Cyber Threat Intelligence Traffic Through Black Widow Optimisation by Applying RNN-BiLSTM Recognition Model

Kanti Singh Sangher[1†], Archana Singh[2] and Hari Mohan Pandey[3],

School of IT, Centre for Development of Advanced Computing, Noida, India
Amity School of Engineering & Technology, Amity University, India
Data Science and Artificial Intelligence, School of Technology, Bournemouth University, UK

Summary
The darknet is frequently referred to as the hub of illicit online activity. In order to keep track of real-time applications and activities taking place on Darknet, traffic on that network must be analysed. It is without a doubt important to recognise network traffic tied to an unused Internet address in order to spot and investigate malicious online activity. Any observed network traffic is the result of mis-configuration from faked source addresses and another methods that monitor the unused space address because there are no genuine devices or hosts in an unused address block. Digital systems can now detect and identify darknet activity on their own thanks to recent advances in artificial intelligence. In this paper, offer a generalised method for deep learning-based detection and classification of darknet traffic. Furthermore, analyse a cutting-edge complicated dataset that contains a lot of information about darknet traffic. Next, examine various feature selection strategies to choose a best attribute for detecting and classifying darknet traffic. For the purpose of identifying threats using network properties acquired from darknet traffic, devised a hybrid deep learning (DL) approach that combines Recurrent Neural Network (RNN) and Bidirectional LSTM (BiLSTM). This probing technique can tell malicious traffic from legitimate traffic. The results show that the suggested strategy works better than the existing ways by producing the highest level of accuracy for categorising darknet traffic using the Black widow optimization algorithm as a feature selection approach and RNN-BiLSTM as a recognition model.

Keywords:
Darknet, Deep Learning, Cyber Attack, Feature Selection, Feature Extraction..

1. Introduction

The term “darknet” refers to a specific encrypted area of the internet that is predominantly utilised for unlawful and criminal activity. Two students were using the Advanced Research Projects Agency Network (ARPANET) at Sandford University in 1971 to trade drugs (i.e., marijuana), and this is where the Darknet first appeared [1-3]. The web is divided in three different types such as the surface, deep, and dark web as depicted in the Figure 1. Though these are not exactly the same, the names Surface, Deep, and Dark Web are closely related. The unencrypted web page is referred to as the Surface Web. It may be accessed quickly and indexed by a variety of search engines (Yahoo, Google, Bing, etc.). There are one billion static web pages on the surface web, which takes up between 4 and 5 percent of the total internet space. The contents of the Deep Web (or secret webs) are located between the searchable engines but are inaccessible via the search engine [4-6]. 95–96% of the data on the Internet is taken up by the Deep Web. The deep web's content is also 500–550 times more extensive than that of the surface web. The small fraction of deep web known as “black web” is not indexed by or accessible by normal search engines [7-10].

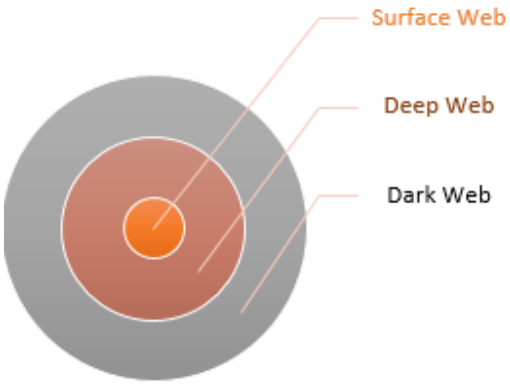

Fig. 1 Categorization of web.

It has becoming more and harder to keep up with these growing cyberthreats, therefore prompt dissemination of pertinent information about these risks is crucial for effective protection and mitigation. Such knowledge, which is frequently referred to as “cyber-threat intelligence”, is typically derived from gathered data and includes the zero-day exploits and vulnerabilities, indicators (system observables or artefacts linked to the attack), threat intelligence reports, security alerts, and suggested security configurations tools. To that end, when use the term “cyber threat intelligence”, is often refer to any data that could aid a company in identifying, evaluating, monitoring, and countering cyber threats. In today’s world of big data, it's

Manuscript received November 5, 2023
Manuscript revised November 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.11.13

critical to keep in mind that the term “intelligence” often refers to the information that has been exploited, gathered, analysed, and transformed into the set of an action that can be taken, or that has been actionable, rather than the data itself.

Particularly involved in gathering cyber threat intelligence from the social, clear, and the dark web where threat actors communicate, collaborate, and do the planning of cyber-attacks. Cyber intelligence can be collected by using the variety of methods (for example, monitoring cyber-feeds) and from the different sources. Such a strategy enables us to find timely cyber threat intelligence, such as zero-day exploits and vulnerabilities, and to give clearness to the sources that threat actors choose. In order to achieve this, envision the integrated architecture that includes key technologies for the purpose of gathering, analysing, and sharing pre-reconnaissance cyber threat intelligence using cutting-edge tools and technologies. In this situation, recently found information from different sources are examined for its applicability to the task (gathering), and recently found cyber threat intelligence in the form of threat actors, vulnerabilities, exploits, or the cyber-crime tools that stored and identified a vulnerability database using CPE and CVE (sharing) [11].

DarkNet is a technique for encrypted networks that gives internet users privacy. Only specific network configurations and technologies can be utilised in this situation to access internet content. The Onion Router (TOR) and other peer-to-peer platforms are used by the darknet to maintain users' anonymity through privacy networks [12-14]. Darknet is mostly used for criminal activity, such as buying illegal substances, cybercrime, child pornography, terrorism, and cyberattacks (such distributed denial of service (DDoS) assaults), among other unlawful activities. In order to identify attack patterns based on traffic data of an internet, effective techniques must be developed. To reduce threats, the model should automatically track attacker's changing behaviour [15-18]. Many promising threat detection methods based on supervised machine learning methods in order to train the model using both legitimate and the malicious data, were proposed in earlier published studies. Concept drift is a problem, yet data labelling is very expensive, and attackers' dynamic behaviours make it difficult to solve [19-22].

