Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-17222-8

LSTM based deep learning approach to detect online violent activities over dark web

Jaspal Kaur Saini[1]

Received: 29 January 2023 / Revised: 15 September 2023 / Accepted: 21 September 2023

Abstract
Dark web discussion forums have become one of the digital communication medium over the public infrastructure of Internet. Monitoring and analysing data from dark web discussion forums and social media platforms can unfold useful insights to the security intelligence.Through our research work we demonstrate the possibility of detecting online terrorist activities from dark web forums using machine learning based and deep learning based algorithms. In order to achieve desired objectives, we presented two specific use cases in this paper :(i) procurement of illegal weapons, (ii) online recruitment of terrorists. LSTM based deep learning classification approach is employed on annotated data for both use cases. We have also compared proposed approach with machine learning classifiers. It is seen that deep learning based text classification is possible with proposed LSTM architecture with acceptable accuracy measures. Automating the process of identifying violent activities over dark web discussion forums is a novel and fruitful contribution of our current work. Machine Learning and Deep Learning algorithms for detecting violent activities can be a powerful tool when developed and used responsibly.

Keywords Machine learning · Deep learning · LSTM · Social media · Dark web

1 Introduction

Digital Discussion forums are becoming new homes to everyone. It is found that violent extremists have also started exploring the various means of surface and dark web in order to fulfill their malicious intentions [2, 31]. In today's digital age where social media plays a significant role in how individuals, businesses, and organizations interact and communicate, it becomes necessary to analyze social media data.

Activities such as procurement of illegal weapons and drugs, recruitment of terrorists and planning massive attacks are just few activities which have gone on digital discussion forums [5, 8, 9, 17, 23, 30]. Machine learning can be a valuable tool for detecting violent activities in

✉ Jaspal Kaur Saini
sainijassi87@gmail.com; jaspalkaursaini@iiitu.ac.in

1 IIIT Una, Una, Himachal Pradesh, India

Published online: 16 October 2023

various contexts, such as online content, surveillance footage, or even in social interactions: mining emotions, etc. [15, 16, 21]. By training machine learning models on relevant data, automated systems can learn to recognize patterns and features associated with a violent behaviors of the extremists [18, 19, 29].

Recruiting and radicalising innocent minds over internet have become another emerging trend amongst terrorist based organisations [4, 5, 10, 12, 14, 17]. There have been numerous social media pages and posts calling for joining terrorist training camps influencing the minds of the young. Terrorist groups are comprehensively targeting online social media and dark web discussion forms to propagate their agendas. Therefore, it becomes necessary to detect the presence of violent extremists on social media and dark web discussion forms. Computational Techniques such as machine learning-based algorithms, deep learning methods, and data visualization tools have been widely studied by researchers to counter the global problem of terrorism, which nowadays have gone digital [24, 25].

In this paper, a deep learning-based approach is proposed to detect online procurement of modern weapons and online recruitment of terrorists over dark web forums. Previously, we have utilized the traditional machine learning-based classifiers to detect online violent activities over the dark web [22, 23]. LSTM-based deep learning architecture is presented in this paper as an extension of previous work [22, 23]. LSTM (Long Short-Term Memory) is a type of recurrent neural network (RNN) architecture that is well-suited for sequence modeling tasks, such as text classification [15, 28]. In this context, LSTM-based deep learning models have been widely used and have shown impressive performance in various natural language processing (NLP) tasks [6, 11, 16].

In addition, the state-of-art scope and review of all currently available dark web markets on dark web as per parameters is presented in related work section. Study of terrorist networks requires large dataset of incidents and attacks along with attributes which can help in understanding nature and other aspects of attacks [1, 26, 27].

2 Related work

The dark web is a part of the internet that is intentionally hidden and inaccessible through standard web browsers, making it difficult to monitor and study. However, law enforcement agencies, academic researchers, and cyber-security experts have been working on various methods to gain insights into dark web activities, including those related to violence. Here are some general steps and approaches that researchers and investigators may use:

1. Data Collection: Gathering data from the dark web is usually the first step. Researchers may use specialized tools to access dark web markets and forums, crawl and scrape data, and extract relevant information related to products and services offered.
2. Machine Learning: Machine learning algorithms can be trained to recognize patterns associated with violent activities or the sale of dangerous goods on the dark web. These algorithms can help automate the detection process.
3. Collaboration with Law Enforcement: Researchers often work closely with law enforcement agencies to share their findings and assist in investigations related to violent activities on the dark web.
4. Ethical Considerations: Studying the dark web raises ethical concerns, as it involves dealing with illegal and harmful content. Researchers must adhere to ethical guidelines and respect individuals' privacy and safety.

