Journal of Harbin Engineering University Vol 45 No. 4
ISSN: 1006-7043 April 2024

Protecting Against Malicious Code Injection in Reviews on Web Applications

R. Shanmuga Priya[1], Dr. Yogesh Rajkumar[2]
Research Scholar -Dept of Computer Science and Engineering [1], Faculty -Dept of Information Technology [2]
Bharath Institute of Higher Education and Research[1][2]

Abstract: - Malware-code injection attack primarily evaluated by an attacker or hacker. These fake user IDs created by continuously sending user links until the attacker clicks on the link. By deliberately clicking on the included link, an attacker steals the user's identity, similar to phishing. These fraudulently inserted reviews are usually confused with the original user reviews of the product on the website. This study uses the Naive Bayes Classifier (NBC) method to detect malicious rating injection attacks. Then use natural language processing techniques to remove unwanted information from your web pages. Natural Language Processing (NLP) is a way to remove unwanted words from a document. Then, for ease of understanding, use the Principal Component Analysis (PCA) algorithm to reduce the score length for a particular sample dataset. This reduces the score dimension. The user-entered ratings are then compared to the sample dataset and categorized into good and bad ratings. It also uses the naive Bayes classifier algorithm used to classify objects and is not detected as malicious.

Index Terms **-**Malware-code injection, NBC, NLP, PCA

1. Introduction

Machine learning is defined as a training machine and a test machine. Machine learning has two phases, a training phase and a test phase. There are three types of machine learning: supervised learning, unsupervised learning, and reinforcement learning[1]-[3]. Supervised learning is defined as a sample dataset that the user provides to the machine for training. Unsupervised learning is defined as a machine for self-validation of datasets. Reinforcement learning is defined as a machine learning method based on rewarding desirable behaviors and punishing unwanted behaviors. Malicious code insertion is defined as malicious code insertion. In this case, an attacker exploits a system input validation vulnerability to inject malicious code.

There are several types of malicious code injection attacks, two of which are simultaneous access injection attacks and profile injection attacks. Simultaneous injection attacks are defined as attacks in which an attacker or hacker continues to browse a website but does not purchase the product, and the attacker posts a product review on the website. A profiling attack[4]-[6] is defined as an attack in which an attacker or hacker uses a fake user ID to provide a website with product reviews.

This proposed treatise is based on a machine learning algorithm. With this algorithm, the sample dataset is trained and tested on the machine to find the result or output. To protect people and users who trust malicious product reviews in your web application, you need to detect and remove those malicious reviews. This malware scan is a malware scan that attackers use to scan for attacks. These attackers or hackers insert malicious code to create these rankings. This check contains malicious code inserted by an attacker or hacker when the web application's site service is vulnerable.

As a result, access control vehicles can use natural language processing (NLP) [7]-[9]technology to detect and remove this malicious code. This technique can be used in web applications to remove unwanted corrupted data. You can implement the NBC (Naive Bayes Classifier) algorithm to classify objects. Here we apply this special algorithm to classify specific user reviews into good and bad reviews. This algorithm belongs to supervised machine learning algorithms. This applied algorithm is very accurate and can be used to facilitate real-time predictions. The Principal Component Analysis (PCA)[10]-[12]algorithm is used to understand the scores contained in the sample data. This PCA algorithm, a machine learning algorithm, is widely used as a

dimensionality reduction method. Here we implement this algorithm to reduce the sample.

2. Existing System

Legacy systems can use a "divide-and-conquer" strategy to detect two types of injection attacks: Direct Suggested Profile Injection (PIA) and Co-Access Fighter Attacks. CIA) [13]. First, it uses List Then Remove (LTE) technology to remove corrupted data by enhancing two injection attacks known as PIA and CIA. Then the size is reduced. That is, use steepest algorithms to reduce the length of data for better understanding. The IMIA HCRF method is defined to use a conditional high-order random field to identify malicious injection attacks. Finally, classification was performed and the results were reported as positive and negative according to the IMIA-HCRF method. The accuracy scale for IMIA HCRF technology ranges from 0.6 to 0.7.

