Hybrid Model for DDOS Attack Detection and Covid-19 Classification

K. Nishitha Sree
Electronics and Communication Engineering
Institute of Aeronautical Engineering
Hyderabad, India
nishithakeshaboina@iare.ac.in

B. Naveen
Electronics and Communication Engineering
Institute of Aeronautical Engineering
Hyderabad, India
naveenbadavath670@gmail.com

Rufus Praleen
Electronics and Communication Engineering
Institute of Aeronautical Engineering
Hyderabad, India
21951a04f6@iare.ac.in

Mr. G. Kiran Kumar
Electronics and Communication Engineering
Institute of Aeronautical Engineering
Hyderabad, India
g.kirankumar@iare.ac.in

Abstract

The COVID-19 pandemic has significantly impacted public health and economies worldwide. The integration of the Internet of Things (IOT) with medical technology, known as the Internet of Medical Things (IOMT), has facilitated advances like rapid diagnosis, remote monitoring, and more efficient healthcare delivery. However, the security, privacy, and integrity of IOMT-generated medical data remain a critical challenge. Current systems are particularly vulnerable to cyber-attacks, such as Distributed Denial of Service (DDOS) attacks, which can disrupt medical services. To address these concerns, a new IOMT-based COVID-19 detection and classification system, named ICDC-Net, is proposed for smart healthcare applications. This system incorporates an Optimized Feistel Block Cipher (OFBC) for encryption to secure COVID-19-related medical data, particularly chest X-ray images, ensuring robust data protection. The OFBC algorithm is optimized using a hybrid approach combining the Gray Wolf Optimizer and Particle Swarm Optimization (HGWO-PSO), providing both encryption and effective DDOS attack detection and prevention. Additionally, the HGWO-PSO method is employed to extract features from chest X-rays, aiding in the detection of specific diseases. For disease classification, a deep learning model, Residual Network50 (ResNet50), is used to identify conditions like COVID-19, pneumonia, and other common lung diseases. Testing and simulations demonstrate that ICDC-Net enhances detection accuracy (ADA), reduces attack detection time (ADT), and lowers the detection error rate (ADER) when compared to existing security protocols. Moreover, the system improves the classification of COVID-19 and other diseases, outperforming traditional models in terms of speed and accuracy.

INDEX TERMS: Chest X-ray image classification, convolutional neural networks, feistel block cipher, grey-wolf optimization, Internet of Medical Things, hybrid ResNet50

1. Introduction

The Internet of Medical Things (IOMT) is extremely popular nowadays and plays an important role in hospitals. COVID-19 is a global epidemic that, within the first six months, will have a great impact on people's lives, with a high mortality rate and mass incarceration. In recent years, novel coronavirus pneumonia (COVID-19) has spread to the world, and contactless treatment has become trendy [1]. Users send massive medical data (images) through the IOMT environment. Figure 1: Basic Application Environment of IOMT. Since IOMT basically uses wireless communication and the Internet to transmit data collected from the human body to the servers of a doctor or a hospital, data stored in various layers of the IOMT system may be exposed to cyber-attacks with the following characteristics: It may cause physical harm. The patient's private health and life are put at risk. Proper security measures should be taken quickly to prevent, detect, and respond to such an attack. This section discusses the basic security requirements of IOT [3]. IOMT ensures the integrity of data in health care, which assures data sent wirelessly to reach the proposed destination without interference or modification. Thus, in other words, data is invariant and doesn't alter while sending. For example, during the treatment of a patient, a critical information such as the strength of medication or test results should reach it intact in order to prevent patients from causing injury to him or her. The process of data integrity ensures that data is maintained intact, undamaged, and reliable at all times in the process of transmission. It can also transmit wirelessly as well [4]. We provide a way in which medical information will be the same for someone other than the recipient, such as the doctor or nurse, in preventing medical malpractice through honest information. This is achieved by ascertaining that data is left in its raw format. The researchers found that various data encryption types applied to the safety of the images. The process of data encryption is changing a clear image using a key into an encrypted image [6]. Such transformation occurs during the time of image encryption. Decryption transforms the cryptographically encrypted data to the original image by use of private keys. The decryption process appears almost the same as the encryption process but uses the inverse step [7]. When it comes to encryption, then the function of the key becomes important. Both private and public keys are used in the encryption process. This is because the key is among those factors on which the encryption security mainly depends. In IOMT, decrypted data can also be decrypted similarly by making use of the same key, typically consisting of a private key, and is used in both the processes [8]. But when public encryption is used, there is a requirement for two different keys; one will be encryption key, and the other will be decryption key. The encryption key must be public, whereas the decryption key must remain secret because it holds sensitive information [9]. It is thus important to protect medical images in the IOT environment.

