International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7991
***Article Received**: 12 May 2023 **Revised**: 15 July 2023 **Accepted**: 05 August 2023*

Enhancing Security in Internet of Healthcare Application using Secure Convolutional Neural Network

Sanjeev Singh[1], Amrik Singh[2*], Suresh Limkar[3]
[1]Department of Electronics and Communication Engineering, M.B.S. College of Engineering and Technology, Jammu, Jammu and Kashmir, INDIA
[2*]Department of Computer Science & Engineering, M.B.S. College of Engineering and Technology, Jammu, Jammu and Kashmir, INDIA
[3]Department of Artificial Intelligence & Data Science, AISSMS Institute of Information Technology, Pune, Maharashtra, INDIA
sanjeevsinghtara@gmail.com[1], amrik.singh@mbscet.edu.in[2*], sureshlimkar@gmail.com[3]

Abstract: The ubiquity of Internet of Things (IoT) devices has completely changed the healthcare industry by presenting previously unheard-of potential for remote patient monitoring and individualized care. In this regard, we suggest a unique method that makes use of Secure Convolutional Neural Networks (SCNNs) to improve security in Internet-of-Healthcare (IoH) applications. IoT-enabled healthcare has advanced as a result of the integration of IoT technologies, giving it impressive data processing powers and large data storage capacity. This synergy has led to the development of an intelligent healthcare system that is intended to remotely monitor a patient's medical well-being via a wearable device as a result of the ongoing advancement of the Industrial Internet of Things (IIoT). This paper focuses on safeguarding user privacy and easing data analysis. Sensitive data is carefully separated from user-generated data before being gathered. Convolutional neural network (CNN) technology is used to analyse health-related data thoroughly in the cloud while scrupulously protecting the privacy of the consumers.The paper provide a secure access control module that functions using user attributes within the IoT-Healthcare system to strengthen security. This module strengthens the system's overall security and privacy by ensuring that only authorised personnel may access and interact with the sensitive health data. The IoT-enabled healthcare system gets the capacity to offer seamless remote monitoring while ensuring the confidentiality and integrity of user information thanks to this integrated architecture.

Keywords: Secure Convolution Neural Network, Internet of Things, Healthcare, Security.

I. INTRODUCTION

Wireless sensor network (WSN) usage has increased and reached previously unheard-of levels. The scalability, interoperability, and user interface of WSN, as well as data processing, have improved. The Internet of Things (IoT) was made possible by technological advancements in wireless networks, mobile devices, and radio frequency identification (RFID). The phrase "Internet of Things" (IoT) was first used in 1999 to describe how the supply chain was managed. In this connected world, each individual has a unique digital identity and is all connected to one another via the internet. These items that can be remotely managed, arranged, and maintained produce a universe of intelligent objects with a wide range of applications, including crowdsourcing, intelligent agriculture, and healthcare.There are still a number of challenges that prohibit IoT from being used effectively, despite these novel uses and technological breakthroughs. Problems with interoperability, security, big data analysis, and quality of service (QoS). Complex connections between data flow and Internet of Things objects are required for the growth of big data, a complex field. Big data analytics combined with the Internet of Things (IoT) provide a wide range of alternatives for improving decision-making and service quality. The automatic learning, which provides specialised solutions, is essential to this data analysis. Due to the adoption of automated learning methods, the economy has consequently grown significantly.

Medical data storage and processing have been complicated by the most recent pandemic. The Internet of Things (IoT) appears to be an effective option for the future of intelligent healthcare due to its capabilities for data processing, intelligent identification, and access control through the use of sensor and network technology. Together, they produce a safe, efficient, and timely health system. However, concerns about data manipulation and breaches highlight the need for secure access management, a major issue in IoT health. There are still some more outdated access control techniques that need to be improved.These challenges are resolved in a novel method by combining Susceptible Infected Recovery (SIR) with Graph Convolutional Networks (GCNs) [1]. But this does not take into account how complex user-generated social networks are. We address these constraints by offering a secure access control architecture for IoT healthcare applications. In this design, the servers for access control and trust generation are used to handle requests for data access and specific user permissions on the access control platform at the intersection. A powerful Secure Access Control Mechanism (SACM) is used by this dynamic framework, assisted by Federated Deep Learning, to provide privacy and security [2]. The likelihood that the Internet of Things will be healthy is therefore increased by creating a secure environment for a variety of medical applications [3].

