RESEARCH PAPER

Dark web crawling for automatic dark web classification using Bayesian Hierarchical Neural Attention Harmonic Network

Vinod Babu Bollikonda[1], K.V.D.Kiran[2]

[1]*Research Scholar,Department of CSE, Koneru Lakshmaiah Education Foundation AP, Vaddeswaram, India*
Email : 2002031023@kluniversity.in
[2]*Professor,Department of CSE, Koneru Lakshmaiah Education Foundation, AP, Vaddeswaram, India.*
Email :kiran_cse@kluniversity.in

ABSTRACT
Dark web is the canopy idea that specifies any sort of illegal actions conducted by unknown organizations or persons, thus making it complicated to track. The illegal contents on dark web are changed and updated constantly. The classification and collection of such activities are highly challengeable tasks, since they are time-consuming and difficult. In present times, it is emerged as a problem that needs rapid attention from academia and industry. In this research, Bayesian Hierarchical Neural Attention Harmonic Network (BHNAHN) is presented for dark web classification. Here, dark web crawling and classification of dark web are the two steps conducted. TorBot is employed for dark web crawling based upon keywords like pornography, financial gambling, drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. In dark web classification process, input web data is acquired and then, Bidirectional Encoder Representations from Transformers (BERT) tokenization is carried out. Afterwards, features are extracted from tokenized word. Finally, dark web classification is accomplished employing BHNAHN. However, BHNAHN is modeled by incorporating Bayesian Neural Network (BNN) and Hierarchical Neural Attention classifier with forward harmonic analysis. Additionally, BHNAHN obtained maximal accuracy, True Negative Rate (TNR) and True Positive Rate (TPR) about 91.362%, 92.440% and 90.799..

Keywords: Dark web, Bidirectional Encoder Representations from Transformers tokenization, Bayesian Neural Network, Hierarchical Neural Attention classifier, forward harmonic analysis

How to cite this article: Bollikonda VB, Kiran KVD: Dark web crawling for automatic dark web classification using Bayesian Hierarchical Neural Attention Harmonic Network .Int J Drug Deliv Technol. 2026;16 (3s): 960-972; DOI: DOI: 10.25258/ijddt.16.3s.116

Source of support:. None

Conflict of interest: None

INTRODUCTION

The World Wide Web comprises an enormous and non-index segment of an internet that is unseen from conventional web search engine [2]. A web is classified into two components such as surface web and deep web [5]. In an internet, visible part refers to surface web that emerges to be an expansive repository of data. Moreover, it indicates the simple fraction of complete web [1]. Deep web is a segment of internet that is not obtainable by classical search engine [6]. Few general instances in every day utilization of dark web are email mailboxes, internet banking, government datasets, medical reports and so on [3]. The subdivision of deep web termed dark web is recognized for its anonymous and connection with illicit actions, when it needs special software for accessing [6]. Additionally, dark web is analyzed and studied in security research communities for uncovering malevolent activities that include illegal online marketplace activities, terrorism, phishing, ransomware ecosystem and abuse of cryptocurrency [2]. The dark web assessment has an important part in combating and understanding illegal activities as well as cybersecurity risks generating from dark web. This offers effective insights that aid law enforcement agencies, cybersecurity experts and organizations remain notified and react efficiently to emergent challenges. Furthermore, dark web evaluation frequently involves an usage of special approaches, expertise and tools for collecting, processing and interpreting web data acquired from dark web during consideration of legal and ethical concerns. This assessment consists of two major systematic processing like dark web crawling and classification of dark web.

In dark web analysis, dark web crawling [11] [12] mentions to a process of systematic data collection from unknown online networks that constitute the portion of deep web [9] [10]. Moreover, it is stated as the processing with several demerits owing to features of The Onion Router (Tor) network [18], specifically, irrelevant websites, wherewith there is weaker link amongst sites, consequently making it difficult for crawler to track [5]. In this, onion routing or tor refers to the encrypted network frequently employed for accessing dark web such as. Tor Network, Tor browser, free and open-source software platforms, enables unknown communications [6]. In addition, classification of dark web implies to a process of analysis and categorizing web data acquired from dark web for identifying patterns, probable

**Author for Correspondence: Vinod Babu Bollikonda*

risks and trends. A process of classifying texts from dark web contains six interconnected phases. The phases are pre-processing of texts, transformation or text representation, reduction of dimension, application and selection of classification methods, classifier estimation as well as validation [8]. Furthermore, huge count of various algorithms and approaches of the dark web data classification helpful for developing crime data classifier are recently developed [4]. Some algorithms and methods utilized for classifying dark web data include Machine Learning (ML) schemes namely Naive Bayes (NB), Decision Trees (DT), Support Vector Machines (SVM), Neural Networks (NN) and Random Forests. Natural Language Processing (NLP) models like Word Embeddings, Bag-of-Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF) are utilized. It can be simply concluded that Deep Learning (DL) and ML approaches are exploited for classification of dark web data.

Conventionally, classifiers employed for dark web classification are tuned utilizing supervised training that is applied in large count of web pages [5]. Thereafter, several approaches are developed for classifying dark web. In ML methodology, forum data or dark web is operated employing DL or ML methods for achieving classification, clustering and detection results [1]. An application of ML for categorizing dark web includes dark web text pre-processing and its transformation into vector form [1]. Relying on learning tasks, the domain provides several ML algorithm classes. Individual of them appears in numerous variants and specifications including instance-enabled techniques, decision trees, regressions models, Artificial Neural Networks (ANNs) and Bayesian approaches [16]. When compared to ML techniques, DL approaches have diverse benefits for classification tasks of dark web. Particularly, DL is helpful in areas having higher and larger dimensional information and it species to a reason of Deep Neural Networks (DNN) to perform the shallow ML schemes better for various applications, wherein image, text, video, audio and speech data must be processed [16]. In addition, DL is specifically beneficial to categorize dark web owing to its capability for automatic learning of complicated patters from

original data without a need of manual feature understanding, making it appropriate for unstructured and varied forms of dark web contents. Presently, DL schemes like Graph Neural Networks (GNN) and NN together with classical models such as SVM, DT and NB have been employed for classification of dark web [1]. Therefore, researchers are progressively concentrating on categorization of dark web by exploiting diverse DL methods for achieving maximum accuracy [15].

The crucial aim is to design BHNAHN for dark web classification. Generally, dark web illustrates to hidden services offered by unknown communication systems. However, dark web has been frequently connected with the crimes in recent days. Therefore, misuse of dark web becomes much serious. In this research, two steps are carried out such as dark web crawling and dark web classification. An open-source intelligence termed TorBot is utilized for dark web crawling based upon pornography, financial gambling, drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. Then, dark web classification is performed by conducting phases like BERT tokenization, feature extraction and classification of dark web. Initially, input web data is acquired from TorBot dataset. After that, BERT tokenization is accomplished to obtain tokenized word. Thereafter, features namely punctuation, emoticon, BoW, count vectorization, TF-IDF, sentence length, hashtags, numerical data and all caps are extracted. Finally, dark web classification is performed employing BHNAHN and it is devised by joining BNN and Hierarchical Neural Attention classifier with forward harmonic analysis.

