Light Gradient Boosted Machine Learning Algorithm and TF-IDF for the purpose of detecting criminal activity.
12.	2020	Social Network Analysis Methodologies	Analyzing the posts made by members in forums and subforums covering wider subjects [44]. recognizing a variety of user profiles.	Results indicate that while most users have fewer connections, some members in most of the forums create hubs and are very connected.
13.	2023	Marketplace Scrapping	Using Python to traverse dark web pages and gather data with the customizable Selenium WebDriver application [45]. identifying strategies and solutions that allow for far reduced risk dark web marketplace scraping.	Presented investigation included marketplace storefront prices, persistent vendor lists, ratings, and other fundamental information, along with a list of kinds of dangerous cyber items sold on them.

Table 1 (continued)

S. No.	Year	Focus of the paper	Techniques & parameters used	Outcome
14.	2021	Monitoring Dark Web	Machine learning algorithms to create classifiers for the CIC-Darknet2020 darknet traffic dataset [46].	There is now binary and multiclass classification. There were four classes in the second classification task: "Tor", "Non Tor", "VPN", and "Non VPN", compared to two in the first: "Benign" and "Darknet". Over 98% prediction accuracy was attained on average.

- List of identified Social Media platforms and their distribution in the dataset.
- List of cyber-crimes/social media crimes.

So, a model needs to be developed to predict the intended cybercrime for a particular platform, here list of identified cybercrime categories mapping with platforms is desired as the research outcome. All the instances of social media exchanges from forum considered for the cybercrime based social media posts. So, here the objective is to perform multilevel analysis using machine learning and deep learning algorithms for darknet markets for proactive intelligence in social media crime. So, it becomes vital cybersecurity concern to check for the real root causes of these data stealing/hacking and other methods of exploiting the digital products, as Darkweb is one of the primary platforms for this kind of illicit activities therefore working on the Darknet forums data can be very helpful. This research work focuses on the Dark Web Forums exchanges to find the information available relevant to the social media platforms.

4 Research design

The study design for this involved four main stages: gathering data, identifying potential threats using popular social media platforms, threat profiling using text processing from machine learning techniques, and applying ML and DL models to classify and categorize the intention of writing a specific set of text, regardless of whether it is intended to commit a cybercrime or not. The research work focuses on identification and exploration of the Dark-Net Market (DNM) Forums. After that selection of most popular social media-based applications and finding their instances within the dataset. The objective of the research is categorization of the Dark-Net based illicit activities conducted exploiting the selected social media platforms. The research work is dedicated for cyber threats identification based on the information exchanges on the social media apps/platforms-based texts from the forum data. To perform the experiments machine learning & Deep Learning models used and classification of the cyber-crime intended interactions was the outcome. Algorithm to get the meaningful context with the extraction of the text from the Darkweb dataset to relate the usage and intent of Social Media platforms:

```
Algorithm: Social Media usage Intent in darkweb forums
1: Data collection, consisting of 6 markets dark-net market
   forums (DNM's) content
2: Text processing of data using TF-IDF

   for Every time step do
      Tokenization
      Normalization
      If (stopword == "the", "is", "and") then
         Remove
      Endif
      Reducing words to their root form

3: Feature extraction for relevant patterns of social media-
   based crime for model learning
4. For each of algorithms, logistic regression,
   RandomForestClassifier

   GradientBoostingClassifier, KNeighborsClassifier,
   XGBClassifier, Voting Classifier, LSTM, BERT

5: Cyber threat intelligence for detection of social media-
   based crime text relevant to the cybercrime
6. Data classification in 4 categories Hacking, Drug, Fraud
   and Phishing
7: model evaluation & validation using confusion matrix
   and f-score
```

The overall research design as shown in Fig. 1, starts with the finding of one of the most popular datasets i.e. DNM with 6 Darknet markets forums data. The challenge was to find out the usage of the most popular set of social media apps, their frequencies in terms of appearance it eh dataset, their context of the usage and then mapping the context with the relevant cybercrimes.

In this research work early detection of the cyber threats by utilizing the AI models on darknet forums content has been proposed. , The research establishes the need of a complete cyber threat intelligence framework to protect and alert the organizations with comprehensive analysis to get

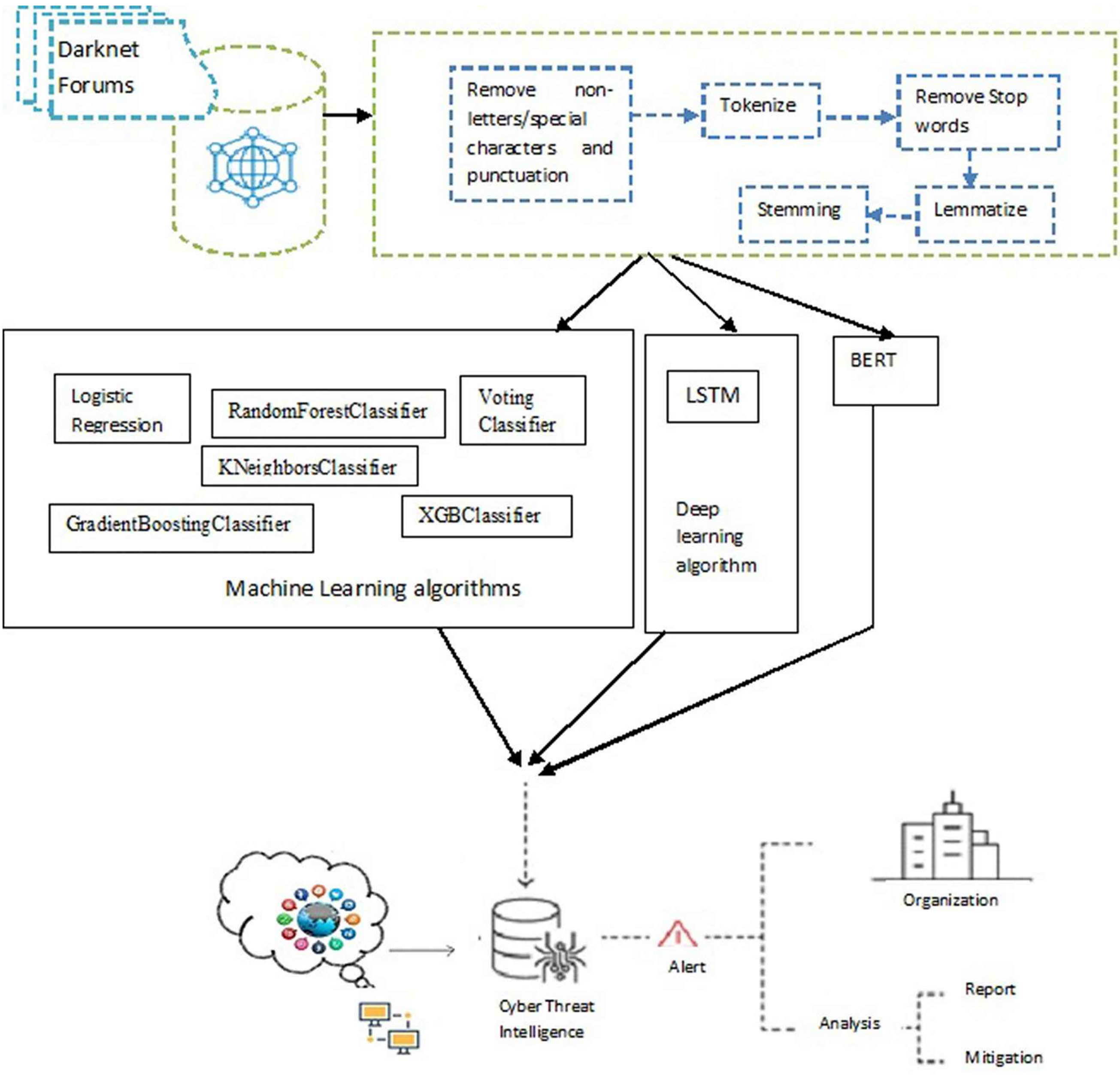


Fig. 1 Overall research design framework

trapped into cybercrimes. Preventive measures, specifically the usage of particular social media applications to perform cybercrimes can be identified and countermeasure's can be taken.