1.1 SECURITY VULNERABILITIES IN THE IOMT

Traditional approaches in IOMT can promise much more stability with better eyesight and efficiency. Cyber-security issues represent one of the biggest threats to patient safety and patient privacy in IOT based diplomacy, including embedded sensors and medical wears, forming an important principle to the systems enabled through IOT. Since such attacks on the IOT devices are heavily layered and diverse in nature, they are likely to be successful. Such weaknesses may be victims of potential types of data injection, denial-of-service attacks, and persistent attacks, among many; they may compromise data and systems, affect whole ecosystems, and much more. Unauthorized access to a patient's medical information may lead to inappropriate or harmful treatment, thus putting that person in danger. Since IOMT is very much beneficial, it is also highly prone to cyber threats, especially the formation of malicious bots, identity theft, phishing, and key-logging. The IOTT digital environment allows processes that compromise the ability of basic security and leads to other things like cyber-attacks and other online threats. It can, therefore, provide IOMT network security that is required to integrate IOMT intelligence into the medical model. Functionality. It is necessary for the integration process to go through smoothly. For this, the first thing is to let known attempts at hijacking which are either purported or already existent against the IOMT infrastructure. There are several aspects and functionalities contained in the IOMT devices similar to IOT devices, hence, those attacks previously developed for the networks of IOT devices are also of concern with regard to IOMT devices.

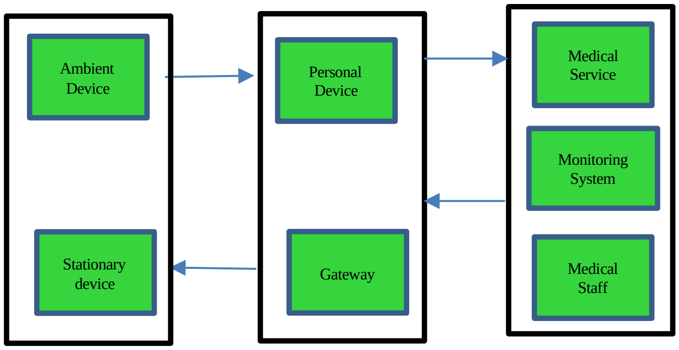


Figure 1:Application Environmental of IOMT

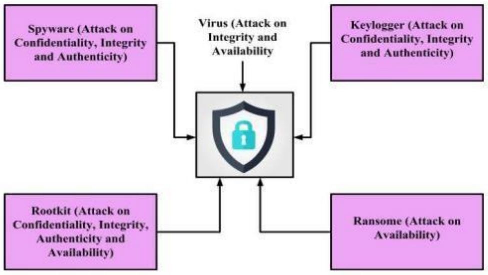

Spyware (Attack on Confidentiality, Integrity and Authenticity)
Virus (Attack on Integrity and Availability
Keylogger (Attack on Confidentiality, Integrity and Authenticity)
Rootkit (Attack on Confidentiality, Integrity, Authenticity and Availability)
Ransome (Attack on Availability)

Figure 2: Variours security Vulnerabilities in IOMT

There are so many vulnerabilities within the IOMT environment:

Spyware attacks: Spyware is the type of malware that is devised to secretly gain access to IOMT devices and systems. After gaining access, it surreptitiously stays inside in operation without the knowledge of the user and collects sensitive patient information. It may include personal health information, medical records, and periodic patient care information. The collected data can be sent to unauthorized sites or used for malicious purposes whereby the secrecy and confidential healthcare services to patients become compromised. Unauthorized access to the IOTT infrastructure.

Rootkits: particularly dangerous because it operates at the deepest levels of the system that makes it difficult to trace and delete. Once it roots into the system, it could control the device function, hide its presence, and provides access for cyber criminals that enables them in controlling IOMT devices or stealing sensitive information. Software transfer risk.

Virus: These viruses can wipe out the mode of operation of IOMT devices, which may lead to hardware or device failure. They can also be so programmed for propagation over the networks of IOMT computers; many devices can be infected via them, and tremendous damage or even loss of data can be caused.

