Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

DYNAMIC TIME ATTACKS DETECTION USING CYBER RISK ASSESSMENT MODEL FOR CRITICAL INFORMATION INFRASTRUCTURE

Avyaktha E, PG Scholar, Dept. of Computer Science, Malla Reddy University, Hyderabad,
avyaktha17@gmail.com
Dr. G Anand Kumar, Professor & HoD, Department of CSE (Cyber Security),
Malla Reddy University, Hyderabad,
dranandkumar@mallareddyuniversity.ac.in

Abstract
In this research an advanced cyber-attack model has been implemented for dynamic DDoS and MITM attacks. Now a days cyber risks were increased on many platforms like clouds, servers, bigdata and networks. Due to attacks on these platforms' applications can affected as wells as sensitive data have been stolen. Many conventional models were available for cyber security but those were failed at dynamic attacks and highly complex risks. Moreover, existing cyber security models were facing high Time of Conversion (ToC) issues as well target of attack issues. In this research work an advanced cyber risk assessment model has been implemented using machine learning techniques. The proposed Lite RFO model was implemented on python software tool with best packages. This model has been tracking the cyber-attacks on any network and finds the target attack in less ToC. The performance measures like detection rate 98.43%, accuracy 98.23%, sensitivity 96.89% and Recall 94.56% had been attained which was better improvement.

Keywords: Ccyber-security, critical information of cyber-attacks, cyber risk.

I. Introduction
Digitization plays an important role in the technology and growth. Security threat also rapidly increased proportionally with technology. The interfacing algorithms are very needful for proving apt able security. The data need to be secured in any system like analog and digital. Any components like physical or human need to be implemented securely. Every organization need to adapt enriched design for cyber security practices. The model is developed which is critical information infrastructure (CII) which has a concept of gradient boosting algorithm which is more popular in the prevention of security attacks. Lite GBM is most commonly used advanced algorithm for various approaches.

Fig 1. Cyber security platform

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Machine learning technique with advanced algorithm is used for measuring the security rate. The internet it's a tool used by every individual in all the fields [1]. Figure 1 shoes the cyber security platforms. The security attacks many be passive or active which considers hacking, misleading etc. denial service attack is the most common attack [2]. There is one more dangerous attack which is distributed denial service attack. Its very important to identify the DDoS attack. In Georgian website this attack was occurred and it shutdown many servers. In July 2008 [3]. Entropy is used on IP address and port number which is at destination which easily detects the attacks like DDoS. Based on the threshold value the statistical calculations are done and attack is determined [4]. The detection is based on the traffic. The network traffic determined the detection. If high traffic is there then only few types of attacks of DDos is identified [5].

II. Literature Survey

In this section a brief survey of cyber security models has been discussed for better attack analysis. Always based on threshold values the rate of false negative and false positive are reduced [6-10].

Table 1. Literature Survey of Existing Models

Author	Technique	Security rate	Limitation
Gatchin, Y 2019	Vulnerabilities of Information Processing	65%	Parallel attacks caching
Wagner, T. D. (2019).	Cyber threat intelligence	79%	High ToC
Legg, P	Tools and Techniques for Improving Cyber Situational Awareness	80%	Parallel attacks caching
Ivanchenko 2020	Physical and Cyber Assets	75%	High ToC
Crowe, J	Cybersecurity Statistics	85%	Attack detection rate limitation

The above all literature survey explains about limitations of existing cyber security models [11-16]. The existing limitations and problems have been overcome through proposed Lite Random Forest Optimization machine learning model [18-22].The main objective is to design a Cyber Risk Assessment Model for Critical Information Infrastructure using Lite RFO regression algorithm and to detect the cyber-attacks in dynamic environment in less ToC with high detection rate and also to compare designed application performance with existed techniques.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

The major Problem would be Cybersecurity models have been facing less ToC detection issues and attack detection rate issues. Cyber threats are sophisticated and falls the reputations against corporate as well as IT growth [23-27]. A variety of cyber security solutions are available but those identify the attack in static manner. Due to VPNs, firewalls counter the attack if attacks enter into network, its functionality is going to be stopped so application may get damage [27-30]. These problems have been over come through proposed cyber security technique [31-33]. The proposed technique is the combination of various advanced algorithms. The major problem is implementing the algorithms through the network [34-38].