The research community has paid intense attention as a result of deep learning's growing popularity. Due to the network traffic's capacity to be automatically classified, deep learning is also be applied to data from internet traffic [23-25]. According to the underlying model, deep learning for the identification of darknet traffic is typically divided into different groups, such as unsupervised learning, convolutional neural networks, and recurrent neural networks. However, using the flow base data (such as gathering packets of various flows over a specific time period and then classifying them into individual packets flow) one can create the new architecture based on the latest deep learning that will be tested offline. The system needs more time to acquire the traffic flow statistics if it relates to a large session [26-28]. Furthermore, the feature extraction from flowbased data of traffic also requires some mean time. Overall, it argued that the profiling procedure for detecting darknet traffic takes a long time. Additionally, classifying natural traffic or darknet traffic requires very precise resources, such as memory, powerful computing power, processing and gathering of accumulated data, etc. Numerous studies shown that tracking just a few data packets in a flow is sufficient to determine the objective of a flow rather than following all the packets in it [29,30].

The key contributions of the research are as follows:

- To apply the various pre-processing phases, including feature selection, data balancing, and data imputation.
- To propose a deep learning architecture for a prediction of harmful activity is able to anticipate the different forms of traffic in addition to classifying the malicious network.
- For optimal feature selection proposed is the black widow optimization algorithm.
- To propose hybrid RNN-BiLSTM for identifying and classifying the traffic darknet network.

To demonstrate the success of the suggested approach, comparative findings employing different machine learning, deep learning, and state-of-the-art techniques will be presented.

The overall structure of the paper is summarized in five different sections: section 1 provides the introduction of the model, section 2 provides the basics if the crimes that were associated with the dark web, section 3 deals with the literature review of the previous developed works in this area, section 4 summarizes the proposed methodology of the paper, whereas the section 5 provides the overall part of the proposed methodology section and at the last section 6 provides the conclusion of the paper.

2. Dark Web Crimes

The Dark Web acts as the gateway to a world of crime and serves as the centre of criminal attacks [31,32]. Following are the some of the well-known crimes committed on Dark Web:

- **Human Trafficking:** The dark web location known as “Black Death” is where human trafficking occurs. British model Chloe Ayling is one of the victims of the dark web's practise of human trafficking. The majority

of human trafficking survivors, according to a 2017 research, were drawn from labor trafficking and the sex tracking.

- **Proxying:** The Tor-like services' ability to maintain user anonymity exposes users to risk of attack. Such site's URL does not contain customary "HTTPS" prefix, which denotes secure site. The user bookmark a TOR page in order to ensure a legitimate website. In the case of website proxies, the con artist deceives the user into believing he is on the original page while rewriting the link to drive user to his own con website. When the user pays using cryptocurrency, money is instead transferred to a con artist.

- **Child Pronography:** The analysis discovered that the most popular content on the TOR hidden sites is child pornography. A typical user would have difficulty finding these sites. It is the act that abuses children during sexual acts and exploits them for sexual arousal. It also contains child pornographic sexual images. A website called Lolita City, which had about 15,000 members and over 100 GB of the child pornographic videos and images, has since been taken down. With over the 200,000 members, PLAYPEN is the biggest child pornographic website on an entire dark web when it was taken down in 2015 by the FBI.

- **Onion Cloning:** The proxy approach is comparable to onion cloning. In order to steal money from users, the con artist creates a replica of the legitimate website or page and alters the links to direct them to their fraudulent websites.

- **Torture:** Users of Red Room websites spend thousands of the dollars to view rapes, murders, child pornography, and various forms of the torture. However, there are no proof of their existence. If they do, then TOR cannot be used to access them because it is too slow to broadcast live videos. Some accounts claim that visitors to a paedophile website paid significant sums of money to view films of Scully torturing and abusing the young child. It was a television show created by Scully's organisation, No Limits Fun. One of the videos, Daisy's Destruction, which featured horrible maltreatment of a young child and real sexual assault, was hotly debated on-site. It was shown on paedophile websites known as "Hurtcore," where paedophiles witness the abuse or torture of children and babies. Peter Gerard Scully was given a life sentence on June 13, 2018.

3. Literature Review

According to Rajawat et al., (2022) [33] dark web structural patterns mining raises a number of problems (including a lot of redundant and unnecessary information), which in turn boosts a variety of cybercrimes such illegal forums, terrorist activity, trade, and unlawful online purchasing. Given abundance of the data, it might be difficult to comprehend illegal conduct online. The Structural Patterns mining of the dark web in the case of the multidimensional data sets produces ambiguous findings, necessitating a technique for the learning of criminal behaviour to examine the current request for enhancing the labelled data as the user profiling. The inability to predict user behaviour is a challenge brought on by uncertain classification findings. Because multidimensional data has feature blends, classification is negatively impacted. Unable to provide the best option given the facts linked with the Dark Web flood. A Fusion Neural network (NN)-S^3VM for the prediction of Criminal Network Activity is developed in the research design and is based on a NN; the NN-S^3VM can enhance the prediction.

Steingartner et al., (2021) [34] seeks to investigate the use of cyber-deception and to create a brand-new conceptual model of hybrid threats that incorporates deception techniques. Security programmes typically concentrate on preventative measures designed to keep attackers from infiltrating the network. By identifying and blocking harmful behaviours, these applications try to leverage endpoint defences and hardened perimeters to find and stop intruders before they can enter. The majority of enterprises put such a plan into practise by arming their networks with tiered preventative controls and defense-in-depth measures. In contrast to how frequently they are used for in-network threat detection, detection controls are typically installed to supplement prevention at a perimeter. With current security controls that are not expressly made for that function, the framework leaves detection gaps that are challenging to close. Defenders are switching to a more balanced approach that combines response and detection rather than relying solely on prevention, a technique that attackers have regularly outperformed. The majority of businesses use next-generation firewall or intrusion detection system (IDS) that detects known threats or tries to identify them through pattern matching. Other detection technologies make use of traffic, behavioural, or monitoring analyses. These defensive measures are intended to react once they are assaulted, however they frequently fall short. They also have some limitations because they are not intended to stop attacks based on what looks to be authorised access or credential harvesting.

Bilan and Ozer, (2021) [35] suggested that the machine learning techniques are used to model two different types of

cybercrimes and forecast that made an impact of the stated variables on the identification of the attack vector and the culprit. The author created a strategy using eight machine learning techniques and found that their accuracy rates were comparable. With an accuracy rate of 95.02 percent, the SVM Linear was discovered to be a most effective cyberattack technique. With excellent accuracy in the first model, the author identified the categories of the attacks that a victims were most likely to experience. The most accurate method for finding attackers was the Logistic Regression, which had a 65.42 percent accuracy rate. Predicted whether an offenders could be identified by comparing the features in the second model. According to the findings, likelihood of a cyberattack diminishes as a victim's money and level of education rise. The model was built with the idea that cybercrime units would use it. Additionally, it will make it easier and more efficient to detect cyberattacks and defend against them.