 Proposed BHNAHN for dark web classification: Presently, the classification of contents on dark web is an interesting topic for the researchers. Here, BHNAHN is introduced for dark web classification that is designed by combining BNN and Hierarchical Neural Attention classifier with forward harmonic analysis.

The following interpreted sections are structured as: Section 2 explains reviewed classical methods and their limitations, section 3 manifests BHNAHN methodology, section 4 represents BHNAHN outcomes and section 5 elucidates conclusion of BHNAHN.

2. Motivation

The dark web permits website operators and users to persist untraceable or anonymous and only available through particular software. As a dark web remains to expand and evolve, there emerges an essential requirement for inventive techniques to classify its unknowable websites exactly. This fact motivated to present a scheme for classifying dark web by collecting various existing approaches developed based on dark web classification. This part describes the collected methods and their drawbacks.

2.1 Literature Survey

Shin, G.Y., *et al.* [1] devised TextCNN for classifying dark web by eliminating insignificant dark web contents. This technique had a capability for discriminating the important keywords as well as their impacts utilizing modeling weights. However, it was incapable to categorize dark web by concerning its dynamic environment. Jin, Y., *et al.* [2] introduced Comprehensive Darkweb Annotations (CoDA) to offer deeper understanding about dark web. This scheme was capable to categorize lexical attributes, even though it did not classify web page structure instead of topics. Sangher, K.S., *et al.* [3] developed BERT-based classification model for identifying illegal

activities corresponding to the cybercrimes on dark web forum. In this model, an unbalanced data was pre-processed and recognized for effective classification, but still it failed to offer cybercrime subcategories. Kumar, P.S., *et al.* [4] presented NN- Semi Supervised Support Vector Machines (S3VM) for prediction of crime network activities to classify dark web. It had a capability to manage high and low-dimensional data, though it failed to track criminal activities.

Alaidi, A.H.M., *et al.* [5] presented Linear Support Vector Machine (LSVM) for crawling and classification of dark web illicit activities. This scheme attained superior performance in text categorization of higher-dimensional

input spaces, but it did categorize the collected web pages in an automated manner. Dalvi, A., *et al.* [6] designed multi-label classification method for assessment of dark web contents. The prediction of numerous labels for particular texts in dark web content was acquired, though it did not improve entity identification concurrently. Devarajan, S., *et al.* [7] introduced SVM with NN for improving classification of dark web. An approach was not able of integrating crawler with Tor network for ensuring privacy and anonymity. However, crawler operations were varied based upon data qualities and dark websites. Murty, C.A. and Rughani, P.H., [8] developed SVM for classifying dark web data. This method was unable to detect illicit activities employing texts of the hosted dark web, even though it did not support the investigators for tracking dark web.

2.2 Challenges

The reviewed technique's experienced challenges for classification of dark web are elucidated as follows.

- An approach presented in [1] did not predict the elimination of redundant words by topic modeling weights for yielding balancing advantages. Also, it failed to design a model that combines DL and topic modeling weights inside fused system for elucidating the NN features affecting overall outcomes.
- In [2], additional assessments by boilerplate elimination of noisy and non-structured texts were not attempted. Moreover, combined surface web data together with augmentation of broad variety of the surface web contents were not included.
- BERT-based classification model [3] led to highly consistent prediction for the unstructured data, even though it cannot be viewed as an alternate to human annotations due to unclear and imperfect information in dataset, which resulted in larger clusters.
- The designed model [5] failed to track and identify individuals involving in illicit activities. Furthermore, it did not highlight the risks and complexities involved to address criminal behaviors in hidden space.
- The conventional dark web structural pattern extraction approaches are not suitable to classify web data exactly owing to two limitations like computation complexities and significant memory requirements. Therefore, an effective system is necessary for classification of dark web.

3. Proposed BHNAHN for dark web classification

Dark web provides a platform for conversation, coordination and diverse activities by forums. The obtained information from dark web sources frequently lacks configuration, making it challengeable for classification and analysis. Here, BHNAHN is designed for dark web classification. Here, dark web crawling and dark web classification are the steps conducted.

Initially, TorBot is employed for dark web crawling based upon pornography, financial gambling, drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. After that, dark web classification is accomplished. Firstly, input web data is obtained from TorBot dataset. Then, BERT tokenization is carried out and next, features namely punctuation, emoticon, BoW, count vectorization, TF-IDF, sentence length, hashtags, numerical data and all caps are extracted. Lastly, dark web is classified utilizing BHNAHN, which is introduced by merging BNN and Hierarchical Neural Attention classifier with forward harmonic analysis. Figure 1 exposes graphical view of BHNAHN

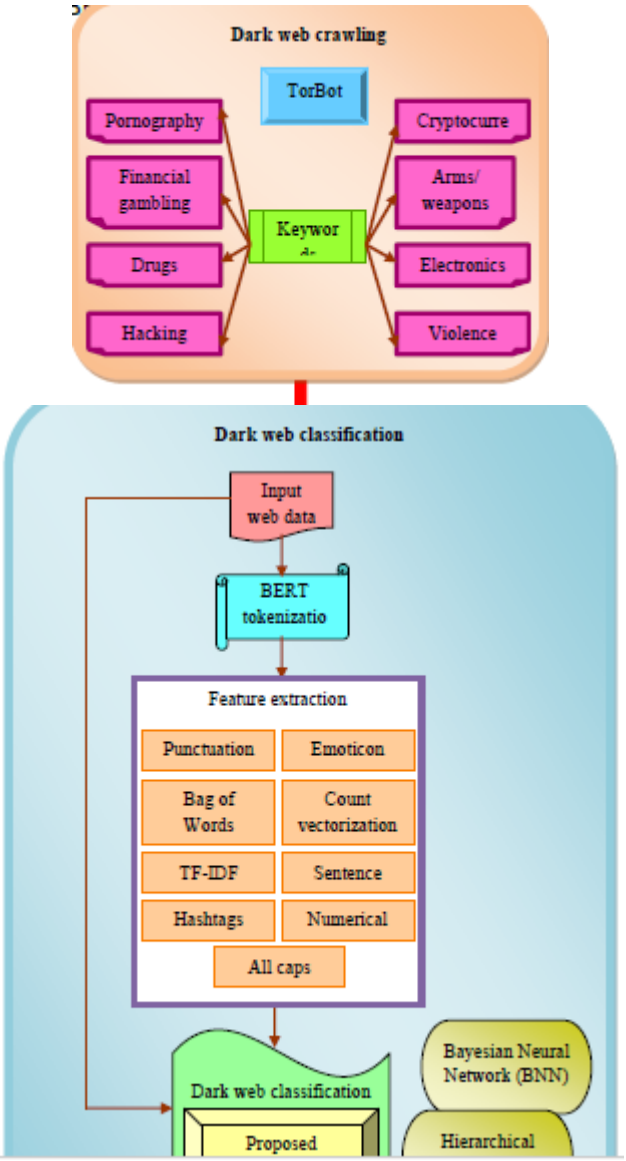


Figure 1. Graphical view of BHNAHN for dark web classification

3.1 TorBot system for dark web crawling

Dark web crawling refers to a process of data collection from the websites, which are not recorded by conventional search engines and are frequently related with illegitimate activities.