In the research work using Bidirectional Encoder Representations from Transformers, or BERT, as shown in Fig. 2, envisaged due to its improved accuracy for a variety of Natural Language processing (NLP) tasks. While predicting a target word, BERT can gather bidirectional context information, which means it considers both words that come before and after it. Compared to unidirectional models like conventional RNNs, this results in a more thorough comprehension of the context. Usually, the final layer of the transformer stack's output embeddings of the special [CLS] token is pooled to create sentence representation. For tasks that come after, this pooled representation serves as a fixed-length representation of the input sentence and gathers contextual information from the complete input sequence. Once the pooled sentence representation is obtained, it is typically fed into task-specific output layers after passing via a feed-forward layer and normalizing (either layer normalization or batch normalization). The sentence representation can be further transformed and abstracted with the help of an extra feed-forward layer, which makes it more appropriate for a

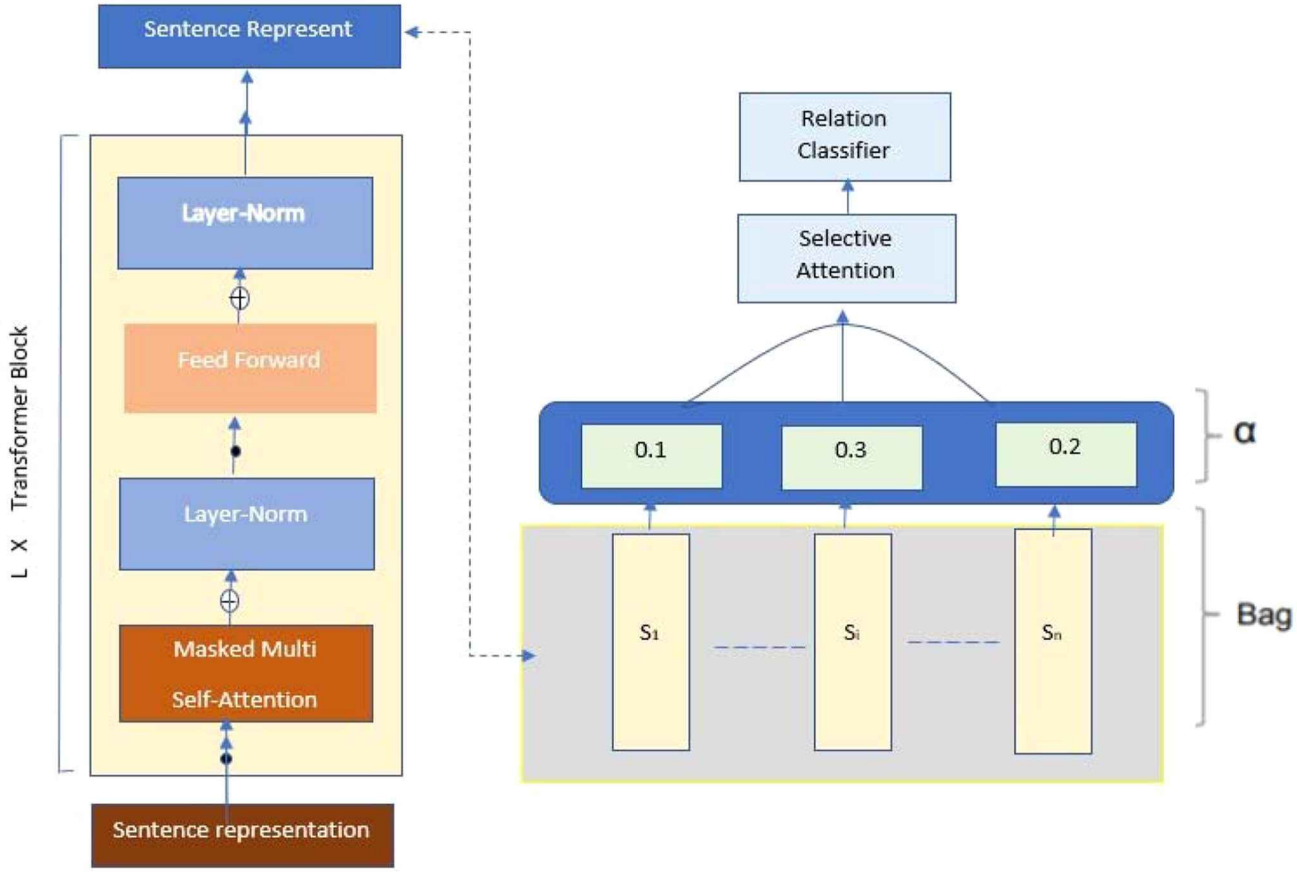


Fig. 2 Overview of BERT

variety of tasks like text categorization, sentence similarity, and other NLP tasks. One or more completely linked (dense) layers with activation functions like GELU (Gaussian Error Linear Unit) or ReLU (Rectified Linear Unit) commonly make up the feed-forward layer. The model can learn non-linear mappings between input feature and task-specific output predictions thanks to these layers. Furthermore, the normalization phase enhances generalization performance and stabilizes the training process. Through the usage of this pipeline, BERT is able to produce a reliable and task-specific representation of the input sentence that is highly accurate and efficient for a variety of NLP applications. Based on the functionalities provided by BERT, it was used for text categorization, considering contextual knowledge in various research work. Bert consistently delivers more accurate predictions, particularly in tasks where context is important. So, to categorize the text into cybercrime context BERT was the most suitable model and hence applied.

4.1 Dataset and exploratory analysis

Online marketplaces known as Dark Net Markets (DNMs) are frequently housed as Tor hidden services that operate as middlemen for transactions involving Bitcoin or other cryptocurrency between buyers and sellers. These transactions typically involve narcotics or other prohibited or illicit commodities. The dataset [15] used in this research work made available by the proprietor of Kilos, a DNM search engine akin to Grams, with publishing a CSV of 235,668 reviews that were scraped from six DNMs: Apollon, CannaHome, Cannazon, Cryptonia, Empire, and Samsara. The attributes listed below are those found in the dataset and will be utilized in the study project implementation according to their importance.

site, **vendor**, **timestamp**, **score**, **value_btc**, **comment**.