It is important to note that monitoring the dark web is an ongoing process, and new challenges emerge as individuals and groups adapt their behaviors and communication methods. Additionally, the legal and ethical implications of studying the dark web require careful consideration. We studied 21 dark web markets as part of our present work. Various available

Table 1 Dark Web Markets Table

SNo.	Market Place	Types of Listing	Discussion Forum
1	Wall Street Market	Used to Deal in Digital frauds but now Banned	No
2	Dream Market, Vendors-bond information and European Drugs reviews	Drugs	Yes
3	Rapture Market,Vendor Bond, Services discussion	Down for operation	Yes
4	Olympus Market	Down for Operations	No
5	Cannazon	Weeds, Drugs and other Cannabis products, Hash	No
6	ACCMARKET	Stolen Paypal,Ebay and Bank Accounts	No
7	THE PEOPLES DRUG STORE	Drugs, stolen Bitcoins	
8	Deep Sea Market	Frauds,Counterfeit Currency, Malwares/Botnets, Bitcoin Stealer	No
9	Elite market	Drugs and chemicals, Counterfeit Credit Cards,Malwares, Jewels, Hacking Services	No
10	Onion Identitiy Services /	Fake ID's,Drivers License,Passports	No
11	CGMC, Invite Only	Invite only marketplace offering cannabis and related products	Yes
12	Point Free Market	Banned	No
13	Berlusconi Market	Seized	No
14	The Majestic Garden,Sale and Purchase of Psychedelics	Forum for Psychedelics requiring registration.	Yes
			Drugs
15	DutchDrugz, Forum for Drugs, Psychedelics enquiries and orders	Banned Drugs, Narcotic drugs, Cannabis	Yes
16	Quality King	Opiods, Stimulations and Banned drugs	No
17	Dutch Magic	Closed	No
18	Rechard Sport	Now closed	No
19	The Church	Drugs Like MDMA, LSD but now closed	No
20	Elherbolario	hash and cannabis based products	No
21	AlphaBay	Market for various services seized by Security Agencies	No

dark web markets as accessed in 2021 are listed in Table 1 with the type of listing on each dark web market and whether the dark web market has a discussion forum or not.

A few of these dark web markets listed in Table 1 may be down by security agencies or are only active during particular months of the year. This study can greatly provide information to researchers who want to target a few dark web markets in order to crawl data.

3 Proposed approach

3.1 Research methodology

In the recent years, terrorism and terrorist activities have intruded into digital world. So, it is required to detect violent intentions of terrorists over online media. We looked at this alarming problem in our current work by detecting discussions regarding procurement of weapons and recruitment of terrorists. Two use cases namely: detection of illegal weapon procurement and detection of online recruitment of terrorists is presented in this section. Research methodology plays a crucial role in the field of machine learning (ML) by providing a structured and systematic approach to conducting research, developing algorithms, and advancing the understanding of ML techniques. It helps in formulating clear research questions, collecting reliable data, designing experiments, developing algorithms, addressing ethical concerns, and promoting transparency and reproducibility. By adhering to sound research methodology, the machine learning field can make more significant and reliable advancements.
Figure 1 shows the block diagram for the proposed research methodology.

(i) **Data Collection**
Research methodology guides the process of collecting relevant and high-quality data. Proper data collection techniques are essential for building accurate and robust ML models. Without sound data collection practices, ML models might suffer from biases, noisy data, or inadequate coverage of the problem space.

(ii) **Data Annotation**
Data annotation is a critical process in machine learning that involves labeling data with relevant information to create a dataset that can be used for training and evaluating machine learning models. This labeled data is essential for supervised learning algorithms, where the model learns from input-output pairs to make predictions or classifications. Data annotation helps the model understand the relationships between input features and desired outputs.

