International journal of engineering science and management (IJESM).
ISSN: XXXX-XXXX.
https://doi.org/XX.XXXXX/XXXXXXXX/IJESM-XXXXXXXXX

Volume: 24, Issue 1, 54-61, October 2024.

Cyber Risk Assessment Model for Critical Information Infrastructure at dynamic time attacks

Dr.P Sampath Kumar[1], Dr.A.Sampath Dakshina Murthy[2]
[1]Dept of ECE, Jawaharlal Nehru Technological University Anantapur,
Email Id: **sampathplag@gmail.com**
[2]Professor, Department of ECE, Vignan's Institute of Information Technology (A), Duvvada, Visakhapatnam, Email Id: sampathdakshinamurthy@gmail.com.

Received: 7 September 2024 Revised: 29 September 2024 Accepted: 1 October 2024 Published: 3 October 2024

ABSTRACT:
In this study, a sophisticated cyberattack model was created for real-time DDoS & MITM attacks. Clouds, servers, big data, and networks are only a few of the modern infrastructures where cyber threats have proliferated. Threats to these platforms mean that private information may have been compromised within their applications. Cyber security experts could choose from a plethora of tried-and-true static models, but they all fell short when faced with dynamic attacks and other, more complicated threats. Furthermore, earlier cybersecurity models had problems with both high-ToC and target-attack scalability. Using machine learning methods, this study develops a sophisticated model for evaluating cyber risks. The recommended Lite RFO model was built using a top-notch Python programing utility. This architecture has been used to monitor cyberattacks on any network and locate the specific attack with a reduced Tree of Controls (ToC). There was a substantial improvement in performance metrics like detection rate (98.43%), accuracy (98.23%), sensitivity (96.89%), and recall (94.56%).

KEYWORD'S: cybersecurity, attacks, critical infromation of cyber-attacks, cyber risk.

1. INTRODUCTION:

Every organization has created its own technological roadmap for deploying information as well as operating innovations in the age of digitization. The technologies (like Automatic Data Collection and Automatic Data Processing Systems) can't be implemented without an architecture that ensures the safe interaction of digital, analogue, physical, and human aspects. The reliability of a utility relies on the cyber-physical security (CPS) of its critical facilities. Potential attack vectors in such a setting compel the organisation to take a proactive stance in creating internal cyber security procedures. These circumstances necessitate that utilities create a cyber security risk assessment model, It will be the cornerstone for building a dependable CII that is safe for sensitive data.

To ensure that the cyber risks associated with each CII are acceptable to the company, the model produced must incorporate the idea of regression evaluation with an input of specified and authorised specifications limitations. The ability use of regression analysis to forecast the risk assessment process would also allow a service to take preventative measures to secure itself, so lowering risk and providing the level of protection that is needed. In the event of a cyberattack, CII to have operational issues, lose

synchronisation, damage CPS components, and disrupt services. The establishment of a single structure for dealing with the diverse taxonomies of dangers, weaknesses, assaults, and regulates on controllers for devices (RTUs, FRTUs, PLCs), distributed control at the plant level, or SCADA elements across the network geographical regions must be done to tackle this new safety difficulties. Denial of service assaults, phishing scams, data theft, and data modification are all frequent types of cyberattacks in the modern world. These occurrences' effects are: harm to the character or reputation of the firm, loss of consumer faith, Quality issues with the products and services, absence in company chances or contracts and Regulations are being broken.

Figure :1 cyber security platform

Researchers have shown that the entropy of the source IP address or destination port number is the most reliable parameter for detecting DoS or DDoS attacks. The disadvantage of using statistical entropy is that a threshold value must be selected in order to identify an assault. When network traffic is minimal, it has a hard time detecting assaults, but when it's high, it can spot them. Inability to distinguish between DDoS assaults and flash crowds, longer time to detect attack occurrence, inability to distinguish among attack and actual traffic flows with high-rate traffic, and detection of just a subset of possible DDoS attacks.

2. LITERATURE SURVEY:

In this section a brief survey of cyber security models has been discussed for better attack analysis. It's challenging to determine the optimal threshold for attack detection, which would both reduce false positives and false negatives. Since it can only identify specific forms of DDoS attacks, it would be unable to tell the difference between an attack and legitimate traffic flows occurring at high rates.