3. Proposed System

The main reason for this project is that when people or users buy a product from a website, they mainly refer to the reviews to learn more about the product. In this case, when you look at the reviews, you're mistakenly confused with the original user rating and confused with the original user rating to determine the product. product. These malware checks look for malicious code injected by an attacker through a malware injection attack when the website service is low. Malicious code insertion occurs when an attacker exploits a system input validation vulnerability to inject malicious code. There are several types of malicious injection attacks, two of which are: Simultaneous injection attack. Identified if an attacker or hacker continues to browse the website, does not purchase the product, and the attacker posts a review. Product price on the website. Profiler attacks are defined when an attacker or hacker uses a fake user ID to provide a product review on a website. So this project was started to solve this problem. The main goal of this project is to prevent users and followers from receiving such malicious reviews. The most accurate naive Bayes classifier (NBC) algorithm is used to determine whether the score is good or bad and even detect it as malicious.

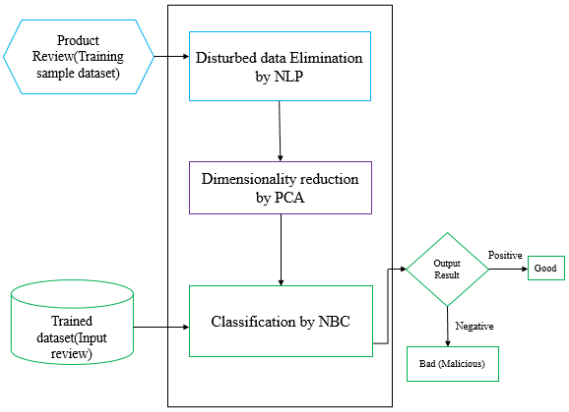


Figure 1: Proposed System Architecture

The figure 1 illustrates the proposed system architecture. In the proposed system, emotionally or unintentionally noisy data was first removed from a particular dataset using natural language processing (NLP) technology. Then the limit is set according to the specified pattern. This reduces the size of the specified dataset and uses Principal Component Analysis (PCA) to extract important data. Finally, for the data sample, we used a naive Bayes classifier (NBC) to classify the inputs into erroneous and initial evaluations. Initial ratings can be positive (good) and even negative (bad). Divided intosections This is displayed as a percentage of the accuracy of the algorithm. Site Noise Cancellation (ENDW) technology removes noise data more effectively. Natural language processing (NLP) technology has a high emotion recognition rate. Principal component analysis (PCA) algorithms run faster because they improve the visibility of the data and speed it up. The NBC algorithm is defined as the algorithm used to classify objects and is called the NBC algorithm. The Naive Bayes Classifier (NBC) [14] algorithm is a very accurate scoring algorithm.

3.1 Pre-processing

In pre-machining, the machine is driven first. It falls into the training phase of machine learning. This machine training is done by collecting datasets from web applications like Amazon and Extras. And the dataset to train this machine comes from a data source called Kaggle. Improvements in the 's injection and behavior profiles continued during concurrent visit. Eliminate noisy data by improving profile injection and simulation injection. Classified

malicious code [15] inserted by an attacker or hacker when a web application's web service is vulnerable. Malware insertion is defined as malicious code injection, where an attacker exploits system input validation vulnerability to inject malicious code. There are several types of malicious injection attacks, two of which are concurrent injection attacks and profile injection attacks. There is a fake user ID created by the attacker by sending the permalink to multiple users until the user clicks on the link. When a user clicks on a link, the attacker steals the identity of that particular user. It's like a scam. These malicious reviews are often mixed with the original user product reviews on the site. Corrupted data is deleted using Natural Language Processing (NLP) technology. Natural language processing has many uses. B. In the tourism industry, tourists can get information about famous places in a particular city, available hotels, best restaurants nearby, etc. Another important application of NLP is chatbots (chat robots). Voice and text exchange. The goal is a computer that can "understand" the content of the document, including nuances of the context of the language contained in the document. This technology can accurately extract the information and ideas contained in a document, and categorize and organize the document itself. NLP bridges the gap between computers and humans by combining database queries into meaningful formats. Natural Language Processing (NLP) technology is defined as technology used to remove corrupted data from web pages. In other words, this erasure process uses NLP technique as follows: First, analyze the meaning of the entry points given by the dataset to gain a better understanding of the machine. Then the password for the record is set. Corrupt data such as symbols, gibberish, and extras are separated by the specified input record. Finally, a data item was removed from the specified input dataset demonstrated in figure 2 and 3.

```
In [101]: raw_reviews.head()
Out[101]:
```