III. Methodology

In this work used deep learning approach over machine learning (ML). the deep learning is the advanced version of machine learning which uses various hash func-tions and volumes. The machine learning is majorly used for fixed and minimum amount of data but the deep learning is used for big data. Deep learning deals with feature extraction and feature selection. At last, the classification is done on the se-lected features. The figure 2 shows that first the cloud network is initiated and it is hosted by local network. Then the monitoring of cyber attacks is done by DDoS and MITM and the dataset is trained. Deep learning is used for training the data. Once training is done then the testing is done. The cyber attacks are found and performance is measured.

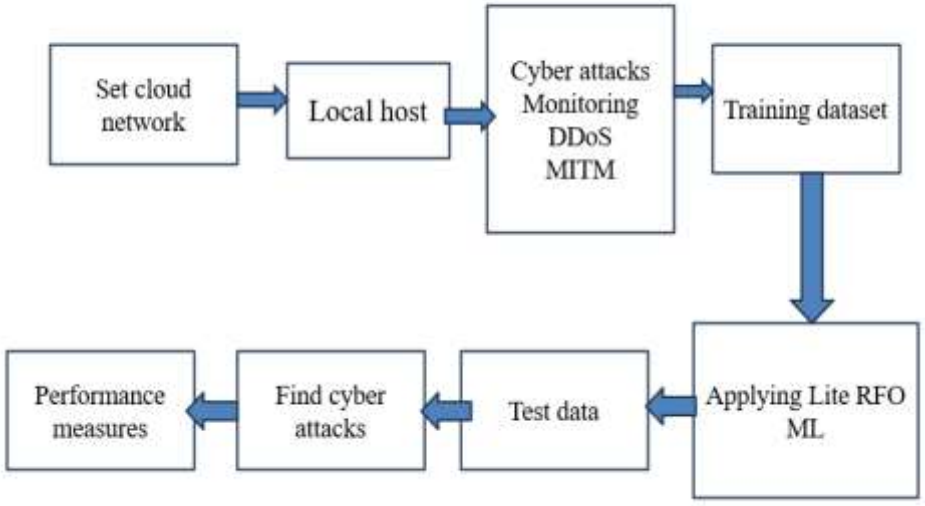

Fig 2. Proposed Model Diagram

LSTM algorithm with deep learning is considered in this research. This have given the promising results for reducing the cyber-attacks. In this research mainly local cloud server has been created, this cloud has link and password. When client open their application cyber security applications has been running. The DDOS, MITM attacks has been applying forcefully to local's host. The proposed machine learning algorithm can be regressing the data and classify the attack. The attack detection details have been displayed on screen for better understanding.

Mathematical computations

$$h_n = f(W_1 x_n + b_1) \quad (1)$$

$$\hat{x}_n = g(W_2 h_n + b_2) \quad (2)$$

$$\emptyset(\theta) = \frac{argmin}{\theta,\theta^1} \frac{1}{n} \sum_{i=1}^{n} \quad L\left(x^i, \hat{x}^i\right) \quad (3)$$