The strings are vendor, site, and comment. While the comment may contain punctuation and other characters, the site and vendor are both alphanumeric. To facilitate sorting, the comment box is enclosed in quote marks and has clear line breaks denoted by "\n". All of the data is in Latin characters only Unicode is not used. The number of seconds since the Unix epoch is represented by the timestamp, which is an integer. For every review, there is a score of 1, 0, and − 1 for a bad review. value_btc represents the product's bitcoin value as of the review date, as determined by calculations. Since the data was taken straight from the Darknet, it

Table 2 Common malpractices in darkweb

List of commonly malpractices occurring in darknet websites	
Phishing	Ransomware
Hacking	Software
Crack	Account
Drug	Data
Porn	DDoS
Weapon	Social Media crimes
VPN	

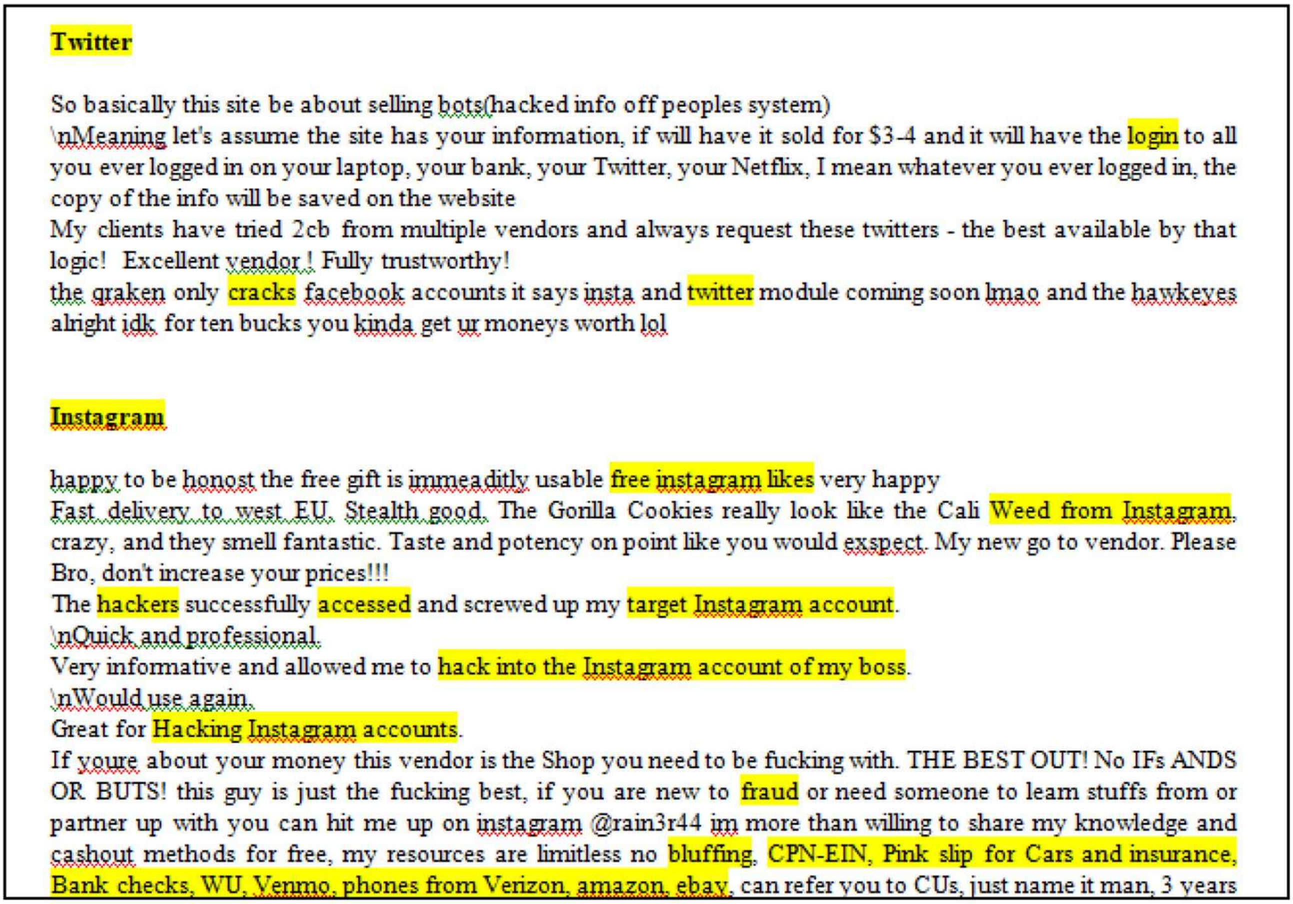
must be processed. All null values and incorrect lines must be removed, resulting in “235342” as the total number of rows. The intent is to find out the most interesting trends and content regarding social media crimes using artificial intelligence-based models. The research work focuses on making social media platforms more secure and making the community aware regarding their usage by utilizing the Darknet Forums data in the forms of the comments exchanged by their usage. Sometimes to sell the credentials, hack the apps, to perform the piracy of the software, or intended to sell or purchase the drugs/weapons/illicit images of kids or women and other mal practices using the anonymous TOR passed Darknet Websites. Analyzing the dataset provided the following major categories of crimes including cybercrimes for overall dataset as shown in the Table 2.

While extracting the comment section from the dataset further provides more information as highlighted in the following image, Fig. 3.

For instance, purchasing and selling of Instagram likes, purchase, hacking of Instagram accounts, selling, and purchasing of the of Weed(drugs) on the Instagram alongwith the offering to perform the financial frauds as a service using the Instagram were found through the Forum’s exchanges from the users.

4.2 Mapping of the crimes for each social media platform

In the research work based on the pre-procession of the data and findings of the instances or frequencies of occurring of social media platforms and as per the popular application used worldwide the set of application identified and shown in the Table 3. Based on the observations and manual findings the dataset includes conversations /comments related to following social media platforms:



Twitter

So basically this site be about selling bots(hacked info off peoples system)
\nMeaning let's assume the site has your information, if will have it sold for $3-4 and it will have the login to all you ever logged in on your laptop, your bank, your Twitter, your Netflix, I mean whatever you ever logged in, the copy of the info will be saved on the website
My clients have tried 2cb from multiple vendors and always request these twitters - the best available by that logic! Excellent vendor ! Fully trustworthy!
the graken only cracks facebook accounts it says insta and twitter module coming soon lmao and the hawkeyes alright idk for ten bucks you kinda get ur moneys worth lol

Instagram

happy to be honost the free gift is immeaditly usable free instagram likes very happy
Fast delivery to west EU. Stealth good. The Gorilla Cookies really look like the Cali Weed from Instagram. crazy, and they smell fantastic. Taste and potency on point like you would exspect. My new go to vendor. Please Bro, don't increase your prices!!!
The hackers successfully accessed and screwed up my target Instagram account.
\nQuick and professional.
Very informative and allowed me to hack into the Instagram account of my boss.
\nWould use again.
Great for Hacking Instagram accounts.
If youre about your money this vendor is the Shop you need to be fucking with. THE BEST OUT! No IFs ANDS OR BUTS! this guy is just the fucking best, if you are new to fraud or need someone to learn stuffs from or partner up with you can hit me up on instagram @rain3r44 im more than willing to share my knowledge and cashout methods for free, my resources are limitless no bluffing, CPN-EIN, Pink slip for Cars and insurance, Bank checks, WU, Venmo, phones from Verizon, amazon, ebay, can refer you to CUs, just name it man, 3 years

Fig. 3 Keyword extracted from the comment sections of the Forum

Table 3 Most popular social media platforms worldwide

S. No.	Social Media Application
1	Facebook
2	Twitter
3	Instagram
4	Whatsapp
5	Telegram
6	Snapchat
7	Reddit
8	Youtube
9	Netflix
10	Amazon Prime

{‘Facebook’: 20, ‘Twitter’: 0, ‘Instagram’: 118, ‘Telegram’: 435, ‘Netflix’: 95, ‘Youtube’: 37, ‘Amazon’: 923, ‘Whatsapp’: 6, ‘Snapchat’: 4, ‘Gmail’: 24, ‘Reddit’: 7, ‘Spotify’: 42}

As per the text processing results the following social media cybercrimes related content in comments are found - Phishing, Hacking, Software crack(purchase/sale), Account, software piracy, website hacking, crashing applications, browser-based crimes, identity spoofing(password), amazon credentials stealing, mobile, bitcoin, porn, network traffic, Spotify hacking, vpn attack. The research work done for the top social media platforms mainly - [‘Facebook’, ‘Twitter’, ‘Instagram’, ‘Telegram’, ‘Netflix’, ‘Youtube’, ‘Amazon’, ‘Telegram’, ‘Whatsapp’, ‘Snapchat’, ‘Gmail’, ‘Reddit’, ‘Spotify’]. And as these words don’t only occur in this form but also occur in forms like facebook or faCebook regex created to deal with such instance’s (variation using uppercases) and the columns ‘vendor’ and ‘comments’ and after analysis visualization results collected. The distribution of the popular social media apps in the comments are given below in Figs. 4 and 5.