(iii) **Data Preprocessing**
Data preprocessing is a critical step in the machine learning (ML) pipeline that involves preparing and cleaning the raw data before it is used to train a model. Effective data

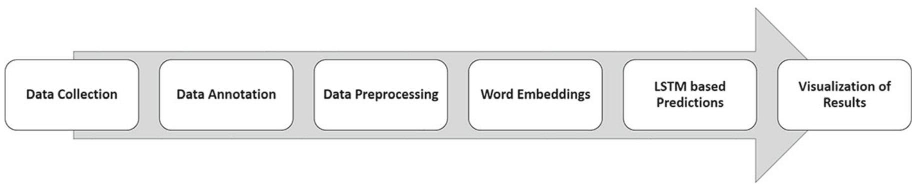

Fig. 1 Proposed Research Methodology

Table 2 Kappa Coefficient for Use Case-1

Category		Expert 2 No	Expert 2 Yes
Expert 1	No	0.4984	0.0287
	Yes	0	0.4728
Kappa	0.9425		
Subjects	312		

preprocessing can significantly impact the performance and reliability of your ML models.

(iv) **Word Embeddings**
Word embeddings are a technique used in natural language processing (NLP) and machine learning to represent words as dense vectors of real numbers in a continuous space. They capture semantic relationships between words, allowing algorithms to understand the meaning and context of words in a more meaningful way compared to traditional sparse representations like one-hot encoding.

(v) **LSTM based Predictions**
In ML, algorithm development is a crucial aspect of research. Research methodology guides the process of developing, refining, and optimizing algorithms. It encourages researchers to document their design choices, making it easier for others to understand, replicate, and build upon their work.
LSTM models are designed to handle sequential data, making them well-suited for text classification where the order of words matters. It can capture the context and dependencies between words, enabling them to understand the meaning of sentences and paragraphs. LSTM (Long Short-Term Memory) based deep learning models offer several advantages when used for text classification tasks such as: Sequential Information Handling, Long-Term Dependencies, Feature Extraction, Variable-Length Input, Contextual Understanding, Multiclass and Multilabel Classification, Adaptability to Various Text Data, and Interpretability.

(vi) **Validation of Results**
Validation of results in machine learning (ML) is a crucial step to assess the performance and generalization capabilities of your trained model. The process typically involves splitting the dataset into training, validation, and test sets, and using various metrics to evaluate the model's performance.

Table 3 Kappa Coefficient for Use Case-2

Category		Expert 2 No	Expert 2 Yes
Expert 1	No	0.5020	0.0066
	Yes	0.0146	0.4726
Kappa	0.9575		
Subjects	758		

Table 4 Hyper-parameters for Use Case 1

Parameter	Value
Training Dataset	188
Validation Dataset	62
Test Dataset	62
Total no of records	312
Epochs	25
Classes	2
Learning rate	0.001
Decay (decay of learning rate)	0
Dropout	0.3
Optimizer	Adam

3.2 Experimental study

The following steps mentions the necessary setup, pre-proessing and annotations, and key parameter selection for the proposed model.

(i) **Setup**
The system used for the implementation of proposed approach consists of *Intel (R) Core(TM) i7-5500U CPU @ 2.40 GHz, 8 GB RAM*. The program is implemented in R Programming using *Keras* library with Tensorflow [3].

(ii) **Pre-Processing and Annotations**
We have pre processed data from various dark web forum as we have done in earlier approach [13, 22]. We used same annotated datasets described in [13, 22] for our current research.
As the two experts have labeled the posts, so there is a need to compare a number of agreements between the two experts to validate consistency between annotations. Cohen's kappa coefficient from statistics is used to check the agreement between experts. We calculated the kappa coefficient for both uses cases using R Programming Package *psych* [20] as shown in Table 2 for Use Case 1 and Table 3 for Use Case 2. The kappa coefficient statistically validated the annotations done by subject domain experts so that we can proceed to feature selection and model training.