$$\{X_n\}_{n=1}^{N}, \quad (4)$$

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

IV. Results and Discussion

Fig 3. Cyber-attack detection window

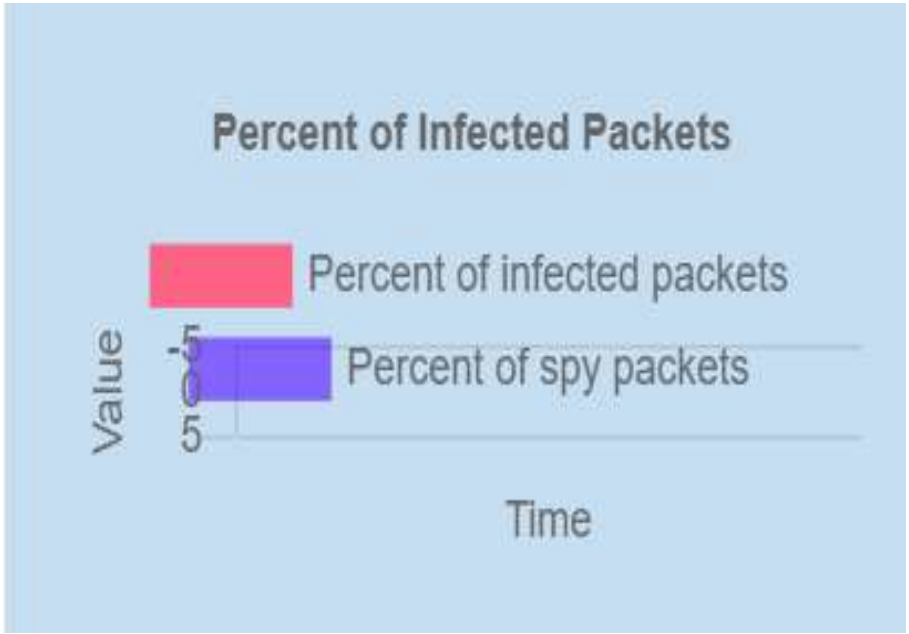

Fig 4. Infected information detection window

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

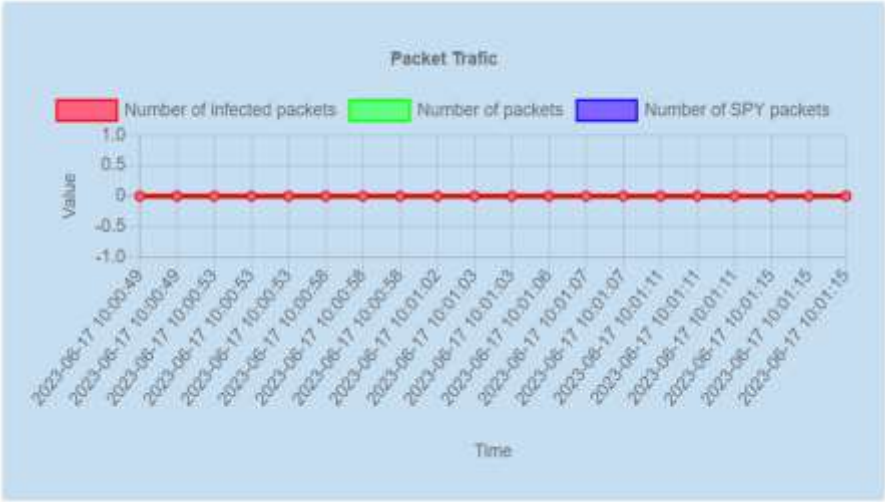

Fig 5. Cyber-attack detection model

Table 2 Test Cases

S.NO	INPUT	If available	If not available
1	Start	Real time attack detection started	There is no process
2	Stop	Real time attack detection stopped	There is no process
3	Real-time attack detection	Detection results displayed	There is no process

Table 3 Performance Measure

	Decision tree	RFO	SVM	Xboosting	Proposed
Accuracy	87.23	88.23	87.92	90.12	97.23
recall	88.23	77.92	89.23	93.28	98.24
F measure	78.23	89.23	88.21	92.32	98.92
Sensitivity	89.12	90.12	90.83	89.23	97.12
Detection score	90.23	92.12	91.02	89.03	98.23

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Fig 6. Performance Measure

This research deals with new technique LSTM which generated 99.97% of promis-ing results. the accuracy obtained is applied on the models which are designed. The advanced combined techniques generated 99.71% accuracy. Further various ad-vanced techniques are combined to generate better designs and models.

V. Conclusion

For dynamic DDoS and MITM assaults, a sophisticated cyber-attack model has been created in this study. Cyber threats have risen recently on a number of platforms, including clouds, servers, big data, and networks. Applications on these platforms may be impacted by attacks, and sensitive data may have been taken. There were several traditional models for cyber security, but they were ineffective against dynamic assaults and extremely complicated dangers. Additionally, there were significant ToC and target of attack vulnerabilities with the current cybersecurity frameworks. Using machine learning techniques, a sophisticated model for assessing cyber risk has been built in this study effort. The best Python software tool was used to implement the suggested Lite RFO model. This model has been monitoring cyberattacks on any network and can quickly identify the intended assault. The performance metrics, which included a detection rate of 98.43%, an accuracy of 98.23%, a sensitivity of 96.89%, and a recall of 94.56%, had all been met, which was an improvement.