The artificial intelligence, which includes machine learning (ML) and deep learning (DL) techniques, is crucial for improving medical procedures when using hospital medical data and medical devices connected to the Internet of Things (IoT). Since the spread of Covid-19 and its transmission between people, healthcare providers have used Internet-based medical devices to identify patients who are infected with the virus. In order to speed up diagnosis and treatment, a variety of fields have integrated deep learning algorithms (DL). These fields include computing tomography (CT) images, inferring ultrasound-based diagnoses, X-ray images, and compiling critical attention data. However, the more sophisticated DL methodologies have discovered significant flaws that enable criminals to compromise the security of the DL algorithms itself [21].

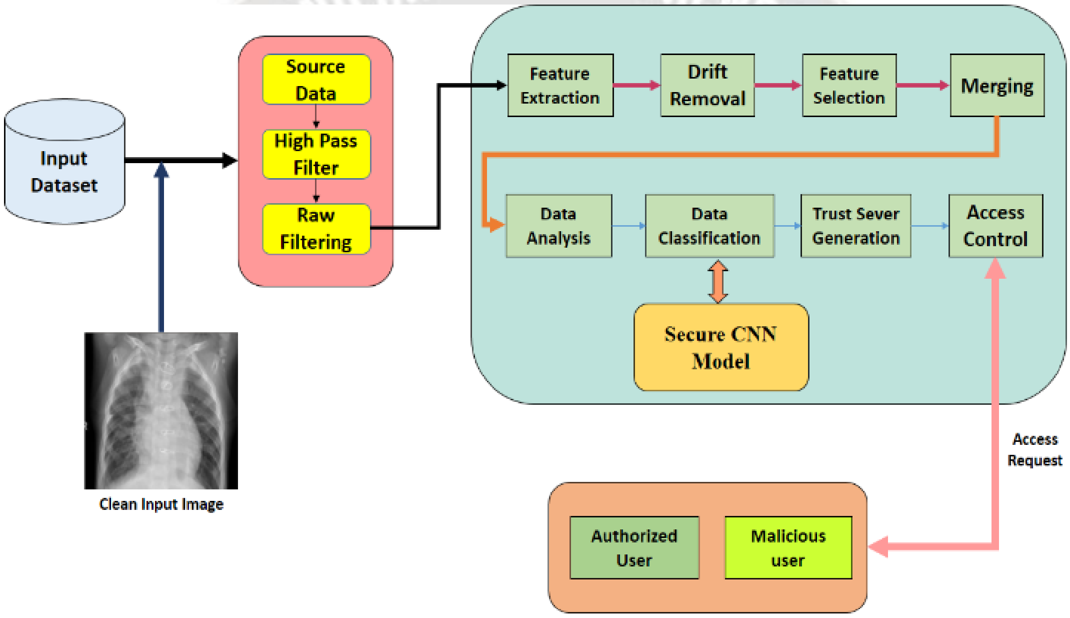

Figure 1: Proposed Secure CNN model for Healthcare application

The performance of the DL model is compromised by hostile attacks on DL algorithms that require the manipulation of data with small perturbations [22], [23]. Due to their local instability, DL models are vulnerable to these attacks since even minor entry deviations can result in seriously poor output coherence [24]. Reduce significantly the precision of the DL models, in contrast to how hostile images are invisible to the human eye when compared to non-damaging photographs [25].The number of media being used to identify hostile situations (AE) is growing steadily. These media include images, sound, and video. Previous studies have demonstrated how the AEs can affect the deep neural networks (DNN)-based recognition systems [26]. This research suggests potential defences as well. By using a support vector machine (SVM) to classify pixel values and examine the key components, a method described in [27] enables the discovery of universal perturbations that are unrelated to an image. Although research on AE tends to focus on scenes based on images, audio and language-based AE are becoming more and more popular.