	reviewerID	asin	reviewerName	helpful	reviewText	overall	summary	unixReviewTime	reviewTime
0	A2IBPI20UZIR0U	1384719342	cassandra tu "Yeah, well, that's just like, u...	[0, 0]	Not much to write about here, but it does exac...	5	good	1393545600	02 28, 2014
1	A14VAT5EAX3D9S	1384719342	Jake	[13, 14]	The product does exactly as it should and is q...	5	Jake	1363392000	03 16, 2013
2	A195EZSQDW3E21	1384719342	Rick Bennette "Rick Bennette"	[1, 1]	The primary job of this device is to block the...	5	It Does The Job Well	1377648000	08 28, 2013
3	A2C00NNG1ZQQG2	1384719342	RustyBill "Sunday Rocker"	[0, 0]	Nice windscreen protects my MXL mic and preven...	5	GOOD WINDSCREEN FOR THE MONEY	1392336000	02 14, 2014
4	A94QU4C90B1AX	1384719342	SEAN MASLANKA	[0, 0]	This pop filter is great. It looks and perform...	5	No more pops when I record my vocals.	1392940800	02 21, 2014

Figure 2. Sample dataset

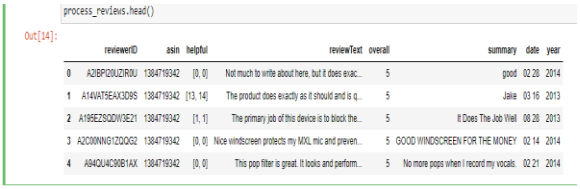
```
In [12]: print(stop_words)

['%', '*', 'urselv', 'itwaen', 'weit', 'siaf', 'ts', 'ase', 'qf', 'isalf', 'ere', 'ur', 'eih', 'e', 'nnodu', 'ihct', 'kfe', 'jl
e', 'hn', 'rsk', 'kal', 'aadu', 'varta', 'y', 'isn', 'fsjuy', 'fep', 'oau', 'nv', 'lnd', 'ila', 'uvs', 'gb', 'rw', 'jxa', 'kj
u', 'iva', 'sda', 'katu', 'mla', 'ip', 'kq', 'bw', 'cx', 'gl', 'oyz', 'lq', 'oz', 'shjf', 'jcb', 'pta', 'hl', 'aur', 'uhb', 'kh
fsgvt', 'rhyx', 'ilak', 'vslu', 'ksnu', 'ku', 'qm', 'unavu', 'pwq', 'xc', 'udu', 'ln', 'obq', 'dc', 'en', 'klp', 'lta', 'azz',
'pz', 'nz', '^', 'j$', 'jjk', 'hj', 'kaal', 'isn', 'udu', 'fk', 'fl', 'qd', 'lal', 'inu', 'jna', 'ktl', 'cela', 've', 'd', 'r
a', 'fthw', 'u', 'you', 'lou', 'oan', 'ece', 'aer', 'of', 'avd', 'amv', 'ore', 'ngl', 'yenga', 'ivunga', 'nee', 'vaa', 'c', 'ye
na', 'ipl', 'ayl', '@', '#']
```

Figure 3. Eliminating disturbed data

3.2 Feature Extraction

The feature extraction phase sets the initial number of constraints based on the sample training dataset specified in the preprocessing stage. Therefore, after removing noisy data in the preprocessing step, the rest of the data set is provided as input for this feature extraction step. Then the size of the specified dataset is reduced. H. The length of each review submitted is kept to a minimum for ease of understanding. Therefore, only significant data is extracted using Principal Components Analysis (PCA) algorithm. Principal component analysis (PCA) is commonly used as a dimensionality reduction technique. Principal Components Analysis (PCA) [16]-[18]calculatesthe principal components and uses them to make fundamental changes to the data. In some cases, only the first main component is used, in other cases it is omitted. PCA is used for exploratory data analysis and building predictive models. PCA is defined as an orthogonal linear transformation that turns data into a new coordinate system. The largest variance due to the scalar projection of the data is the first coordinate (called the first principal component). And the second largest variance is the second coordinate. In a word, the steps involved in dimensionality reduction using the Principal Components Analysis (PCA) algorithm are as follows: First, the data set is the output of the collected module preprocessing.The record headers are listed first for machine references. Only the unwanted data headers are then individually recognized. Finally, remove those unwanted data headers to reduce record length and make it easier for machines to understand. Principal component analysis (PCA) algorithms improve data visibility. The PCA algorithm also has a high performance rate. Therefore, the PCA algorithm runs fast. Principal component analysis improves the performance of machine learning algorithms. Principal component analysis provides larger variance and better

visualization. PCA algorithm is one of the machine learning algorithms.