Demertzis et al., (2021) [36] using the weighted-NN architecture, an unique network management framework and darknet traffic analysis was built to automate the process of malicious intent detection in real-time. For the analysis of network traffic, deciphering of malware traffic, and the real-time detection of encrypted communication, it is a reliable and accurate computational intelligence forensics tool. The author created the automated searching neural net architectural strategy based on a weight agnostic NN architecture that can accomplish a variety of tasks, such as finding zero-day attacks. The advanced created solution lowers the skill and an effort barrier that hinders many organisations from efficiently securing their most important assets by an automating the malicious intent identification procedure from darknet.

Research on the dark web is becoming more and more popular. The focus of the cyber security literature review was on the anomaly-based network intrusion detection systems [37-40]. Additionally, network traffic classification is a topic of research [31-43], whereas the IoT has recently gained a lot of interest in network traffic analysis and machine learning [44-46]. Yang et al., [47] suggested the visual dark web analysis forum post association system in order to graphically depict inter relation between different posters and message forums, which aids analysts in exploring deeper levels. introduced the current popular dark network communication protocol TOR. Another article [48] also develops a Hadoop-based architecture for concealed threat intelligence. The characteristics of significant darknet criminal networks are determined using the web crawler and the anonymous TOR tool, and this information serves as the foundation for further dark network study. The framework stores and manages threat intelligence data in a distributed database that is based on the Hadoop database (HBase). Samrin et al., [49] offered a survey of various methods for classifying intrusions on the KDD-Cup 99 dataset and recommended a useful method for categorising and identifying intrusions in these datasets. The trading unlabeled data was mapped into the series of 2-D grids by Summerville et al. in [50], creating the set of bitmaps that distinguished between abnormal and typical sessions. A review of several intrusion detection systems and approaches for categorization and reduction in data volume was done in the survey work by Kwon et al., [51]. The KDD-Cup 1999 dataset [52] or its sequel NSL-KDD [53], which addresses some of first's intrinsic problems and has been broadly embraced by an academic community, were used in the majority of these studies. The majority of anomaly network intrusion detection models use the supervised based approaches; however, Zhang et al., [54] identified inefficiencies in existing systems and recommended the unsupervised outlier detection technique as the solution to the inefficiencies. As an example, Singh et al. [55] combined a k-means clustering algorithms and random forest classification technique, and Song et al. [56] developed a combination of a ensemble k-nearest neighbour graphs and deep autoencoder based anomaly detectors. Other researchers also proposed hybrid models for intrusion detection, with the improving results.

Decision tree and the bayesian networks algorithms were among the technologies studied for network traffic classification [40] and were shown to be effective for the categorization of high-speed traffic flow. In [41], Pacheco et al., conducted the systematic review of the classification of darknet traffic approaches for machine learning, and the number of trends emerged from an analysis. In contrast, Dhote et al. evaluated three key methods to classify various types of Internet traffic in [43], outlining their advantages and drawbacks. The temporal feature-based hierarchical spatial intrusion detection system is also developed. To learn the low-level spatial network properties of network traffic, this system first builds deep CNNs, and to learn the high-level temporal network features, it builds LSTM networks. The authors claim that created method exhibits the low false alarm rate, as well as a high accuracy and detection rate. Pre-processing and classification make up the two sections of the rapid and extensive monitoring system that HaddadPajouh et al. built for keeping track of the traffic on the darknet in [57]. During the pre-processing phase, darknet packets are transformed into the feature vector containing 17 darknet traffic features. Using traffic attributes from well-known distributed denial-of-service (DDoS) attacks as training data enables quick online learning for categorization. The measurement data supplied by the authors demonstrates that the suggested system accurately detects the backscatter packets brought on by the attack of DDoS. Additionally, it adjusts to new attacks quite quickly.

4. Research Methodology

This section provides the in-depth study of the proposed methodology of the model. The proposed methodology of the model for the detection of malicious traffic depends on five steps such as Feature extraction, Handling missing data, Data balancing, Feature selection, and Classification using hybrid RNN-BiLSTM method as shown in the Figure 4. Although there are many different versions of the LSTM model are suggested by the different authors like Hierarchical-LSTM model [58], Sequenced-LSTM model [59] but for this particular problem the BiLSTM is best fitted model therefore in this work a hybrid model of BiLSTM model is used.

4.1 Dark Net Crawler

Utilizing TOR proxies, the sub-component is utilised to conduct in-depth crawls on certain dark web websites. A crawler does this by monitoring the talks for relevant information and is given a onion connections that correlate to marketplaces selling the cyber-crime tools or hacker forums and the zero-day exploits/vulnerabilities. The dark web crawler necessitates a first-time manual login in order to get beyond user authentication barriers that are frequently present in dark web forums and markets. Following the successful user authentication, session cookies are saved and used by the crawler in subsequent visits to mimic a user login (through HTTP requests). The content parser sub-component analyses the crawled HTML sites once each crawl has finished at a certain interval and take out a textual content together with important metadata (such as the value of bitcoin of purchased cyber-crime tools or a user's reputation level/activity/fame). For the further processing, all content from the various (social/clear/dark) web crawling components is been downloaded in its the raw HTML format and stored in the mongoDB[4].

4.2 Feature Selection using Black Widow Optimization

A single optimal value would be reached by the entire population if the model were run for up to N generations. Each generation begins with the Black widow optimization process at several points, such as parent selection, cannibalism, reproduction, mutation, and fitness evaluations. Black widow optimization's temporal complexity is based on the fitness function. Let Np represent the population's size, with a value of 40. The number of reproductions is computed based on the procreating rate. The procreating rate is equal to 0.8. Then, the population's top-scoring reproduction options are chosen and saved in population_01. The population pairs are then randomly chosen from population_01 to carry out the procreating stage.