Key-loggers: Key-loggers are a type of malware meant for recording every keystroke a user inputs in a compromised IOMT device. This includes admission certificates, medical records amongst others. The Keystrokes are transmitted to criminals who can take advantage of the information to steal, commit fraud amongst other crimes. Key-loggers are a big threat in the security of patient data

Ransom-ware: Ransom-ware threatens the IOMT system. It encrypts important medical information and then demands a victim to pay for a decryption password. Ransom-ware infection into IOMT devices or systems causes significant disruptions of health care delivery systems and also affects patient safety and care. Most of the time, paying the ransom provides a false hope of retrieving data, and it encourages further crime. The three types, or properties, are impacted in DDOS attacks, which distinguish them from other cyber-attacks: availability, scale and scope, easy access, camouflage capability, financial disruption, and difficulty in mitigation. In DDOS attacks, certain websites or online services are targeted to be flooded with so much traffic so as to prevent the access of genuine users for a certain period.

These attacks can be carried out at a large scale using many different interception devices, creating big tools that can even disrupt the most powerful devices. DDOS attack tools and services are easy to acquire and may be utilized by people with technical skills. Further, DDOS attacks can be used as a distraction campaign, leaving the security teams distracted from other attacks taking place simultaneously. The financial impact of DDOS is that it leads to loss, reputational damage, and the overall loss of customer trust. DDOS attacks are difficult to mitigate since it is a big challenge to filter out malicious traffic without harming legitimate traffic. In general, the importance of DDOS attacks is in their ability to disrupt online services, effectiveness, and challenges related to prevention and mitigation.

B. DDOS ATTACK

A DOS attack would be defined as an attack that is meant to render a computer or network incapable of providing normal services. A DOS attack is said to only occur if access to the computer or network apparatus is intentionally blocked or corrupted through malicious actions of other users. Though these attacks may not cause damage to data immediately, or permanently, they do interfere with currently available resources. DOS attacks fall into several categories.

Network device level: DOS attacks involve the exploitation of a software bug or hardware device failure attempt at the network device level.

Operating system level: At the operating system level, DOS attacks exploit how the operating system makes use of the protocols.

Application- based attacks: Most attacks try to break systems or services by employing specially designed viruses running on the target host or by using these applications to steal resources from their victims.

Data Flooding: An attacker may try to increase the available bandwidth of a network, host, or device by sending too much data, which creates too much data.

Signature based attacks: Where dos uses some signature patterns, some attacks exploit the fact that the P address can be spoofed.

The attack uses multiple computers to launch a coordinated DOS attack against one or more targets. Criminals can exploit DOS by utilizing client-side Ewer technology to compromise resources of many conflicting computers running the attack platform. A DDOS attack comprises four components, as illustrated in Figure 2: The true attacker. The owner or host of the infected host can control

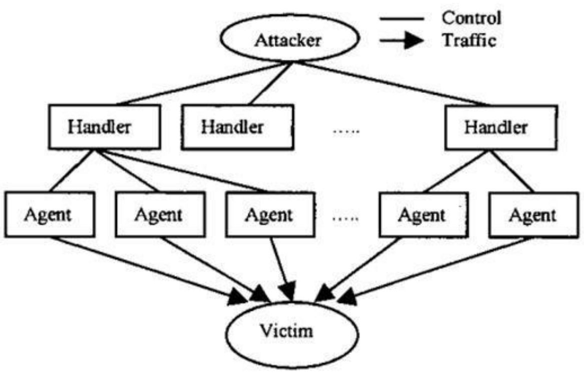
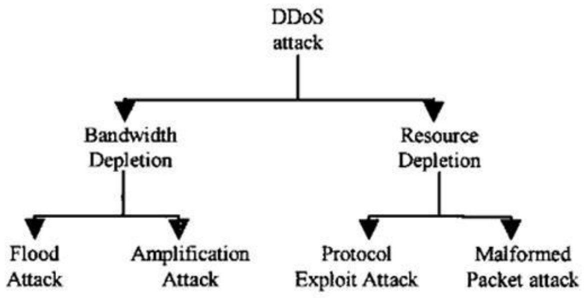


