Enhanced Cybercrime Detection on Twitter Using Aho-Corasick Algorithm and Machine Learning Techniques

[1]Romil Rawat[*], [2]A Samson Arun Raj, [3]Rajesh Kumar Chakrawarti, [4]Krishnan Sakthidasan Sankaran, [5]Sanjaya Kumar Sarangi, [6]Hitesh Rawat, [7]Anjali Rawat
[1*]Department of Computer Science Engineering, Shri Vaishnav Institute of Information Technology, Shri Vaishnav Vidyapeeth Vishwavidyalaya Indore, India
[2]Division of Computer Science and Engineering, School of Computer Science and Technology, Karunya Institute of Technology and Sciences, Tamil Nadu, Coimbatore, India
[3]Department of Computer Science and Engineering, Sushila Devi Bansal College (SDBC), Bansal Group of Institutions (BGI), Indore (MP) – India
[4]Department od Electronics and Communication Engeneering, Hindustan Institute of Technology and Science, Chennai, India
[5]Department of Computer Science and Engineering, Utkal University, Bhubaneswar, India
[6]Department of Business Management and Economics, University of Extremadura, Spain
[7]Department of Computer and Communication Technology, University of Extremadura, Spain
E-mail: rawat.romil@gmail.com, [2]samsonarunraj@karunya.edu , [3]rajesh_kr_chakra@yahoo.com , [4]sakthidasan.sankaran@gmail.com, [5]sanjaya.res.cs@utkaluniversity.ac.in ,[6]hrawat88@gmail.com , [7]rawatanjali457@gmail.com
[*]Corresponding author

Keywords: cyber terrorism, ternary search, aho-corasick automata, threat, online social network, machine learning

Received: May 27, 2024

The proposed work objective is to adapt Online social networking (OSN) is a type of interactive computer-mediated technology that allows people to share information through virtual networks. The microblogging feature of Twitter makes cyberspace prominent (usually accessed via the dark web). The work used the datasets and considered the Scrape Twitter Data (Tweets) in Python using the SN-Scrape module and Twitter 4j API in JAVA to extract social data based on hashtags, which is used to select and access tweets for dataset design from a profile on the Twitter platform based on locations, keywords, and hashtags. The experiments contain two datasets. The first dataset has over 1700 tweets with a focus on location as a keypoint (hacking-for-fun data, cyber-violence data, and vulnerability injector data), whereas the second dataset only comprises 370 tweets with a focus on reposting of tweet status as a keypoint. The method used is focused on a new system model for analysing Twitter data and detecting terrorist attacks. The weights of susceptible keywords are found using a ternary search by the Aho-Corasick algorithm (ACA) for conducting signature and pattern matching. The result represents the ACA used to perform signature matching for assigning weights to extracted words of tweet. ML is used to evaluate Twitter data for classifying patterns and determining the behaviour to identify if a person is a terrorist. SVM (Support Vector Machine) proved to be a more accurate classifier for predicting terrorist attacks compared to other classifiers (KNN- K-Nearest Neighbour and NB-Naïve Bayes). The 1st dataset shows the KNN-Acc. -98.38% and SVM Accuracy as 98.85%, whereas the 2nd dataset shows the KNN-Acc. -91.68% and SVM Accuracy as 93.97%. The proposed work concludes that the generated weights are classified (cyber-violence, vulnerability injector, and hacking-for-fun) for further feature classification. Machine learning (ML) [KNN and SVM] is used to predict the occurrence and incident of crime. The accuracy and efficacy are evaluated using several parameters in the model.

Povzetek: Raziskava predstavlja izboljšano metodo za zaznavanje kibernetskega kriminala na Twitterju, ki združuje algoritem Aho-Corasick in strojno učenje. Z uporabo algoritma Aho-Corasick (ACA) za ujemanje podpisov z uporabo ključnih besed ter strojnega učenja (KNN, SVM) zagotavlja visoko tončnost pri klasifikaciji vzorcev terorizma.

1 Introduction

Cyber terrorism operates across borders using a virtual platform by sharing posts or statuses on the OSN [1] platform to attract people in order to receive financial assistance and recruitment. From their social status, police, security agencies, and the normal user try to relate the ideology, relevant facts, patterns, and hidden

information of the message. Our major goal is to create a system that analyses terrorist attacks and operations and related tweets from Twitter to identify terror events. Twitter is a medium for disseminating information and a source of educational engagement. Several complex processes, with the assistance of numerous current technologies, are implemented to build a robust security model for preventing this threat and vulnerability.
The below figure shows the phases of malfeasance [2]. The criminal activity is the sequence developed to find the loopholes.

1. Malfeasance Prevention: The system and model should be framed with security measures for generating alerts when unauthorised activity is found (by insiders and outsiders) and auto-upgrading to discover new patterns for future vulnerability prediction.
2. Awareness: Online users must be aware of malicious behaviours and signatures, with available tools and techniques to detect the threat.
3. Countermeasures: a reverse attacking system designed to trace the route of host-generating malicious events.
4. Occurrence: A threat classification mechanism to identify and analyse the purpose of a threat with categorisation for activating security measures.
5. Evolution: Loopholes originate threats to enter the system, and patches provide details for recognising the source of the attack originator. Identification of infected systems and threat distribution mechanisms with the network.
6. Cessation: recognising the route (ToR Network—The Online Router) [2], followed by a threat to infect networking nodes sharing information, and removing the vulnerabilities using automated learning techniques as shown in Figure 1: Phases of Malfeasance.