The occurrences and distribution of top social media names in the column’s vendor and comments. After this the main task was to extract the keywords for the comments and add them into a new column, the keywords were chosen manually and were extracted using the regex in python. Following the text processing the data manually 4 classes as shown in Fig. 6 were marked, the base was analysis of the comments and the vendor’s name. For example, after looking at vendor’s name like netflixking and its comment which tells they deal in selling hacked accounts.

The cybercrime instances were divided into four classes:

- Hacking
- Drug
- Fraud
- Phishing

Feature list = [‘target’,‘account’,‘contact’,‘hackers’,‘crack’,‘software’,‘password’,‘hack’,‘supplied’,‘money’,‘sold’, ‘login’,‘likes’,‘weed’,‘hash’,‘target’,‘Bank’,‘WU’,‘Verizon’,‘ebay’,‘btc’,‘carding’,‘login’,‘venmo’,‘phones’,‘cashout’, ‘Marijuana’,‘stimulants’,‘delivery’,”Paypal’,‘email’,‘premium’,‘stealth’,‘scam’,‘credential’,‘porn’,‘premium’,‘USD’, ‘BTC’,‘buy’,‘lifetime’,‘free’,‘upgrade’,‘plan’,‘emails’,‘Username’,‘software’,‘system’,‘subscriber’,‘youtuber’,’subs’,‘likes’,‘views’,‘channel’,‘amazing’,‘faster’,‘prime’,‘legit’,‘Dose’,‘UPS’,‘quality’,‘pills’,‘order’,‘xanax’,‘arrived’,‘stoned’,‘vendor’,‘buissness’,‘deal’,‘strong’,‘cannabis’,‘stuff