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	Methods to Increase Cyber Security Awareness	80%	Parallel attacks caching
Ivanchenko, O. 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. The existing limitations and problems have been overcome through proposed Lite RFO machine learning model.

Objectives of research:

- To design Using the Lite RFO Regression Algorithm, We Have Created a Cyber Risk Assessment Model for CII.
- To detect the cyber-attacks in dynamic environment in less ToC with high detection rate.
- To compare designed application performance with existed techniques.

Problem statement:

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. A variety of cyber security solutions are available but those identify the attack in static manner. Security measures such as anti-virus software, a firewall to prevent hackers from entering a network, and a virtual private network (VPN) for encrypted remote access. if attacks enter into network, its functionality is going to be stopped so application may get damage. These problems have been over come through proposed cyber security technique.

3. METHODOLOGY:

In this work used deep learning approach over machine learning (MLWhen comparing to low-volume methods, deep learning shines when applied to massive datasets. The rules-based, limited-data approach used by conventional machine learning has proven effective. Expert judgement is required for feature selection in ML, because the features used to train the model have a direct impact on how well it performs. In contrast, deep learning immediately pulls out high-level features from the data. This means that while DL algorithms require a lot of time to train, they can be tested quickly, saving money. Contrarily, some ML algorithms require little time to train but considerable time to test.

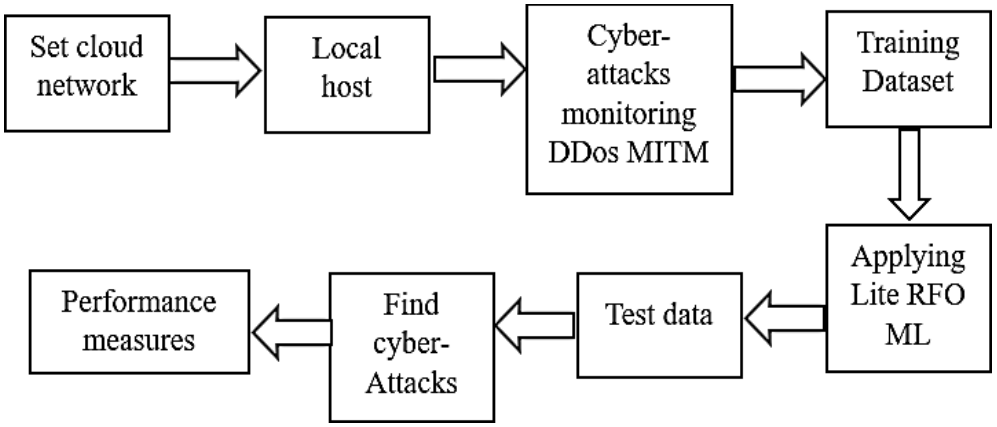


Figure: 2 proposed model block diagrams

For identifying Portman DDoS attacks, the reporting findings reveal that LSTM Deep Learning technique delivers the best results compared to other Deep Learning based algorithms. From our experiments, we know that once we're linked, we achieve a performance rate of 99.97%. 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 and the risk assessment methods are shown in Figure 3.