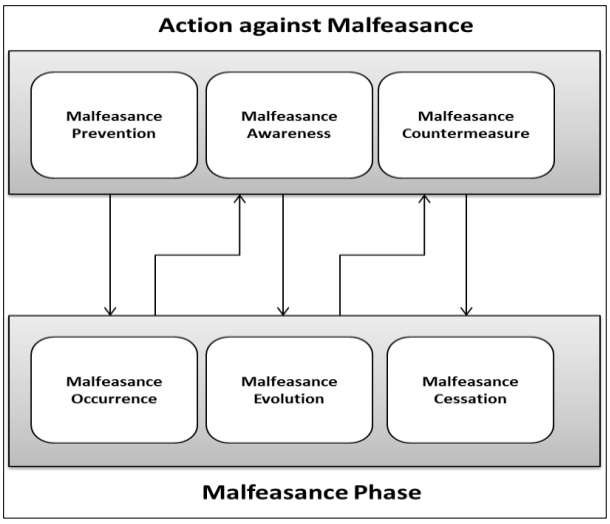

Figure 1: Phases of malfeasance

Here, the detection of a specific terrorist act and its location is evaluated by analysing Twitter data, which attracted researchers to the development of ML classifiers and approaches in order to evaluate Twitter data [4], addressing the use of OSN analysis [5] for classifying patterns and determining the behaviour, whether or not a person is a terrorist. SVM proved to be a more accurate classifier for predicting terrorist attacks compared to other classifiers [6].
The OSN comprises divergent channels and forums for discussion and sharing of messages. Data mining (DM) techniques generate patterns and classifications of users actively communicating on the social platform. According to livestats.com [7], in March 2019, the OSN users reached a count of 4,804,649,792 across the world. Figure 2 shows the OSN forum for communication and user statistics across the globe.

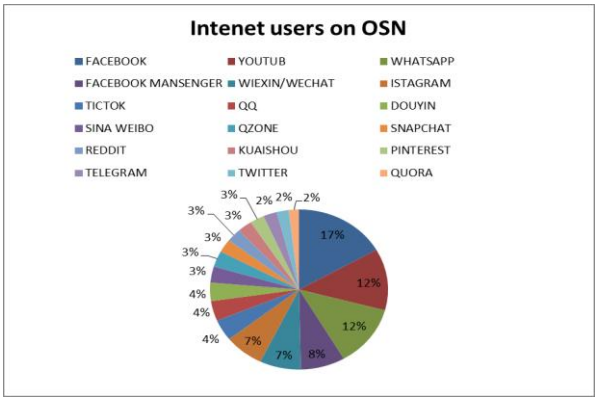

Figure 2: OSN Platforms user statistics

Tweets including hashtags of terrorist groups (like #Al-Qaeda, #Jihad, and #Extremism) [8], and data collection methods to create a threat dictionary with techniques for predicting future support and clauses using ISIS-related tweets [7], the Twitter data used to investigate the connected chains and associated links at social platforms supporting criminal events. Another study based on the ML technique in tweet sentiment categorisation was conducted by [10]. The geolocation of the tweet was retrieved by a Python package called Geopy for extracting the location of profile access.
The present work develops a Signature Mapping and Supporting Weight Distribution (SMSWD) model for discovering the weights using the count of tweeted words with linear time complexity (LTC) [8] of filtered character sets, word lists, and geolocations using ACA [23][24].
Figure 3 below provides a chaining framework for OSN for user communication using nodes, shares, and posts for retweeting. The difficult task faced by security agencies and cyberpolicing is to track the originator and route of criminals and fraudulent posts while reaching the audience. Example Node (N9) received the post in the form of a direct tweet or retweet [9]. The complexity is finding the exact node involved in malicious post-distribution, as shown in Figure 3-OSN Chaining Framework.

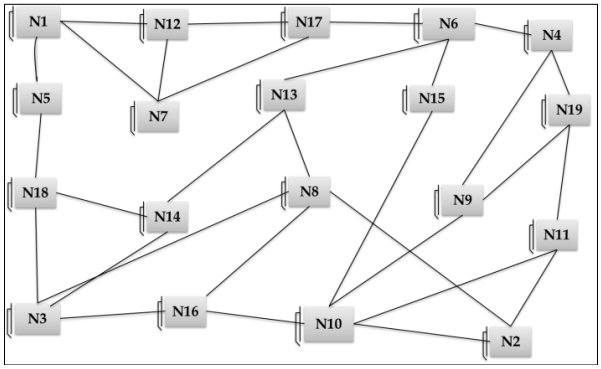

Figure 3: OSN chaining framework

a) The novelty of the work focusses:

On a Signature Mapping and Supporting Weight Distribution (SMSWD) model for discovering the weights using the count of tweeted words with linear time complexity (LTC) of filtered character sets, word lists, and geo-locations using ACA.

b) Contribution:

- The improved technique for detecting a terrorist threat operated on a dark web platform is used as the most challenging point is to detect cybercrime [26][27][28] and criminals on social media.
- These cybercriminals only activate during specific events or sessions to perform specified tasks; at that time, they can only be traced.
- ACA technique is used to perform signature matching for assigning weights to extracted words of tweet during terrorist incidents. Individuals usually use Twitter to disseminate the news. Using this concept, the system traces the illicit actors.

c) The Work is focussed on:

- An enhanced model for detecting and predicting terrorist attacks, even those that have already occurred, is presented by analysing OSN obtained from Twitter.
- To find the weights of tweeted terms, the ACA helped in extracting words (series of characters), and SPPM (string parsing and pattern matching) had linear time complexity.
- The weighted count of classifiers (SVM and KNN) used for categorising the data and the demonstrated results show the appreciable outcomes. The primary drawback of applied modelling is that datasets are insufficient to produce reliable outcomes.
- We collected a varied number of tweets from various locations and times for each dataset. A graphic depiction of the fractions (real value and anticipated value) of different groups is done using a confusion matrix using ML classification techniques.

The remainder of this work is summarized as follows: Section 2 outlines the related work; Section 3 shows about the modelling of the theoretical approach; Section 4 shows about the proposed model; section 5 represents result experiments; and finally, Section 6 concludes the manuscript with future work.

2 Related work

In the work [6], the authors describe a method for detecting Arabic tweets that makes use of feature extraction, N-gramme models, ML approaches, as well as performance metrics computation. The neural network (NN) approach beat other methods and exceeded quick text by 0.5%, with the greatest F1-score of 99.73%.
Logistic regression (LR), support vector machines (SVM), and naive Bayes are examples of traditional machine-learning approaches. Quick text learning models and deep learning (DL) techniques. In order to identify illegal statements in tweets with high accuracy, precision, and recall, the work in the publication [7] suggests employing classifiers like NB and Random Forest (RF). Algorithms for ML provide practical tools for detecting illegal conduct. The Table-1 shows about the Literature review comparison.