Generally, dark web crawling is carried out for accessing and extracting information from the hidden websites on dark web. This section explains the TorBot system and the keywords utilized for performing dark web classification.

3.1.1 TorBot explanation

TorBot employs Tor network for providing unknown and securable communications. It is

devised for protecting user's privacy and assures that their conversations are highly encrypted.
TorBot can be employed for diverse purposes like secured messaging, anonymous internet
browsing and accessing the websites that are prohibited in specific regions. TorBot consists of
features [25] like Onion Crawler (.onion), returns back host name or page titles while no title is
obtainable and provides short explanation of particular site, save the links to database, output
HTML from sites or saves it to HTML files, saves link tree as JSON file, crawls custom domain,
verify whether link is live, built-in updater and construct visual tree of link relations that can be
viewed or saved quickly. Moreover, it includes curated features namely visualization module
revamp, implementation of BFS search for web crawler, enhanced stability, increased test
coverage, saving of latest search resultants to database, randomizes Tor link, phrase or keyword
search, social media incorporation, improve anonymity and capturing of screenshot.

3.1.2 Keywords

Some of the keywords considered for dark web crawling are pornography, financial gambling,
drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. The keywords assist to
identify particular themes or topics within enormous and frequently unindexed contents of dark
web.

3.2 Dark web classification

The dark web classification is based upon anonymity it offers to users and illicit nature of
various activities that happen on specific platforms. Here, the phases like input web data
collection, BERT tokenization, feature extraction and dark web classification are performed.

3.2.1 Input web data collection

An input web data is collected from various websites based upon the keywords mentioned above
and an input web data can be represented asW .

3.2.2 BERT tokenization

BERT tokenization is carried out by considering input web data denoted asW . The BERT
tokenization is a technique for breaking down texts into individual tokens, which are thereafter
employed as an input for BERT model. BERT [13] is developed for pre-tuning deep
bidirectional systems from an unlabelled text by cooperatively tuning both left-side and rightside
texts in every layer. Therefore, it is trained finely with an output layer to generate traditional
schemes for large number of processes without considerable task-definite structural adjustments.
An input model is capable for clear depiction of one sentence or two sentences in a single token
sequence to build BERT highly efficient in controlling several downstream tasks. Herein,
"sentence" refers to unlimited span of adjacent texts except normal language sentences whereas
"sequence" signifies as the input token sequences to BERT that specifies a sentence or pair of
sentences joined together. A prime token of all sequences mentions to special classification token
always. A lastly present hidden state according to this token is employed as incorporated
sequence depiction for a purpose of classification. Moreover, paired sentences are packed
collectively into a sequence. From BERT tokenization, tokenized word is acquired and it is
indicated as □ , such that,

$$\mathbf{B} = \{B_1, B_2, ..., B_i\} \quad (1)$$

3.2.3 Feature extraction based on tokenized word

Feature extraction is a process to select and transform raw input data into group of features that
are highly helpful and simple to support classification of dark web contents. Here, features
namely punctuation, emoticon, BoW, count vectorization, TF-IDF, sentence length, hashtags,
numerical data and all caps are extracted. An input given to extract features is tokenized word
denoted as □ .

(i) Punctuation

The punctuation [22] includes apostrophe, exclamation mark or dot comprised in web data and it
can be evaluated as,

$$G_1 = \sum_{z=1}^{\zeta} V_p^z \quad (2)$$

Here, z V□ mentions total punctuation comprised in th z web data whereas 1 G denotes extracted
punctuation marks.

(ii) Sentence length

The sentence length refers to count of characters or words in a sentence. The length of sentence
in web data is implied as 2 G .

(iii) Emoticon

Emoticons [22] are pictographic depiction of the facial appearances utilizing definite characters
such as letters, punctuation marks or numbers. The extracted number of emoticons in web data
can be illustrated as 3 G .

(iv) Hashtags

Hashtag [22] is generally employed to depict concentration, promote and arrange. The hashtag
utilization assists people to contribute, follow and determine in a conversation. 4 G illustrates the
number of hashtags in web data.

(v) BoW

BoW [20] is a simpler format of representing texts in numbers and it can be exploited for
transforming texts into BoW that maintains overall occurrence of most basically exploited
words. The number of occurrence of words in web data is symbolized as 5G .

(vi) Numerical data

Numerical data illustrates to a data that is represented in the format of numbers like decimals or

integers. The number of numerical data in web data can be signified as 6G .
(vii) Count vectorization
Count vectorization [21] represents to total occurrences of a word appearing in the web data. The
term 7G refers to count vectorization.
(viii) All caps
All caps elucidate to the capital letters in a web data and count of all capital words in web data
can be described as 8 G .
(ix) TF-IDF
TF-IDF [14] is same like count vectorization, but it presents weight factor. TF-IDF comprises of
two segments namely Term Frequency (TF) as well as Inverse Document Frequency (IDF). TF
concerns overall occurrence of particular word within web data. TF-IDF can be computed as
mentioned below.

$$TF = \frac{\mathrm{H}}{\mathrm{M}} \quad (3)$$

$$IDF = \log\frac{\mathrm{A}}{\mathfrak{Z}} \quad (4)$$

$$G_9 = TF \times IDF \quad (5)$$

Here, □ denotes overall occurrence of word in web data, □ specifies overall words in web data,
□ manifests count of every web data, □ mentions frequency of web data and 9 G reveals TF-IDF
feature.
From feature extraction phase, feature vector J is acquired, such that,

$$J = \{G_1, G_2, G_3, \ldots, G_9\} \quad (6)$$

3.2.4 Dark web classification utilizing BHNAHN
The stronger anonymousness and difficult-to-trace processes of dark web offers shelter for
illegitimate activities. The illicit contents on dark web is varied and regularly updated. The
conventional dark web classification utilizes larger-scale web pages for training. However,
complexity of gathering sufficient illicit dark web contents and time consuming of manual
labeling web pages have been become challenges of present researches. Here, BHNAHN is
introduced for dark web classification. BHNAHN is designed by incorporating BNN and
Hierarchical Neural Attention classifier with forward harmonic analysis.
Initially, feature vector J is multiplied with $1Q^{c}_{c=1}$ and thus, summation of weight □ 1 Q is acquired.
On the other side, feature vector J is passed to BNN and its outcome is multiplied with □ 1 Q to
attain BNN output. Simultaneously, input web dataW is fed to Hierarchical Neural Attention
classifier and then, weight 2Q is applied to its outcome. The obtained resultant is again multiplied
with BNN outcome for obtaining Hierarchical Neural Attention classifier output. Finally,
forward harmonic analysis concept is applied to both outputs attained from BNN and
Hierarchical Neural Attention classifier. From this process, dark web classified outcome is
achieved and the general view of BHNAHN for dark web classification is demonstrated in figure
2.