process_reviews.head()

Out[14]:

	reviewerID	asin	helpful	reviewText	overall	summary	date	year
0	A2IBPI20UZIR0U	1384719342	[0, 0]	Not much to write about here, but it does exac...	5	good	02 28	2014
1	A14VAT5EAX3D9S	1384719342	[13, 14]	The product does exactly as it should and is q...	5	Jake	03 16	2013
2	A195EZSQDW3E21	1384719342	[1, 1]	The primary job of this device is to block the...	5	It Does The Job Well	08 28	2013
3	A2C00NNG1ZQQG2	1384719342	[0, 0]	Nice windscreen protects my MXL mic and preven...	5	GOOD WINDSCREEN FOR THE MONEY	02 14	2014
4	A84QU4C90B1AX	1384719342	[0, 0]	This pop filter is great. It looks and perform...	5	No more pops when I record my vocals.	02 21	2014

Figure 4. Before downsizing

process_reviews.head()

Out[17]:

	reviewerID	asin	helpful	overall	date	year	reviews
0	A2IBPI20UZIR0U	1384719342	[0, 0]	5	02 28	2014	Not much to write about here, but it does exac...
1	A14VAT5EAX3D9S	1384719342	[13, 14]	5	03 16	2013	The product does exactly as it should and is q...
2	A195EZSQDW3E21	1384719342	[1, 1]	5	08 28	2013	The primary job of this device is to block the...
3	A2C00NNG1ZQQG2	1384719342	[0, 0]	5	02 14	2014	Nice windscreen protects my MXL mic and preven...
4	A84QU4C90B1AX	1384719342	[0, 0]	5	02 21	2014	This pop filter is great. It looks and perform...

Figure 5: After downsizing

3.3 Classification

In the classification phase, the rating is given as an input for classifying the output. This particular input validation is compared to the template dataset, which is the output of the feature extraction module. When the comparison is complete, the input score will be either positive (good) or negative (bad) and will be detected as malicious or unused using the Naive Bayes Classifier (NBC) algorithm. The naive Bayes classification algorithm is defined as the algorithm used to classify objects, called the NBC algorithm. The naive Bayes classifier is very scalable and requires a set of linear parameters for the number of variables (features / predictors) in the learning problem. Naive Bayes is an easy way to create a classifier and model that assigns a class label to an instance of Problem ,[19]-[21]where the class label is drawn from a finite set and represented as a vector of feature values. There is no single algorithm for training such a classifier. Rather, it is a family of algorithms based on common principles. All naive Bayes classifiers assume that the value of one feature is independent of the value of another feature if the class variable is. For example, if the fruit is red, round, and about 10 cm in diameter, it can be considered an apple. The NBC algorithm is one of the supervised machine learning algorithms. Independent feature model, naive Bayes probability model. The naive Bayes classifier combines this model with a decision rule. The general rule is to choose the most probable hypothesis. This is known as the post-maximum or MAP decision rule. {\ displaystyle {\ hat {y)) = {\ underset {k \ in \ {1, \ ldots, K \)) {\ operatorname {argmax))) \ p (C_ {k}) \ displaystyle \ prod _ {i = 1} ^ {n} p (x_ {i} \ center C_ {k}). Simply put, the step-by-step procedure for the naive Bayes classifier (NBC) algorithm is as follows: When the post-sampled dataset is fed to the engine, the train classification engine forms a unique word from one specified dataset. The engine then also forms the frequency of each word in the document from the unique words formed. Then, search the keyword dictionary to remove unwanted words. Then, for negative labels, calculate the probability of being negative. Calculate the positive probability of a positive label. For malicious labels, calculate the possibility of malicious intent. For positive, negative and malicious class probability calculations: take the positive first. Then use the following formula to calculate the probability of each unique word in the positive label.

$$P(wk/+) = \frac{(nk+1)}{n} + |\text{Vocabulary}|\text{----------}$$

(1)

Where nk: the frequency with which the word k appears if positive.

n: Number of positive words.

Vocabulary: An overall unique word.