Through the use of common attacks as the fast gradient sign (FGSM) and projected gradient decay (PGD), the study [28] examines adversarial resistance in the context of Covid-19 classifiers. Additionally, an attack opposed to DNN-based tasks is explained [29]. For the creation of AE and the evaluation of its effects, the authors advise using a target marker. A new technique for producing AEs using generative adversarial networks (GANs) from benign source images is also presented in [31], which moves beyond the emphasis on mimicking the benign image.Numerous strategies for combating the AE have been developed as a result of the research. According to a study [32], blockchain is used to maintain the well-known DL model characteristics and metrics. This enables the algorithm's integrity to be checked by careful users. The researchers developed a lightweight classifier AE to counteract adversarial physical attacks by using adversarial patches in audio and photographic materials [33]. To protect model characteristics, entry data, and decision-making processes using blockchain technology. The authors offer an AE defence system that can effectively fend off attacks from members-only and malicious attacker classification systems [34].

The following are this paper's main contributions:

1. We offer an upgraded neural network architecture for Internet-connected healthcare systems to secure patient data and maintain decision integrity during classification and recognition.
2. The security of these designs is strengthened via adversarial training. We also established a criterion at which the model's classification accuracy (resistance) starts to decline.
3. The study is validated through an experiment using a real-time dataset. The results of the trial carefully track, document, and examine how well the IoT-Healthcare system functions in terms of little privacy leakage and solid data integrity.

II. REVIEW OF LITERATURE

Due of their efficiency in data collection, the Internet of Things devices are attracting researchers and industry enthusiasts. The system's scalability and availability are significantly increased when these devices are linked to cloud computing. To maximise cloud resources and provide improved medical care solutions, the health sector uses machine learning (ML) and virtual machine (VM) algorithms. The applications of this collaboration in the field of health are excellent. The models without parametric assumptions provide useful alternatives in the event that sufficient or prior data are unavailable. The idea of "no-brainer computing" also helps the devices cooperate and work together with quick data transmission and response times.

The development of novel architectural designs, such as the Hierarchical Computerised Architecture (HiCH), in the health field has relied heavily on deep learning. By combining these architectures with the Internet of Things and methods like convolutional neural networks (CNN), wireless body area networks (WBAN) for wearable technologies are created. Algorithms for automatic learning such as EM, KNN, C4.5, and C5.0 are essential for the creation of decision trees, the management of missing values, and other AI-enhanced procedures in order to create effective structures or modules.

Autonomous learning algorithms are made more effective by meta-algorithms, which have grown to be powerful tools. For the purpose of resolving the access control issues in IoT-Sanitary, numerous algorithms have been developed. Yang et al.'s [4] proposal for an access control policy based on attributes and an access control policy aims to prevent the theft of encrypted medical data. Liu et al.'s [5] approach to access control is based on multiple authorities in an effort to prevent collision attacks. An access control mechanism with a final lock combined with cloud computing is presented by Roy et al. [6]. For the secure exchange of medical data, Edemacu and colleagues discuss the resistance to collaboration in access control [7].

Sun et al. [8] explain how user properties and access control protocols can be turned into distorted vectors to speed up access to the data. By using blockchain technology, Fan et al. [9] manage data exchange and access while guaranteeing user certification and denial. This discussion focuses on access issues, highlighting two key issues: establishing a specific, secure access based on user characteristics without compromising privacy and using user data to assess influence and trust.As a solution to these issues, a secure access control mechanism for Internet of Things health systems that depends on the user's characteristics is presented. The demand for IoT-connected health products is high, especially for mobile devices. One of the many applications is real-time biomonitoring with the help of surface electromyography (sEMG), another is interior RFID-based collision avoidance systems, and still another is portable retroaction systems [10,11]. It is vital that the Internet of Things (IoT)-connected health systems are protected from unauthorised access to personal information. More and more people are using methods to protect their private lives, such as blockchain-based security [12] and ECG-based identity.

