IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER ATTACK DATECTION WITH QR CODES USING LIGHTWEIGHT DEEP LEARNING MODEL

[1]Sudarshan Gaikar, [2]Ajay Bichukale, [3]Deep Barvekar

[1]Writer, [2]Creator, [3]Writer
[1]Prof.Pradnya Patil,
[1]Pillai HOC College Of Engineering And Technology, Rasayani, India

Abstract : In today's world information technologies are rapidly evolving because of that servers are attacked by cyber attacks. This cyber attack causes a big data loss to the organization and it becomes a big concern in such an organization. In the existing system, it only detects attacks when that attack happens once because of that it fails to detect the new attack that is going to happen. But our detection with QR code images using a lightweight deep learning model is able to detect the cyber attacks that have been identified. We have collected and curated a large dataset of QR code images, encompassing a wide range of use cases and variations. This dataset serves as the foundation for training and evaluating our lightweight deep-learning model. We propose a specially designed deep learning model optimized for QR code image analysis. This model is computationally efficient and effective at detecting anomalies and potential cyberattacks within QR codes. Our model differentiates between legitimate QR codes and potentially malicious ones. It identifies various forms of tampering, such as data manipulation, structural alterations, and hidden malware payloads. We evaluate the model's robustness against adversarial attacks and its ability to generalize to unseen QR code variations, ensuring its effectiveness in the ever-evolving threat landscape. Our experimental results demonstrate the effectiveness of our lightweight deep model in detecting cyber attack threats within QR code images with high accuracy and low False-Positive rates. The model's efficiency and real-time capabilities make it a promising tool for enhancing cybersecurity in various domains where QR codes are utilized. In conclusion, this research paper approach to cyber attack detection through QR code image analysis leverages the power of deep learning to enhance security in digital applications.

Keywords – ***Cybersecurity, Lightweight deep learning model, QR code, Generalization.***

I. INTRODUCTION

In today's digital landscape, the proliferation of technology and the widespread use of the internet have led to an unprecedented increase in cyber threats and attacks. Cyber attackers are constantly devising new methods to exploit vulnerabilities in digital systems, posing significant risks to individuals, organizations, and governments alike. One prevalent avenue for cyber attacks is the use of [11]QR (Quick Response) codes, which are barcodes widely used for different purposes, including product labeling, advertising, and information sharing. QR codes serve as efficient conduits for information exchange due to their quick readability and ease of use. However, their convenience also makes them susceptible to malicious exploitation. Cybercriminals often embed harmful payloads, such as malicious URLs or malware, within QR codes, leading to a variety of cyber-attacks, including phishing, ransomware, and data breaches. In recent years, there has been a trend towards developing lightweight deep learning models. Lightweight models are designed to be computationally efficient, enabling them to perform complex tasks while conserving processing power and memory. The combination of deep learning and lightweight models presents a promising avenue for enhancing the accuracy and efficiency of cyber-attack detection systems, particularly concerning the analysis of QR code images. By exploring the application of lightweight deep learning models to QR code images, researchers aim to create a robust and real-time detection system capable of identifying malicious QR codes promptly. Such a system would significantly contribute to strengthening cybersecurity measures, safeguarding users and organizations from the ever-growing threats posed by cybercriminals. This research builds on the foundation of deep learning technologies and adapts them to address the specific challenges posed by QR code-based cyber attacks, marking a significant advancement in the field of cybersecurity. In an era dominated by digital transactions and interconnected systems, the proliferation of cyber threats has become a significant concern. With the ubiquity of Quick Response (QR) codes in various industries, they have become a vector for potential cyber attacks. As businesses and individuals increasingly rely on QR codes for payment transactions, authentication, and data sharing, the need for robust security measures to detect and prevent cyber threats is paramount.This paper introduces an innovative approach to enhance cyber attack detection, specifically targeting QR code images. Leveraging the power of deep learning, a lightweight neural network [4] model is proposed to efficiently analyze QR code images and identify potential cyber threats in real-time. This model aims to strike a balance between accuracy and computational efficiency, to make suitable for resource-constrained environments, like mobile devices and edge computing system. The significance of securing QR code transactions cannot be overstated, as a compromise in the integrity of these codes could lead to financial losses, data breaches, and compromised privacy. Traditional methods of detecting cyber threats often fall short in addressing the unique challenges posed by QR code vulnerabilities. Therefore, a dedicated approach utilizing advanced technologies is essential to fortify the security infrastructure against evolving cyber threats.