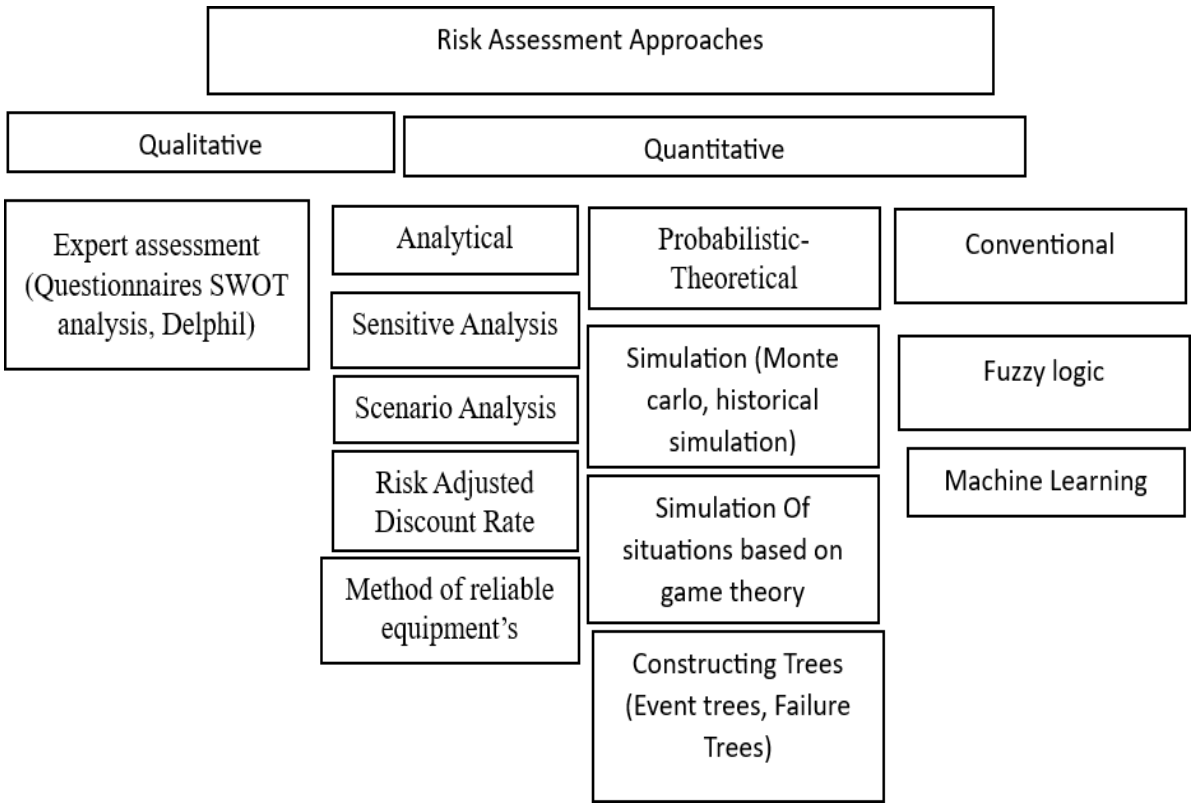


Figure 3. Classification of risk evaluation strategies.

Mathematical computations:

