IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ჯ Impact Factor 8.066 ჯ Peer-reviewed / Refereed journal ჯ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.107107

# Machine Learning-Based Networks Surveillance System with cross-evolution

**Pooja C Viraktamath[1], Dr. T. Vijaya Kumar[2]**

Student, Department of MCA, Bangalore Institute of Technology, Bengaluru[1]

Professor & Head Department of MCA, Bangalore Institute of Technology, Bengaluru[2]

**Abstract:** The proposed IDS model isaimed at detecting network intrusions by classifying all the packet traffic in the network as benign or malicious classes. The Canadian Institute for Cyber security Intrusion Detection System (CICIDS2017)dataset has been used to train and validate the proposed model. The model has been evaluated in terms of the overall accuracy, attack detection rate, false alarm rate, and training overheadDDOS attacks based on Canadian Institute for Cyber security Intrusion Detection System (KDD Cup 99)dataset has been used to train and validate. We are used for comparison for 2 dataset (CICIDS2017 and KDD Cup 99 ) Then, wehave to implement the Deep learning algorithms is Proposed Method Classification Using LSTM algorithm Model predict .Testing dataset for anomaly detection model finally classified attack or normal. Finally, the experimental resultsshows that the performance metrics such asaccuracy, precision, recall and confusion matrix.

## I. INTRODUCTION

The DDoS attacks on the cloud computing environment are mainly application layer which sends out requests following the communication protocol which are then hard to distinguish in the network layer because their pattern matches the legitimate requests thus making the traditional defence systems not applicable. DDoS flooding attacks on cloud can be of various categories like session and request flooding attacks, slow response and asymmetric attack. All these flooding attacks generate traffic which resembles that of a legitimateuser which becomes tougher for the target to distinguish between attack and legitimatetraffic thus blocking the services for the legitimate user.

### Problem statement:

A more common approach for detectingmain problem in detecting slow DDoS attacks is the inability to prevent them, since the determination process is based onthe study of existing traffic without thepossibility of predicting it depending onusers' activity

### Scope of the project:

DoS or Denial-of-Service attack is an attacktargeting the availability of web applications. Unlike other kinds of attacks, the primary goal of a DoS attack is not to steal information but to slow or take down a web site .Prevention can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. A Denial-of-Service (DoS) attack is an attack meant to shut down a Deep or network, making it inaccessible toits intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

### Objectives:

The main objective of our project is,

□ To detect the DDOS attackeffectively.
□ To implement the Deep learningusing LSTM.
□ To enhance the overall performance analysis.

.

## II. LITERATURE SURVEY

**Abdul Raoof** [1] The study is implementedon the Structure for cloud security withefficient security in communication systemand AES based file encryption system. Thissecurity architecture can be easily applied on PaaS, IaaS and SaaS and one time password provides extra security in the authenticating users.

Advantages:

- Performance time and accuracyDisadvantages:
- Training model prediction on Timeis High
- It is based on Low Accuracy.

Nitin Pandey[2] The cloud computing environment is adopted by a large number of organizations so the rapid transition toward the clouds has fuelled concerns about security perspective. There are numbers of risks and challenges that have emerged due to use of cloud computing. The aim of this paper is to identify security issues in cloud computing which will be helpful to both cloud service providers and users to resolve those issues. As a result this paper will access cloud security by recognizing security requirements and attempt to present the feasible solution that can reduce these potential threats.

Advantages:

More effective and efficient.

Disadvantages:

Not give accurate prediction result.

**Faisal Hussain[3] In this work, we proposed a** Traffic monitoring is a challenging task which requires efficientways to detect every deviation from thenormal behavior on computer networks. Inthis paper, we present two models to detectnetwork anomaly using flow data such as bits and packets per second based on: Firefly Algorithm and Genetic Algorithm. Both results were evaluated to measure their ability to detect network anomalies, and results were then compared. We experienced good results using datacollected at the backbone of a university.
Advantages:

Efficiency measure and theaccuracy

Disadvantages:

Not give accurate prediction

result.