In this way, the researchers in [13] developed a cutting-edge method for real-time validation. Unfortunately, this technique does not ensure the security of IoT devices. The system has had issues with the authentication process due to the complicated calculations required for the encryption of the public key, similar to [14], who proposed an authentication method for asymmetric cryptography protocols.The authors describe an innovative method for identifying adversarial disruptions that cross points of view [15]. This technique uses a support vector machine as a classifier and an examination of principal components and pixel values as features. It also suggests strong defences against the abuse of DNN-based face recognition systems. Conflicting strategies are more visible as picture and sound techniques are investigated.

Researchers have proposed the concept of targeted watermarking in order to develop evolving adversaries (EA) and tools for analysing the effects of integrated EA [16]. Contrarily, a novel method for creating adverse examples (AEs) from high-quality images is presented [17]. This is distinct from earlier techniques, which mostly focused on altering the distorted image such that it appeared smaller. A system of defence against member-based inferential attacks that aim to confuse the attacker's encoder [18].The blockchain's potential to prevent change during the stages of formation, presentation of criteria, and decision-making is up for dispute [19]. In the meanwhile, physical attacks may be stopped by a quick AE detection system for audio and visual files [20]. Numerous applications of deep learning (DL) can be found in the field of health. For instance, the FDA- and HealthPNX-approved emergency medical systems are based on DL.The likelihood of malicious attacks on medical systems is increased by the conversion of medical imaging entry points to DL-based devices. These modifications may have an impact on patient treatment plans by delaying processing or paying health insurance providers incorrectly. To deliver accurate disease prognoses, adversarial instances can be constructed, with ubiquitous adversarial disturbances achieving high success rates at a lower cost.

Table 1: Related work for healthcare application security

Method	Key Points	Limitations	Advantages	Scope
Cloud-IoT Collaboration [1]	Makes the most of cloud resources to provide better healthcare solutions.	Heavy calculations for public key encryption in authentication process	Enhanced scalability, resource utilization	Healthcare sector, medical data management
Hierarchical Computerized Architecture (HiCH) [2]	The development of Wireless Body Area Networks (WBAN) for wearable technology.	High computational complexity	Enhanced healthcare architectures, wireless networks	Wearable health devices, remote monitoring
Meta-Algorithms [3]	Increases the efficiency of algorithms for autonomous learning.	-	Improved performance, adaptability	Machine learning, algorithm enhancement
Access Control Solutions [4]	IoT-Healthcare access control difficulties should be addressed.	Varying degrees of resistance to specific attacks	Robust security, controlled data exchange	Healthcare data protection, user privacy
Secure Access Control Mechanism [5]	Based on user characteristics, offers secure access.	May require significant computational resources	Enhanced privacy, precise access control	IoT-Healthcare systems, user data management
Adversarial Disruption Detection [6]	Guards against DNN-based assaults and recognizes adversarial interruptions.	Limited to specific types of attacks	Improved system security, thwarted attacks	Medical imaging systems, security enhancement
Targeted Watermarking [11]	For analysis, creates evolving enemies (eas).	May not cover all potential attack scenarios	Improved understanding of adversarial effects	Security enhancement, adversarial research
Adverse Example Generation [12]	Uses high-quality pictures to create aes.	Focuses on AEs, less attention to other attacks	Novel approach to AE generation	Enhancing defense mechanisms, adversarial research
Blockchain for Prevention [9] [19]	Prevents change while forming and making decisions.	Effectiveness subject to blockchain adoption	Enhanced data integrity, prevention of tampering	Security enhancement, data integrity assurance
Quick AE Detection System [10]	Detects aes in audio and video files quickly.	Limited to specific types of attacks	Swift AE identification, reduced vulnerability	Audio and visual data protection, security
Deep Learning in Healthcare [14]	Applications for disease detection in healthcare	Potential susceptibility to adversarial attacks	Improved disease diagnosis, advanced technologies	Medical diagnostics, disease detection
Adversarial Attacks in Medical Systems [18]	Impact on patient safety and susceptibility to hostile attacks.	May disrupt proper medical assessment	Heightened awareness, need for robust defenses	Healthcare cybersecurity, adversarial defense