Figure 3- Architecture of DDoS attack



Many agents. The attack agent daemon, or bot generates packets to be sent to the victim. Victim or target host. Compromise: An attacker exploits a vulnerability in the domain and places code while avoiding detection and weakening it. Communication: Agents notify protesters through activists that they are ready. Attack The attacker orders the attack. It gets increased risk by powerful and powerful DDOS tools used by potential attackers that increase the risk to be victimized by a DOS or DDOS attack. Some of the most famous DDOS tools include Trinoo, TFN, Stcheldraht, TFNZK, mstream, and Shaf. Classification of DDOS attacks There are two main categories of DDOS attacks. Those are as illustrated in Figure 3:

Bandwidth exhaustion attacks and resource logging attacks. Bandwidth exhaustion attacks are used to overload the victim's network with unnecessary traffic, thereby preventing legal traffic from reaching the victim's physical system.

Bandwidth attacks can be sub-categorized into flood attacks and mass attacks. A workout attack is an attack meant to tie up the victim's resources.

This attack can be classified into two broad categories: malicious protection techniques and malicious packet attacks. DDOS attacks can be further classified into two broad categories: direct attacks and indirect attacks. The direct attack was discussed in the previous section.

A reflector is an indirect, intermediate node used to fire the launchers. A reflector is an IP host that sends a packet and returns it. The first classification separates DDOS defense systems according to the functions used, and the second classification separates DDOS defense systems according to where they are deployed. In the first category, we are going to describe DDOS protection in detail while in the second category we would just touch on DDOS protection as well as deployment.

C. ESSENTIAL DDOS ATTACK TOOLS

A. h-ping: h-ping is a command line for TCP/IP packet analysis/testing. Things you can do with this tool include: firewall testing, advanced port scanning, network testing using different protocols, and more.

B. Rudy (R-U-Dead-Het): This uses HTTP requests to send long messages using long content. This dynamic tool provides the user with an environment that uses only the target's URL. The victim's server is bombarded with frequent HTTP requests. It can handle 256 sessions at a time.

D. Low Orbit Ion Cannon (LOIC): It sends HTTP requests at a rate that is extremely high and makes the victim's system fail. The main disadvantage of the main attacker is that it does not hide the identity because it does not spoof the IP address of the user and the agent.

E. Hyenae: It is a network generator package that is flexible and used to detect vulnerabilities in the network.

This paper proposes a method to detect DDOS attacks faster by splitting the dataset into multiple locations and distributing these elements in a Hadoop cluster for parallel processing and detection using Hadoop HDFS and Map Reduce.

It detects DDOS by counting the number of requests received by IP addresses other protocols, including ICMP, TCP, and HTTP, which uses a counter-based algorithm for the count to have reached a threshold in a specified time frame if it exceeds it. The IP address will then be declared an attacker and blocked temporarily or permanently basing on the detailed information on the attack. However, sometimes, the DDOS attacks are not noticed since the specific malicious code is emulating a valid user and sends traffic that does not breach the legitimate domain within the given window. Therefore, we introduce another technology based on multi-window peak analysis to boost the efficiency of detection. The paper also has the contribution of using time estimation techniques in early detection of IP addresses that may be part of a DDOS attack. The short period may go up to one minute. Based on packets sent by a source in a one-minute window, we perform an estimation process based on time series analysis in order to predict the IPs to be blocked in the near future. Now, once the potential attackers are identified, traffic from that specific IP can be monitored because specific logs would have been created about that IP.

Covid-19

It is the novel coronavirus, COVID-19, which is brought about by a hitherto known extreme respiratory syndrome coronavirus 2, and it has swept across the globe. Other than asymptomatic infections, another factor that fosters the proliferation of the virus is massive testing in light of the limited supply of personal protective equipment for health care workers. Patients with COVID-19 infection expressed the need to understand clinical, radiological, and diagnostic factors related to morbidity and mortality. The following is an update providing early demographic, clinical, disease, immunological, hematological, biochemical, and radiological factors that may be associated with severe injuries caused by COVID-19 infection. In this study, we classify the WHO definition of severe pneumonia in classifying severe pneumonia. Up to May 27, 2020, the latest clinical guidelines set by the WHO defined as "severe disease" in adults patients with symptoms of pneumonia such as fever, shortness of breath, cough, and dyspnea combined with at least one of the following: ¿30 breaths/minute, severe respiratory distress or failure; Based on evidence from non-controllers, the D614G mutation in the S (viral) protein appears in European and American, but not Chinese, strains of the disease and facilitates transmission.