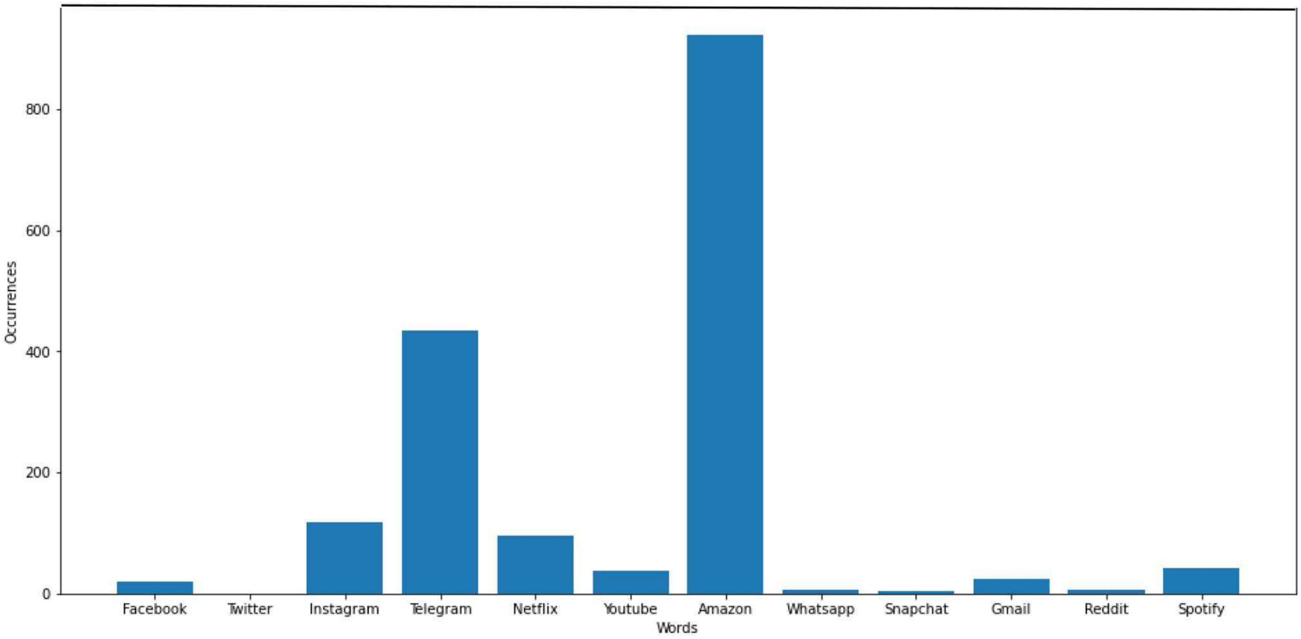


Fig. 4 Occurrences of social media in dark net from product transaction feedback

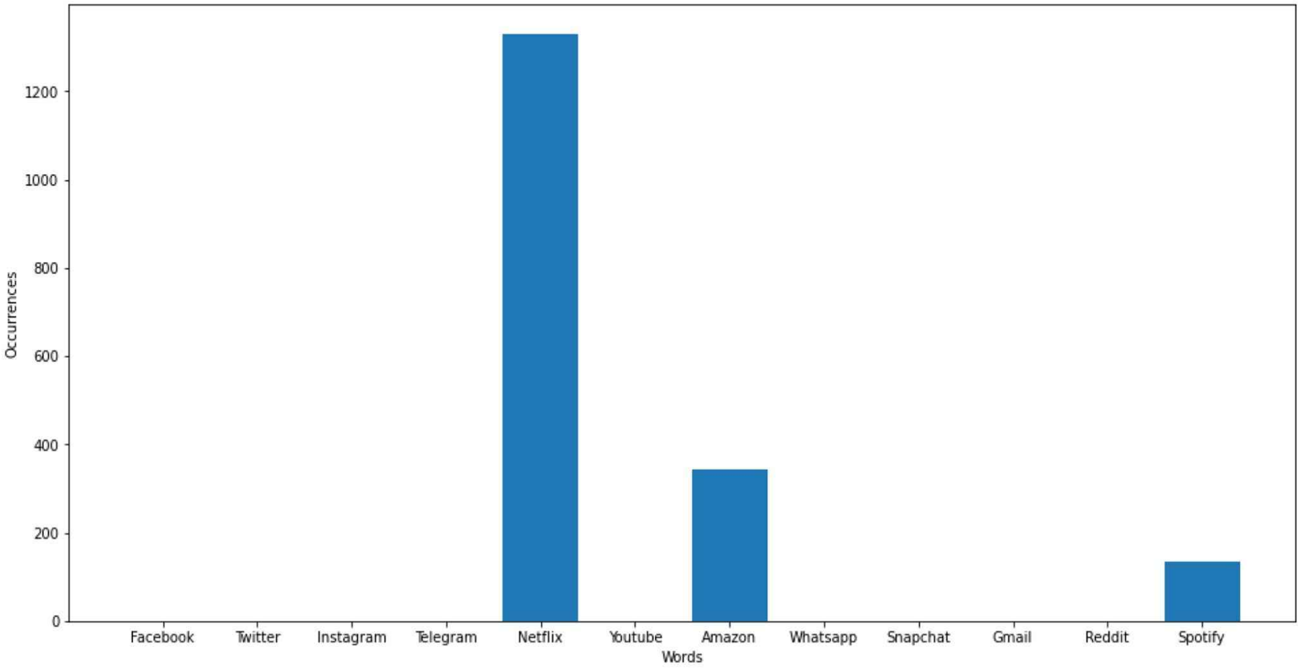


Fig. 5 Occurrences of social media in darknet from vendor names

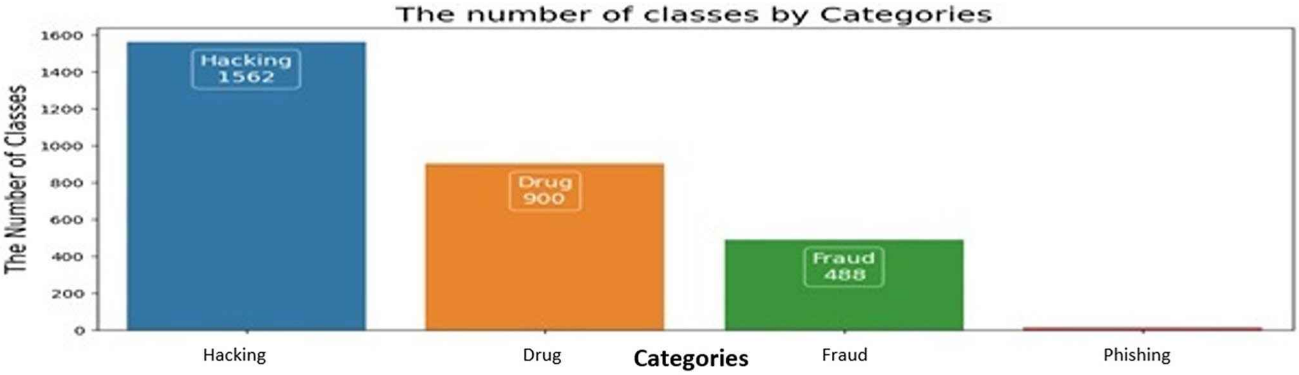


Fig. 6 Four classes identified for the cybercrime categories

',‘package’,‘schnell’,‘carts’,‘shipping’,‘vape’,‘reliable’,‘good’,‘rapide’,‘schneller’,‘vendor’,‘texture’,‘buzz’]. These keywords were chosen after the manual analysis of the data.

5 Experiments & findings

Token encodings are one-hot vectors that are created by tokenizing text. The dimension of the token encodings is determined by the amount of the tokenizer vocabulary, which typically has between 20k and 200k distinct tokens. These token encodings were then transformed into vectors called token embeddings, which resided in a lower-dimensional space. After that, the encoder block layers processed the token embeddings to produce a hidden state for every input token. Each hidden state is sent to a layer that predicts the masked input tokens in order to achieve the pretraining goal of language modelling. The research work uses a classification layer for the language modeling layer in the classification task.

Using the transformers to work on the text BERT Encoding more efficiently was used as it provides the following advantages. The Tokenizer class includes a very useful function named encode plus. It can carry out the following tasks with ease:

- Tokenization of text and includes unique tokens ([CLS] and [SEP])
- Generates token IDs.
- Extension of the sentences to a standard length; and
- Design of attention masks.

The DistilBERT model is frozen and only offers features for a classifier in the feature-based approach and hence it has been utilized in the proposed research work.

5.1 Results

The research [47] focuses on analyzing how difficult it is to gather relevant information from dark web forums to strengthen cyber defense systems. By analyzing dark web forums, the study builds on our previous research by identifying fresh trends and patterns [48] that might provide a unique viewpoint on the evolution of cyberthreats. Specifically, in authors tackled the issue of identifying well-known hackers on dark web social networks [49]. This study details attempts to develop a text mining engine (called Threat Miner) that uses semantic analysis to accurately detect novel cyberthreats from the most well-known hackers in the CrimeBB dataset. They [50] achieved this by utilizing hacker and influencer analytics.

The existing research [51], in this study, which encrypts discussions in deep web forums using TOR relay nodes. We propose a novel approach to cyberthreat identification using the deep learning Long Short-Term Memory (LSTM) algorithm. The created model performed better than the experimental results of earlier researchers in this issue domain, with an accuracy of 94% and a precision of 90%. In the [52] presented a simple framework for identifying novel cybersecurity threats in darknet markets by removing recently found cybersecurity-related terms. The framework aims to alert relevant authorities and give enough time for developing patchworks or other countermeasures to stop potential cyberattacks or at least minimize losses. The platform makes use of machine learning and data mining techniques, as well as the objects and content found in their names and descriptions on darknet markets. In [53], in order to find important cyber threat intelligence, this study applies machine learning to both predictive and descriptive analytics on a darknet forum postings dataset.

Table 4 Comparison of research outcome with existing work

S.No.	Model Name	Accuracy (%)	Precision (%)	Recall (%)	F1-score (in %)
Proposed research work	LSTM Architecture	91.24	95.12	91.24	91.35
	Transformer Architecture - BERT	90.46	89.88	90.46	90.12
	Logistic Regression	93	96	97	97
	RandomForestClassifier	89	90	98	93
	GradientBoostingClassifier	91	94	97	96
	KNeighborsClassifier	91	94	98	96
	XGBClassifier	91	94	97	95
	Voting Classifier	91	94	97	95
Adewopo [51]	LSTM	94	90	91	91
	Random Forest (RFC)	80	95	95	75
Dong [52]	SVM	81	90		
Azene [53]	Random Forest	97			91
Arora [54]	Random Forest (RFC)	80	81	80	79

The research made use of the machine learning application WEKA and IBM Watson Analytics. Relationships and trends in the data were displayed via Watson Analytics. Machine learning models were made available by WEKA to categorize the different kinds of exploits that hackers target from the form posts. The findings indicated that the most popular tools in the darknet were Crypter, Password Cracker and RATs (Remote Administration Tools), Buffer Overflow Exploit Tools, and Keylogger System Exploit Tools. Research work also revealed the presence of prominent writers who regularly participate in the forums. Furthermore, machine learning aids in the development of exploit type classifiers. The accuracy of the Random Forest classifier was higher than that of the Random Tree and Naive Bayes classifiers. In this research work, researchers [54] used the Random Forest tool, a data mining tool, to analyze cybercrime on social media, they put forth a model that is very implementable and will enable us to create features that will enable us to classify threats automatically and capture users in multiple ways.

The research work focuses on the popular social media apps discussed on the darknet forums with their context. Here, all the cybersecurity conversations processed using the machine learning and deep learning models and the results shown in the Table 4. The research is novel in nature itself as the social media based interaction and their data breaches are most prominent information in the work, the performance of the models i.e. Logistic Regression, RandomForestClassifier, GradientBoostingClassifier, KNeighborsClassifier, XGBClassifier, Voting Classifier, LSTM with variations and Transformer Architecture with BERT performed successfully and compared with existing Darknet forums research and found that proposed research work produces better in terms of classification of cybercrimes prediction.

Performance comparison of current deep learning and machine learning models based darknet forum analysis done with proposed research. Here BERT model implementation requires necessarily to instantiate a tokenizer object that is specific to the chosen model because different pre-trained models use different methods to tokenize textual inputs (DistilBERT's tokenizer includes special tokens like [CLS] and [SEP] in its tokenization scheme). Models implemented to the pretrained method of the DistilBertTokenizerFast class to obtain the tokenizer utilized by DistilBERT-base-uncased Fig. 7.