III. DATASET DISCRIPTION

Chest X-rays allow us to see distinguishing features that aid in differentiating between healthy lung states and different kinds of pneumonia. The left panel of a typical, healthy chest X-ray shows a distinct image of the lungs, free from any signs of aberrant opacification or areas of concern.However, the X-ray may exhibit a distinct visual pattern when bacterial pneumonia is present, as seen in the middle panel, in figure 2. A focal lobar consolidation, which occurs when fluid and inflammatory material collect in one particular lung lobe, is a common symptom of bacterial pneumonia. White arrows in the accompanying image denote a consolidation in the lung's

DOI: https://doi.org/10.17762/ijritcc.v11i8.7991
***Article Received**: 12 May 2023 **Revised**: 15 July 2023 **Accepted**: 05 August 2023*

right upper lobe. This accumulation of tissue in the lung indicates an infection that has made a specific region of the tissue more opaque and dense.

The right panel shows in figure 2 a radiographic image of viral pneumonia, which has a significantly different radiographic appearance. Viral pneumonia typically presents with a more sporadic pattern known as "interstitial" pattern, in contrast to bacterial pneumonia. The interstitial tissues, or tissues between the air sacs, of the lung are inflamed in this pattern. Both lungs may show as cloudy on the X-ray as a result of this. The interstitial pattern illustrates the viral infection's pervasiveness throughout the lung tissues.

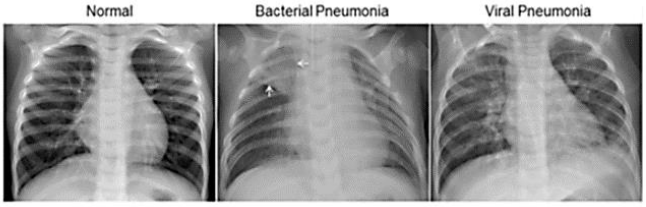

Figure 2: Examples of thoracic radiographs in patients with pneumopatia to illustrate [35]

The well-organized dataset for this analysis consists of three primary folders: "train," "test," and "val," each of which has a subfolder for each of the two separate image categories, "Pneumonia" and "Normal." The dataset consists of 5,863 chest X-ray images in JPEG format that have been divided into two categories: "Pneumonia" and "Normal."These chest X-ray photos of paediatric patients, aged one to five years, were specifically picked from retrospective cohorts. The Guangzhou Women and Children's Medical Centre in Guangzhou was where these individuals were treated.

Table 2: Description of Dataset

Attribute	Details
Dataset Organization	The dataset has three primary folders: "train," "test," and "val," each of which has subfolders for the "Pneumonia" and "Normal" categories.
Total Images	There are 5,863 JPEG photos of chest X-rays in the dataset.
Patient Cohorts	The Guangzhou Women and Children's Medical Center's paediatric patients, aged one to five, were used to create the images.
Clinical Context	The chest X-ray pictures were taken as a standard clinical procedure for the patients.
Quality Control Screening	The dataset was first screened to get rid of any poor-quality or illegible scans.
Expert Diagnosis Grading	The diagnosis for each image were evaluated and rated by two qualified doctors, which served as the foundation for AI training.
Validation Process	An evaluation set was examined by a third expert in order to confirm and improve consistency between assessments.

These photos were utilised as part of their standard clinical treatment and diagnostic techniques.An extensive screening procedure was first carried out to guarantee the calibre and dependability of the chest X-ray pictures employed in the study. The photos that were judged illegible or of low quality were eliminated during this screening. Following this stage of quality assurance, two experienced doctors evaluated the photos' diagnostic value. They were able to correctly identify the medical issues shown in the photographs because to their significant training and knowledge. The AI system was then trained using these diagnoses as a starting point.An additional evaluation process was implemented as an additional layer of quality control. The evaluation set was evaluated by a third expert doctor to confirm the findings and guarantee consistency between assessments. This validation procedure sought to reduce any possible grading inaccuracies and improve the overall accuracy of the training data for the AI system [35].