(iii) **Key Parameters Selection**
Dataset is partitioned into 80:20 for the training and testing. The hyper-parameters used to train the model are tuned attentively. The hyper parameters tuned for the required model are described in Tables 4 and 5 for both use cases respectively.
The hyper-parameters were tuned carefully using a grid search in which several values are tried and tested. The amalgamation of parameters that led to the best results is finally utilized for the rest of the experiments. Additionally, the "adam" (Adaptive Moment Estimation) optimizer was chosen for updating the values of parameters on each epoch.
A description of Adam optimizer is given below:

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t$$
$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2$$

where m_t is aggregate of gradients at time t. [current] (initially, $m_t = 0$), m_{t-1} is aggregate of gradients at time t-1. [previous], v_t is sum of square of past gradients at

Table 5 Hyper-parameters for Use Case 2

Parameter	Value
Training Dataset	478
Validation Dataset	119
Test Dataset	161
Total no of records	758
Epochs	25
Classes	2
Learning rate	0.001
Decay (decay of learning rate)	0
Dropout	0.3
Optimizer	Adam

time t. (initially = 0), v_{t-1} is sum of square of past gradients at time t-1, 'g' is gradient on current mini-batch, and $\beta1$ and $\beta2$ are newly introduced hyper-parameters of the algorithm (default values of 0.9 and 0.999 respectively). More details about Adam optimizer can be found in [7].

4 Results and discussions

LSTM-based deep learning mechanism is employed for both use cases. For evaluating the proposed system, we presented training and testing phase details as per the following:

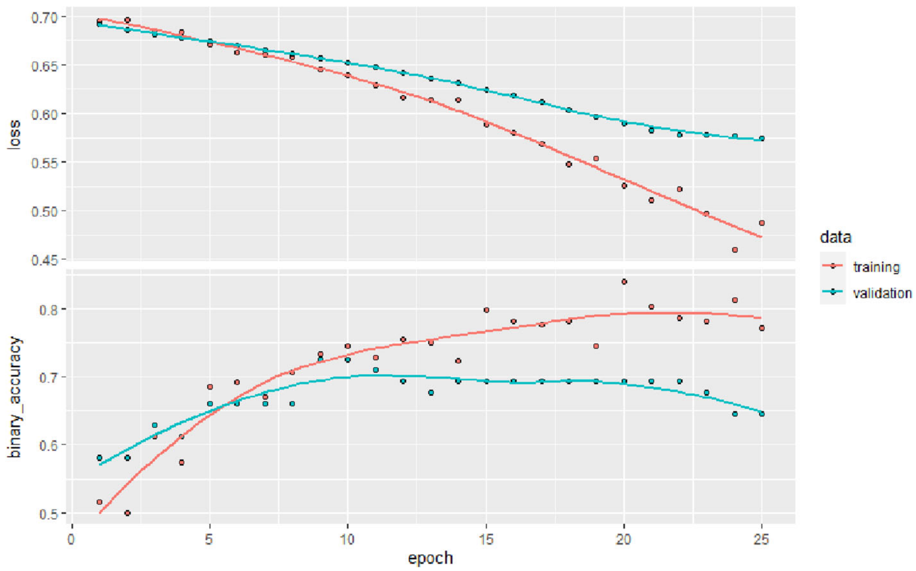

Fig. 2 Use Case 1: Loss and Metrics Curve (Detection of Weapon Procurement)

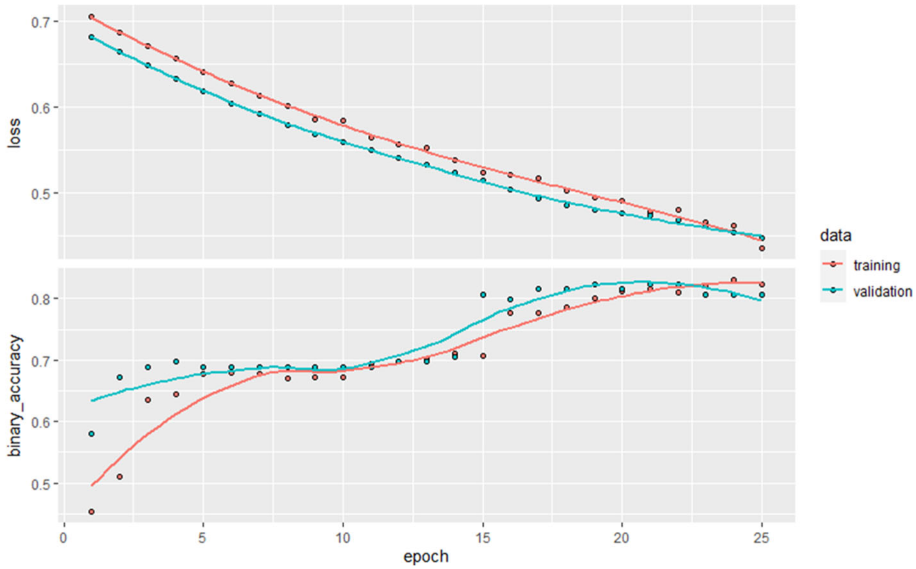

Fig. 3 Use Case 2: Loss and Metrics Curve (Online Recruitment of Terrorists)