Table 1: Literature review comparison

Ref	Method	Features	Results
[22]	Focused on multi pattern matching algorithm, ACA, based on SUNDAY algorithm for optimizing unnecessary string matching.	Used multiple patterns matching technique for the security of Automated systems.	Effectively reduces the memory consumption and threat detection rate.
[23]	Focused on ML and DL technique and based on lexicon for tracing crime databases in tweets by ACA technique.	Based on Arabic tweets and features	Work represents and shows that ML models exhibit superior accuracy.
[24]	Focused on to identify illicit tweets for Cybercrime based acts.	Based on the snake optimization Approach for feature selection for enhancing the Arabic Twitter crime identification.	Shows the accuracy of 88% based on the tweets for improving the public safety.
[25]	Focused on SQL Injection vulnerability, and threats.	Based on the system to secure web applications using Hashing	Shows the payload of malicious query

		and ACA algorithm.	patterns and detect with 90.23% accuracy.
[26]	Focused on data analysis approach for helping the security agencies by sharing details relating to suspects.	Based on the automation steps for tracing the crime spot using signature matching and fingerprinting,	Shows the model is able to generate the appreciable accuracy.
[27]	Focused on towards the extraction of information to understand crime attributes and generate predictions for security measures for the Arabic text.	Based on ACA technique for addressing the dynamic nature of language and evolving criminal taxonomy for preprocessing and extracting relevant tweet attributes.	Shows the analysis of an Arabic tweet dataset and features with a high accuracy of 99.25%.
Proposed Work	The method used is focused on a new system model for analyzing Twitter data and detecting terrorist attacks.	• The weights of susceptible keywords are found using a ternary search by the ACA for conducting signature and pattern matching. • An enhanced model for detecting and predicting terrorist attacks, even those that have already occurred, is presented by analyzing OSN obtained from Twitter.	• ML is used to evaluate Twitter data for classifying patterns and determining the behavior to identify if a person is a terrorist. SVM proved to be a more accurate classifier for predicting terrorist attacks compared to other classifiers (KNN and NB-Naïve Bayes). • The 1st dataset shows the KNN-Acc. -98.38% and SVM Accuracy as 98.85%, whereas the 2nd dataset shows the KNN-Acc. -91.68% and SVM Accuracy as 93.97%.

3 Modeling of theoretical approach

a) 4J Twitter API (application programming interface):

The Twitter 4j-API is used to gather data from Twitter and Java library [10]. The API makes it simple to utilize a Java application with the Twitter service. Using the streaming API, data may be retrieved from the most current Twitter data, which is typically 1 or 2 weeks old and based on hashtags.

b) ACA

The ACA, designed by Alfred V. Aho and Margaret J. Corasick [11], is an dictionary-matching technique that locates the elements of a finite collection of strings (the "dictionary") inside an input text [11]. All strings are matched at the same time. Based on the length of strings, searched text, and the count of output matches, the algorithm's complexity is linear. This technique creates a finite-state machine (FSM) that quadrates a tyre by adding extra linkages between the interior nodes. This technique may be used to search for each string in a collection to see if it appears in the text. For example, in O (|P| + |Q|), where |P| and |Q| is the total length of the text and pattern respectively, marking the first occurrence of a string in the text.

Array pi[I] = max(x): a[0….. n) = s(i – x....i], where pi(I) is the length of the extended own suffix that matches the pre-fix of the sub-string [0….. I]. Building automata is required to determine the length of the extended suffix of some text P, which is also the pre-fix of the string Q. The suffix link is a pointer to the state since it feeds the automata text one by one and adds characters matching the extended own suffix of the current state. We can determine whether a string Q is a substring of text P for a specified string Q. In trie, also called digital tree (DT) [12], we are combining our pattern set. At each vertex of the DT, a suffix link to the state corresponding to the

biggest suffix of the path to the specified vertex in automata that are present in the DT will be recorded, just as in the pre-fix automaton. It's only a matter of figuring out how to get these connections using a BFS(breadth-first search), starting at the root. Then, using the same technique, we "push" the suffix connections to all of their descendants. To extract tweeted terms, we used the ACA to conduct pattern matching for assigning weights. With extra words in the keyword, it might be difficult to determine the category of the tweet.

c) Ternary search (TS)

It is a method for locating the uni-modal function's reference to having only one of two possible outcomes.
(a) The function increases towards its peak value and further declines.
(b) Function decreases first, reaching its least value, then further increases.
A search point is classified into three pieces in a ternary search (TS), and one portion is dismissed when the result is certain not to exist. If f(y) is a unimodal function on the interval [l, s], we wish to tune the function's Max_Value. Consider two points, n1 and n2, with l &lu; m1 &lu; n2 &lu; s and values f(n1) and f(n2). Now we have three choices: f(n1) and f(n2). The left side of n1 is discarded since the desired Max_Value cannot be found on the interval [l, n1], and the Max_Value is found in the segment [n1, s]. Further f(n1) and hi; f(n2),, The right side of n2 is discarded because the Max_Value is placed on [l, n2], thus the interval [n2, s] is also discarded. n1=f(n2) , We reject either the left interval [l, n1] or the right interval [n2, r] in this situation.
Then we may substitute l = n1 or s = n2 for the current interval [l, s] and continue until the difference between l and s is not near enough. Then the Max_Value will be the average of l and s. The most frequent method for determining n1 and n2 is to use the formulas n1 = l + (s-l)/3 and n2 = s-(s-l)/3.
The TS is the best method for locating a Max_Value or minimum point in a U-shaped graph. As a result, TS is utilised to determine the time period in which tweets were appeared on Twitter [13]. TS decides if the minimum or Max_Value cannot be in the first third or last third of the domain, then repeats the process on the left-over two-thirds. We require the Max_Value and minimum TOT (in minutes) from the file to calculate the weight, as well as a ratio that we found using a TS.

Data-availability: We start with a pre-defined term and then assign it. Table 1 contains the instances.