The next step in this technique is to create an array named alpha that will be replicated until a widow array made up of random integers is produced. The offspring α is then created by utilising the equation, where y1 and y2 represent the offspring and x1 and x2 represent the parents.

$$y_1 = \alpha.x_1 + (1-\alpha)x_2;\ y_2 = \alpha.x_2 + (1-\alpha)x_1 \quad (1)$$

While this method is performed Nvar/2 times, the numbers that were randomly selected should not be duplicated. Equation 1 is used to generate D-dimensional children. The female black widow consumes the male here either during or right after mating. The father is shattered as a result. The mother and offspring spiders are then added to an array and sorted by fitness value.

Strong spiders eat their weaker siblings in sibling cannibalism. The number of survivors is now determined by the cannibalism rating, or "pCannibalism". 'pCannibalism' has a value of 0.5. In population_02, the remaining children are rescued but others are destroyed due to the cannibalism rate. The number of mutation children, or "pmutation," is then computed using the mutation rate. Pmutation has a value of 0.4. Individuals from population_01 are chosen at random to determine the number of mutation offspring. Each of the chosen solutions creates a new solution by randomly changing two members in the array. In population_03, this remedy works. Then population is updated by adding population_02 and population_03.

$$\text{Population} = \text{population\_01} + \text{population\_03} \quad (2)$$

Finally, the very best solution is selected from the available options and used for the efficient sentiment classification. All of the features are examined once during the feature selection process and used to anticipate the optimum features from the set of features. The hybrid classifier receives its input from the chosen features.

4.3 The Recurrent Neural Network (RNN)

RNN is the type of a NN, which uses the method of backward propagation, where a result obtained from the before step is fed to a current step as an input. In the typical NN, all the inputs and the outputs are independent. However, there are times when it is critical to remember the previous words, such as when it is crucial to anticipate the next word in a phrase. This prompted the development of RNN, which then resolved this problem with the aid of a hidden layer. The hidden state, which has some memory of the sequence, is the main and most important aspect of RNNs. The ability of the RNN's hidden state to retain data about a sequence is its most crucial characteristic. It has a memory that can retrieve any needed information. This neural network's lower difficulty of parameters makes it distinct from others.

The basic block diagram of the RNN architecture is depicted in the Figure 2. The input layer, hidden layer with the feedback unit, and output unit make up the three layers of the RNN. The output of the RNN is given by the following equation:

$$y(N) = \sum_{j=1}^{n} W_j \cdot \varepsilon_j(|| x_i(N) - v_{ij}||, \sigma_{ij}, r_j, \varepsilon_j(N-1)) \quad (3)$$

Where, $x = x_i$, $i = 1,\ldots,m$ and the "y" contains the input and output variables, "Wj" represents the connective weights between hidden and output layer, "N" is the number of iterations, "ε_j" represents the firing weights of the "jth" neuron in the hidden layer, "v_{ij}" *and* "σ_{ij}" are the centre and width of the radial basis function, "net_j" is the internal feedback gain.

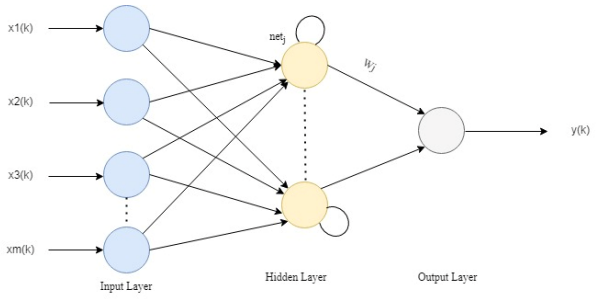

Fig. 2 Basic architecture of the RNN model.

Time "t" is used by an RNN to indicate the steps that an input sequence must take to get to the required final output sequence. The input processing NN system has the hidden state h_t that represents its condition at a specific moment t. RNN accepts the input "x_t" at a time "t", and the non-linear function helps in predicting the status of system at time "t" using the "t-1" time status,

$$h_t = f\ (h_{t-1}, x_t) \quad (4)$$

The above-mentioned non-linear function f is in normal situations signified as the linear transformation function summation with the form of nonlinear activation function,

$$h_t = \tanh(W\ [h_{t-1}, x_t] + b) \quad (5)$$

The RNN model is used to evaluate and analyze the results and helps creating better hybrid models.

4.4 The Bi-directional Long Short-Term Memory (Bi-LSTM)

Networks can always have knowledge about the sequence's past and future due to the BiLSTM structure. The difference between bidirectional LSTM and unidirectional LSTM is that bidirectional LSTM operates backwards, allowing you to preserve knowledge from the future and use the two hidden states together to maintain details from the past and the future at any point in the time. Your inputs will run in two directions using bidirectional LSTM: one from the past to the future and another from the future to the past.

Bidirectional RNNs operate on a relatively straightforward principle. The first repeated layer in the network must be replicated, the input sequence must be supplied as it is provided to the first layer, and the input sequence must then be presented to the replicated layer in reverse order. This gets around the restrictions of traditional RNNs. Using all of the input data available, the bidirectional RNN can be trained to learn about the past and future of a specific time-step. In a normal RNN, forward states (positive direction of time) and backward states are produced by splitting state neurons (negative direction of time). Figure 3 displays the Bi-fundamental LSTM's block diagram.

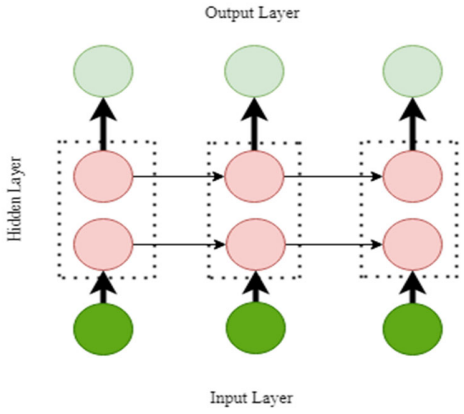

Fig. 3 Basic structure of Bi-LSTM.

4.5 Proposed Framework

The proposed schematic block diagram of the proposed methodology is depicted in the Figure 4. In the initial stages the data is extracted with the help of the darknet crawler. The extracted data is gathered in one place for the further pre-processing of the data. After crawling the data the next step is to pre-process the extracted data in order to use for the further steps. In the pre-processing steps different steps are done in order to process the data such as handling missing data, data balancing, and feature selection. Furthermore the extracted features are optimized with the help of the black widow optimization algorithm. Now the training of the model is done with these extracted features on the basis of the hybrid RNN-BiLSTM algorithm. On the basis of the model the darknet traffic is categorize in two different parts i.e., the benign and the malign traffic, which is used to identify the suspicious activity on the web. The performance of the model outperform the previous state-of-the-art approaches in terms of the various performance

metrics. The in-depth description of the results phase is shown in the next section.