Confusion Matrix for all the machine learning algorithms implemented shown in Figs. 7 and 8. Logistic Regression performs the best as compared to others. The F1-score provides a combined understanding of Precision and Recall as it is a harmonic mean of these two measurements. When Precision and Recall are equal, it is maximum. There's a catch, though. The F1-score has low interpretability.

As a result, after combining with other assessment indicators to provide a comprehensive view of the outcome the findings of multivariate analysis presented using score plots. Comparative score plot based on F1-Score accuracy of each implemented machine learning and deep learning model are shown in Fig. 9.

The LSTM Arch-4 performs the best among the LSTM variations used at different epochs i.e. 20,40,60,80.. Although the observed output of the Transformer Architecture employing BERT is now not superior to the LSTM, it will undoubtedly perform better with a larger collection of keywords and larger datasets.

6 Conclusion

Social media is a huge source of information exchange where the users put and absorb sentiment, business statistics, religion-based thoughts, government, and international concerns too. Dark web when used as platform where users can share and get a lot of information about the illegal items and services purchase [55], source of steeled data from the surface web and hacked data [56]. Sometimes the data is sensitive and critical from the national and international security concerns. In the research paper the concern about the Cyber Security and how the information shared in dark market discussion forums can reveal the target apps and what kind of cyber-attacks most popular or talked about between the hacker's community and cyber criminals attained. The results show that Hacking, Drugs, Financial frauds, and Phishing are among the most popular crime used on popular social media apps. The most popular social media apps used to perform these types of targeted attack use and exploit the data as well as utilities of Facebook, Twitter, Instagram, WhatsApp, Telegram, Snapchat, Reddit, YouTube, Netflix and Amazon Prime. The research was performed using one of the latest datasets which consists of the 6 darknet market forum data, with machine learning and deep learning to predict the cybercrimes associated with the most popular social media apps. The outcome of the work showcases the immediate need to make policies and regular monitoring of the context of usage and to make the apps intelligent enough to protect against.

7 Future scope

In the era of cyber space covering all the aspects of personal and professional verticals, it is the needed to explore the interconnectedness between dark web forums, marketplaces, and other underground platforms. Investigation of how information flows between these different entities and the role of social media platforms in facilitating communication and coordination among users is one of the most prominent works in future. It is also required to examine the privacy and security implications of social media platforms operating within the dark web. Research could focus on the vulnerabilities of these platforms, the risks to user privacy, and the strategies employed by law enforcement agencies and security experts to monitor and combat illicit activities. existingr ,Based on the existing research work it is essential to explore the emerging cybercrimes using latest technologies such as quantum computing & edge computing within Darknet research. Addressing ethical considerations related to studying dark web forums, including the potential harm to individuals or communities, the dissemination of illegal or harmful content, and the responsibility of researchers to ensure their work does not inadvertently contribute to criminal activity, is also future area for the research.