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

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

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

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

4. RESULTS:

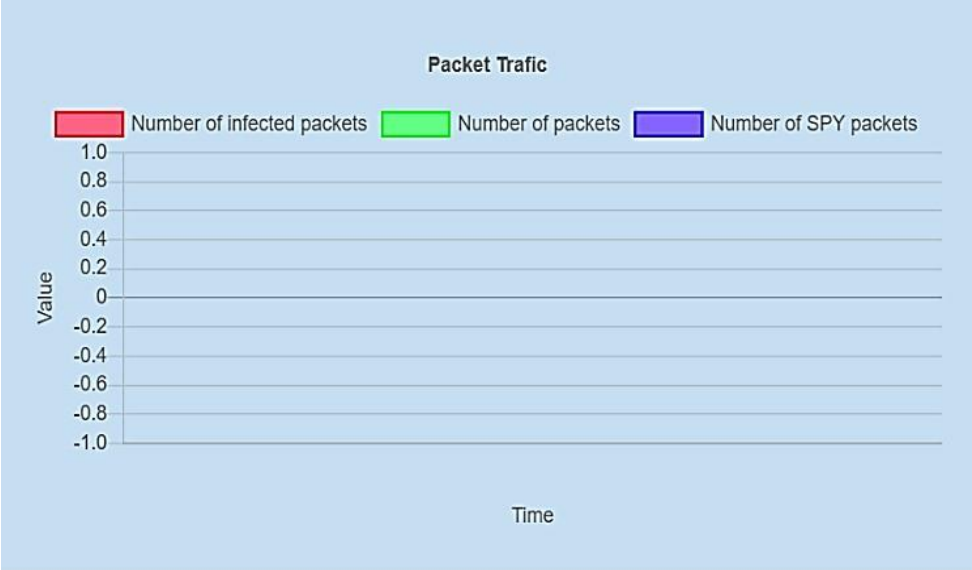


Figure:2 cyber-attack detection window

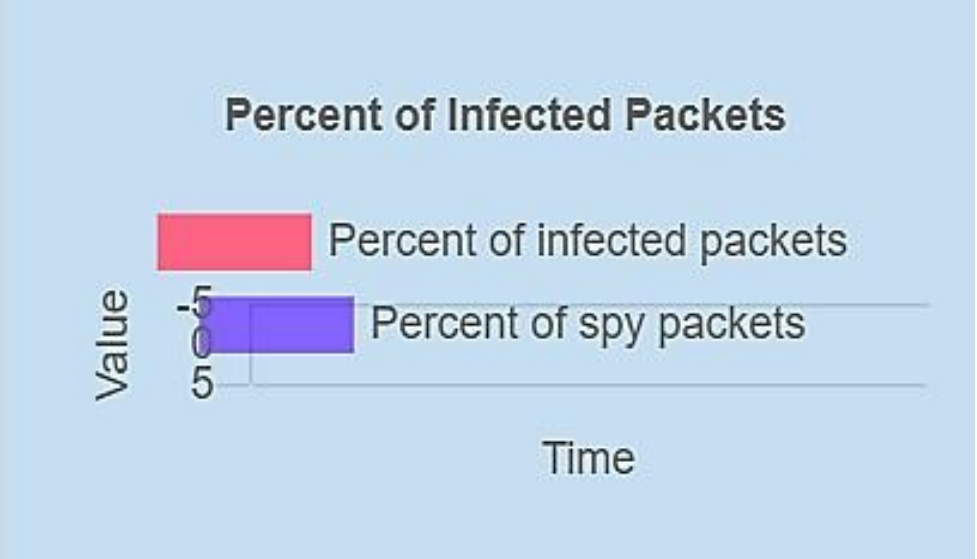


Figure:3 Infected information detection window

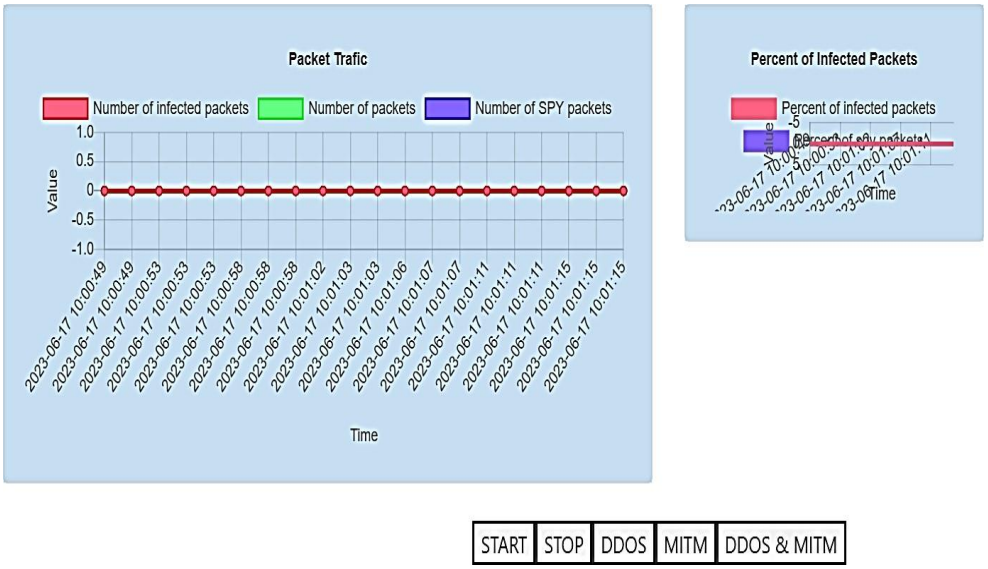


Figure: 4 cyber-attack detection model

TABLE : 2 TEST CASES

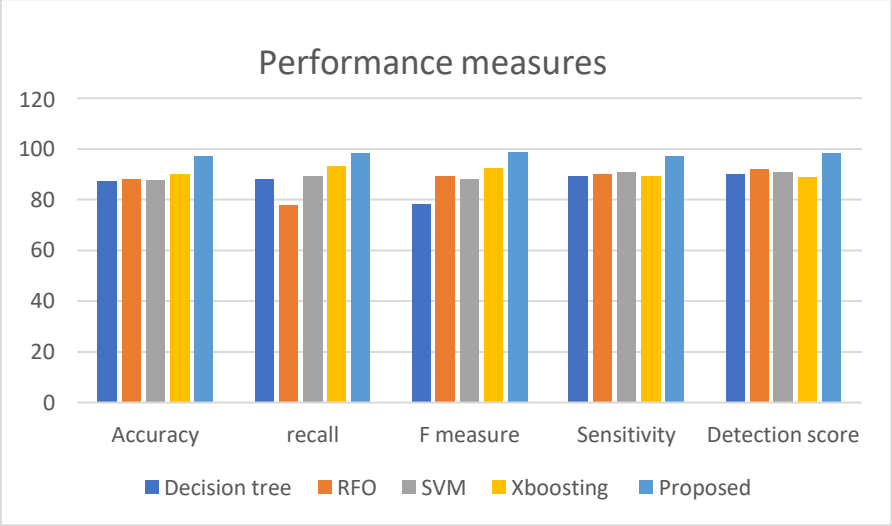
S.NO	INPUT	If available	If not available
1	Start	Real time attack detection started	There is no process
2	Stop	Real time attack detection stoped	There is no process
3	Real-time attack detection	Detection results displayed	There is no process

There is no substitute for actually executing software in order to ensure its quality. Structural testing, also known as white-box testing, is essential for finding and fixing faults and problems in software before it goes into production. Now that the programme structure has been established, unit tests may be carried out with the aid of regression testing. Automation within a test automation framework is commonly used to speed up this stage of development. To detect and analyse any changes (mutation testing) in the system's behaviour, developers and QA engineers can compare the results of new tests with those of old tests (control flow testing) thanks to having full visibility into the software's architecture and data flows (data flows testing). The focus of the software's final round of testing shifts from its mechanics to how it reacts to various stimuli. To put it another way, in order to observe the product from the user's perspective, behavioural testing (also known as black-box testing) necessitates a large number of tests, the most majority of which are performed manually. In order to simulate how normal customers would use the product and respond to issues like bugs, QA specialists need to know specifics about the software's intended commercial or other purposes (what we call "the black box").

Automation (regression tests) may be used in behavioural testing to remove the possibility of human mistake from routine tasks. It is recommended to automate this test, as To test how well a product scales to a large number of visitors, you might, for instance, register 100 unique users on the website.

Table.3.

	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