To allocate a weight to a tweet, we create an equation. The formula is as follows:

tweet_weight =(max_time – min_time) *ratio *count of matches ----------(1)

A TS is used to find the ratio. The TS lower and upper bounds values are 0.0 and the 1.0. Each ratio point's real value is derived by averaging the accuracy of 5- random iterations.

d) KNN

Training data is used to classify and locate its KNN [14], a assigning the newer point specified to most classes. The following measurements are used to determine the distance: Manhattan, Euclidean, and Minkowski as shown in Table -2-Predefine words.

Table -2: Predefine words

Predefine Words [Cyber-Violence, vulnerability injector, and Hacking-for-Fun]	
Words	**Belongs to**
1. terrorism recruitment	Cyber-Violence, vulnerability injector
2. attack	Cyber-Violence
3. financial fraud	Vulnerability injector
4. malware	Vulnerability injector
5. cyber extortion	Cyber-Violence
6. Social Engineering	Hacking-for-Fun
7. illegal pornography	Hacking-for-Fun, Vulnerability injector, Hacking-for-Fun
8. cyber sociology	Cyber-Violence, vulnerability injector
9. Exploit	Vulnerability injector
10. Botnet	Vulnerability injector
11. Propaganda	Hacking-for-Fun
12. Fund raising	Cyber-Violence, vulnerability injector
13. Clickjacking	Hacking-for-Fun, Vulnerability injector
14. Deepfake	Cyber-Violence, Vulnerability injector
15. Smart Device Compromise	Cyber-Violence, Vulnerability injector

$$Euclidean: \sqrt{\sum_{i=1}^{k}(a_i - b_i)^2} \quad \text{------} \quad (2)$$

$$Minkowski: \sum_{i=1}^{k} \mid a_i - b_i \mid \quad \text{---------} \quad (3)$$

$$Manhattan: \left(\sum_{i=1}^{k}(\mid a_i - b_i \mid)^n\right)^{1/m} \text{-----} \quad (4)$$

When there is a problem with standardisation of numerical variables between 0 and 1, Hamming distance is employed. When the dataset has both numerical and category variables.

$$Hamming: \sum_{i=1}^{k} \mid n_i - m_i \mid \quad \text{---------} \quad (5)$$

e) SVM [15]

SVM is a binary classification method that has a collection of M points, each falling into two classes: 1

and the -1. Further these points appear with their respective class names, The data set may therefore be represented as and can be classified using SVM datasets. Using the KNN algorithm, comparisons of projected data with real data are to be made to determine the efficacy of the results for prediction.

f) Confusion matrix (CM)[16]

The CM is used for storing details about actual and predicted classifications to represent the classifier. The efficacy of the model is defined for calculating the accuracy level.

4 Proposed model

a) ACA is important in Twitter data analysis:

- The ACA is frequently used in systems like spell checks, search engines, and spam filters to perform efficient functions in the Twitter network.
- It is used to rapidly search for many patterns in a massive blob of Twitter text.
- And used for pattern matching in enormous volumes of text.
- The ACA method builds a triple data structure and adds connections to facilitate transitions between unsuccessful pattern matches, allowing it to search for numerous patterns in a huge text corpus rapidly and effectively.

b) System working:

We used the Twitter 4j [17] API in JAVA to extract social data based on hashtags, and after discovering the weights of filtered words, the SMSWD was introduced. It is divided into two parts: ACA and TS to give weights to pre-defined terminologies. We require Max_Value and minimum time_of_tweets (TOT) (in min) values from the file to calculate the weight and ratio taken from TS. Information is divided into three groups by utilising techniques (SVM and KNN) [18] to forecast the phases of the data, as well as a confusion matrix to calculate the accuracy of our experiment with efficiency evaluation parameters. The flowchart of the violence event prediction model suggested is shown in Figure 3.

Multiple tweets may be monitored after a terrorist incident on Twitter. We utilise OSN to track relevant data from Cyber-Violence's [19], and this data is required for categorising into three phases, as established by our study using public data [20] and [21] for algorithm training as shown in Figure 4-Violence events prediction model.

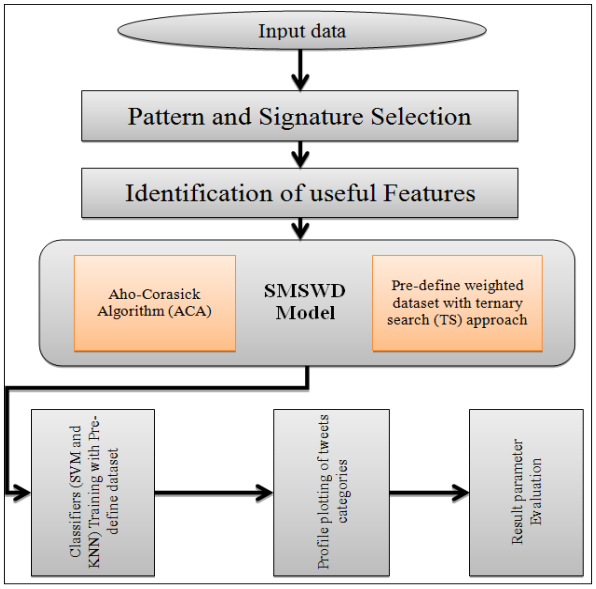

Figure 4: Violence events prediction model

c) Algorithm:

The proposed method is assessed using Twitter data analysis and terrorist attack detection and performs ternary search to find the weights of vulnerable keywords in order to match patterns and perform signatures. By examining OSN gathered from Twitter, an improved model for identifying and forecasting terrorist attacks—including those that have already happened in the extraction of words (character sequences)—and the linear time complexity of SPPM (string parsing and pattern matching) in determining the weights of keywords that were tweeted. The Figure 5 shows about the Algorithm for Evaluation of Threat based on Text Analysis.

```
set of features for signature matching  J,
set N of all features,
begin
assigning weights Rules( Library- Tweepy) ← $ for Text Analysis
for each features n∈N
do
for each value Z of features n
 do
count how often each class appears
find the most frequent class CL
construct j rule IF n = Z Then, CL
end for
calculate Text similarity and matching for all rules and  feature classification
choose the best rule pS
pattern matching-Rules ← pS
End for
Show Levels for predict and occurrence with incident of crime
end
```

Figure 5: Algorithm for evaluation of threat based on text analysis

5 Result experiments

The Twitter interface is used to gather real-world datasets. For the purpose of classifying tweets about crimes [28][29][30][31], the findings are represented using two machine learning classifiers', and the results parameters are compared.

a) Dataset details:

The experiments contain two datasets. The first dataset has over 1700 tweets, whereas the second dataset only comprises 370 tweets. We collected a varied number of tweets from various locations and times for each dataset. A graphic depiction of the fractions (real value and anticipated value) of different groups is done using a confusion matrix using ML classification techniques.