References

1. S. Singh, E. G. Rajan, "Vector quantization approach for speaker recognition using MFCC and inverted MFCC", *International Journal of Computer Applications,* Vol. 17, No. 1, March 2011.
2. B. W. Sahle, A. J. Owen, K. L. Chin, and C. M. Reid, "Risk prediction models for incident heart failure: A systematic review of methodology and model performance," J. Cardiac Failure, vol. 23, no. 9, pp. 680–687, Sep. 2017, doi: 10.1016/j.cardfail.2017.03.005.
3. E. R. C. Millett and G. Salimi-Khorshidi, "Temporal trends and patterns in mortality after incident heart failure a longitudinal analysis of 86 000 individuals," JAMA Cardiol., vol. 4, pp. 1102–1111, 2019, doi: 10.1001/jamacardio.2019.3593.
4. N. Conrad et al., "Temporal trends and patterns in heart failure incidence: A population-based study of 4 million individuals," Lancet, vol. 391, no. 10120, pp. 572–580, 2018, doi: 10.1016/S0140-6736(17)32520-5.
5. F. Rahimian et al., "Predicting the risk of emergency admission with machine learning: Development and validation using linked electronic health records," PLOS Med., vol. 15, no. 11, Nov. 2018, Art. no. e1002695, doi: 10.1371/journal.pmed.1002695.
6. K. W. Johnson et al., "Artificial intelligence in cardiology," J. Amer. College Cardiol., vol. 71, no. 23, pp. 2668–2679, 2018, doi: 10.1016/j.jacc.2018.03.521.
7. J. R. A. Solares et al., "Deep learning for electronic health records: A comparative review of multiple deep neural architectures," J. Biomed. Informat., vol. 101, 2020, Art. no. 103337. [Online]. Available: https: //doi.org/10.1016/j.jbi.2019.103337
8. P. Nguyen, T. Tran, N. Wickramasinghe, and S. Venkatesh, "Deepr: A convolutional net for medical records," IEEE J. Biomed. Health Informat., vol. 21, no. 1, pp. 22–30, Jan. 2017, doi: 10.1109/JBHI.2016.2633963.
9. E. Choi, M. T. Bahadori, J. A. Kulas, A. Schuetz, W. F. Stewart, and J. Sun, "RETAIN: An interpretable predictive model for healthcare using reverse time attention mechanism," in Proc. Int. Conf. Adv. Neural Inf. Process. Syst., 2016, pp. 3512–3520.
10. M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should i trust you?' Explaining the predictions of any classifier," in Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining, 2016, vol. 13-17, pp. 1135–1144, doi: 10.1145/2939672.2939778.
11. D. Smilkov, N. Thorat, B. Kim, F. Viégas, and M. Wattenberg, "SmoothGrad: Removing noise by adding noise," 2017. [Online]. Available: http: //arxiv.org/abs/1706.03825.
12. Kumar,Cheruku&Roy,Ratnadeep&Rawat,Sanyog&Kumar,Archek.(2020). ActivationMapNetworkswithDeepGraphicalModelforSemanticSegmenta-tion. 10.1007/978-981-15-0214-9_89.
13. Kumar, Cheruku& Sharma, Abhay&Yadav, Ashwani& Kumar, Archek. (2020). Semantic Segmentation of color images via Feature Extraction Tech- niques. Journal of Physics: Conference Series. 1478. 012025. 10.1088/1742-6596/1478/1/012025.
14. Yadav, Ashwani& r.roy, & kumar, archek & kumar, cherku & Dhakad, Shailendra. (2015). De-noising of Ultrasound Image using Discrete Wavelet Trans- form by Symlet Wavelet and Filters. 10.1109/ICACCI.2015.7275776.
15. Shahabaz, & Somwanshi, Devendra & Yadav, Ashwani& Roy, Ratnadeep. (2017). Medical images texture analysis: A review. 436-441. 10.1109/COMPTELIX.2017.8004009.
16. Isolated Telugu Speech Recognition on T-DSCC and DNN Techniques, Inter- national Journal of Recent Technology and Engineering, ISSN: 2277- 3878, Volume 8, No. 11, pp. 2419-2423, Sep 2019.
17. Continuous Telugu Speech Recognition on T-LPC and DNN Techniques, International Journal of Recent Technology and Engineering, ISSN: 2277-3878, Volume 8, No. 3, pp. 4728-4731, Sep 2019.
18. Continuous Telugu Speech Recognition Through Combined Feature Extraction by MFCC And DWPD Using HMM Based PNN Techniques, International Journal of Pure and Applied Mathematics, ISSN: 1311-8080(printed version); ISSN: 1314-3395 (on-line version), Volume 118, No. 20, pp. 865-872, 2018.
19. Continuous Telugu Speech Recognition Through Combined Feature Extraction by MFCC And DWPD Using HMM Based DNN Techniques, International Journal of Pure and Applied Mathematics, ISSN:13118080(printedversion);ISSN:13143395(onlineversion),Volume114,No.11,pp.187-197,2017.
20. Speech Recognition with Combined MFCC, MODGDF and ZCPA Features Extraction Techniques Using NTN and MNTN Conventional Classifiers for Telugu Language, SOCTA, Springer Nature Singapore Pte Ltd, Book ID: 430915_1_En,BookISBN:978-981-10-5698-7,ChapterNo.:66,DOI 10.1007/978-981-10-5699-4_66,pp.1-10,2017.