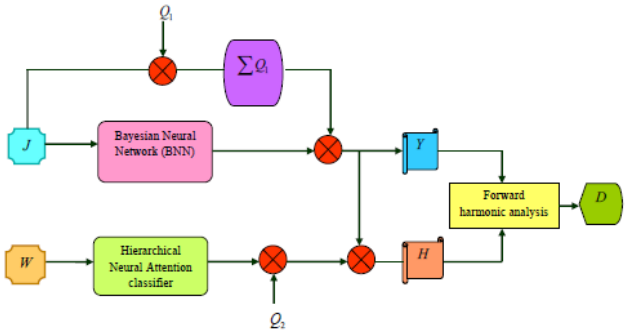


Figure 2. General view of BHNAHN for dark web classification

(i) Structure of BNN
BNN [17] leverages a power of ML in the data and predictive analysis for computing spatiotemporal altering model biases and weights. A feature vector J is subjected as an input to BNN.

Consider the observations $g(u.l)$ at certain position u as well as time l can be designed as sum over ensemble of κ model prediction $K_c\ (u,l\ )$ weighted by their corresponding weights $\xi_c(u,l)$, bias $\varpi(u,l)$ and data noise $\eta(u,l)$. BNN takes data position (u) and time (l) as input and evaluates weight, bias and data noise at given (u,l) by measuring an output against the observations.
Initially, BNN utilizes group of dense layers for extracting normal data of model biases, data noises and weights. Thereafter, three groups of dense layers are designed for learning information definite to individual element. After that, BNN integrates numerous model predictions $K_c\ (u,l\ )$ and incorporates them with computed model's biases, data noises and weights
in loss function for matching ensemble predictions with observation as follows

$$Y = \left[\sum_{1}^{\kappa}\xi\ (u,l)K\ (u,l)+\varpi\ (u,l)\right]*\left[\sum Q\ *J\right]$$

A network is tuned in Bayesian contexts utilizing randomized maximum a posteriori (MAP). MAP sampling technique employs numerous NNs for quantifying ML system prediction
improbability. Particularly, for ∂^{th} NN, the sample is drawn from previous distribution across network parameter $\theta_{a,\partial} \sim R(\varphi_p, \Sigma_{prior}\ )$ and evaluates MAP related to previous re-centered at $\theta_{a,\partial}$

. When considering the database of R observations $\{g_c, u_c, l_c\}$ and reveal a data likelihood by concerning Gaussian noise $\eta(u,l)$, an evaluation of MAP is similar to minimization of beneath loss function for ∂^{th} NN,

$$L_\partial = \sum_{c=1}^{R} \frac{(g_c - \hat{g}_\partial(u_c, l_c))^2}{\eta^2_\partial(u_c, l_c)} + \sum_{c=1}^{R} \log(\eta^2_\partial(u_c, l_c)) + \left\| \Sigma_n^{-1/2}(\upsilon_\partial - \upsilon_{a_\partial}) \right\|_2^2 \quad (6)$$

$$L_\partial = \sum_{c=1}^{R} \frac{(g_c - \hat{g}_\partial(u_c, l_c))^2}{\eta^2_\partial(u_c, l_c)} + \sum_{c=1}^{R} \log(\eta^2_\partial(u_c, l_c)) + \left\| \Sigma_n^{-1/2}(\upsilon_\partial - \upsilon_{a_\partial}) \right\|_2^2 \quad (6)$$

A prediction of tuned ensemble with r_ε NNs is thus an integration of r_ε Gaussians, given as $R(\hat{g}_\partial(u_c, l_c), \eta^2_\partial(u_c, l_c))$. A mean value of NN predictions $\frac{1}{r_\varepsilon}\sum \hat{g}_\partial$ is the last BNN outcomes and variance $\frac{1}{r_\varepsilon}\sum \eta^2_\varepsilon + \frac{1}{r_\varepsilon}\sum \hat{g}^2_\partial - \left(\frac{1}{r_\varepsilon}\sum \hat{g}_\partial\right)$ computes predictive uncertainties, wherein initial term measures data uncertainties and next term evaluates epistemic uncertainties. An outcome from BNN is mentioned as Y and the structural design of BNN is delineated in figure 3.

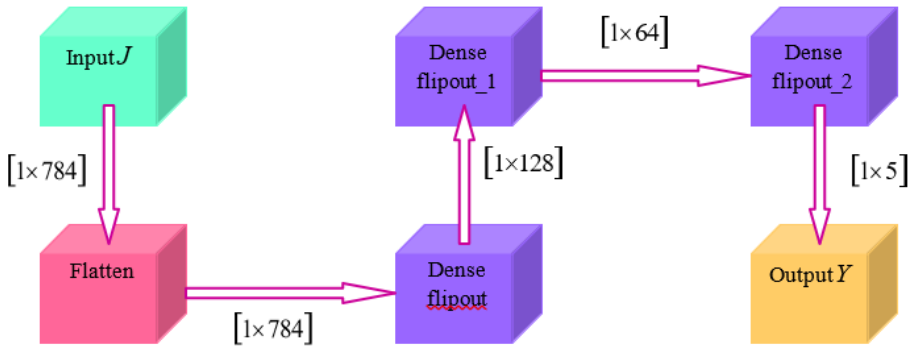


Figure 3. Structural design of BNN

Architecture of Hierarchical Neural Attention classifier

Hierarchical Neural Attention classifier [19] is developed to address the problems of explosion models. The keystone of this classifier is single encoder-decoder configuration that successively predicts a class label of subsequent level, trained on dynamic web data representation attained based upon modification of attention process. In Hierarchical Neural Attention classifier, web data W is subjected as an input.

Assume, web data having w tokens as well as categorization labels of d levels $S = (s_1, ..., s_d), s_\nu \in \{s^{\tau_\nu}_1, ..., l^{\tau_\nu}_{\chi_\nu}\}$, whereint τ_ν represents ν^{th} level of category taxonomy whereas χ_ν indicates total classes in ν level. Initially, bidirectional Long Short-Term Memory (LSTM) is employed to extract appropriate features from web data.

$$\overrightarrow{y_T} = \overrightarrow{LSTM}\left(\underline{m_T}, \overrightarrow{y_{T-1}}\right) \quad (9)$$

$$\overleftarrow{y_T} = \overleftarrow{LSTM}\left(\underline{m_T}, \overleftarrow{y_{T+1}}\right) \quad (10)$$

A hidden state of an encoder specified as $Y = (y_1, \ldots, y_w)$ are introduced by concatenating $\left(\overrightarrow{y_T}\right)$ and $\left(\overleftarrow{y_T}\right)$ as $y_\alpha = \left[\overrightarrow{y_T}, \overleftarrow{y_T}\right]$, wherein $\overrightarrow{y_T}, \overleftarrow{y_T}$ indicates input web data W.