II. LITERATURE SURVEY

For developing this model we have take reference of so many research paper to develop a system which don't have the problem which have faced by existing systems. For development of this model we take reference of Harris of hawk optimization model research paper [1].This optimization technique aims to mimic the collaborative hunting strategy of these birds to solve complex optimization problems. While not directly related to cybersecurity, HHO's adaptability and efficiency make it a potential candidate for optimizing parameters in cybersecurity algorithms or systems. But this model have lack of universality, limited exploration. QR code technology [9], QR code technology developed in Japan in 1994. QR codes are scanned by camera enabled device in this project it helps to store and preprocess data. it has ability to store large amount of data including URLs, text etc.

Research paper [11], from this research paper we take reference of how data is classified by using Random Forest algorithm. It takes less time for training as compared to other machine learning algorithm. It's accuracy of prediction is very high, it can handle large dataset and run efficiently. If any portion is missing in dataset then also it maintain it's accuracy

Research paper [6], from this research paper we are getting information about threats and attacks. The research paper addresses the critical need for comprehensive it makes classification of cyber threats on mobile devices and applications. Existing classifications are often limited and fail to cover all potential threats, leaving users vulnerable. The proposed framework aims to fill this gap by providing an exhaustive list of threat categories and principles. By systematically identifying and highlighting these threats, the framework empowers mobile users to take proactive measures to safeguard their privacy and security.

Research paper [5], The paper addresses the increasing threat of DDoS attacks on internet services, detecting the attack in starting phase make it easy to mitigate the network traffic. It proposes the use of deep neural networks (DNN) for effectively detecting DDoS attacks by analyzing packet samples from network traffic. Experiments conducted on the CICDDoS2019 dataset demonstrate the high success rate of 99.99% in detecting attacks and an accuracy rate of 94.57% in classifying attack types, but it only detects single D-Dos attack this is disadvantage of the system and accuracy is less as compared to our model.

Research paper [12], The paper focuses on Intrusion Detection Systems (IDS),Its is develop to keep eye on the network system and respond to malicious threats. With the increasing reliance on the internet, ensuring the security of digital information has become paramount. Hackers can deploy different attacks to gain access to important information, prompting the need for(IDS), methods. The paper aims to provide a comprehensive overview of intrusion detection, including types of methods, attacks, tools, techniques, research needs, and challenges. Additionally, it proposes the development of an IDS tool for research purposes capable of detecting and preventing intrusions.[3] [4] these two models are used in this system.

III. METHODOLOGY

In this research paper, we propose a comprehensive methodology for enhancing cyber attack detection through the integration of QR code images and a lightweight deep learning model. The main goal is to fortify the security of QR code-based systems by leveraging advanced techniques in the realm of deep learning. Our methodology consists of several key steps. First, we collect a diverse dataset of QR code images, encompassing various environments and potential attack scenarios. We preprocess the dataset to ensure uniformity and quality. Subsequently, we design a lightweight deep learning model tailored to the unique characteristics of QR codes, emphasizing efficiency and speed without compromising accuracy. The model is trained on the prepared dataset, utilizing transfer learning strategies to leverage pre-existing knowledge from relevant domains. To improve the model's performance, we employ rigorous testing methodologies, using metrics such as precision, recall, and F1 score. Additionally, we assess the model's robustness against adversarial attacks to ensure its reliability in real-world scenarios. The proposed methodology aims to provide an effective and efficient solution for cyber attack detection in QR code systems, contributing to the broader field of cybersecurity and paving the way for enhanced protection in digital communication channels. The figure 3.1 shows the system architecture. In this project the sample dataset is taken of cyber attack is taken. This dataset is trained for the model so it can make prediction of the attack. The values taken from the dataset so it will make prediction of the attack. In this model all the network fields are initiated. Because when any attack is happen at that time changes is get happen on network setting for that this model is train such way that any setting values are get any changes. Then after that values get enter in our system it should predict which attack is happened.