This paper introduces a new LSTM-based method for finding out if an assault is a DDoS (distributed denial of service). The experimental findings indicate that following the link is made, the performance increases to 99.97%. After correct formulations have been established, the accuracy score can be used to compare the two models. The Attack-Detection class we created offers methods for performing network packet classification using the LSTM model, even though the autoencoder model is clearly the superior model. The Attack-Detection tool based on these models shows up to 99.71% net accuracy in simulations.

To detect hacked endpoints, future research should strive to duplicate results in a bigger system, and algorithms should be kept up-to-date through feasible retraining methods to deal with anomalies in network performance.

5. CONCLUSION:

A complex cyber-attack model that can simulate dynamic DDoS and MITM assaults has been developed as part of this research project. Recent years have seen an increase in the frequency and severity of cyber-attacks across a variety of systems, including networks, clouds, servers, and big data. Attacks could have an effect on the applications running on such platforms, and sensitive data could

have been compromised. There were a few different conventional approaches for cyber security, but none of them were successful against the dynamic attacks and incredibly complicated threats that were out there. In addition, the existing cybersecurity frameworks had substantial flaws in both their targets of compromise (ToC) and attacks (targets of attack). During the course of this research project, a complex model for determining the level of cyber risk was developed making use of machine learning strategies. In order to successfully execute the suggested Lite RFO model, the most effective software tool for Python was utilised. This model has been keeping an eye out for cyberattacks on any network and is able to swiftly determine whether or not an attack was intended. The performance measures, which comprised 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 satisfied, which represented an improvement.

6. REFERENCE'S:

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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

[7] 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.

[8] 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.

[9] 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.

[10] 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