During categorization of class labels at a level v, the $\overline{Y_v}$ features are developed initially by performing concatenation of s_{v-1} with every output of an encoder implied as $Y = (y_1, \ldots, y_w)$ is given by,

$$\overline{Y_v} = Y \oplus \tau_{v-1} \quad (11)$$

Thereafter, w vectors in $\overline{Y_v}$ are converted to w attention scores by sequences of linearity and non-linearity transformations as follows.

$$\mu_v = soft\max\left(m_{\chi 2} \tanh\left(Z_{\chi 2}\overline{Y_v}^{\mathrm{T}}\right)\right) \quad (12)$$

The representation of web data for y level is acquired by conducting multiplication of multi-head attention matrix as well as features that can be modeled as,

$$M_v = Z_{\chi 3} K_v \overline{Y_v} \quad (13)$$

Lastly, two layer Multi-Layer Perceptron (MLP) is exploited to categorize classes at v level.

$$\gamma_v = RELU\left(Z_M\left[\underline{M_v}, \gamma_v - 1\right]\right) \quad (14)$$

$$H = \left[soft\max\left(Z_v \gamma_v\right)\right] * Q_2 * Y \quad (15)$$

$$H = \left[soft\max\left(Z_v \gamma_v\right)\right] * Q_2 * \left[\sum_{c=1}^{\kappa} \xi_c(u,l) K_c(u,l) + \varpi(u,l)\right] * \left[\sum Q_1 * J\right] \quad (16)$$

Here, H specifies outcome from Hierarchical Neural Attention classifier and an architectural depiction of Hierarchical Neural Attention classifier is exhibited in figure 4.

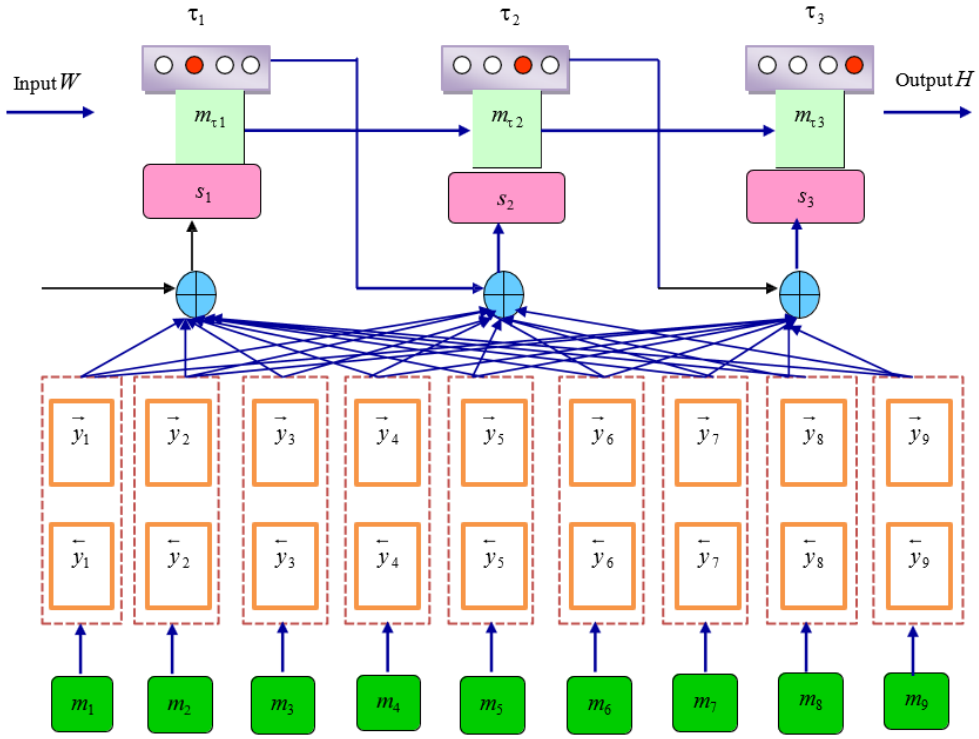


Figure 4. Architectural depiction of Hierarchical Neural Attention classifier

Forward harmonic analysis

Forward Harmonic analysis [24] is exploited as initiation value in cooperation with impacts estimated by most recent and efficacious model of Bolviken. Furthermore, frequency is determined in the harmonic analysis by a numerical search. The inputs passed to forward harmonic analysis are BNN outcome Y and Hierarchical Neural Attention classifier outcome H .

For time series q□1□, q□2□,..., q□b□,..., q□x□ , a standard formulation of the harmonic analysis is described as

$$q_{(b)} = v_0 + \sum_{\ell=1}^{K} (v_\ell \cos(2\pi\ \ell / x) + t_\ell \sin(2\pi\ \ell / x)) \tag{17}$$

Assume, $x = 2$ and $K = 1$, therefore above equation becomes,

$$q_{(b)} = v_0 + v_1 \cos\left(\frac{2\pi\ \ell}{2}\right) + t_1 \sin\left(\frac{2\pi\ \ell}{2}\right) \tag{18}$$

$$q_{(b)} = v_0 + v_1 \cos\pi\ \ell + t_1 \sin\pi\ \ell \tag{19}$$

Here, the expressions for v_0, v_1 and t_1 are interpreted as follows.

$$v_0 = \frac{1}{2}[q_{(1)} + q_{(2)}] \tag{20}$$

$$v_\ell = \frac{2}{x} \sum_{b=1}^{x} q_b \cos\left(\frac{2\pi\ \ell}{2}\right) \tag{21}$$

$$v_1 = \frac{2}{2}\left[q_{(1)} \cos\left(\frac{\cos 2\pi}{2}\right) + q_{(2)} \cos\left(\frac{2\pi\ 2}{2}\right)\right] \tag{22}$$

$$v_1 = q_{(1)}(-1) + q_{(2)}(1) \tag{23}$$

$$t_\ell = \frac{2}{x} \sum_{b=1}^{x} q_1 \sin(2\pi\ \ell / x) \tag{24}$$

$$t_1 = \frac{2}{2}\left[q_{(1)} \sin\left(\frac{2\pi}{2}\right) + q_{(2)} \sin\left(\frac{2\pi\ 2}{2}\right)\right] \tag{25}$$

$$t_1 = q_{(1)} \sin(\pi) + q_{(2)} \sin(2\pi) \tag{26}$$

As $\sin\pi = 0$ and $\sin 2\pi = 0$, an above equation becomes,

$$t_1 = q_{(1)} * 0 + q_{(2)} * 0 \tag{27}$$

Herein, time series model can be expounded as $q(b-1), q(b), q(b+1)$ and thus,

$$q_{(1)} = q(b-1) \tag{28}$$

$$q_{(2)} = q(b) \tag{29}$$

$$q_{(3)} = q(b+1) \tag{30}$$

Substitute Eq. (28), Eq. (29) and Eq. (30) in Eq. (19), Eq. (20), Eq. (23) and Eq. (27), thus the equations can be revealed as,

$$q(b+1) = v_0 + v_1 \cos\pi\ell + t_1 \sin\pi\ell \tag{31}$$

$$v = \frac{1}{2}[q(b-1) + q(b)] \tag{32}$$

$$v_1 = -q(b-1) + q(b) \tag{33}$$

$$t_1 = 0 \tag{34}$$

Substitute Eq. (32), Eq. (33) and Eq. (34) in Eq. (31), therefore an equation can be formulated by,

$$q(b+1) = \frac{1}{2}[q(b-1) + q(b)] + (-q(b-1) + q(b))\cos\pi\ell \tag{35}$$

$$q(b+1) = \frac{1}{2}q(b-1) + \frac{1}{2}q(b) - q(b-1)\cos\pi\ell + q(b)\cos\pi\ell \tag{36}$$

$$q(b+1) = q(b)\left[\frac{1}{2} + \cos\pi\ell\right] + q(b-1)\left[\frac{1}{2} - \cos\pi\ell\right] \tag{37}$$

$$q(b+1) = q(b)\left[\frac{1+2\cos\pi\ell}{2}\right] + q(b-1)\left[\frac{1-2\cos\pi\ell}{2}\right] \tag{38}$$