The dataset represents English tweets linked to cyberattacks and is tagged and focused on cybersecurity. Each tweet has been individually tagged. We carried out extensive tests utilising many supervised machine learning techniques and numerous refined language models to evaluate the quality and appropriateness of the dataset for the intended use in order to guarantee its correctness and dependability. dataset not only confirms the excellent quality and comprehensiveness of its annotations but also shows the potential of our method.

Preprocessing, often known as data cleansing, is a crucial phase in the creation of prediction models. To categorise tweets on crimes and non-crimes [30][31], textual data from Twitter is used. Classification findings that are deceptive can be directly caused by textual data. Therefore, prior to using machine learning algorithms, data pretreatment and cleaning techniques are utilised. The stages are followed throughout the procedure.

- Sentence segmentation is employed to separate the tweets into individual words or tokens. Using hashtag expansion, joint hashtags may be made longer.
- Because the non-content-bearing phrases don't offer any information concerning criminal analysis, Stop Words Removal is utilised to eliminate them.
- Slang and Acronyms Expansion of acronyms and popular slang terms during treatment.
- Punctuation Terms such as 'the', 'is', and 'what' that do not contain content are removed.
- The terms associated with crime are highlighted using the TF-IDF (term frequency-inverse document frequency) converter.

b) 1st dataset use in experiment:

The CM obtained using KNN and SVM is shown in Figure 6. The correct value is represented by the primary diagram, while the false value is represented by the rest of the cell. The classifier of SVM shows appreciable accuracy compared to KNN. The CM is primarily used to ensure accuracy with vulnerability injector data weighted counts as parameters. With an increase in the quantity of tweets (SVM and KNN), similar results were shown nearby. However, when the count of tweets decreases, the SVM outcome surpasses the KNN result as shown in Figure 6. (a)-KNN-CM and Figure 6.(b)-SVM-CM respectively.

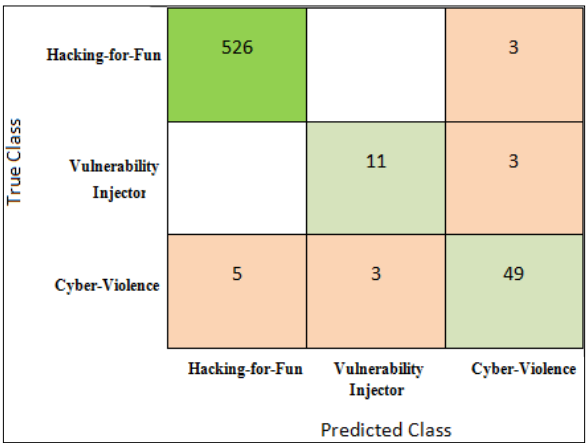

Figure 6: (a) KNN--CM

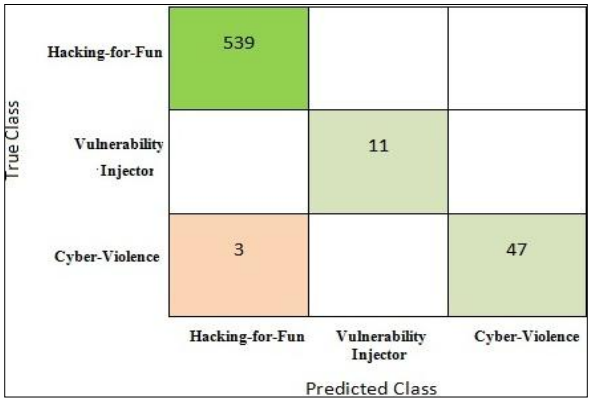

Figure 6: (b) SVM--CM

Figure 7. (a)-Real chart, Figure 7. (b) KNN Predicted chart and Figure 7. (c) SVM Predicted chart shows about the real proportion of vulnerability injector threat data by around 41%, and we got 41 percent (KNN) and 37.58 percent (SVM). Whereas the real percentage of cyber-violence is 35 percent, we obtained 34.21 percent (KNN) and 36.16 percent (SVM). The real percentage for hacking-for-fun data is 53 percent, whereas the projected percentage is 61.24 percent (KNN) and 54.75 percent (SVM).