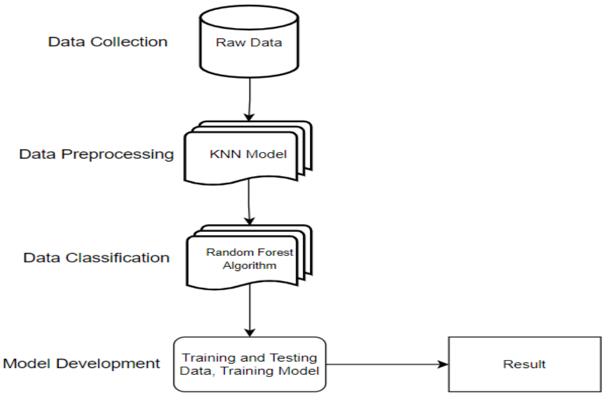

Fig3.1 System Architecture

IV. ALGORITH

1.Random Forest Algorithm:-

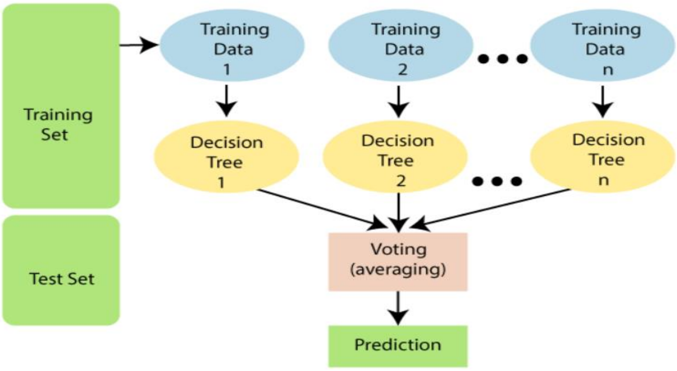

Fig 4.1 Random Forest Algorithm

The Fig 4.1 shows the Random Forest Architecture. It belongs to ensemble learning technique, which means it combines multiple individual models to improve its performance. Random forest algorithm is built on the concept of decision trees. Decision tree is follows flowchart – structure concept each insider node shows test on each attribute, all branches represent the outcome of the test. The randomness is the main feature of this algorithm. Every decision tree in random forest algorithm is trained on random subset of training data. And this process is known as bootstrapping. It ensure the diversity. Random subset of features helps the co-relation between trees in the forest. Voting is main task in random forest, each tree in the forest independently predict the class of the input. Final result is based on the majority of voting among all trees. Final decision is usually based on the average prediction made by all trees.

The purpose of selecting Random Forest Algorithm:-

- Random forest is robust to overfitting problem.
- It perform both classification and regression.
- Random forest gives more accuracy as compare to other algorithms.
- Random forest is more versatile and robust, it have ability to handle complex data.
- It is used different machine learning task because of its robustness and able to handle complex data.

Random forest can solve the generalization problem using OOB(Out-of-bag) samples. It provides measure of feature, which helps in feature selection for model and also unyielding data get understand. The random forest is having scalability to handle large dataset.