Let us consider,

$$q(b) = Y \tag{39}$$

$$q(b-1) = H \tag{40}$$

$$q(b+1) = D \tag{41}$$

Therefore, Eq. (38) becomes,

$$D = Y\left[\frac{1+2\cos\pi\ell}{2}\right] + H\left[\frac{1-2\cos\pi\ell}{2}\right] \tag{42}$$

$$D = \left[\sum_{i=1}^{K} \xi\,(w_i)K_{(w_i)} + \varpi\,(w_i)\right] * \left[\sum Q * J\right]\left[\frac{1+2\cos\pi\ell}{2}\right] + \left[[softmax(Z\,\gamma\,\ldots)] * Q\right] * \left[\sum_{i=1}^{K} \xi\,(w_i)K_{(w_i)} + \varpi\,(w_i)\right] * \left[\sum Q * J\right]\left[\frac{1-2\cos\pi\ell}{2}\right] \tag{43}$$

$$D = \left[\sum_{i=1}^{K} \xi\,(w_i)K_{(w_i)} + \varpi\,(w_i)\right] * \left[\sum Q * J\right]\left[\frac{1+2\cos\pi\ell}{2}\right] + \left[softmax(Z\,\gamma\,\ldots) * Q\right]\left[\frac{1-2\cos\pi\ell}{2}\right] \tag{44}$$

Here, D mentions dark web classified outcome whereas Y and H are outputs from BNN and Hierarchical Neural Attention classifier.

RESULTS AND DISCUSSION

The outcomes achieved by BHNAHN for performance and comparative evaluations are elaborated in this section.

Experiment setup

In this research, BHNAHN devised for dark web classification is experimentally implemented in PYTHON tool.

Dataset description

TorBot dataset [25] includes the keywords like pornography, financial gambling, drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. Based on the provided depth and keywords, the web data contents are collected. This dataset comprises of nine features and ten curated features that are mentioned in section 3.1.1.

Evaluation metrics

Accuracy, TNR and TPR are concerned as evaluation metrics to conduct performance and comparative analysis of BHNAHN.

Accuracy

Accuracy [23] illustrates to a degree of exactness in labeling and categorizing data identified on dark web, which can be given by

$$A = \frac{E+G}{E+G+I+L} \tag{45}$$

Here, E denotes true positive (TP) and G mentions true negative (TN) whereas I represents false positive (FP) and L depicts false negative (FN).

TNR

TNR [23] refers to a proportion of normal non-dark web data that is identified exactly by the model, which is evaluated as

$$N = \frac{G}{G+I} \tag{46}$$

4.3.3 TPR

TPR [23] measures a proportion of normal dark web activities that are preciously detected by particular classification model and it is formulated as,

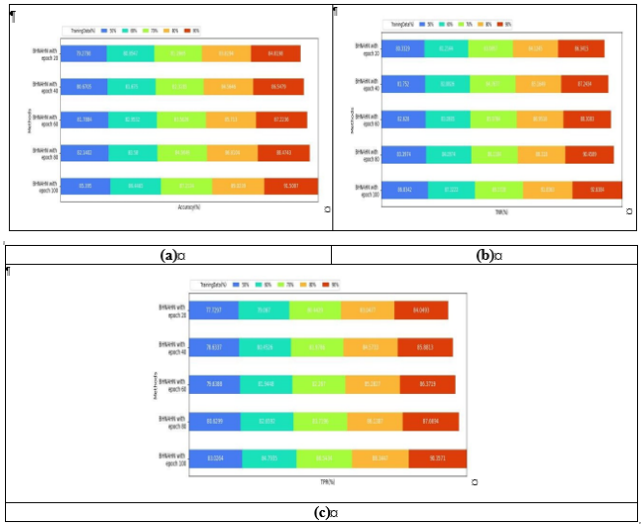
$$P = \frac{E}{E+L} \tag{47}$$

Performance analysis

An analysis to reveal the performance of BHNAHN is accomplished based upon training data and K-fold.

Analysis regarding training data

Figure 5 exposes estimation of BHNAHN considering measures by varying training data. This section represents the acquired performance values of BHNAHN while training data is 90%. Figure 5 a) interprets analysis of BHNAHN in accordance with accuracy. BHNAHN achieved accuracy of 84.820%, 86.548 %, 87.224%, 88.474% and 91.509% with epochs 20, 40, 60, 80 and 100. Estimation of BHNAHN regarding TNR is described in figure 5 b). TNR obtained by BHNAHN with 20, 40, 60, 80 and 100 epochs is 86.342%, 87.243%, 88.308%, 90.459% and 92.638%. Figure 5 c) describes analysis of BHNAHN with concern to TPR. With 20, 40, 60, 80 and 100 epochs, BHNAHN acquired TPR of 84.049%, 85.881%, 86.372%, 87.669% and 90.357%



(a)¤ (b)¤

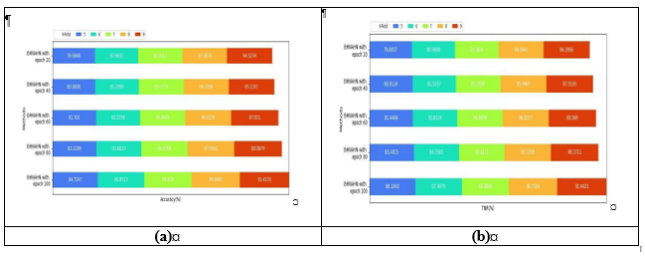
(c)¤

Figure 5. Performance analysis concerning training data, a) Accuracy, b) TNR, c) TPR

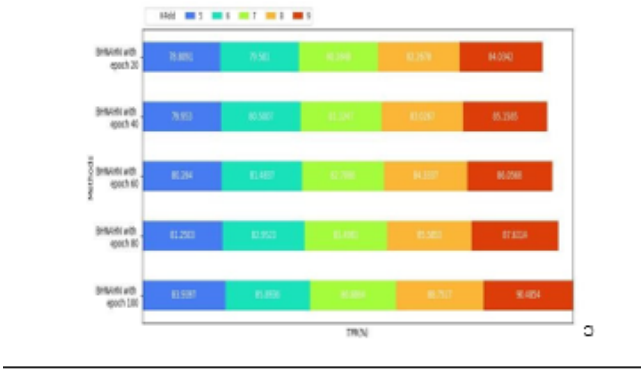
Analysis regarding K-fold

Analysis of BHNAHN concerning metrics by varying K-fold is delineated in figure 6. This portion elucidates obtained performance values by BHNAHN for K-fold=9. Estimation of BHNAHN in regards of accuracy is mentioned in figure 6 a). Accuracy acquired by BHNAHN with 20, 40, 60, 80 and 100 epochs is 84.523%, 85.120%, 87.921%, 88.888% and 91.423%.