4.1 Training and validation

In Use Case1 (Dataset Size:312), all algorithms are performing similarly as the size of our data is smaller in comparison to Use Case2 (Dataset Size:758). Irrespective of the use of different machine learning and deep learning algorithms, marginal difference in accuracy is obtained (71% for Proposed LSTM, 69% for SVM, 68% for RF 68% for BOOSTING). In Use Case 2, as the size of the dataset is increased by 446 records, our machine-learning algorithms are performing well.

Figure 2 (Detection of Weapon Procurement) illustrates the loss and metrics curve for proposed LSTM based method, which is referred to as Use Case 1 in our study. Figure 3 (Detection of Online Recruitment of Terrorists) shows the performance (loss an metrics curve) of the proposed LSTM-based approach, which is referred as Use Case 2 in our study. Furthermore, we summarize the performance in Table 6 for Use Case 1 (Detection of Weapon Procurement) and Table 7 for Use Case 2 (Detection of Online Recruitment of Terrorists).

4.2 Testing

The testing performance is shown in the 4th row of both tables: Table 6 for Use Case 1 (Detection of Weapon Procurement) and Table 7 for Use Case 2 (Detection of Online Recruitment

Table 6 Use Case 1: Performance Parameters

Dataset Type	Accuracy (%)	Loss
Training	77.13	0.4880
Validation	64.52	0.5740
Testing	70.96	0.4871

Table 7 Use Case 2: Performance Parameters

Dataset Type	Accuracy (%)	Loss
Training	82.22	0.4350
Validation	80.67	0.4463
Testing	83.22	0.4230

of Terrorists), where the parameters of the classifier were fixed from the training process at epoch=25. In the previous work, we have seen how machine learning algorithms can be utilised to classify the annotated records.

Comparing deep learning models with traditional machine learning models is essential to understand the relative strengths, weaknesses, and suitability of each approach for different tasks and datasets. Here are some reasons why such comparisons are important:

(i) **Performance Benchmarking**
Comparing deep learning models with traditional machine learning models establishes a baseline for performance. This benchmarking helps researchers and practitioners gauge whether the added complexity of deep learning architectures leads to significant improvements in accuracy, efficiency, or other relevant metrics.

(ii) **Task Suitability**
Different tasks have varying requirements in terms of data size, complexity, and available features. Comparing models helps identify which approach is better suited for a particular task. Deep learning might excel in tasks where there are complex patterns and large amounts of data, while traditional machine learning models might be more appropriate for simpler tasks with limited data.

(iii) **Interpretability**
Traditional machine learning models often provide more interpretability than deep learning models. Comparing the two approaches can help decide whether the level of interpretability provided by traditional models is necessary for a given application, or if the predictive performance of deep learning outweighs the interpretability trade-off.

(iv) **Data Efficiency**
Traditional machine learning models might require less data to achieve reasonable performance compared to deep learning models. If limited data is available, it's important to compare whether deep learning's increased complexity is justified by the data quantity and quality.

(v) **Resource Requirements**
Deep learning models often require more computational resources, such as GPUs or TPUs, and longer training times compared to traditional models. A comparison can help weigh the computational costs against the performance gains.

We have compared previously build machine learning-based classifiers with the proposed LSTM-based deep learning approach as shown in Fig. 4. The accuracy is improved in the case of the proposed LSTM-based deep learning algorithm by 12% (Use Case 1 Accuracy for Proposed LSTM-71% Use Case 2 Accuracy for Proposed LSTM-83%). Observing the small difference, we can conclude that both machine learning and deep learning-based classifiers fit to our current study.