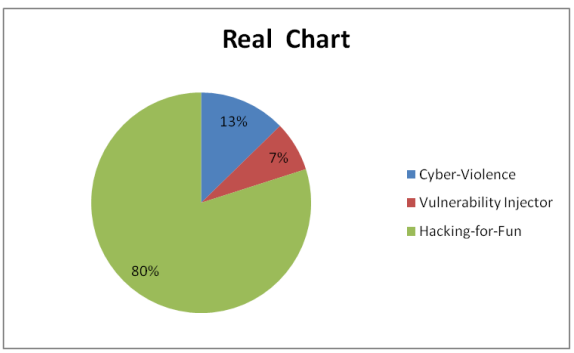

Figure 7: (a) RC

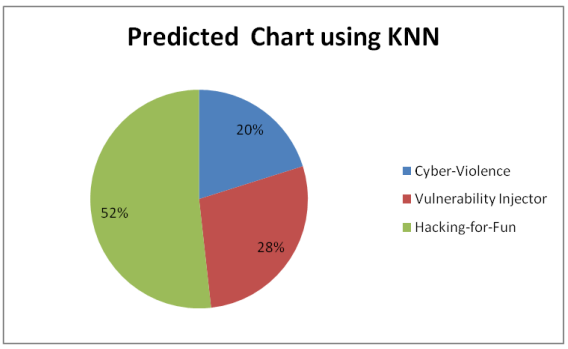

Figure 7: (b) KNN-PC

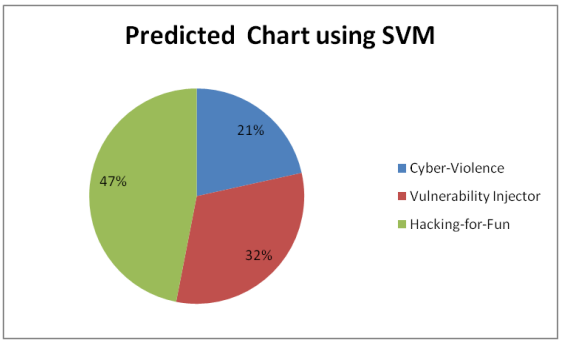

Figure 7: (c) SVM-PC

c) 2nd dataset use in experiment

The second dataset consists primarily of 370 tweets. Figure 9 plots data (tweet information) against a weighted count using hacking-for-fun data, cyber-violence data, and vulnerability injector data as parameters to demonstrate the profile of tweet categorization. With an increase in the quantity of tweets (SVM and KNN), similar results were shown nearby. However, when the count of tweets decreases, the SVM outcome surpasses the KNN result.

The CM obtained using KNN and SVM is shown in Figure 8. (a)-KNN-CM and Figure 8. (b)-SVM-CM. The authenticated value is represented by the primary diagram, while the false value is represented by the rest of the cell having appreciable accuracy of SVM compared to KNN classifier.

Figure 9. (a)-Real pie chart, Figure 9. (b)-KNN-PC and Figure 9. (c)-SVM-PC shows about the real proportion of vulnerability injector threat data by 42 percent, and we got 35.29 percent (KNN) and 37.58 percent (SVM). Whereas the real percentage of cyber-violence is 35 percent, we obtained 34.21 percent (KNN) and 36.16 percent (SVM). The real percentage for hacking-for-fun data is 53 percent, whereas the projected percentage is 61.24 percent (KNN) and 54.75 percent (SVM). The Table-3 shows about the Classifiers (SVM and KNN) Accuracy Comparison.

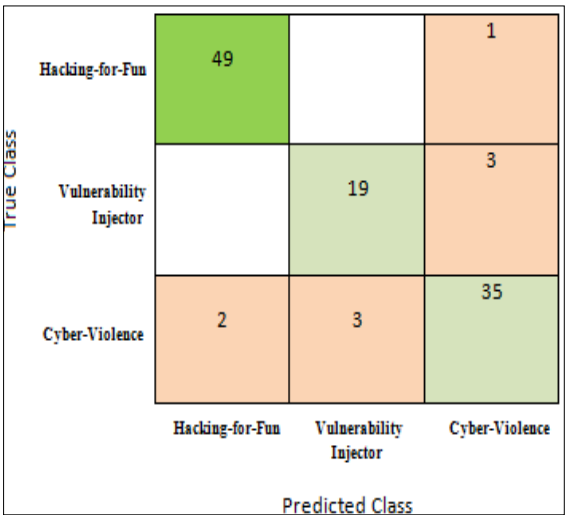

Figure 8: (a) KNN-CM

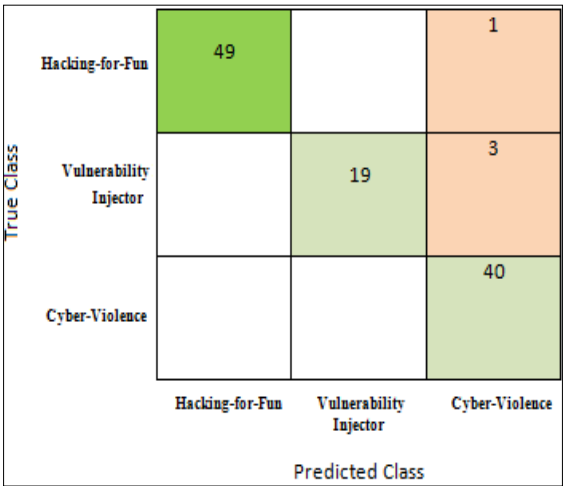

Figure 8: (b) SVM-CM

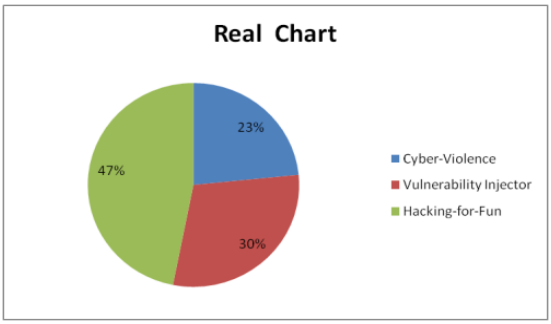

Figure 9: (a) RC

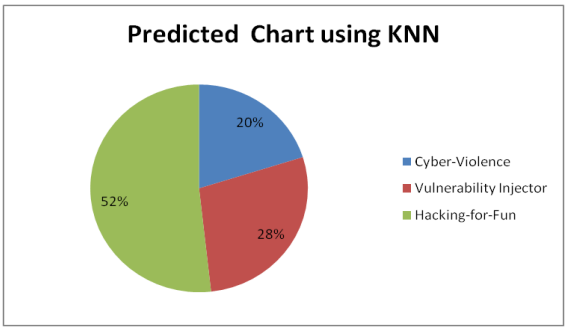

Figure 9: (b) KNN-PC

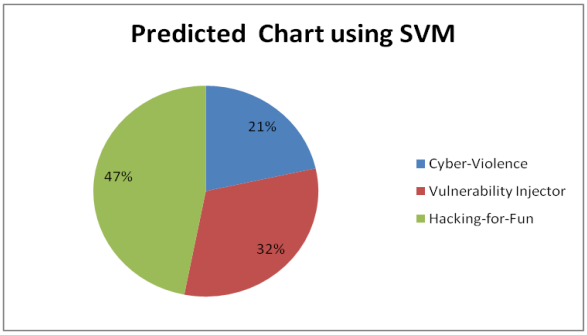

Figure 9: (c) SVM-PC

Table-3: Classifiers (SVM and KNN) accuracy comparison.