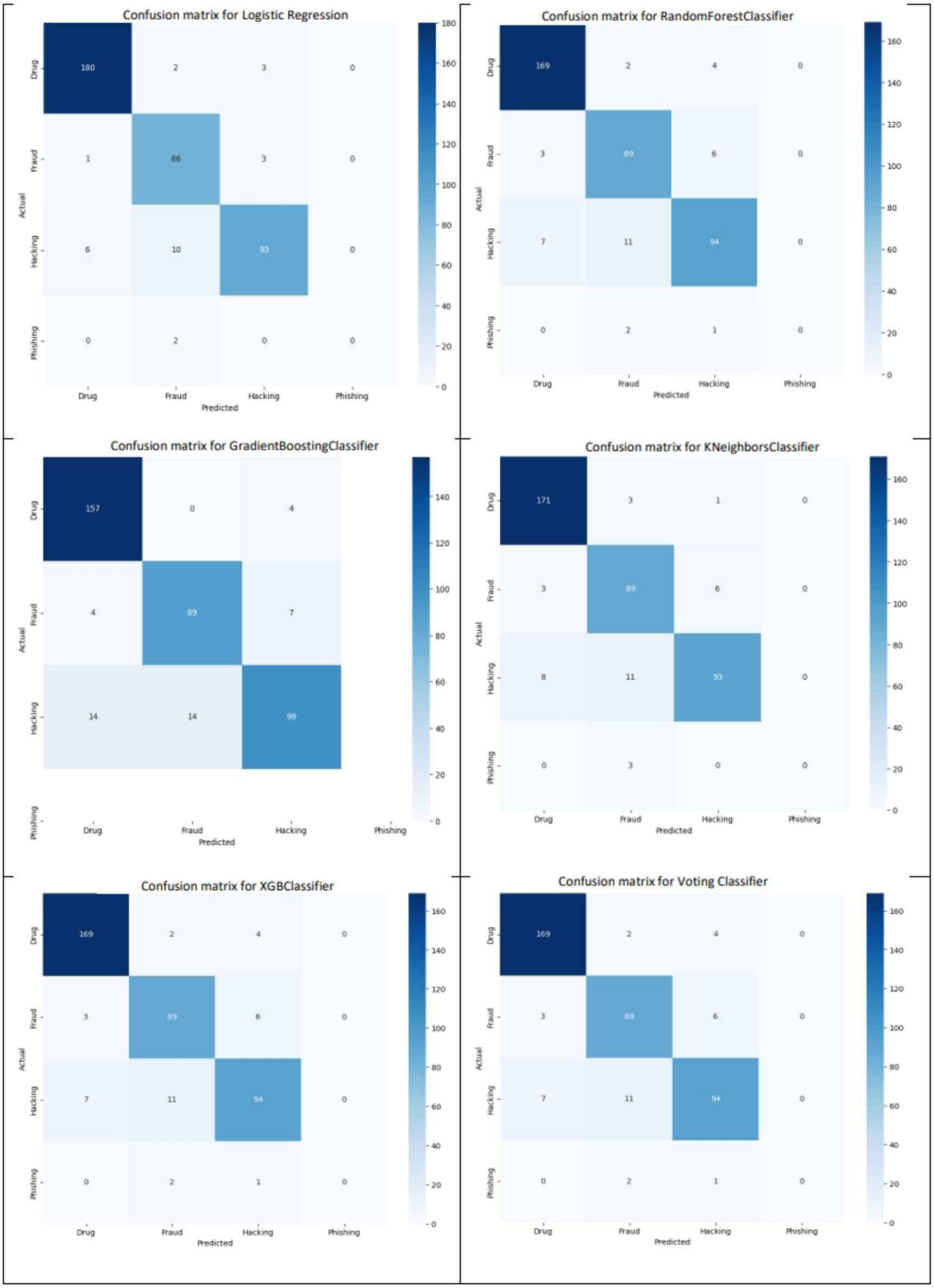


Fig. 7 Confusion matrix for all the machine learning models implemented

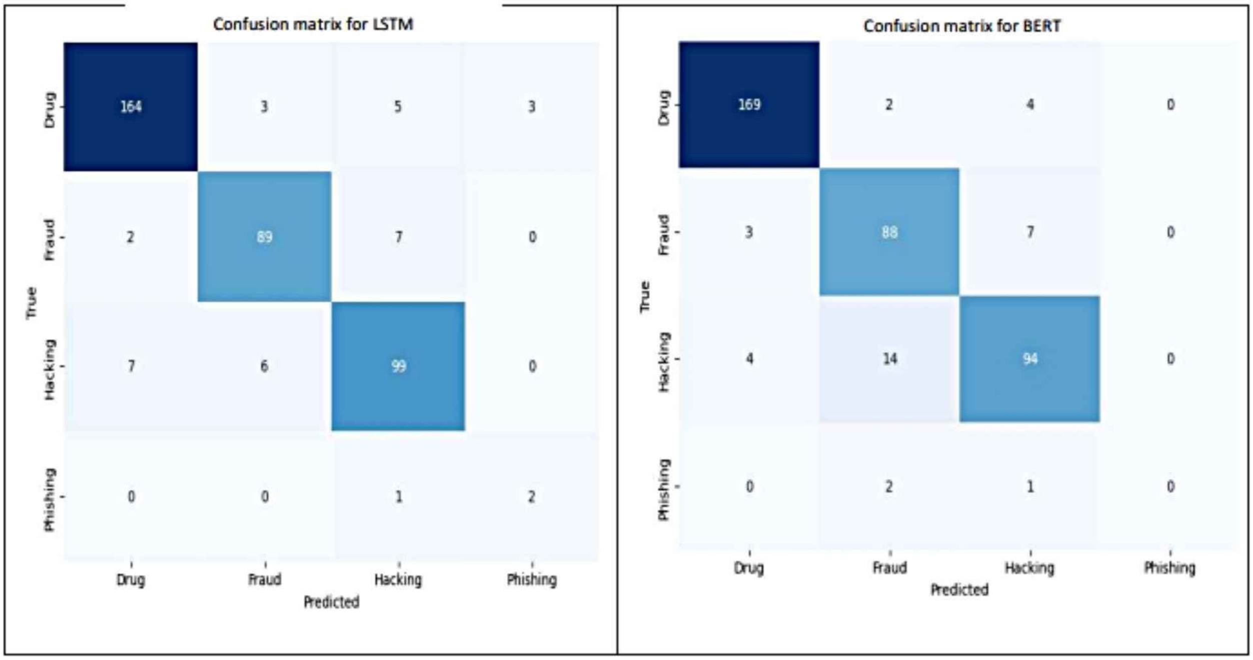


Fig. 8 Confusion matrix of LSTM & BERT

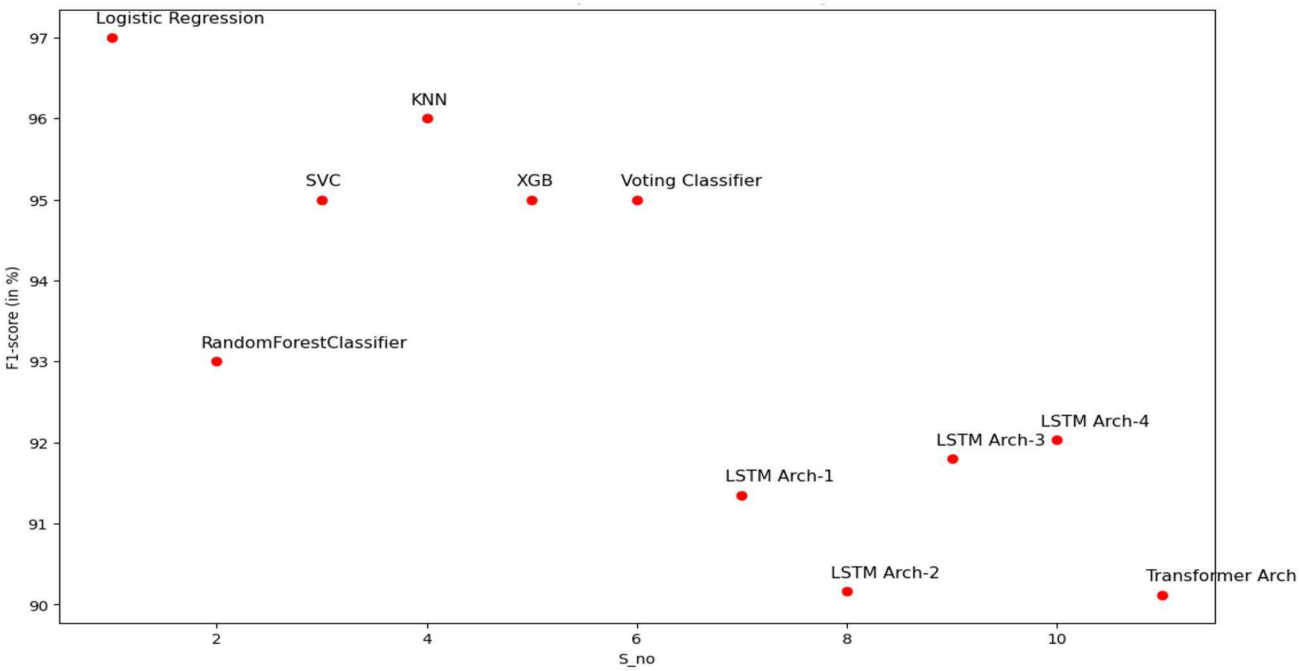


Fig. 9 Comparative score plot using F1-Score accuracy

Declarations

Research involving human participants and/or animals This study follows a human research ethics committee, and all procedures performed in the study involve human participation only.

Informed consent Research does not involve humans.