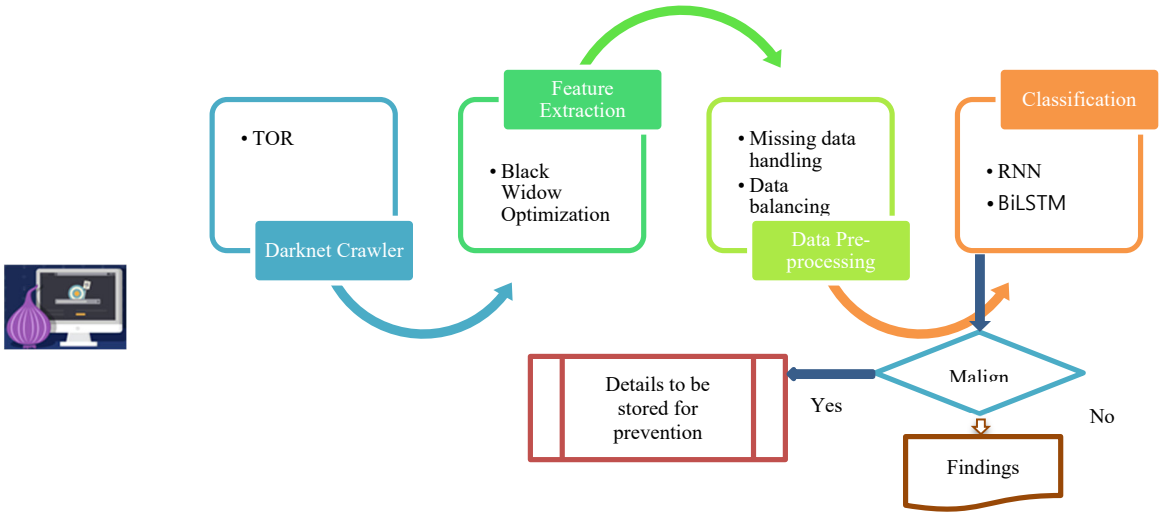

Fig. 4 Schematic block diagram of the proposed methodology.

5. Implementation Results

This section provides the in-depth analysis of the results of the proposed methodology. The performance of the methodology is measure on the basis of different performance matrices such as accuracy score, recall, precision, and F-1 score. To assess the efficacy of the suggested technique, an experimental analysis was performed on the Python platform and the results were compared with some recent work. Experiments are implemented on two public datasets: ISCXVPN2016 and ISCXTor2016. The malicious darknet traffic constitutes Browsing, Audio-Stream, Chat, P2P, Email, Transfer, Voice over Internet Protocol, and Video-Stream. At the end the result of the proposed methodology is compared with the state-of-the-art technique in order to better perform the results in terms of the performance metrices. The step-by-step explanation of the results of the methodology is seen in the detail in this section.

Firstly, the confusion matrix of a proposed methodology is shown in the Figure 5. The confusion matrix is the main part of the results because with this we can be able to evaluate the value of various performance matrices that were used in order to calculate the overall efficiency of the model. The confusion matrix contains the value in the form four different classes such as true positive, false positive, true negative, and false negative. With these classes we can be able to calculate the value of different performance matrices.

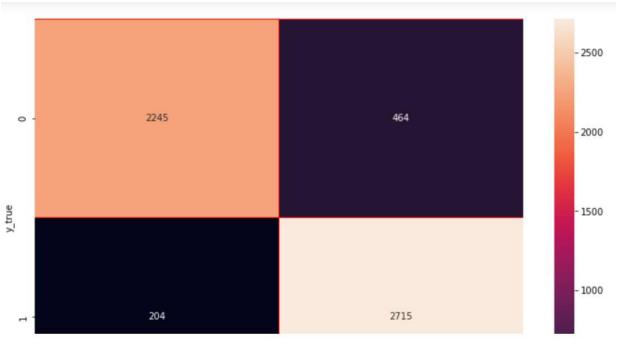

Fig. 5 Confusion matrix for the results of the propose methodology.

Figure 6 shows the results of propose model in terms of the AUC curve. The value of the AUC curve with the logistic is 0.903, which is greater in comparison with the value of the no skill value which is 0.500 that shows the ideal condition. Furthermore, Figure 7 and 8 shows the results of the training and testing loss and accuracy of the model. From these curves it is noticed that the result of the training is highest in comparison with the value of the testing. This performs that the efficiency of the model is good because when the training of the model is good then the performance of the model is better.

The value of the different performance matrices is shown in the Figure 9. The efficiency of the system is judge on the basis of the accuracy, recall, precision, and F1-score. With this metrices we can be able to judge the performance of the model. The value of the accuracy, precision, recall, and F1-score is 98.96% respectively

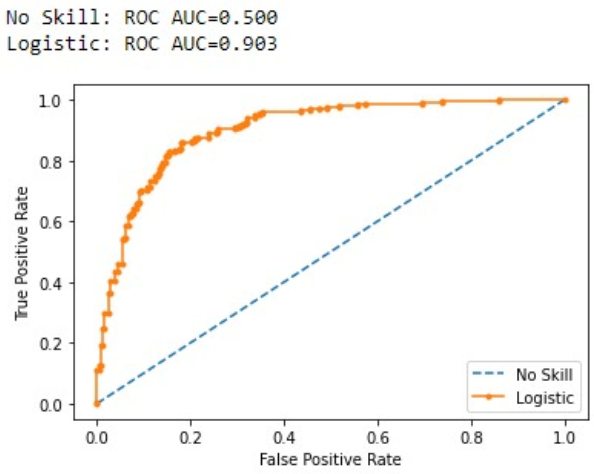

Fig. 6 AUC curve of the propose methodology.