Pathology can significantly help the physicians better stratify their patients, self-treat their patients, monitor treatment, and allocate appropriate resources to all levels of care with a view to reducing morbidity and death. Here, we review the current literature on factors that have been suggested as determinants of COVID-19 severity and mortality.

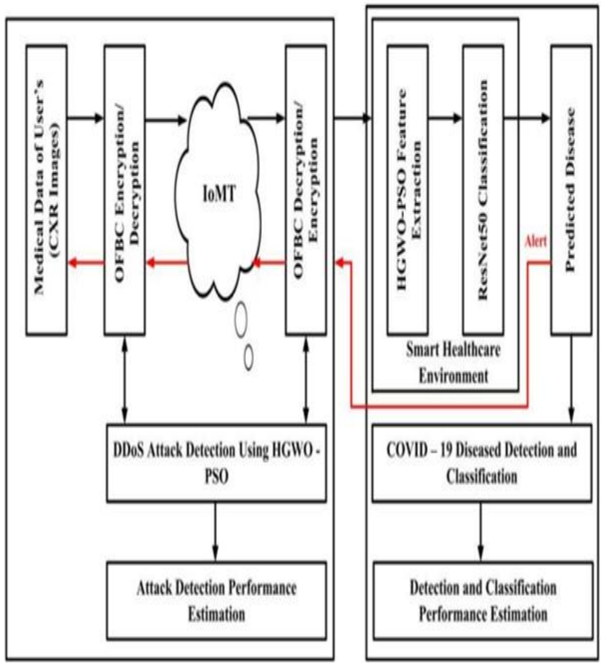
2. METHODOLOGY

With the impact of Covid19 on every nook and corner of the earth, there is an enormous surge in online activities like virtual online dating, online education, online medical consultation, and more. This invention presents a new opportunity for attackers or hackers to attack medical information that is transmitted over the Internet, known as IOMT (Internet of Medical Things). Currently, there are no detection and mitigation tools. Use deep learning techniques to select relevant features to identify diseases or image classification. Because of the structure of medical images, nothing seen can even possibly be known or identified by the attacker. This algorithm transforms the image pattern block by block using XOR operation and then creates an encrypted image. Optimization is done using PSO algorithm with a selection or extraction process of relevant features, then ignore irrelevant features. Then the actual value is calculated by training and applying the model to the new measurement image. Accuracy can also be referred as Attack Detection Accuracy (ADA), Attack Detection Time, and Attack Detection Reduced Error

Rate (ADER).

Following this, we are extracting features from the trained model of ResNet50 and rettrain it with the random forest distribution to obtain a hybrid classification model. ResNet50 is said to optimize removing processes, and by doing so, optimization may also help in the case of other classifiers in order to get good accuracy. The random forest was trained with Hybrid ResNet50 features and achieved 100 percent accuracy. The need for proper messaging during the pandemic is immense, as misinformation or delayed information spreading may culminate in fear and panic. An attack like DDOS has been employed by the attackers to target the governments and media houses, causing undue panic. One such example is when the virtual portal of the Australian government known as my-Govt was hacked by a DDOS attack and became unavailable to use for the residents, which elicited frustration and anxiety.

More and more, healthcare is depending on digital technology, and information technology is relied on by doctors and nurses as well as researchers to more effectively manage patients and address many contagious issues. Medical facilities have not been immune to insurgent attacks during the COVID-19 pandemic, rendering the health facilities less capable of tending to many persons in need. Even the research hospitals for COVID-19-for example, in France and the Czech Republic - were not immune to DDOS attacks.


Medical Data of User's (CXR Images)
OFBC Encryption/ Decryption
IoMT
OFBC Decryption/ Encryption
HGWO-PSO Feature Extraction
ResNet50 Classification
Predicted Disease
Alert
Smart Healthcare Environment
DDoS Attack Detection Using HGWO - PSO
COVID – 19 Diseased Detection and Classification
Attack Detection Performance Estimation
Detection and Classification Performance Estimation

For instance, the exposure of HHS departments to unknown DDOS attacks has brought out the vulnerability that exists in hospitals. Figure 3 illustrates the approach that the ICDC-Net gives, where the encryption and classification techniques are employed to combat such issues.

This method offers the strongest encryption in terms of protecting patient data.