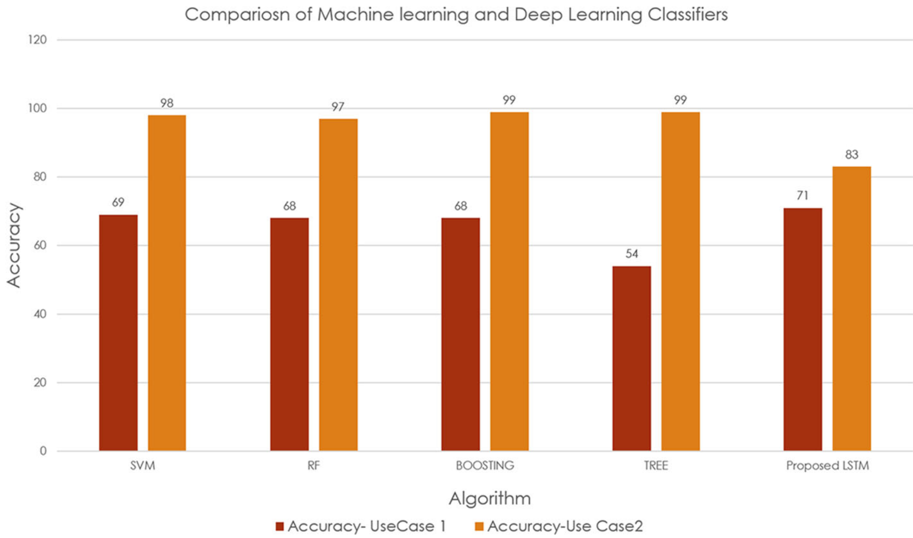

Fig. 4 Comparison of Deep Learning vs Machine Learning Classifiers

5 Conclusions

Studying dark web markets to detect violent activities is a complex and challenging task that often involves a multidisciplinary approach, including computer science, criminology, cyber-security, and data analysis. We developed an automated approach to detect purchasing of illegal weapons (Use Case 1) and the recruitment of innocent minds (Use Case 2) over the dark web in our current work. The online procurement of illegal weapons can also have serious implications for national security. Identifying and thwarting attempts to acquire weapons for terrorist organizations or other extremist groups can help safeguard a country's security interests. By monitoring and detecting recruitment activities, law enforcement agencies can identify and intervene in the early stages of radicalization, disrupting terrorist networks before they can carry out attacks. To the best of our knowledge, the proposed model presents a novel contribution to automate the process of detecting violent activities over the dark web. This type of automation is helpful for any national security agency to keep track of illegal procurement or online recruitment of terrorists.

Funding and Competing Interests NA

Research Data Policy and Data Availability Statements The datasets analysed during the current study are available in the Dark Web Project Portal [2] cited in the paper Section 3.2 .