Figure 6 b) reveals evaluation of BHNAHN by means of TNR. With 20, 40, 60, 80 and 100 epochs, TNR obtained by BHNAHN is 86.396%, 87.554%, 88.569%, 89.271% and 92.442%. Figure 6 c) depicts evaluation of BHNAHN in relation of TPR. BHNAHN attained TPR of 84.034%, 85.158%, 86.057%, 87.631% and 90.485% with epochs 20, 40, 60, 80 and 100



(a)¤ (b)¤



(c)¤

Figure 6. Performance analysis concerning K-fold, a) Accuracy, b) TNR, c) TPR

Comparative techniques

The conventional schemes like TextCNN [1], CoDA [2], BERT-based classification model [3] and LSVM [5] are taken as comparative methods to carry out assessments of BHNAHN to reveal its effectiveness.

Comparative evaluation

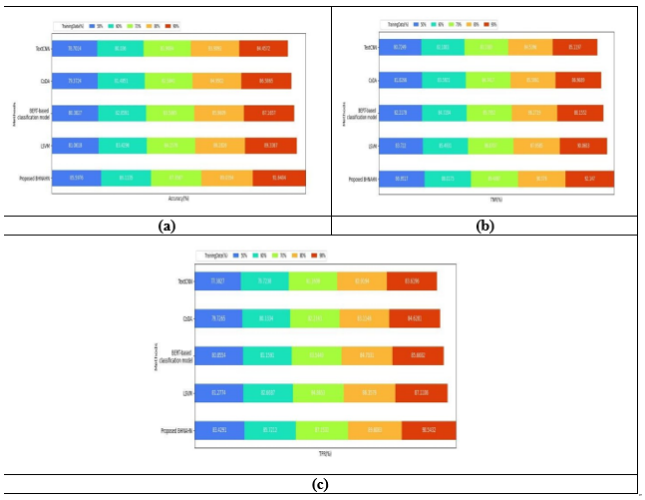
The evaluation to prove the effectiveness of BHNAHN is performed regarding training data and K-fold.

Analysis regarding training data

Figure 7 displays assessment of BHNAHN based upon measures by varying training data. This part describes the values of BHNAHN and classical models while training data is 90%. Figure 7

a) represents estimation of BHNAHN corresponding to accuracy. BHNAHN attained accuracy of 91.648% whereas TextCNN, CoDA, BERT-based classification model and LSVM obtained 84.457%, 86.586%, 87.166 % and 89.337%. This explains enhancement in performance by 7.846 %, 5.523%, 4.891% and 2.522%. Analysis of BHNAHN as regards TNR is illustrated in figure 7 b). TNR acquired by TextCNN, CoDA, BERT-based classification model and LSVM is 85.120%, 86.969%, 88.155% and 90.060% whereas BHNAHN obtained 92.147%. It interprets

enhancing in performance about 7.626%, 5.619%, 4.332% and 2.264%. Figure 7 c) demonstrates evaluation of BHNAHN with respective of TPR. TPR attained by TextCNN, CoDA, BERT- based classification model and LSVM is 83.620%, 84.628%, 85.668% and 87.111% while TPR achieved by BHNAHN is 90.543%. This mentions improvement in performance by 7.647%, 6.533%, 5.384% and 3.791%



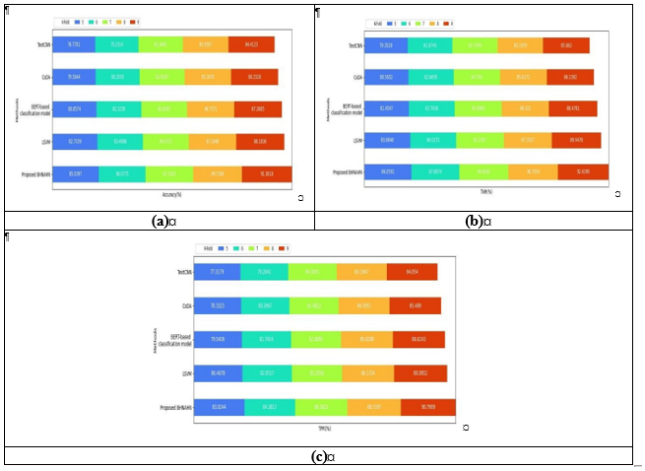
(a) (b) (c)

Figure 7. Comparative analysis regarding training data, a) Accuracy, b) TNR, c) TPR

Analysis regarding K-fold

Evaluation of BHNAHN considering metrics by changing K-fold is indicated in figure 8. This section elucidates the values of existing methods and BHNAHN when k-fold is 9. Analysis of BHNAHN relative to accuracy is described in figure 8 a). Accuracy acquired by TextCNN, CoDA, BERT-based classification model and LSVM is 84.412%, 86.153%, 87.269% and 88.184% whereas BHNAHN achieved 91.362%. It illustrates enhancement in performance by 7.607%, 5.702%, 4.480% and 3.479%. Figure 8 b) displays assessment of BHNAHN based upon TNR. TNR obtained by TextCNN, CoDA, BERT-based classification model and LSVM is 85.062%, 86.139%, 88.478% and 89.948% while TNR acquired by BHNAHN is 92.440%. This

specifies performance enhancement about 7.981%, 6.816%, 4.285% and 2.695%. Estimation of BHNAHN according to TPR is represented in figure 8 c). BHNAHN achieved TPR of 90.799% whereas TextCNN, CoDA, BERT-based classification model and LSVM acquired 84.054%, 85.489%, 86.624% and 88.095%. This describes performance enhancing about 7.428%, 5.848%, 4.598% and 2.978%



(a)¤ (b)¤ (c)¤

Figure 8. Comparative analysis regarding K-fold, a) Accuracy, b) TNR, c) TPR

Comparative discussion

Table 1 manifests the values obtained for comparative assessments by TextCNN, CoDA, BERT- based classification model, LSVM and designed BHNAHN. When K-fold=9, BHNAHN achieved accuracy of 91.362% whereas TextCNN, CoDA, BERT-based classification model and LSVM obtained 84.412%, 86.153%, 87.269% and 88.184%. A maximal accuracy achieved by BHNAHN specifies that it can efficiently combat and monitor illicit activities in dark web. For considered K-fold=9, TextCNN, CoDA, BERT-based classification model and LSVM achieved TNR of 85.062%, 86.139%, 88.478% and 89.948% whereas BHNAHN attained 92.440%. A maximum TNR implies that BHNAHN is effectual in differentiating non-dark web data and dark web data. TPR acquired by BHNAHN is 90.799% while K-fold=9 whereas TextCNN, CoDA, BERT-based classification model and LSVM attained 84.054%, 85.489%, 86.624% and 88.095%. A high TPR reveals that BHNAHN is capable to exactly detect an occurrence of dark web activities. From the evaluations conducted, BHNAHN is revealed as a best scheme for dark web classification as it acquired maximum accuracy, TNR and TPR of 91.362%, 92.440% and 90.799% while K-fold=9.