Datasets	KNN-Acc.	SVM Accuracy	DR (%)	TPR (%)	FPR (%)	F-Value	Recall
1st	98.38%	98.85%	99.13	99.61	0.69	99.13	97.29
2nd	91.68%	93.97%	97.73	98.43	0.93	96.85	97.86

The evaluated accuracy of SVM is greater than that of SVM with all supporting parameters when applied to datasets 1 and 2.

6 Discussion

By using the ACA algorithm, a sophisticated technique for graph and metadata analysis is created, allowing tweets pertaining to criminal activity to be categorised. Before creating models, recent tweets are taken out for examination, with an emphasis on threats across various platforms and the detection of crimes in Arabic tweets.

The suggested study focusses on OSN, a sort of interactive computer-mediated technology that enables individuals to exchange information through virtual networks, in contrast to the existing body of work.

For the sake of subsequent feature categorisation, the produced weights (cyber-violence, vulnerability injector, and hacking-for-fun) are classified. Crime incidence and occurrence are predicted using machine learning (ML). The model evaluates the accuracy and efficacy based on many parameters.

This work is done for Twitter's microblogging function, which draws attention to cyberspace, which is typically accessed through the dark web.

7 Conclusion and future work

The outcome shows the ACA that has been utilised to match signatures and provide weights to tweet extracts. Twitter data is evaluated using machine learning (ML) to categorise trends and analyse behaviour to determine whether an individual is a terrorist. When it came to forecasting terrorist attacks, SVM outperformed alternative classifiers (KNN and NB-Naïve Bayes). In the first dataset, the KNN-Acc. is -98.38% and the SVM Accuracy is 98.85%; in the second dataset, these values are -91.68% and 93.97%, respectively.

An enhanced model for detecting and predicting terrorist attacks, even those that have already occurred, is presented by analysing OSN obtained from Twitter. To find the weights of tweeted terms, the ACA helped in extracting words (series of characters), and SPPM (string parsing and pattern matching) had linear time complexity. The weighted count of classifiers (SVM and KNN) used for categorising the data and the demonstrated results show the appreciable outcomes. The primary drawback of applied modelling is that datasets are insufficient to produce reliable outcomes.

For future implementation, a new AI and ML-based approach can be implemented by taking Max_Value features and posts of threat signatures and fingerprinting for terrorism event prediction and detection.

Future research will assist in identifying remedies to uncover various patterns in a large volume of text; the paraphrase extraction can greatly enhance the selected domain of entity pairs from other distinct domains and the relation labelling method.

Abbreviation used

OSN	Online Social Networking
ACA	Aho-Corasick Algorithm
ML	Machine Learning
KNN	K-Nearest Neighbor
NN	Neural Network
LR	Logistic regression
RF	Random Forest
DL	Deep Learning
SVM	Support Vector Machine
ToR	The Online Router
NB	Naïve Bayes
DM	Data Mining
LTC	Linear Time Complexity
SMSWD	Signature Mapping and Supporting Weight Distribution
API	Application Programming Interface.
FSM	Finite-State Machine
DT	Digital Tree
TS	Ternary Search
CM	Confusion Matrix
TOT	Time_Of_Tweets
RC	Real Chart
PC	Predicted Chart (
TPR	True Positive Rate
FPR	False Positive Rate
Acc.	Accuracy
Max.	Maximum
min	Minutes
DR	Detection Rate
SPPM	String Parsing and Pattern Matching
BFS	Breadth-First Search
TF-IDF	Term Frequency-Inverse Document Frequency

References

[1] Sarker, A., Chakraborty, P., Sha, S. S., Khatun, M., Hasan, M. R., & Banerjee, K. (2020). Improvised technique for analyzing data and detecting terrorist attack using machine learning approach based on twitter data. *Journal of Computer and Communications*, *8*(7), 50-62.doi: 10.4236/jcc.2020.87005

[2] Nandhini, B. S., & Sheeba, J. I. (2015). Online social network bullying detection using intelligence techniques. *Procedia Computer Science*, *45*, 485-492.https://doi.org/10.1016/j.procs.2015.03.085

[3] Galán-García, P., Puerta, J. G. D. L., Gómez, C. L., Santos, I., & Bringas, P. G. (2016). Supervised machine learning for the detection of troll profiles in twitter social network: Application to a real case of cyberbullying. *Logic Journal of the IGPL*, *24*(1), 42-53.https://doi.org/10.1093/jigpal/jzv048

[4] Rathi, S. K., Keswani, B., Saxena, R. K., Kapoor, S. K., Gupta, S., & Rawat, R. (Eds.). (2024). *Online Social Networks in Business Frameworks*. John Wiley & Sons.https://onlinelibrary.wiley.com/doi/book/10.1002/9781394231126

[5] Elghanuni, R. H., Ali, M. A., & Swidan, M. B. (2019, August). An overview of anomaly detection for online social network. In *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)* (pp. 172-177). IEEE.DOI: 10.1109/ICSGRC.2019.8837066

[6] Kaddoura, S., & Henno, S. (2024). Dataset of Arabic spam and ham tweets. *Data in Brief*, *52*, 109904.https://doi.org/10.1016/j.dib.2023.109904

[7] Lal, S., Tiwari, L., Ranjan, R., Verma, A., Sardana, N., & Mourya, R. (2020). Analysis and classification of crime tweets. *Procedia computer science*, *167*, 1911-1919.https://doi.org/10.1016/j.procs.2020.03.211

[8] Rasheed, J., Akram, U., & Malik, A. K. (2018, December). Terrorist network analysis and identification of main actors using machine learning techniques. In *Proceedings of the 6th international conference on information technology: IoT and smart city* (pp. 7-12).https://doi.org/10.1145/3301551.3301573

[9] Mashechkin, I. V., Petrovskiy, M. I., Tsarev, D. V., & Chikunov, M. N. (2019). Machine learning methods for detecting and monitoring extremist information on the Internet. *Programming and*