IV. PROPOSED METHODOLOGY

The suggested system architecture is thoroughly described in this section. The user, trust generation, and access control servers are three crucial components of this architecture that work together to create the framework for trust-based access control. In the context of IoT-based healthcare systems, this approach fulfils the dual purposes of preserving data integrity and protecting user privacy.A specific privacy-isolation zone is painstakingly created at the user level. This area efficiently filters out background noise and speech-related noises, allowing only non-speech body sounds and important information to be transmitted. The gait signal is painstakingly retrieved at the user's end with this design. Along with this extraction process, other crucial medical data are also obtained from the accelerated stream using the privacy-isolation zone.

A specific data extraction technique run by a non-privacy module is combined with strong security safeguards on the architecture's cloud side. Through the pipeline of data transmission and processing, this setup makes sure that the confidentiality of medical data is preserved. The potential risks of unauthorised data manipulation, data tampering, and privacy breaches loom large in IoT-based healthcare systems.

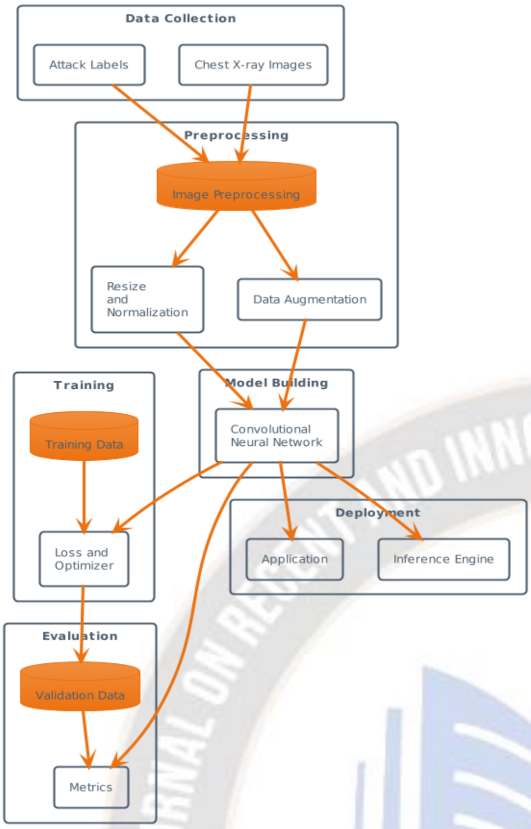

Figure 3: Different Attack Categorization using CNN

Therefore, implementing thorough security measures at every level becomes crucial.The trust generation servers are one of the key elements of this design. The estimate of trust levels for various system users is the responsibility of these servers. The access control server can make well-informed decisions about data access rights thanks to the trust assessments that these servers give. Users who are new to the system are initially viewed as untrusted individuals in this dynamic. The data sent by the trust generation and access control servers is categorised as semi-trusted, showing a level of mutual dependability, as data interactions proceed and confidence is gradually developed.At the data source, a special privacy-isolation zone is created in order to guarantee complete data security and privacy protection. In order to construct a secure channel for data transfer and potential cloud-based storage, this zone is specifically created to receive and separate non-speech body noises and related data. The deep convolutional neural network (CNN) technique is used at the cloud endpoint in a sophisticated modification. The basis for data extraction and handling is this algorithm, along with a security module housing access control and trust generating servers. For all medical data, this integrated approach ensures end-to-end privacy protection.