**Suresh** M[4] The proposed solutions are this ensures fine-grained detection of various attacks. The proposed framework has been compared with the existing deep learning models using three real datasets (anew dataset NBC, a combination of UNSW-NB15 and CICIDS2017 consistingof 101 classes).

**Advantages**:
It performs accurate classification ofhealth state in comparison with other methods

**Disadvantages:**

It is low in efficiency.

**Linga[5] In this study, we** DDoS (Distributed Denial of Service) attack has affected many IoT networks in recent past that has resulted in huge losses. We have proposed deep learning models andevaluated those using latest CICIDS2017 datasets for DDoS attack detection which has provided highest accuracy as 97.16% also proposed models are compared with machine learning algorithms.

DOI: 10.17148/IARJSET.2023.107107

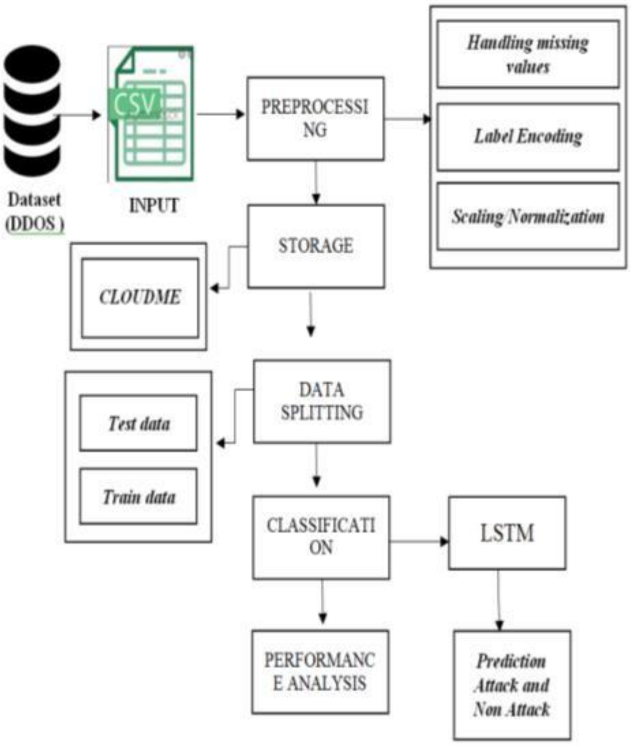

**Fig. 1. Proposed Architecture**

## III. EXISTING MODEL

- In existing system, DDoS attacks and then, selected features are passed to the classifiers, i.e. support vector machine, decision tree, naïveBayes, and multilayer perceptron toidentify type of attack.
- The publicly available dataset as KDD Cup 99 are used for our experimental study. From the results of the simulation, it is clear that GOIDS with decision treeacquires high detection and accuracy with a low false–positive rate.
- For instance, the use of denoising asfeature extractors may improve the performance in the presence of high levels of noise

## DISADVANTAGES

- Doesn’t Efficient for handlinglarge volume of data.
- Theoretical Limits
- Incorrect Classification Results.
- Less Prediction Accuracy.

## IV. PROPOSED METHODOLOGY

The proposed IDS model is aimed at detecting network intrusions by classifying all the packet traffic in the network as benign or maliciousclasses.

- DDOS attacks based on Cyber security Intrusion Detection System (KDD Cup 99) dataset hasbeen used to train and validate.
- Classification Using CNN, SVM ,NB algorithm Model predict
- Testing dataset for anomaly detection model finally classifiedattack or normal.
- It is more effective of performanceanalysis.

DOI: 10.17148/IARJSET.2023.107107

### ADVANTAGES

- High performance.
- Provide accurate prediction results.
- It avoid sparsity problems.
- Reduces the information Loss and the bias of the inference due to the multiple estimates.

## V. IMPLIMENTATION

### DATA SELECTION AND LOADING

- Data selection is the process of determining the appropriate data type and source, as well as suitable instruments to collect data.

Data selection precedes the actual practice of data collection and it is the process where data relevant to the analysis is decided and retrieved from the data collection.

□ In this project, the Malware dataset is used for detecting Malware type prediction.