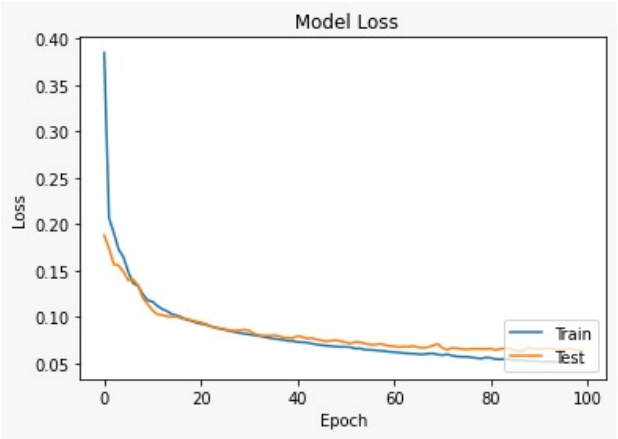

Fig. 7 Training and testing loss of the propose methodology.

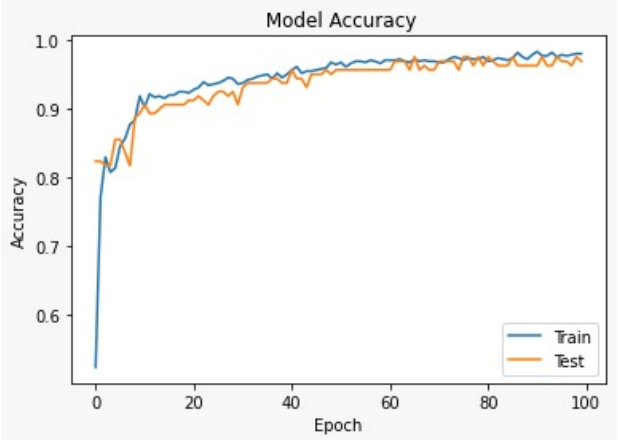

Fig. 8 Training and testing accuracy of the propose methodology.

```
Accuracy: 0.9896437448218725
Precision : 0.9896983346592282
Recall : 0.9896437448218725
F1-score: 0.9896381882953339
              precision    recall  f1-score   support

         0.0       1.00      0.98      0.99       239
         1.0       0.99      0.99      0.99       471
         2.0       0.95      0.97      0.96        98
         3.0       1.00      1.00      1.00       246
         4.0       0.99      0.95      0.97        76
         5.0       1.00      0.98      0.99       321
         6.0       0.99      1.00      1.00       270
         7.0       0.99      1.00      0.99       693

    accuracy                           0.99      2414
   macro avg       0.99      0.98      0.98      2414
weighted avg       0.99      0.99      0.99      2414
```

Fig. 8 Overall results of the propose methodology based on various performance parameters.

The comparison of results of proposed methodology with the state-of-the-art techniques is shown in the below Table 1. The comparison is done on the basis of the accuracy score. The author of the [58] works on 4 different algorithms and achieved accuracy scores of 50.02% on the logistic regression, 97.60% with gaussian naive bayes, 97.98% with support vector machine, 98.89% with random forest classifier. The results of the proposed system is 98.96% which outperforms the results of the state-of-the-art techniques in terms of accuracy scores.

Table 1: Comparison of the results with the state-of-the-art approaches

Algorithm	***Accuracy***
Logistic Regression [60]	50.02%
Gaussian Naïve Bayes [60]	97.60%
Support Vector Machine [60]	97.98%
Random Forest Classifier [60]	98.89%
Propose Methodology	98.96%

6. Conclusion

The proposed methods develops a hybrid model to characterize and monitor the darknet traffic. The proposed model provides the rule discovery model by executing the hybrid model of the RNN and BiLSTM algorithms for the classification phase. Furthermore the features are selected with the help of the black widow optimization algorithm. The created intelligent data can be used as objective proof of the criminal activity taking place on the Dark Web. The execution of the model is limited to the two public datasets: ISCXVPN2016 and ISCXTor2016 that are applied on any Dark Net forums. Implementing a hybrid deep learning system with an improved feature selection technique could

improve the paper by examining the dataset. The proposed model is able to classify the darknet traffic into malign and benign with a classification accuracy of the 98.96 %. At last with the help of the comparison table it is observed that the results of the proposed model outperforms the state-of-the-art algorithms in terms of the accuracy score. In the future, suggest a framework for a semi-supervised approach that combines supervised approaches with an unsupervised approach. The overall effectiveness of our suggested strategy demonstrates that our model might be successfully applied to classify the data from Dark Web forums and produce insightful information that would be useful to cyber security experts and law enforcement.

Acknowledgments

The author of the manuscript did not receive funding from the other sources.

References

[1] Jardine, Eric. "Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies." *new media & society* 20, no. 8 (2018): 2824-2843.

[2] Hayes, Darren R., Francesco Cappa, and James Cardon. "A framework for more effective dark web marketplace investigations." *Information* 9, no. 8 (2018): 186.

[3] da Cunha, Bruno Requião, Pádraig MacCarron, Jean Fernando Passold, Luiz Walmocyr dos Santos, Kleber A. Oliveira, and James P. Gleeson. "Assessing police topological efficiency in a major sting operation on the dark web." *Scientific reports* 10, no. 1 (2020): 1-10.

[4] Alharbi, Abdullah, Mohd Faizan, Wael Alosaimi, Hashem Alyami, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Exploring the topological properties of the Tor Dark Web." *IEEE Access* 9 (2021): 21746-21758.

[5] Nazah, Saiba, Shamsul Huda, Jemal H. Abawajy, and Mohammad Mehedi Hassan. "An Unsupervised Model for Identifying and Characterizing Dark Web Forums." *IEEE Access* 9 (2021): 112871-112892.

[6] Shakarian, Paulo. "Dark-web cyber threat intelligence: from data to intelligence to prediction." *Information* 9, no. 12 (2018): 305.

[7] Wilson, Emily. "Disrupting dark web supply chains to protect precious data." *Computer Fraud & Security* 2019, no. 4 (2019): 6-9.

[8] Alkhatib, Bassel, and Randa S. Basheer. "Mining the Dark Web: A Novel Approach for Placing a Dark Website under Investigation." *International Journal of Modern Education & Computer Science* 11, no. 10 (2019).

[9] Hayes, Darren R., Francesco Cappa, and James Cardon. "A framework for more effective dark web marketplace investigations." *Information* 9, no. 8 (2018): 186.

[10] Samtani, Sagar, Weifeng Li, Victor Benjamin, and Hsinchun Chen. "Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal." *Digital Threats: Research and Practice (DTRAP)* 2, no. 4 (2021): 1-10.