Step1- The medical data of the users CXR images were encrypted using OFBC, which gives the best security that is available for data about patients.

Step2: HGWO-PSO model for detecting DDOS attacks in an IOMT environment

Protect OFBC against various kinds of attacks, particularly DDOS attacks

Step4: Then send them to the IOMT environment via the gateways that are respectively implemented to the Internet such as (UDP, WLAN, etc.).

Step 5: Sent the IOMT data directly to the physician(s).

Step 6: Used smart clinic as an intelligent tool for data analysis.

Step 7: The CXR image based on COVID- 19 will undergo HGWO-PSO processing to give a particular disease signature.

Step 8: Classifies the different diseases based on CXR images with the help of ResNet50 model including common diseases, COVID-19, and pneumonia.

Step 9: Using the same IOMT gateway send the predicted results to the patient Two-step process

3. Planning process

Step 1: Encrypting user's CXR image using OFBC to increase security in data of the associated patient. DDOS attack on HGWO-PSO

Step 2: OFBC method for the attack of all type attacks. These type attacks are DDOS attacks.

Step 3: Data analysis is created as an intelligent tool for smart clinics.

Step 4: Utilize ResNet50 model to detect common viruses, COVID-19 and pneumonia diseases using CXR images.

DDOS attack prediction HGWOPSO optimization OFBC encryption mechanism for medical information:

COVID-19, especially CXR images, stores such medical information and DDOS attacks, attack services or resources so that that information is unavailable to users. Even encryption mechanisms might be problematic for DDOS attacks as the attackers will have a hard time accessing data. It will also prevent the attacker to tamper with the system encryption, and hence the attacker's chances of breaking into this system are close to zero. It can be used to detect and prevent DDOS attacks because it may be able to help identify different patterns in traffic that indicate an attack. It can also be used to limit how much bandwidth the attacker is allowed to consume, which can cause the system to flood under too much data. Symptoms of DDOS-based attacks include slow website response times, increased server errors, and increased bandwidth consumption. A DDOS attack can be used for data theft, disruption of services, and disruption of online transactions. DDOS attacks also prove to be expensive by the loss in monetary terms because of downtime, loss of customers, and loss of business due to lower revenue. Further, reputation of a smart healthcare company is also damaged because customers cannot get access to the website or services of the company because of an attack. Character. The optimization algorithm to balance the fitness cost of all access paths for addressing the problem due to DDOS attacks in D-dimensional space is HGWO-PSO. This allows the application of the HGWO-PSO method in tracking the best path with network information against a potential attack.

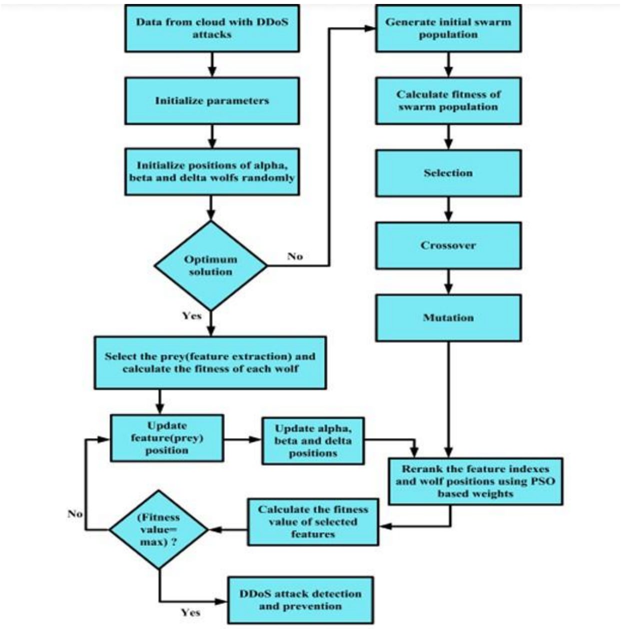
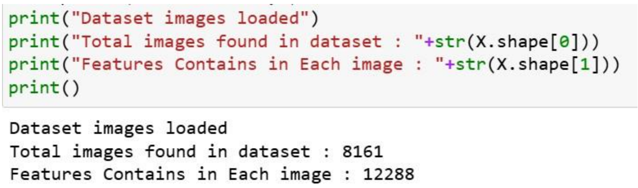

Data from cloud with DDoS attacks
Initialize parameters
Initialize positions of alpha, beta and delta wolfs randomly
Optimum solution
No
Yes
Generate initial swarm population
Calculate fitness of swarm population
Selection
Crossover
Mutation
Select the prey(feature extraction) and calculate the fitness of each wolf
Update feature(prey) position
Update alpha, beta and delta positions
Rerank the feature indexes and wolf positions using PSO based weights
Calculate the fitness value of selected features
(Fitness value= max) ?
No
Yes
DDoS attack detection and prevention

FIGURE 3.2 Flowchart of HGWO-PSO-based DDoS attack detection.