21. Telugu Speech Recognition Using Combined MFCC, MODGDF Feature Ex- traction Techniques and MLP, TLRN Classifiers, SOCTA, Springer Nature Singapore Pte Ltd, Book ID: 430915_1_En, Book ISBN: 978-981-10-5698-7, Chapter No.: 65, DOI 10.1007/978-981-10-5699-4_65, pp. 1-10, 2017.
22. ContinuousTeluguspeechrecognitionthroughcombinedfeatureextractionby MFCC and DWPD using HMM based DNN techniques, International journal of pure and applied mathematics, ISSN 1314-3395, Sep 2017.
23. Review of Speech Recognition on South Indian Dravidian Languages, Indian Journal of Control Theory and Applications, ISSN 0974-5572, 10 (31), pp. 225-233 May 2017.
24. MFCC based Telugu speech recognition using SVM technique, Indian Journal of Control Theory and Applications, ISSN0974-5572,9(46), pp.105-113December2016.
25. Security Enhanced Image Watermarking using Mid-Band DCT Coefficient in YCbCr Space, Indian Journal of Control Theory and Applications, ISSN0974- 5572, 9(23), pp. 271-278, May 2016.
26. Velocity Estimation and Speed Tracking through Segmentation, Indian Journal of Control Theory and Applications, ISSN0974-5572,9(23),pp.101-106, May2016.
27. Telugu Speech Features Extraction by MODGDF and MFCC using Naive MODGDF and MFCC using NaiveBayes Classifier, Indian Journal of Control Theory and Applications, ISSN 0974-5572, 9(21), pp. 97-104 May 2016.
28. Speech Recognition using Arithmetic Coding and MFCC for Telugu Language, Proceedings of IEEE Digital Library, ISSN 0973-7529; ISBN 978- 93- 8054420-5, pp. 391-394, March 2016.
29. Segmentation on Moving Shadow Detection and Removal by Symlet Transform for Vehicle Detection, Proceedings of IEEE Digital Library, ISSN 0973- 7529; ISBN 978-93-8054420-5, pp. 385-390March 2016.
30. De-noising of color image using median filter, Proceedings of IEEE Digital Library, 978-1-5090-0148-4, Dec 2015.
31. De-noising of ultrasound image using discrete wavelet transform by symlet wavelet and filters, Proceedings of IEEE Digital Library, pp. 1204-1208, ISBN- 978-1-4799-8790-0, Aug 2015.
32. Wavelet Based Texture Analysis for Medical Images, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 4, No. 5, pp. 3958-3963, may 2015
33. Performance Evolution of40T Different parameters in RRC filter for MRC scheme in WCDMA system, International Journal of Innovative Science, Engineering & Technology, vol. 2, No. 5, pp. 443-451, may 2015
34. Speech Compression by Adaptive Huffman coding Using Vitter Algorithm, International Journal of Innovative Science, Engineering &Technology, vol.2, No.5,pp.402-405,may2015
35. Histogram Equalization for Image Enhancement using Kidney Ultrasound Images, Journal of Image Processing & Pattern Recognition Progress, vol. 2, No. 2, pp. 20-26, STM Journals, April 2015
36. Analysis of Histogram Processing for Brain MRI using MATLAB, International Journal of Innovative Research in Engineering & Science, vol.3, No.4, ISSN2319-5665, March2015
37. Survey on Content-based Image Retrieval and Texture Analysis with Applications, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 7, No. 6, pp. 41-50, ISSN: 2005-4254 IJSIP, Dec 2014
38. Advanced Digital Arithmetic coding with AES algorithm" International Journal of Computer Applications, vol. 2, IJCA, pp. 15-18, Dec 2013
39. TAV Machine with Pulse Sensor Circuit in International Conference of Computational Electronics& Nanotechnology at Amity university, Jaipur, March 2013