Declarations

Disclosure of potential conflicts of interest NA

Research involving Human Participants or Animals NA

Informed consent NA

References

1. Bowie NG (1968–2009) Terrorism events data: An inventory of databases and data sets. Perspect Terror 11(4):50–72. http://www.rand.org/nsrd/projects/terrorism-incidents.html
2. Chen H (2011) Dark web: Exploring and mining the dark side of the web. In: 2011 European intelligence and security informatics conference, IEEE, pp 1–2. http://www.azsecure-data.org/about.html
3. Chollet F, Allaire J et al (2017) R interface to keras. https://github.com/rstudio/keras
4. Desmarais BA, Cranmer SJ, Hill C et al (2011) Forecasting the locational dynamics of transnational terrorism : a network analytic approach. In: European intelligence and security informatics conference, pp 171–177, https://doi.org/10.1109/EISIC.2011.44
5. Dhote Y, Mishra N (2013) Survey and analysis of temporal link prediction in online social networks. In: International conference on advances in computing, communications and informatics (ICACCI), pp 1178–1183
6. Domingo JD, Gomez-Garcia-Bermejo J, Zalama E (2022) Optimization and improvement of a robotics gaze control system using lstm networks. Multimed Tools Appl 81(3):3351–3368
7. Duchi J, Hazan E, Singer Y (2011) Adaptive subgradient methods for online learning and stochastic optimization. J Mach Learn Res 12(7)
8. Fernandez M, Asif M, Alani H (2018) Understanding the roots of radicalisation on twitter. In: Proceedings of the 10th ACM conference on web science, ACM, pp 1–10
9. Goyal T, Saini JK, Bansal D (2019) Analyzing behavior of isis and al-qaeda using association rule mining. In: Proceedings of 2nd international conference on communication, computing and networking: ICCCN 2018, NITTTR Chandigarh, India, Springer, pp 669–675
10. Hsiao Hw, Lin CS, Chang Sy (2009) Constructing an ARP attack detection system with SNMP traffic data mining. In: Proceedings of the 11th international conference on electronic commerce. ACM, pp 341–345
11. Kapil P, Ekbal A (2020) A deep neural network based multi-task learning approach to hate speech detection. Knowl-Based Syst 210:106458
12. Katipally R, Gasior W, Cui X et al (2010) Multistage attack detection system for network administrators using data mining. In: Proceedings of the sixth annual workshop on cyber security and information intelligence research, ACM, pp 51
13. Kaur A, Saini JK, Bansal D (2019) Detecting radical text over online media using deep learning. arXiv:1907.12368
14. Kengpol A, Neungrit P (2014) Computers & Industrial Engineering A decision support methodology with risk assessment on prediction of terrorism insurgency distribution range radius and elapsing time?: An empirical case study in Thailand. Comput Ind Eng 75:55–67. https://doi.org/10.1016/j.cie.2014.06.003
15. Kour H, Gupta MK (2022) An hybrid deep learning approach for depression prediction from user tweets using feature-rich cnn and bi-directional lstm. Multimed Tools Appl 81(17):23649–23685
16. Majeed A, Beg MO, Arshad U et al (2022) Deep-emoru: mining emotions from roman urdu text using deep learning ensemble. Multimed Tools Appl 81(30):43163–43188
17. Munezero M, Montero CS, Kakkonen T et al (2014) Automatic detection of antisocial behaviour in texts. Informatica 38(1)
18. Naik AJ, Gopalakrishna M (2021) Deep-violence: individual person violent activity detection in video. Multimed Tools Appl 80(12):18365–18380
19. Rehman AU, Malik AK, Raza B et al (2019) A hybrid cnn-lstm model for improving accuracy of movie reviews sentiment analysis. Multimed Tools Appl 78:26597–26613
20. Revelle W (2021) psych: procedures for psychological, psychometric, and personality research. Northwestern University, Evanston, Illinois, r package version 2.1.9. https://CRAN.R-project.org/package=psych
21. Rezaeenour J, Ahmadi M, Jelodar H et al (2023) Systematic review of content analysis algorithms based on deep neural networks. Multimed Tools Appl 82(12):17879–17903
22. Saini JK, Bansal D (2019) A comparative study and automated detection of illegal weapon procurement over dark web. Cybern Syst 50(5):405–416. https://doi.org/10.1080/01969722.2018.1553591
23. Saini JK, Bansal D (2021) Detecting online recruitment of terrorists: towards smarter solutions to counter terrorism. Int J Inf Technol 13:697–702
24. Saini JK, Bansal D (2023) Computational techniques to counter terrorism: a systematic survey. Multimed Tools Appl 1–26
25. Thakur D, Saini JK, Srinivasan S (2023) Deepthink iot: the strength of deep learning in internet of things. Artif Intell Rev 1–68
26. Vinyard Software (2016) International terrorism: attributes of terrorist events, 1968-1977 [ITERATE 2]. https://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/07947. Accessed 8 May 2016
27. Wigle J (2010) Introducing the worldwide incidents tracking system (wits). Perspect Terror 4(1):3–23

28. Yechuri PK, Ramadass S (2021) Classification of image and text data using deep learning-based lstm model. Trait du Signal 38(6)
29. Zhang T, Yang Z, Jia W et al (2016) A new method for violence detection in surveillance scenes. Multimed Tools Appl 75:7327–7349
30. Zhang Y, Zeng S, Fan L et al (2009) Dark web forums portal: searching and analyzing jihadist forums. In: 2009 IEEE international conference on intelligence and security informatics, IEEE, pp 71–76
31. Zhou Y, Qin J, Reid E et al (2005) Studying the presence of terrorism on the web : a knowledge portal approach. In: Proceedings of the 5th ACM/IEEE-CS joint conference on digital libraries. ACM, 2005, pp 402