Disclosure of potential conflicts of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Raghavan S, Garcia-Molina H (2001) Crawling the hidden web. In Vldb, vol. 1, pp. 129–138
2. Fu T, Abbasi A, Chen H (2010) 'A focused crawler for dark web forums. ' J Amer Soc Inf Sci Technol 61(6):1213–1231
3. Zulkarnine AT, Frank R, Monk B, Mitchell J, Davies G (2016) "Surfacing collaborated networks in dark web to find illicit and criminal content," in Proc. IEEE Conf. Intell. Secur. Informat. (ISI), pp. 109–114, Sep
4. Yang L, Liu F, Kizza JM, Ege RK (2009) "Discovering topics from dark websites," in Proc. IEEE Symp. Comput. Intell. Cyber Secur., pp. 175–179, Mar
5. Pineau T, Schopfer A, Grossrieder L, Broséus J, Esseiva P (Nov. 2016) Rossy,"The study of doping market: how to produce intelligence from internet forums". Forensic Sci Int 268:103–115
6. Afilipoaie A (2015) and Patrick Shortis. From dealer to Doorstep—How drugs are sold on the Dark Net. GDPO Situation Analysis. Swansea University
7. Buxton J, Bingham T (2015) "The rise and challenge of dark net drug markets," Policy Brief, vol. 7, pp. 1–24, Jan
8. Lacson W, Jones B (2016) 'The 21st century DarkNet market: lessons from the fall of silk road," int. J Cyber Criminol 10(1):40
9. Van Hout MC, Bingham T (2014) "Responsible vendors, intelligent consumers: Silk road, the online revolution in drug trading," Int. J. Drug Policy, vol. 25, no. 2, pp. 183–189, Mar
10. Rhumorbarbe D, Staehli L, Broséus J, Rossy Q, Esseiva P (Oct. 2016) 'Buying drugs on a darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data'. Forensic Sci Int 267:173–182
11. Liu L, Tang L, Dong W, Yao S, Zhou W (2016) "An overview of topic modeling and its current applications in bioinformatics," SpringerPlus,vol. 5, no. 1, p. 1608, Dec
12. Porter K (2018) "Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling," Digit. Invest., vol. 26, pp. S87–S97, Jul
13. Nazah S, Huda S, Abawajy JH, Hassan MM (2021) An Unsupervised Model for Identifying and Characterizing Dark Web Forums, in IEEE Access, vol. 9, pp. 112871–112892
14. Ríos SA, Muñoz R (2012) "Dark web portal overlapping community detection based on topic models," in Proc. ACM SIGKDD Workshop IntellSecur. Informat. (ISI-KDD), pp. 1–7
15. Branwen G, Christin N, Décary-Hétu D et al Dark Net Market archives, 2011–2015, https://www.gwern.net/DNM-archives, dataset, Accessed: 2019-01-23, July 2015, url: https://www.gwern.net/DNM-archives
16. Georgoulias D, Yaben R, Vasilomanolakis E (2023) Cheaper than you thought? A dive into the darkweb market of cyber-crime products. In Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1–10
17. Christin N (2019) and Jeremy Thomas. Analysis of the supply of drugs and new psychoactive substances by Europe-based vendors via darknet markets in 2017–18. EMCDDA. Retrieved February 19: 2022
18. Biryukov A, Pustogarov I (2015) Bitcoin over Tor isn't a good idea, 2015 IEEE Symposium on Security and Privacy, pp. 122–134
19. Graczyk M, Kinningham K (2015) Automatic product categorization for anonymous marketplaces. Comput Sci, pp. 1–6
20. Moore D, Rid T (2016) Cryptopolitik Darknet Survival 58(1):7–38
21. Ghosh S, Das A, Porras P, Yegneswaran V, Gehani A (2017) Automated categorization of onion sites for analyzing the darkweb ecosystem. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1793–1802
22. Al-Nabki MW, Fidalgo E, Alegre E, Fernández-Robles L (2019) Torank: identifying the most influential suspicious domains in the tor network. Expert Syst Appl 123:212–226
23. Arnold N, Ebrahimi M, Zhang N, Lazarine B, Patton M, Chen H, Samtani S (2019) Dark-net ecosystem cyber-threat intelligence (CTI) tool. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 92–97
24. Hong T, Choi JA, Lim K, Kim P (2020) Enhancing personalized ads using interest category classification of SNS users based on deep neural networks. Sensors 21(1):199
25. Shan S, Sankaranarayana R Behavioral profiling of darknet marketplace vendors,2020
26. Jeziorowski S, Ismail M, Siraj A (2020) Towards image-based dark vendor profiling: an analysis of image metadata and image hashing in dark web marketplaces. In Proceedings of the Sixth International Workshop on Security and Privacy Analytics,pp. 15–22
27. Schäfer M, Fuchs M, Strohmeier M, Engel M, Liechti M, Lenders V (2019) BlackWidow: Monitoring the dark web for cyber security information. In 2019 11th International Conference on Cyber Conflict (CyCon), Vol. 900, pp. 1–21
28. Keim Y, Mohapatra AK (2022) Cyber threat intelligence framework using advanced malware forensics. Int j inf Tecnol 14:521–530
29. Sharma P, Nagpal B (2020) Regex: an experimental approach for searching in cyber forensic. Int J Inform Technol 12:339–343
30. Tank D, Aggarwal A, Chaubey N (2022) Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. Int j inf Tecnol 14:847–862
31. Jain G, Sharma M, Agarwal B (2019) Optimizing semantic LSTM for spam detection. Int j inf Tecnol 11:239–250
32. Raju E, Ramadevi Y, Sravanthi K (2018) CILPA: a cohesion index based label propagation algorithm for unveiling communities in complex social networks. Int j inf Tecnol 10:435–445
33. Burbano D, Hernandez-Alvarez M (2017) Identifying human trafficking patterns online. In 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), pp. 1–6
34. Décary-Hétu D, Giommoni L (2017) Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime Law Social Change 67:55–75
35. Takaaki S, Atsuo I (2019) Dark web content analysis and visualization. In Proceedings of the ACM International Workshop on Security and Privacy Analytics,pp. 53–59
36. Mahor V, Rawat R, Kumar A, Chouhan M, Shaw RN, Ghosh A (2021) Cyber warfare threat categorization on cps by dark web terrorist. In 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON),pp. 1–6
37. Zeid RB, Moubarak J, Bassil C (2020) Investigating the darknet. In 2020 International Wireless Communications and Mobile Computing (IWCMC),pp. 727–732
38. Bahamazava K, Nanda R (2022) The shift of DarkNet illegal drug trade preferences in cryptocurrency: the question of traceability and deterrence. Forensic Sci International: Digit Invest, 40, p.301377
39. Al-Ramahi M, Alsmadi I, Davenport J (2020) Exploring hackers assets: topics of interest as indicators of compromise. In Proceedings of the 7th Symposium on Hot Topics in the Science of Security, pp. 1–4
40. Li Z, Du X, Liao X, Jiang X, Champagne-Langabeer T (2021) Demystifying the dark web opioid trade: content analysis on anonymous market listings and forum posts. J Med Internet Res, 23, 2
41. Shin GY, Jang Y, Kim DW, Park S, Park AR, Kim Y, Han MM (2023) Dark Side of the Web: Dark Web Classification Based on

TextCNN and Topic Modeling Weight. IEEE Access, Vol. 12, pp. 36361–36371, 2024

42. Tavabi N, Bartley N, Abeliuk A, Soni S, Ferrara E, Lerman K (2019) Characterizing activity on the deep and dark web. In Companion proceedings of the 2019 world wide web conference, pp. 206–213
43. Rawat R, Mahor V, Chirgaiya S, Shaw RN, Ghosh A (2021) Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm. In Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2021, pp. 671–681
44. Pete J, Hughes YT, Chua, Bada M, A Social Network Analysis and Comparison of Six Dark Web Forums, 2020 IEEE European Symposium on Security and, Workshops P (2020) (EuroS&PW), Genoa, pp. 484–493
45. Connolly K, Klempay A, McCann M, Brenner P (2023) Dark Web Marketplaces: Data for Collaborative Threat Intelligence. Digital Threats: Research and Practice, Vol. 4, No. 4, pp. 1–12
46. Iliadis LA, Kaifas T (2021) Darknet traffic classification using machine learning techniques. In 2021 10th international conference on modern circuits and systems technologies (MOCAST), pp. 1–4
47. Samtani S, Zhu H, Chen H (2020) Proactively identifying emerging hacker threats from the dark web: a diachronic graph embedding framework (d-gef). ACM Trans Priv Secur (TOPS) 23(4):1–33
48. Paracha AA, Arshad J, Khan MM (2023) SUS you're SUS! — Identifying influencer hackers on dark web social networks. Comput Electr Eng 107:108627
49. Pastrana S, Thomas DR, Hutchings A, Clayton R (2018) Crimebb: Enabling cybercrime research on underground forums at scale. In Proceedings of the 2018 World Wide Web Conference, pp. 1845–1854
50. Adewopo V, Gonen B, Elsayed N, Ozer M, Elsayed ZS Deep learning algorithm for threat detection in hackers forum (deep web). arXiv preprint arXiv:2202.01448, 2022.
51. Dong F, Yuan S, Ou H, Liu L, New Cyber Threat Discovery from Darknet Marketplaces, 2018 IEEE Conference on Big Data and, Analytics (2018) (ICBDA), Langkawi, Malaysia, pp. 62–67
52. Zenebe A, Shumba M, Carillo A, Cuenca S (2019) Cyber threat discovery from dark web. In: EPiC Series in Computing. vol. 64, pp. 174–183
53. Arora T, Sharma M, Khatri SK (2019) Detection of cyber crime on social media using random forest algorithm. In: 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC). pp. 47–51
54. Samtani S, Chinn R, Chen H, Nunamaker JF Jr (2017) Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. J Manage Inform Syst 34(4):1023–1053
55. Ali F, Basheer R, Kawas M, Alkhatib B (2023) Towards detecting influential members and critical topics from Dark web forums: A Data Mining Approach. J Inform Organizational Sci 47(1):1–20
56. Ambika N (2024) Early detection of Darknet Traffic in internet of things applications. Automated Secure Computing for Next-Generation Systems, pp. 139-153

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.