The HGWO-PSO concept is used in the design of a metaheuristic method to enhance the diversity of multi-attack vectors in the scenario of the DDOS attack problem. It supports the use of the HGWO-PSO method solving the DDOS attack problem through data collection, ensemble learning, and optimization. Step One: Network topology design In this paper, we mainly focus on network security management, particularly the security management of network services. With the help of the experimental study of the model, a service-oriented network topology is designed and constructed. The network topology is prepared on a random graph based on the Waxman test protocol. Testing the proposed topology is done with a limited number of packets and by using the classical HGWO-PSO method to generate the attack path. Step 2: Calculate health benefits of the plausible approach: The design phase guarantees that all elements of the population get their chances to probe in detail at all times t that are scheduled by the optimum position of its neighbors. This enables the swarm to reconstruct the best path from the sink towards the attack area. The team will determine stochastic search strategies, evaluate and pick the best one using some methods. People go through this process until no more cases are left. Therefore, all of the health values of all the nodes along each route have been used in computing the optimal route from the sink to the stop. Based on that, the new location on the route is evaluated to decide whether to include that item in a particular class. In such case, the calculation would be the point on the connecting path from the best job in the world to the current best job. Usage fees are calculated for registration in the network. Recovery method: Adopt the atomic group, create a road from the pool to the attacker, and make use of HGWO-PSO to solve the problem of a DDOS attack.

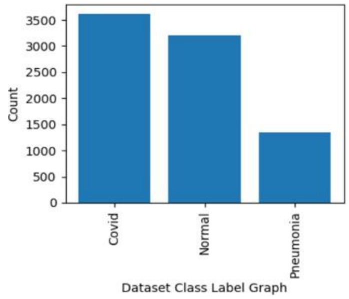
4. RESULT

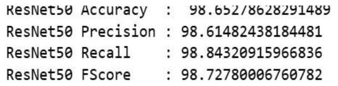


```
print("Dataset images loaded")
print("Total images found in dataset : "+str(X.shape[0]))
print("Features Contains in Each image : "+str(X.shape[1]))
print()
```

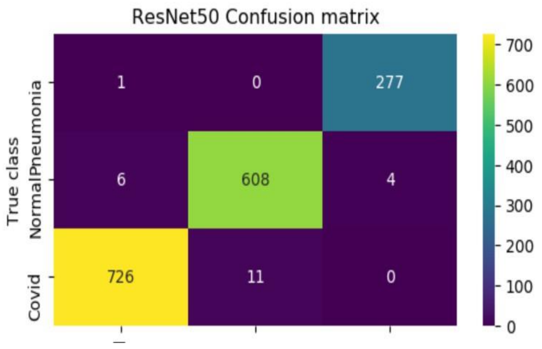
```
Dataset images loaded
Total images found in dataset : 8161
Features Contains in Each image : 12288
```

In below picture displaying graph of different class labels where x-axis represents label names and y-axis represents number of images under that class label

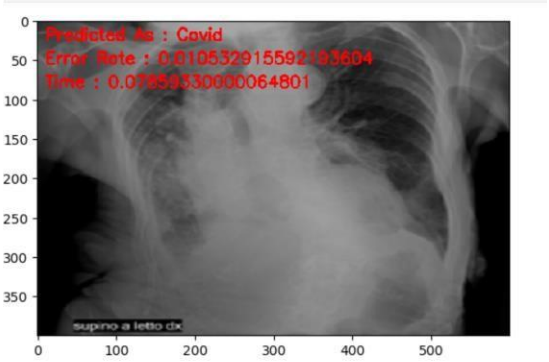




```
ResNet50 Accuracy  :  98.65278628291489
ResNet50 Precision : 98.61482438184481
ResNet50 Recall    : 98.84320915966836
ResNet50 FScore    : 98.72780006760782
```