Repeat step 4.1.2 for negative and harmful labels. When searching for unfamiliar words, use nk = 0 to determine the probabilities of all positive, negative, and harmful tags. The test classifier inputs the entered test data to the machine. Then repeat step 3 for the test data you entered. Compares the results of all the test data entered with the generated dataset labels and separates the results into positive, negative, and harmful labels. The probability of each 3 label rating is calculated. Then sum all the validation probabilities for each label to get the sum for each class. Once added, it will be evaluated and the total score for each class will be displayed. This is the final version. The Naive Bayes Classifier (NBC) algorithm is compared to several other algorithms to calculate the accuracy score of the algorithm. The naive Bayes classifier used in recommender systems has a higher algorithm accuracy value of up to 0.9. Bayesian classifiers are simple and easy to implement and process both continuous and discrete data. NBC is very accurate and can be used for real-time predictions.

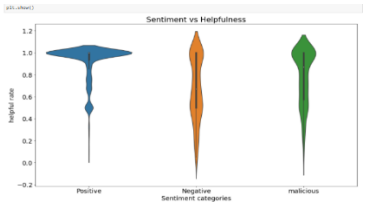


Figure 6: Output of malicious positive and negative ratings from trained datasets

3.4 Model Accuracy Comparison

This model accuracy comparison module compares the final module algorithm with several other algorithms. This algorithm model comparison is performed to prove that the used algorithm has the highest accuracy in the proposed system. The accuracy value of existing system algorithms is only 0.6-0.7. Therefore, the exact value of the proposed system's algorithm changes from 0.8 to 0.9[22]. The highest accuracy of this proposed system algorithm is displayed as a value. The recommended algorithm with this highest accuracy is the Naive Bayes Classifier (NBC) algorithm. Naive Bayes classification algorithm is defined as the algorithm used to classify objects, called NBC algorithm. As proof, of the displayed algorithm model accuracy values, the proposed system algorithm has the highest accuracy value up to 0.9. The highest precision obtained is greater than 0.95 and more precise is 0.96[23].

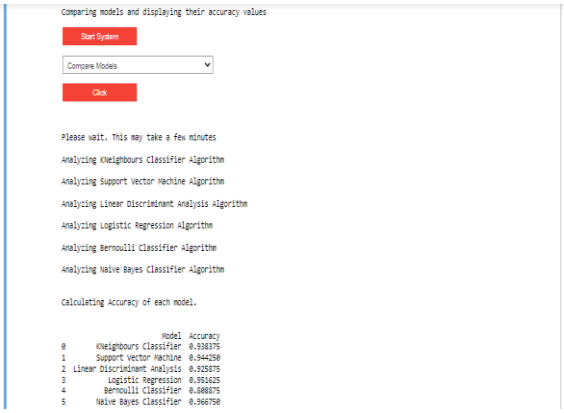


Figure 7: Output of malicious positive and negative ratings

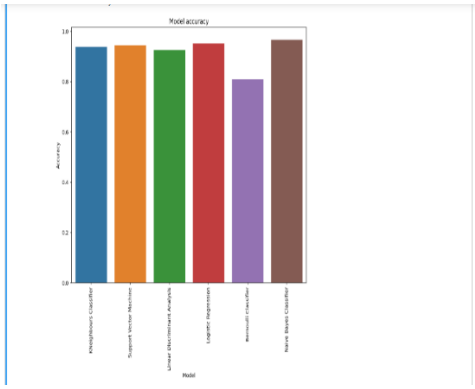


Figure 6. Compare algorithms

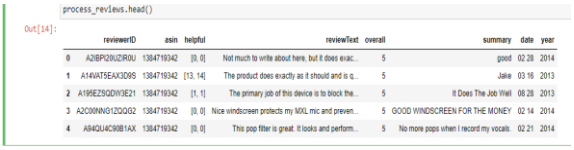
Algorithm: 1 Pseudocode of proposed ML-NBC

Input: Publicly available review datasets

Output: Malicious reviews total count with positive reviews total count and negative reviews total count from given dataset

Begin

1. **Set** $C_d(x)$ = (r'C:\Users\baska\sentiment\Musical_instruments_reviews.csv') /* Review dataset for training phase*/
2. **or** x = 1 to l do /* length of the review */
3. **unction**pd.read_csv($C_d(x)$)
4. **Import** sklearn
5. **Import** pandas
6. **Import** numpy
7. **Import** nltk /*for disturbed data elimination*/
8. **Import** PCA /*for dimensionality reduction*/
9. **Read**$C_d(x)$
10. **Apply** natural language processing /* disturbed data elimination */
11. **Print** processed reviews



4.Result And Discussion

First and foremost, the machine was successfully trained. It then uses the naive Bayes classification algorithm to detect reviews with malicious code inserted. Then the check using the NLP technique removes the corrupted data. First and foremost, the affected malicious reviews are successfully detected using the NBC algorithm. Therefore, the main goal of preventing people and users from unknowingly trusting reviews with malicious code inserted has been successfully achieved. This NBC algorithm is used in the classification process to detect whether a review is good, bad, or malicious, and the detection rate is high when the algorithm accuracy is up to 0.9.