2.HHO Algorithm:-

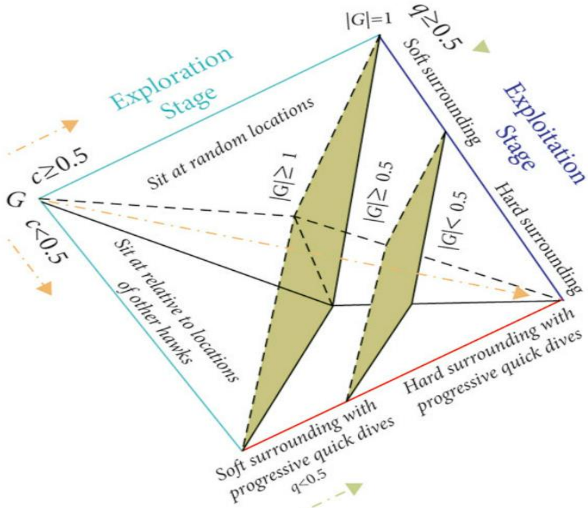

Fig 4.2 HHO Algorithm

The Fig.4.2 shows the HHO model. This model is proposed by the Dr.Y.S.Abu-Mustafa. It is metaheuristic optimization algorithm. It solves the optimization problem. HHO is inspired by the Harris Hawk hunting technique of prey birds. This collaborative approach involve various stages like scouting, surprise pouncing and coordinated attacks. The HHO algorithm[1] is designed to emulate the exploration and exploitation phases seen in optimization. The algorithm incorporates mathematical model inspired by the hunting behavior of harris and hawk. HHO is population based optimization algorithm, means it operates on a population of candidate solution. Initially, a population of potential solution is generated, and this population evolve iteratively through successive generation. During each iteration, the population of solution evolves based on the predefined rules and operator inspired by the hunting strategies of Harris Hawk. This rules govern how solution are get selected, modify, and evaluate to guide the optimization process towards better solution. From the perspective of algorithmic behavior, HHO has a number of useful qualities, including: The dynamic, randomized, time-varying nature of the escaping energy parameter can enhance and balance the

HHO's exploratory and exploitative patterns. This element also helps HHO carry out a seamless transition from exploration to exploitation. Throughout the first iterations of HHO, several exploration strategies in relation to the average location of hawks can increase the exploring tendencies.

3.KNN Model:-

This article dives into the K-Nearest Neighbors (KNN) Algorithm, a powerful tool in machine learning used for solving various types of problems like predicting outcomes or classifying data. Developed in 1951 by Evelyn Fix and Joseph Hodges, it was later improved by Thomas Cover. The article explores how KNN works and where it can be used in simple terms. Fig.4.3 shows the KNN model architecture.

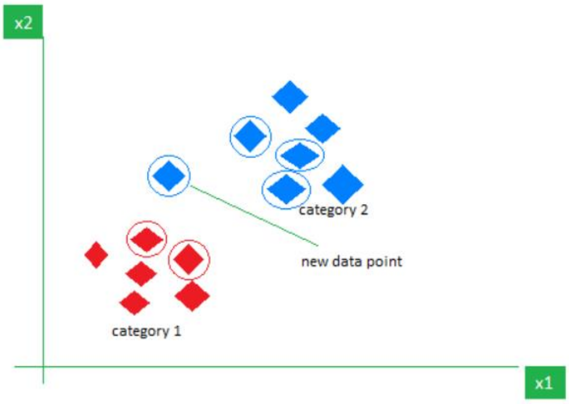

Fig 4.3 KNN Model

The K-Nearest Neighbors (KNN) algorithm is favored for its simplicity and adaptability, making it widely used in machine learning. Unlike other methods, it doesn't require assumptions about the data's distribution, so it fits well with different types of datasets for classification and regression tasks. KNN handles both numerical and categorical data easily, making it versatile. It's also robust against outliers, meaning it's not heavily influenced by unusual data points. By looking at the nearest neighbors to a data point, KNN can make predictions based on the local structure of the data, making it flexible in identifying various patterns. Moreover, it's easy to implement due to its straightforward nature. KNN dynamically adapts to new data, continuously improving predictions. With only a few hyperparameters to tune—primarily the number of neighbors (K) and the distance metric—training a KNN model is relatively simple. Overall, KNN's simplicity, adaptability, and robustness make it a preferred choice for many machine learning tasks, especially when dealing with diverse datasets and real-world applications.