In above screen ResNet50 got 98.71% accuracy closer to 99% and can see other metrics like precision, recall and FSCORE. In confusion matrix graph x-axis represents ‘Predicted Labels’ and y-axis represents True Labels and then all different colour boxes in diagonol represents correct prediction count and remaining blue boxes represents incorrect prediction count which are very few



```
Predicted As : Covid
Error Rate : 0.010532915592193604
Time : 0.0785933000064801
```

In above screen calling predict function with test image path and then in RED colour text can see image predicted as 'Covid19' along with error rate and prediction time

5. CONCLUSION

We propose, for the first time, a COVID-19 detection and distribution network based on IOMT for smart healthcare applications. In this work, we incorporated several factors that would help enhance the safety and accuracy of COVID-19 diagnosis. We also introduced OFBC encryption to ensure confidentiality in patient medical information, especially the CXR data involved in the COVID-19 testing process. Using OFBC encryption technology to support protecting sensitive data. We improve the FBC encryption and decryption process using HGWO-PSO. Therefore, this technology not only improves security in transmitting data but also helps identify and predict DDOS attacks, thereby enhancing the totality of security. To precisely find the disease, we propose an application to extract specific diseases from COVID-19 CXR data with the help of HGWO-PSO. We will be presenting multiple natural conditions results of the deep learning model of ResNet50, that is, COVID-19 and pneumonia-related diseased cases. Our proposed model gives more accuracy, sensitivity, specificity, f1 score, precision, and return values than the existing models. In an experiment, we demonstrated the effective enhancement of

ADA, ADT, and decreases ADER compared to existing security standards. Our work will pave the way for further research. Future Directions Therefore, future directions will include the allotment of additional resources for various types of DDOS attacks and will include the distribution of CXR images. Healthcare application is an application where the security and deployment of ICDC- Net will have a major impact on patient care. And the scalability of design concept of ICDC-Net architecture should be validated because the whole global healthcare system will need to change the model in re-managing and managing big data. In addition, the work should aim at real issues of actual deployment for ICDC-Net, such as integration with healthcare IT infrastructure, management problems, and problems related to data privacy and security. Finally, it will have its model improved with continuous improvement in deep learning and optimization to more broadly bolster the ICDC-Net's robustness and performance in general and make it a tool in machine learning toward disease prevention and all sorts of health-related problems.

REFERENCES

[1] Z. Y. Zu, M. D. Jiang, P. P. Xu, W. Chen, Q. Q. Ni, G. M. Lu, and L.J. Zhang, "Coronavirus disease 2019 (COVID-19): A perspective from China," Radiology, vol. 296, no. 2, pp. E15–E25, Aug. 2020.

[2] A. Bernheim, X. Mei, M. Huang, Y. Yang, Z. A. Fayad, N. Zhang, K. Diao, B. Lin, X. Zhu, K. Li, S. Li, H. Shan, A. Jacobi, and M. Chung, "Chest CT findings in coronavirus disease-19 (COVID-19): Relationship to duration of infection," Radiology, vol. 295, no. 3, Jun. 2020, Art. no. 200463, doi: 10.1148/radiol.2020200463.

[3] L. Wang, Z. Q. Lin, and A. Wong, "COVID-net: A tailored deep convolutional neural network design for detection of COVID-19 cases from chest X-ray images," Sci. Rep., vol. 10, no. 1, Nov. 2020, Art. no. 19549.

[4] T. Ozturk, M. Talo, E. A. Yildirim, U. B. Baloglu, O. Yildirim, and U. Rajendra Acharya, "Automated detection of COVID-19 cases using deep neural networks with X-ray images," Comput. Biol. Med., vol. 121, Jun. 2020, Art. no. 103792, doi: 10.1016/j.compbiomed.2020.103792.

[5] A. I. Khan, J. L. Shah, and M. M. Bhat, "CoroNet: A deep neural network for detection and diagnosis of COVID-19 from chest X-ray images," Comput. Methods Programs Biomed, vol. 196, Nov. 2020, Art. no.105581, doi: 10.1016/j.cmpb.2020.105581.

[6] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDOS) Flooding Attacks," in IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter 2013.

[7] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDOS attack," 2014 6th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 143-147.

[8] B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDOS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIA.Com), New Delhi, 2015, pp. 342-346.