Computer Software, *45*(3), 99-115.https://doi.org/10.1134/S0361768819030058

[10] Ji, X., Chun, S. A., Wei, Z., & Geller, J. (2015). Twitter sentiment classification for measuring public health concerns. *Social Network Analysis and Mining*, *5*, 1-25.https://doi.org/10.1007/s13278-015-0253-5

[11] Ourlis, L., & Bellala, D. (2019). SIMD Implementation of the Aho-Corasick Algorithm Using Intel AVX2. *Scalable Computing: Practice and Experience*, *20*(3), 563-576.https://doi.org/10.12694/scpe.v20i3.1572

[12] Tam, S., & Tanriöver, Ö. Ö. (2023). Multimodal Deep Learning Crime Prediction Using Tweets. *IEEE Access*, *11*, 93204-93214.DOI: 10.1109/ACCESS.2023.3308967

[13] Agarwal, P., Sharma, M., & Chandra, S. (2019, August). Comparison of machine learning approaches in the prediction of terrorist attacks. In *2019 Twelfth International Conference on Contemporary Computing (IC3)* (pp. 1-7). IEEE.DOI: 10.1109/IC3.2019.8844904

[14] Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, *78*, 13-21.https://doi.org/10.1016/j.knosys.2015.01.009

[15] Badri, N., Kboubi, F., & Habacha Chaibi, A. (2024). Abusive and Hate speech Classification in Arabic Text Using Pre-Trained Language Models and Data Augmentation. *ACM Transactions on Asian and Low-Resource Language Information Processing*.https://doi.org/10.1145/3679049

[16] Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016, September). Surfacing collaborated networks in dark web to find illicit and criminal content. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 109-114). IEEE.DOI: 10.1109/ISI.2016.7745452

[17] Saini, S., Punhani, R., Bathla, R., & Shukla, V. K. (2019, April). Sentiment analysis on twitter data using R. In *2019 International Conference on Automation, Computational and Technology Management (ICACTM)* (pp. 68-72). IEEE.DOI: 10.1109/ICACTM.2019.8776685

[18] Silivery, A. K., Rao, K. R. M., & Kumar, S. L. (2024). Rap-Densenet Framework for Network Attack Detection and Classification. *Journal of Information & Knowledge Management*, 2450033.https://doi.org/10.1142/S0219649224500333

[19] L'huillier, G., Alvarez, H., Ríos, S. A., & Aguilera, F. (2011). Topic-based social network analysis for virtual communities of interests in the dark web. *ACM SIGKDD Explorations Newsletter*, *12*(2), 66-73.'https://doi.org/10.1145/1964897.1964917

[20] Rawat, R., & Rajavat, A. (2024). Perceptual Operating Systems for the Trade Associations of Cyber Criminals to Scrutinize Hazardous Content. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *14*(1), 1-19.DOI: 10.4018/IJCWT.343314.

[21] Godawatte, K., Raza, M., Murtaza, M., & Saeed, A. (2019, December). Dark Web along with the dark Web marketing and surveillance. In *2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)* (pp. 483-485). IEEE.DOI: 10.1109/PDCAT46702.2019.00095

[22] Cai, Y. (2024). Multi pattern matching algorithm for embedded computer network engineering intrusion detection system. *Intelligent Decision Technologies*, *18*(2), 705-716.DOI: 10.3233/IDT-230249.

[23] Abdalrdha, Z. K., Al-Bakry, A. M., & Farhan, A. K. (2023, December). Crimes Tweet Detection Based on CNN Hyperparameter Optimization Using Snake Optimizer. In *National Conference on New Trends in Information and Communications Technology Applications* (pp. 207-222). Cham: Springer Nature Switzerland.https://doi.org/10.1007/978-3-031-62814-6_15

[24] Kini, S., Patil, A. P., Pooja, M., & Balasubramanyam, A. (2022, May). SQL Injection Detection and Prevention using Aho-Corasick Pattern Matching Algorithm. In *2022 3rd International Conference for Emerging Technology (INCET)* (pp. 1-6). IEEE.DOI: 10.1109/INCET54531.2022.9825040

[25] Rawat, R., Chakrawarti, R. K., Raj, A. S. A., Mani, G., Chidambarathanu, K., & Bhardwaj, R. (2023). Association rule learning for threat analysis using traffic analysis and packet filtering approach. *International Journal of Information Technology*, *15*(6), 3245-3255.https://doi.org/10.1007/s41870-023-01353-0

[26] Felix Enigo, V. S. (2020). An Automated System for Crime Investigation Using Conventional and Machine Learning Approach. In *Innovative Data Communication Technologies and Application: ICIDCA 2019* (pp. 109-117). Springer International Publishing.https://doi.org/10.1007/978-3-030-38040-3_12

[27] Abdalrdha, Z. K., Al-Bakry, A. M., & Farhan, A. K. (2023, December). Improving the CNN Model for Arabic Crime Tweet Detection Based on an Intelligent Dictionary. In *2023 16th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 748-753). IEEE.DOI: 10.1109/DeSE60595.2023.10469560

[28] Rawat, R., Oki, O. A., Sankaran, K. S., Olasupo, O., Ebong, G. N., & Ajagbe, S. A. (2023). A new solution for cyber security in big data using machine learning approach. In *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023* (pp. 495-505). Singapore: Springer Nature

Singapore.https://doi.org/10.1007/978-981-99-0835-6_35

[29] Taiwo, G. A., Saraee, M., & Fatai, J. (2024). Crime Prediction Using Twitter Sentiments and Crime Data. *Informatica*, *48*(6). https://doi.org/10.31449/inf.v48i6.4749

[30] Liu, Y., & Pan, B. (2024). Profit Estimation Model and Financial Risk Prediction Combining Multi-scale Convolutional Feature Extractor and BGRU Model. *Informatica*, *48*(11).https://doi.org/10.31449/inf.v48i11.5941

[31] Sabir, A., Ali, H. A., & Aljabery, M. A. (2024). ChatGPT Tweets Sentiment Analysis Using Machine Learning and Data Classification. *Informatica*, *48*(7).https://doi.org/10.31449/inf.v48i7.5535