[11] Koloveas, Paris, Thanasis Chantzios, Christos Tryfonopoulos, and Spiros Skiadopoulos. "A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence." In *2019 IEEE World Congress on Services (SERVICES)*, vol. 2642, pp. 3-8. IEEE, 2019.

[12] Woodhams, Jessica, Juliane A. Kloess, Brendan Jose, and Catherine E. Hamilton-Giachritsis. "Characteristics and behaviors of anonymous users of dark web platforms suspected of child sexual offenses." *Frontiers in Psychology* 12 (2021): 623668.

[13] AlKhatib, Bassel, and Randa Basheer. "Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation." *J. Digit. Inf. Manag.* 17, no. 2 (2019): 51.

[14] McMeel, Dermott John James. "The Dark Web of Urban Data: Fitness Data Ecosystems, Urban Design and Privacy in the Modern City." *International Journal of Art, Culture and Design Technologies (IJACDT)* 7, no. 2 (2018): 12-25.

[15] Rajawat, Anand Singh, Romil Rawat, Kanishk Barhanpurkar, Rabindra Nath Shaw, and Ankush Ghosh. "Vulnerability analysis at industrial internet of things platform on dark web network using computational intelligence." In *Computationally intelligent systems and their applications*, pp. 39-51. Springer, Singapore, 2021.

[16] Mador, Ziv. "Keep the dark web close and your cyber security tighter." *Computer Fraud & Security* 2021, no. 1 (2021): 6-8.

[17] Topor, Lev, and Pnina Shuker. "Cyber Influence Campaigns in the Dark Web." *Cyber, Intelligence, and Security* 3, no. 2 (2019): 63-79.

[18] Hiramoto, Naoki, and Yoichi Tsuchiya. "Measuring dark web marketplaces via Bitcoin transactions: From birth to independence." *Forensic Science International: Digital Investigation* 35 (2020): 301086.

[19] Goldstein, Fay, Oded Yarkoni, Lihi Shalmon, Haim Glikman, Shachar Azriel, and Guy Molho. "Monitoring automotive cyber risks throughout the deep and dark web." (2021).

[20] Coffey, Mollie L. "Library application of Deep Web and Dark Web technologies." *School of Information Student Research Journal* 10, no. 1 (2020): 8.

[21] Haasio, Ari, J. Tuomas Harviainen, and Reijo Savolainen. "Information needs of drug users on a local dark Web marketplace." *Information Processing & Management* 57, no. 2 (2020): 102080.

[22] Sarkar, Soumajyoti, Mohammad Almukaynizi, Jana Shakarian, and Paulo Shakarian. "Predicting enterprise cyber incidents using social network analysis on dark web hacker forums." *The Cyber Defense Review* (2019): 87-102.

[23] ElBahrawy, Abeer, Laura Alessandretti, Leonid Rusnac, Daniel Goldsmith, Alexander Teytelboym, and Andrea Baronchelli. "Collective dynamics of dark web marketplaces." *Scientific reports* 10, no. 1 (2020): 1-8.

[24] Montieri, Antonio, Domenico Ciuonzo, Giuseppe Aceto, and Antonio Pescape. "Anonymity services tor, i2p, jondonym: classifying in the dark (web)." *IEEE Transactions on Dependable and Secure Computing* 17, no. 3 (2018): 662-675.

[25] Wu, Hsin-Te, and Chun-Wei Tsai. "An intelligent agriculture network security system based on private blockchains." *Journal of Communications and Networks* 21, no. 5 (2019): 503-508.

[26] Hayes, Darren R., Francesco Cappa, and James Cardon. "A framework for more effective dark web marketplace investigations." *Information* 9, no. 8 (2018): 186.

[27] Samtani, Sagar, Weifeng Li, Victor Benjamin, and Hsinchun Chen. "Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal." *Digital Threats: Research and Practice (DTRAP)* 2, no. 4 (2021): 1-10.

[28] Allhusen, Andrew, Izzat Alsmadi, Abdullah Wahbeh, Mohammad Al-Ramahi, and Ahmad Al-Omari. "Dark Web Analytics: A Comparative Study of Feature Selection and Prediction Algorithms." *Available at SSRN 3949786* (2021).

[29] Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark web: a web of crimes." *Wireless Personal Communications* 112, no. 4 (2020): 2131-2158.

[30] Sharma, Shweta, Parvesh Sharma, and Gyanendra Singh. "Dark Web and Trading of Illegal Drugs." *J Forensic Science & Criminal Investigation* 9, no. 4 (2018): 555766.

[31] Naseem, Iflah, Ashirr K. Kashyap, and Dheeraj Mandloi. "Exploring anonymous depths of invisible web and the digi-underworld." *International Journal of Computer Applications, NCC* 3 (2016): 21-25.

[32] Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark web: a web of crimes." *Wireless Personal Communications* 112, no. 4 (2020): 2131-2158.

[33] Rajawat, Anand Singh, Pradeep Bedi, S. B. Goyal, Sandeep Kautish, Zhang Xihua, Hanan Aljuaid, and Ali Wagdy Mohamed. "Dark Web Data Classification Using Neural Network." *Computational Intelligence and Neuroscience* 2022 (2022).

[34] Steingartner, William, Darko Galinec, and Andrija Kozina. "Threat defense: Cyber deception approach and education for resilience in hybrid threats model." *Symmetry* 13, no. 4 (2021): 597.

[35] Bilen, Abdulkadir, and Ahmet Bedri Özer. "Cyber-attack method and perpetrator prediction using machine learning algorithms." *PeerJ Computer Science* 7 (2021): e475.

[36] Demertzis, Konstantinos, Konstantinos Tsiknas, Dimitrios Takezis, Charalabos Skianis, and Lazaros Iliadis. "Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework." *Electronics* 10, no. 7 (2021): 781.

[37] Samrin, Rafath, and D. Vasumathi. "Review on anomaly based network intrusion detection system." In *2017 international conference on electrical, electronics, communication, computer, and optimization techniques (ICEECCOT)*, pp. 141-147. IEEE, 2017.

[38] Devaraju, S., and S. Ramakrishnan. "PERFORMANCE COMPARISON FOR INTRUSION DETECTION SYSTEM USING NEURAL NETWORK WITH KDD DATASET." *ICTACT Journal on Soft Computing* 4, no. 3 (2014).