### DATA PREPROCESSING

□ The data can have many irrelevant and missing parts. To handle this part, data cleaning is done. It involves handling of missing data, noisy dataetc.

□ **Missing Data:**

This situation arises when some data is missingin the data. It can be handled in various ways.

✓ Ignore the tuples:This approach is suitable only when the datasetwe have is quite large and multiple values are missing within a tuple.

### SPLITTING DATASET INTO TRAIN ANDTEST DATA

□ Data splitting is the act of partitioning availabledata into two portions, usually for cross- validator purposes.

□ One Portion of the data is used to develop a predictive model and the other to evaluate the model's performance.

□ Separating data into training and testing sets is an important part of evaluating data miningmodels.

**CLASSIFICATION :** Classification is the problem of identifying to which of a set ofcategories, a new observation belongs to, on thebasis of a training set of data containing observations and whose categories membershipis known.

**Random forests** or random decisionforests are an ensemble learning method for classification, regression and other tasksthat operate by constructing a multitudeof decision trees at training time andoutputting the class that is the mode of the classes (classification) or mean/average prediction (regression) of the individual trees.

## VI. CONCLUSIONS

- Intrusion Detection System (IDS) for cybersecurity basedon a Convolutional Neural Network (CNN)classifier is proposed.
- The convolution and poolingprocess of CNN allow the proposed IDS model to learncomplicated patterns of features form network traffic,while maintaining reasonablestorage and computation overhead.
- class classification performance of the proposedLSTM based IDS

## REFERENCES

[1] Pathan A- SK, Azad S, Khan R, et al. Security mechanisms and data access protocols in innovative wireless networks. London: Sage; 2018.

[2] Yong-xiong Z, Liang-ming W, Lu-xia Y. A network attack discovery algorithm based on unbalanced sampling vehicleevolution strategy for intrusion detection. Int J Comput Appl. 2017:1–9.

[3] Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEECommun Surv Tutorials. 2013;15(4):2046–2069.

DOI: 10.17148/IARJSET.2023.107107

[4] Toledo AL, Wang X. Robustdetection of MAC layer denial-of- service attacks in CSMA/CA wireless networks. IEEE Trans Inf Forensics Secure. 2008;3(3):347– 358.

[5] Guo Y, Ten CW, Hu S, et al. Modeling distributed denial of service attack in advanced meteringinfrastructure. 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT); 2015. p. 1–

[6]A. A. Khan, M. H. Rehmani, and M.Reisslein, ‘‘Cognitive radio for smart grids: Survey of architectures,spectrum sensing mechanisms, and networking protocols,’’ IEEE Commun. Surveys Tuts., vol. 18,no. 1, pp. 860–898, 1st Quart., 2016.

[7]Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, ‘‘The individual identification method of wireless device based on dimensionality reduction,’’ J. Supercomput., vol.75, no. 6, pp. 3010–3027, Jun. 2019.

[8]T. Liu, Y. Guan, and Y. Lin, ‘‘Research on modulation recognition with ensemblelearning,’’ EURASIP J. Wireless Commun. Netw., vol. 2017, no. 1, p.179, 2017.

[9]Y. Tu, Y. Lin, J. Wang, and J.-U. Kim, ‘‘Semi-supervised learning with generative adversarial networks on digital signal modulation classification,’’Comput. Mater. Continua, vol. 55, no. 2, pp. 243–254, 2018.

[10]C. Shi, Z. Dou, Y. Lin, and W. Li, ‘‘Dynamic threshold-setting forRFpowered cognitive radio networks in non-Gaussian noise,’’

[11] EURASIP J. Wireless Commun.Netw., vol. 2017, no. 1, p. 192, Nov.2017.

[12] Z. Zhang, X. Guo, and Y. Lin, ‘‘Trust management method of D2D communication based on RF fingerprint identification,’’ IEEEAccess, vol. 6, pp. 66082–66087, 2018.

[13]H. Wang, J. Li, L. Guo, Z. Dou, Y.Lin, and R. Zhou, ‘‘cFractalcomplexitybased feature extraction algorithm of communication signals,’’ Fractals, vol. 25, no. 4, pp.1740008-1–1740008-3, Jun. 2017.