Table 1. sample dataset

Table 2. Eliminating disturbed data's

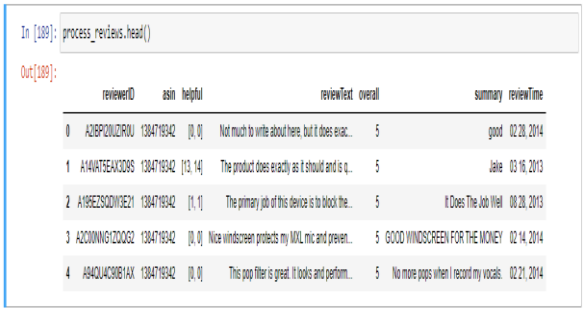


Table 3. Before Dimensionality-reduction process

Table 4. After Dimensionality-reduction process

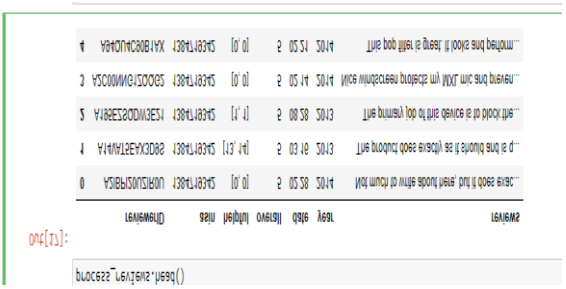


Table 5. Returns the total number of malicious reviews, including a total of positive and negative reviews from the specified dataset

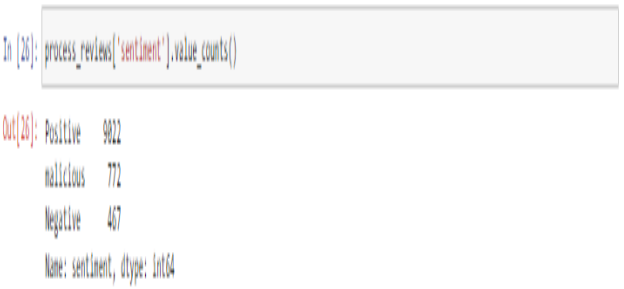


Table 6. Output of reviews total count displayed in values

5.Conclusion

This assessment provides the ability to detect malicious injection attacks in scoring using a highly accurate scoring algorithm. This proposed treaty also acknowledges the nature of the review from the first review given, whether it is positive (good) or negative (bad) and whether it is malicious. get a raise. Manufacturing. It also detects if it exists. This white paper uses a sample dataset to train your machine. Thus, the tool compares the inputs with the formed data set and provides the outputs. The algorithm used in this document to classify the output as good, bad or malicious is the system for which the algorithm used was proposed and the

accuracy score is when comparing it with many algorithms. It will be calculated. It is made of many things. Indicates that you have the highest accuracy rating.