[39] Kwon, Donghwoon, Hyunjoo Kim, Jinoh Kim, Sang C. Suh, Ikkyun Kim, and Kuinam J. Kim. "A survey of deep learning-based network anomaly detection." *Cluster Computing* 22, no. 1 (2019): 949-961.

[40] Dhanabal, L., and S. P. Shantharajah. "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms." *International journal of advanced research in computer and communication engineering* 4, no. 6 (2015): 446-452.

[41] Pacheco, Fannia, Ernesto Exposito, Mathieu Gineste, Cedric Baudoin, and Jose Aguilar. "Towards the deployment of machine learning solutions in network traffic classification: A systematic survey." *IEEE Communications Surveys & Tutorials* 21, no. 2 (2018): 1988-2014.

[42] Pacheco, Fannia, Ernesto Exposito, Mathieu Gineste, Cedric Baudoin, and Jose Aguilar. "Towards the deployment of machine learning solutions in network traffic classification: A systematic survey." *IEEE Communications Surveys & Tutorials* 21, no. 2 (2018): 1988-2014.

[43] Dhote, Yogesh, Shikha Agrawal, and Anjana Jayant Deen. "A survey on feature selection techniques for internet traffic classification." In *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 1375-1380. IEEE, 2015.

[44] Sun, Xiaochuan, Guan Gui, Yingqi Li, Ren Ping Liu, and Yongli An. "ResInNet: A novel deep neural network with feature reuse for Internet of Things." *IEEE Internet of Things Journal* 6, no. 1 (2018): 679-691.

[45] Pustokhina, Irina Valeryevna, Denis Alexandrovich Pustokhin, Deepak Gupta, Ashish Khanna, Kannan Shankar, and Gia Nhu Nguyen. "An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems." *IEEE Access* 8 (2020): 107112-107123.

[46] Shaikh, Farooq, Elias Bou-Harb, Jorge Crichigno, and Nasir Ghani. "A machine learning model for classifying unsolicited iot devices by observing network telescopes." In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 938-943. IEEE, 2018.

[47] Yang, Ying, Lina Yang, Meihong Yang, Huanhuan Yu, Guichun Zhu, Zhenya Chen, and Lijuan Chen. "Dark web forum correlation analysis research." In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, pp. 1216-1220. IEEE, 2019.

[48] Yang, Ying, Huanhuan Yu, Lina Yang, Ming Yang, Lijuan Chen, Guichun Zhu, and Liqiang Wen. "Hadoop-based dark web threat intelligence analysis framework." In *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 1088-1091. IEEE, 2019.

[49] Samrin, Rafath, and D. Vasumathi. "Review on anomaly based network intrusion detection system." In *2017 international conference on electrical, electronics, communication, computer, and optimization techniques (ICEECCOT)*, pp. 141-147. IEEE, 2017.

[50] Summerville, D. H., N. Nwanze, and V. A. Skormin. "Anomalous packet identification for network intrusion detection." In *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, pp. 60-67. IEEE, 2004.

[51] Kwon, Donghwoon, Hyunjoo Kim, Jinoh Kim, Sang C. Suh, Ikkyun Kim, and Kuinam J. Kim. "A survey of deep learning-based network anomaly detection." *Cluster Computing* 22, no. 1 (2019): 949-961.

[52] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In *2009 IEEE symposium on computational intelligence for security and defense applications*, pp. 1-6. Ieee, 2009.

[53] Demertzis, Konstantinos, and Lazaros Iliadis. "A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification."

In *International Conference on e-Democracy*, pp. 11-23. Springer, Cham, 2013.

[54] Zhang, Jiong, and Mohammad Zulkernine. "Anomaly based network intrusion detection with unsupervised outlier detection." In *2006 IEEE International Conference on Communications*, vol. 5, pp. 2388-2393. IEEE, 2006.

[55] Singh, Pradeep, and M. Venkatesan. "Hybrid approach for intrusion detection system." In *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, pp. 1-5. IEEE, 2018.

[56] Song, Hongchao, Zhuqing Jiang, Aidong Men, and Bo Yang. "A hybrid semi-supervised anomaly detection model for high-dimensional data." *Computational intelligence and neuroscience* 2017 (2017).

[57] HaddadPajouh, Hamed, Ali Dehghantanha, Raouf Khayami, and Kim-Kwang Raymond Choo. "A deep recurrent neural network based approach for internet of things malware threat hunting." *Future Generation Computer Systems* 85 (2018): 88-96.

[58] Sharma, Rishabh, and Shashi Shekhar. "An Automatic Pun Word Identification Framework for Code Mixed Text." In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 1-5. IEEE, 2021.

[59] Nourani, Vahid, and Nazanin Behfar. "Multi-station runoff-sediment modeling using seasonal LSTM models." *Journal of Hydrology* 601 (2021): 126672.

[60] Nazah, Saiba, Shamsul Huda, Jemal H. Abawajy, and Mohammad Mehedi Hassan. "An Unsupervised Model for Identifying and Characterizing Dark Web Forums." *IEEE Access* 9 (2021): 112871-112892.

Kanti Singh Sangher is working as Principal Technical Officer in the Centre for Development of Advanced Computing (CDAC).
She has experience of more than 17 years. She worked in Indian Space Research Organization, Regional Remote Sensing Service Centre, Kharagpur as Junior Research Fellow.She has done projects funded by MeitY, in various domains including Cyber Forensics,e-Learning and software development. She has published 4 research papers and given co-ordinated national level FDP's.She actively involved in teaching,research and CMMI processes in the CDAC.

Dr. Archana Singh, having experience of more than 20 years in Academic and IT Industry. Presently, she is working as a Professor and Head of Department of Artificial Intelligence, Amity University, Uttar Pradesh, Noida. Her research area interests include Data Sciences, Deep Learning algorithms, AI, Image Processing, AR/VR, Cognitive Sciences, ICT, Business Intelligence, Data Analytics, Big Data, and its applications. She has more than 70+ research papers including SCI-indexed and Scopus Indexed Journals like ACM, Springer, Elsevier, Wiley, and others. She has been working on various research projects related AI and Machine Learning.

Hari is in data science and artificial intelligence at school of technology Bournemouth University, UK. He is specialized in Computer Science & Engineering. His research area includes artificial intelligence, soft computing techniques, natural language processing, language acquisition, machine learning, deep learning and computer vision