V. RESULT ANALYSIS

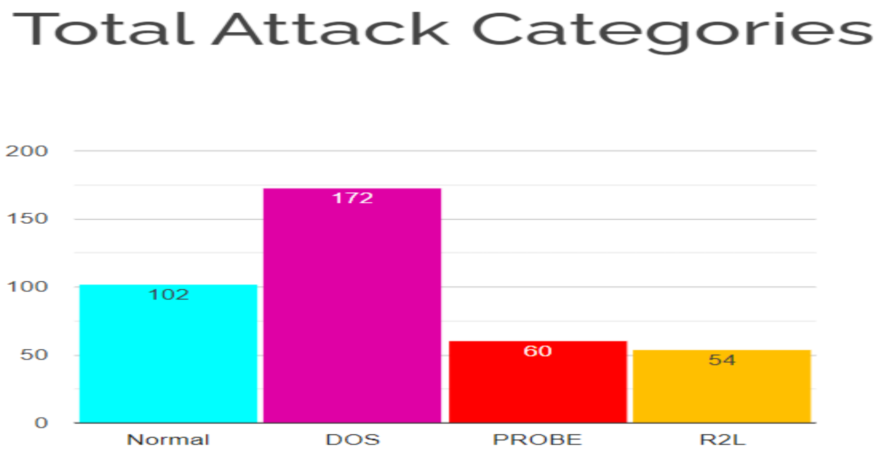

Fig 5.1 Attack Categories Analysis

The Fig 5.1 shows the which attacks we are going to detect. And we can easily see the analysis of each attack. In this we can predict the attack and also find out which attack category it is

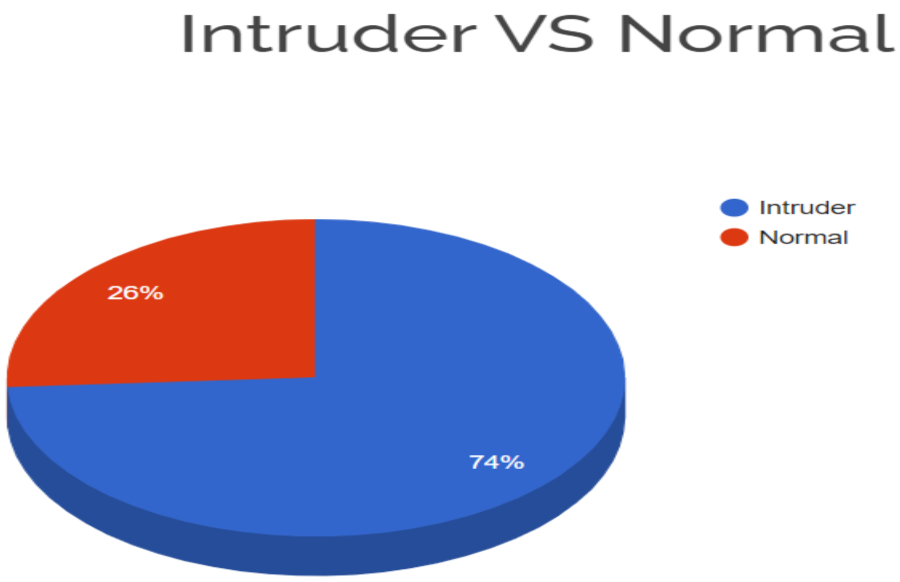

Fig 5.2 Intruder vs Normal

In Fig 5.2 we can easily seen the intruder vs normal connections in the intrusion detection system. Which dataset we have from that it differentiate the intruder and normal connections.