REFERENCES

1. Naufal Riza Fatahillah, PulutSuryati, Cosmas Haryaan,"Implementation Of Naive Bayes Classifier Algorithm On Social Media (Twitter) To The Teaching Of Indonesian Hate Speech",2017
2. Revathy M, Minu Lalitha Madhavu, "Efficient Author Community Generation OnNlp Based Relevance Feature Detection", 2017
3. Yunjing An, Shutao Sun, Shujuan Wang, "Naive Bayes Classifiers for Music Emotion Classification Based on Lyrics",2017
4. Ershad Sharifahmadian, Alireza Ahmadian, "Adaptive Signal Processing Algorithm for Remote Detection of Heart Rate (HR) Using Ultra-Wideband Waveforms based on Principal Component Analysis", 2009
5. Moch. Fadli ShadiqinThirafi, Faisal Rahutomo, "Implementation of Naïve Bayes Classifier Algorithm to Categorize Indonesian Song Lyrics Based on Age", 2018
6. Rushrukh Rayan, Md. Sabir Hossain, and Asaduzzaman, "Compression of Large-Scale Image Dataset using Principal Component Analysis and K-means Clustering", 2019
7. Uma M, Sneha V, Sneha G, Bhuvana J, Bharathi B, "Formation of SQL from Natural Language Query using NLP", 2019
8. Sidharth Prasad Mishra, Uttam Sarkar, Subhash Taraphder, Sanjay Datta, Devi Prasanna Swain, Reshma Saikhom, Sasmita Panda and Menalsh Laishram, "Multivariate Statistical Data Analysis- Principal Component Analysis (PCA)", 2018
9. Dr. N. Srinivasan, Anandaraj Selvaraj, "Mobile Based Data Retrieval using RDF and NLP in an Efficient Approach", 2017
10. Anggit Dwi Hartanto, Ema Utami, Sumarni Adi, Harish Setyo Hudnanto, "Job Seeker Profile Classification of Twitter Data Using the Naïve Bayes Classifier Algorithm Based on the DISC Method",2019
11. Julia Moser, Katrin Sippel, Franziska Schleger and Hubert Prei, "Automated Detection of Fetal Brain Signals with Principal Component Analysis", 2019
12. Jian Li, Xiangjing An and Hangen He, "Line Segments Detection with Scale Analysis: A Principal Component Analysis Based Approach", 2009
13. Chetan Arora, Mehrdad Sabetzadeh, Lionel Briand and Frank Zimmer, "Automated Checking of Conformance to Requirements Templates using Natural Language Processing", 2015
14. Pengyu Chen, Qiao Liu, Lan Wei, Beier Zhao, Yin Jia, HairongAndXiaolu Fei, "Automatically Structuring on Chinese Ultrasound Report of Cerebrovascular Diseases via Natural Language Processing", 2019
15. Yuxin Shi, Xinjin Lu, Yingtao Niu and Yusheng Li, "Efficient Jamming Identification in Wireless Communication: Using Small Sample Data Driven Naive Bayes Classifier", 2021
16. Niruban, R., Deepa, R., Vignesh, G.D., A novel iterative demosaicing algorithm using fuzzy based dual tree wavelet transform, Journal of Critical Reviews, 2020, 7(9), pp. 141–145
17. Niruban, R., Sree Renga Raja, T., Deepa, R., Similarity and Variance of Color Difference Based Demosaicing, International Journal of Applied Engineering Research, 2014, 9(23), pp. 21657–21668.
18. Chakrabarti, S., Suresh Babu, G.N.K., The Security Enhancement of Symmetric Key Crypto Mechanism based on Double Stage Secret Model Information Security Journal , 2021, Vol.30, Issue 6, pp. 325–341
19. Shirley, D.R.A., Sundari, V.K., Sheeba, T.B., Rani, S.S. (2021). Analysis of IoT-Enabled Intelligent Detection and Prevention System for Drunken and Juvenile Drive Classification. In: Kathiresh, M., Neelaveni, R. (eds) Automotive Embedded Systems. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-59897-6_10
20. V. S. Harshini and K. K. S. Kumar, "Design of Hybrid Sorting Unit," 2019 International Conference on Smart Structures and Systems (ICSSS), 2019, pp. 1-6, doi: 10.1109/ICSSS.2019.8882866.

21. Balaji, V., Umapathy, N., Duraisamy, V., Umapathy, K., Venkatesan, P., &Saravanakumar, S. (2015). ENHANCING VARYING OVERHEAD AD HOC ON DEMAND DISTANCE VECTOR WITH ARTIFICIAL ANTS. JurnalTeknologi, 77(28). https://doi.org/10.11113/jt.v77.6784
22. Dhaya R., Ujwal U. J., Tripti Sharma, Mr. Prabhdeep Singh, Kanthavel R., Senthamil Selvan, Daniel Krah, "Energy-Efficient Resource Allocation and Migration in Private Cloud Data Centre", Wireless Communications and Mobile Computing, vol. 2022, Article ID 3174716, 13 pages, 2022. https://doi.org/10.1155/2022/3174716
23. Niruban Rathakrishnan, and Deepa Raja, Optimized convolutional neural network-based comprehensive early diagnosis method for multiple eye disease recognition, Journal of Electronic Imaging, Vol. 31(4), 2022, DOI: 10.1117/1.JEI.31.4.043016.