Table 1. Comparative discussion of BHNAHN

Datasets	Metrics/ Methods	TextCNN	CoDA	BERT-based classification model	LSVM	Proposed BHNAHN
Training data=90%	*Accuracy (%)*	84.457	86.586	87.166	89.337	91.648
	TNR (%)	85.120	86.969	88.155	90.060	92.147
	TPR (%)	83.620	84.628	85.668	87.111	90.543
K-fold=9	*Accuracy (%)*	84.412	86.153	87.269	88.184	**91.362**
	TNR (%)	85.062	86.139	88.478	89.948	**92.440**
	TPR (%)	84.054	85.489	86.624	88.095	**90.799**

CONCLUSION

Dark web has been become the larger repository of an unauthorized data while comparing with surface web owing to its advantage of privacy and anonymity. A dark web is becoming secure location for illegitimate activities. With an enhancing utilization of dark web users, it is necessary for the cyber security experts all over the world to perform dark web classification. This classification assists to understand several illicit activities for controlling and categorizing it with the feature engineering. In this research, BHNAHN is presented for dark web classification. Here, dark web crawling and dark web classification are the two steps performed. At first, TorBot is utilized for dark web crawling based upon pornography, financial gambling, drugs, hacking, cryptocurrency, arms/weapons, electronics and violence. Next, dark web classification is carried out. Initially, input web data is acquired from TorBot dataset and thereafter, BERT tokenization is conducted. Afterwards, features like punctuation, emoticon, BoW, count vectorization, TF-IDF, sentence length, hashtags, numerical data and all caps are extracted. Finally, classification of dark web is accomplished employing BHNAHN that is devised by combining BNN and Hierarchical Neural Attention classifier with forward harmonic analysis. Moreover, BHNAHN attained maximal accuracy, TNR and TPR about 91.362%, 92.440% and 90.799% for K-fold=9. As a future task, this research will be extended by labeling newer dark web pages

REFERENCE

1. Shin, G.Y., Jang, Y., Kim, D.W., Park, S., Park, A.R., Kim, Y. and Han, M.M., "Dark Side of the Web: Dark Web Classification Based on TextCNN and Topic Modeling Weight", IEEE Access, 2023.

2. Jin, Y., Jang, E., Lee, Y., Shin, S. and Chung, J.W., "Shedding new light on the language of the dark web", arXiv preprint, arXiv:2204.06885, 2022.

3. Sangher, K.S., Singh, A., Pandey, H.M. and Kumar, V., "Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes", Information, vol.14, no.6, pp.349, 2023.

4. Kumar, P.S., Rubia, J.J., Anitha, R. and Degadwala, S., "Dark web data classification using deep neural network", International Journal of Electronic Security and Digital Forensics, vol.16, no.2, pp.202-212, 2024.

5. Alaidi, A.H.M., Roa'a, M., ALRikabi, H.T.H.S., Aljazaery, I.A. and Abbood, S.H., "Dark web illegal activities crawling and classifying using data mining techniques", iJIM, vol.16, no.10, pp.123, 2022.

6. Dalvi, A., Bhoir, S., Naik, N., Kitkaru, A., Siddavatam, I. and Bhirud, S., "A Hybrid TF-IDF and RNN Model for Multi-label Classification of the Deep and Dark Web", International Journal of Advanced Computer Science and Applications, vol.14, no.7, 2023.

7. Devarajan, S., Panneerselvam, P., Mudigonda, A. and Hemalatha, P.K., "Enhancing Dark Web Classification: A Dynamic Crawler and Robust Classification Framework", International Journal of Intelligent Systems and Applications in Engineering, vol.12, no.6, pp.01-09, 2024.

8. Murty, C.A. and Rughani, P.H., "Dark web text classification by learning through SVM optimization", J Adv Inf Technol, vol.13, no.6, 2022.

9. Nazah, S., Huda, S., Abawajy, J. and Hassan, M.M., "Evolution of dark web threat analysis and detection: A systematic approach", Ieee Access, vol.8, pp.171796-171819, 2020

10. Kaur, S. and Randhawa, S., "Dark web: A web of crimes", Wireless Personal Communications, vol.112, pp.2131-2158, 2020.

11. Alkhatib, B. and Basheer, R., "Crawling the dark web: A conceptual perspective, challenges and implementation", J. Digit. Inf. Manag., vol.17, no.2, pp.51, 2019.

12. Yunelfi, P.R., Purwanto, Y., Ruriawan, M.F., Popalia, A.S. and Fahrani, F., "DarkWeb Crawling using Focused and Classified Algorithm", [CEPAT] Journal of Computer Engineering: Progress, Application and Technology, vol.1, no.02, pp.1-6, 2022.

13. Zhao, W., Hu, H., Zhou, W., Shi, J. and Li, H., "Best: Bert pre-training for sign language recognition with coupling tokenization", In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, no. 3, pp.3597-3605, June 2023.

14. Artama, M., Sukajaya, I.N. and Indrawan, G., "Classification of official letters using TF- IDF method", In Journal of Physics: Conference Series, IOP Publishing, vol.1516, no.1, pp.012001, April 2020.

15. Salur, M.U. and Aydin, I., "A novel hybrid deep learning model for sentiment classification", IEEE Access, vol.8, pp.58080-58093, 2020.

16. Janiesch, C., Zschech, P. and Heinrich, K., "Machine learning and deep learning", Electronic Markets, vol.31, no.3, pp.685-695, 2021.

17. Xie, X., Liu, X., Lee, T. and Wang, L., "Bayesian learning for deep neural network adaptation", IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol.29, pp.2096-2110, 2021.

18. Fajana, O., Owenson, G. and Cocea, M., "Torbot stalker: Detecting tor botnets through intelligent circuit data analysis", In 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), pp.1-8, IEEE, November 2018

19. Kowsari, K., Brown, D.E., Heidarysafa, M., Meimandi, K.J., Gerber, M.S. and Barnes, L.E., "Hdltex: Hierarchical deep learning for text classification", In IEEE international conference on machine learning and applications (ICMLA), pp. 364-371, December 2017.

20. Tamrakar, L., Shrivastava, P. and Ghosh, S.M., "Student sentiment analysis using classification with feature extraction techniques", arXiv preprint arXiv:2102.05439, 2021.

21. Wendland, A., Zenere, M. and Niemann, J., "Introduction to text classification: impact of stemming and comparing TF-IDF and count vectorization as feature extraction technique", In proceedings of Systems, Software and Services Process Improvement: 28th European Conference, EuroSPI 2021, Krems, Austria, September 1–3, 2021, Proceedings 28, Springer International Publishing, pp.289-300, 2021.

22. Banbhrani, S.K., Xu, B., Lin, H. and Sajnani, D.K., "Spider Taylor-ChOA: Optimized deep learning based sentiment classification for review rating prediction", Applied Sciences, vol.12, no.7, pp.3211, 2022.

23. Hoek, J.M., "Predicting purchasing intent of website visitors with deep feature learning",Bachelor's thesis, University of Twente, 2020.

24. Damsleth, E. and Spjøtvoll, E., "Estimation of trigonometric components in time series", Journal of the American Statistical Association, vol.77, no.378, pp.381-387, 1982.

25. TorBot dataset is taken from “https://github.com/DedSecInside/TorBot”, accessed on July 2024.

.