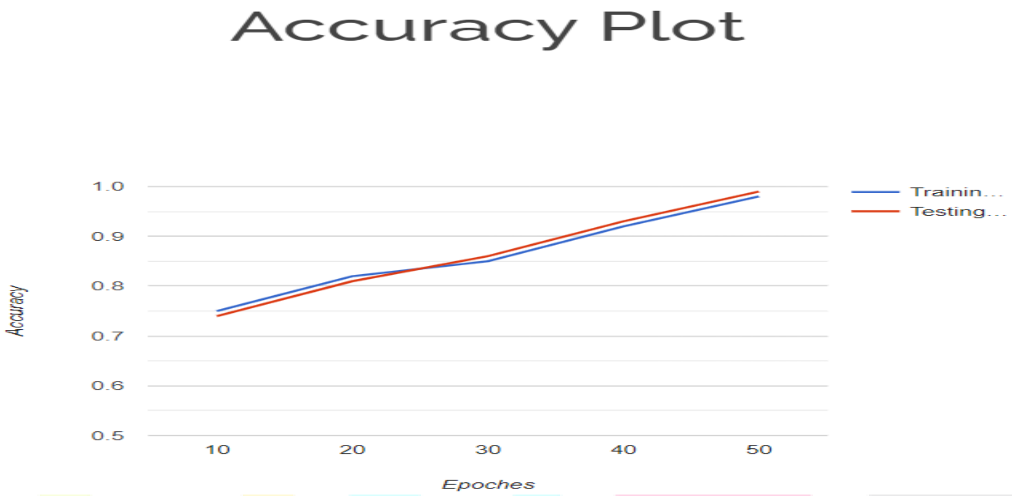

Fig 5.3 Accuracy Plot

In Fig 5.3 this we can see how much accuracy is achieved by our model. In this model we are achieving the 98% accuracy. In existing system the accuracy is 88% which is less than the accuracy which we have achieved

Model	**Accuracy**
Cyber Attack Detection with Machine Learning Model (Existing system)	88.78%
Cyber Attack Detection with QR Codes Using Lightweight Deep Learning Model (Current System)	98%
Random Forest Algorithm	87% -99%
CNN Model	78% - 90%

Table 5.1 Efficiency

Table 5.1 shows the comparison of the models which are present and used in existing and current system. This comparison shows the which system and model is more efficient to use.

VI. CONCLUSION

In this study, High accuracy and performance were achieved by applying image processing techniques in machine learning methods with the images of these data codes, which were formed as QR code images of cyberattack data in this study. For image processing different models are used so processing speed is get faster. In the first stage, the Random Forest Algorithm was employed, and 98% of the attempts were successful. In the subsequent phase, distinct deep features were retrieved from the QR code images and utilized for categorization.

In future we add the protection from the attack which we are detected. In future we create application software so anyone can download software and use it and maintain the security of users system. We also use newly developed model so that it should give more accurate

REFERENCES

[1] A.A. Heidari et al. Harris hawks optimization: algorithm and applications Future Gener. Computer Syst.(2019). https://www.sciencedirect.com/science/article/abs/pii/S0167739X18313530

[2] C.H. Karadal et al. Automated classification of remote sensing images using multileveled MobileNetV2 and DWT techniques Expert Syst. Appl.(2021) https://www.sciencedirect.com/science/article/abs/pii/S0957417421010502

[3] KNN Model-Based Approach in Classification August 2004.
https://www.researchgate.net/publication/2948052_KNN_Model

[4] Convolutional Neural Network (CNN) for Image Detection and Recognition
December 2018 DOI:10.1109/ICSCCC.2018.8703316
Conference: 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)

[5]A.E. Cil et al.
Detection of DDoS attacks with feed forward based deep neural network model
Expert Syst. Appl.(2021)

[6]M.A. Almaiah et al.Classification of cyber security threats on mobile devices and applications
Artificial Intelligence and Blockchain for Future Cybersecurity Applications(2021)

[7]M.J. Awan et al.
Real-time DDoS attack detection system using big data approach
Sustainability(2021)

[8] Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning
Indones. J. Electr. Eng. Comput. Sci(2020)

[9] An Introduction to QR Code Technology

December 2016 DOI:10.1109/ICIT.2016.021 Conference: 2016 International Conference on Information Technology (ICIT)

[10] KNN Model-Based Approach in Classification

August 2004 Gongde Guo, Hui Wang https://www.researchgate.net/publication/2948052_KNN_Model-Based_Approach_in_Classification.

[11] Random Forests and Decision Trees

September 2012 Jehad Ali, Nasir Ahmad
https://www.researchgate.net/publication/259235118_Random_Forests_and_Decision_Trees