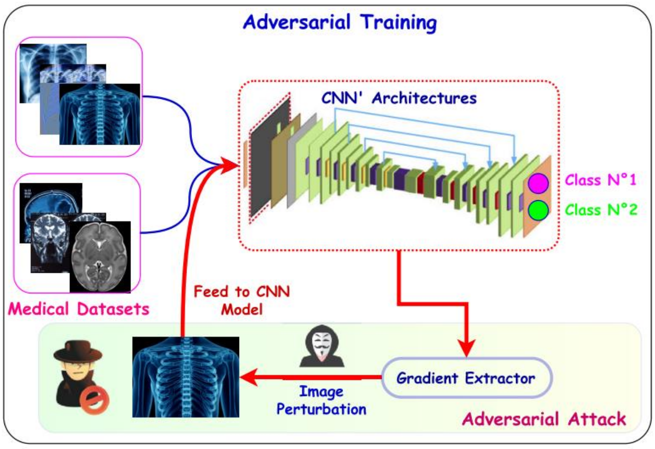

Figure 4: Adversarial Training Model

Under simulated privacy leakage and data tampering attack scenarios, the suggested system's robustness is put to rigorous testing. This empirical analysis gives a measurable estimate of how well it performs under pressure, demonstrating its resilience under difficult circumstances.It's important to recognise that a user's identity, linked to information about their unique gait, is frequently entangled within a larger dataset that includes gestures, motions, and other health-related data collected by wearable devices at the user's end. This combination of data, however, creates a possible vulnerability that malevolent individuals could take advantage of to extract the gait information and associated identification if they manage to acquire unauthorised access to the cloud-stored data. A vital step is added before data is uploaded to the cloud in order to prevent this problem from occurring.Data is carefully analysed and segmented within the privacy-isolation zone before being sent to the cloud. This rigorous procedure entails changing the signal values outside of predetermined limits. In particular, the regions outside the boundary are set to zero, while the parts inside the boundary are kept using a sophisticated smoothing window function. The gathered signal is multiplied by the signal inside the defined border during this operation, efficiently separating the important data and preserving the accuracy of the data. With this complete strategy, the risk of unauthorised access or compromise is reduced while data protection is strengthened.

A. Convolution Neural Network:

Convolutional neural networks (CNNs) have excelled in a number of fields, including cybersecurity, computer vision, and natural language processing. CNNs can be extremely helpful in protecting sensitive medical data and guaranteeing patient privacy when it comes to boosting security in Internet-of-Healthcare Applications (IoT-Healthcare).IoT-Healthcare security is improved via CNNs: Strong anomaly detection systems are developed by CNNs to identify unusual data patterns that could indicate security breaches. Alerts are set off by unusual data access or unauthorised efforts.Medical image security is achieved via CNNs, which also maintain diagnostic accuracy by detecting tampering. Picture integrity is guaranteed through picture categorization, segmentation, and anomaly detection.Secure Access Control, Biometric authentication uses CNNs to grant authorised users access to vital medical devices and data while blocking unauthorised entry.CNNs develop intrusion detection systems, which analyse network data for hostile activity and launch prompt responses.Keeping your information private, CNNs process data at the edge, transmitting only pertinent data to the cloud. Essential diagnostic features are transmitted while protecting patient privacy. Secure Data Transmission, by including encryption and decryption operations, CNNs improve data transmission security and provide strong security during IoT-cloud transfers. Real-Time Threat Detection CNNs examine live patient data to find anomalies that can point to security risks or equipment failures, enhancing patient safety.Convolutional Neural Networks, which provide cutting-edge capabilities in anomaly detection, image security, access control, intrusion detection, and privacy preservation, considerably improve the security of Internet-of-Healthcare Applications. Their utilisation upholds high healthcare standards while guaranteeing the confidentiality, integrity, and availability of patient data.

Step 1: Data preprocessing

- Gather information about patients, sensor readings, and medical photos from IoT devices.
- The data should be preprocessed to eliminate noise, standardise scales, and deal with missing values.
- Divide the dataset into subsets for training, validation, and testing.

Step 2: Convolutional neural network architecture

- Consider the application and the types of input data (such as photos and sensor data) when designing the CNN architecture.

$$\mathrm{conv} = \mathrm{x} * \mathrm{W} + \mathrm{b}$$

- Build the layers: pooling layers for down-sampling, convolutional layers with filters, and fully connected layers for classification.
- After each layer, add activation functions (like ReLU) to add non-linearity.

$$f(x) = \max(0, x)$$

  Where, The ReLU function's input is represented by x in this equation. If x is larger than or equal to zero, the function returns x; otherwise, it returns zero. The CNN architecture gains non-linearity from this non-linear activation function, enabling the network to understand and represent complex relationships in the data.
- Dropout layers can be used to prevent overfitting.

Step 3: Training as a model

- Randomise the weights and biases of the CNN model.
- To calculate the gap between expected and actual classes, define a loss function, such as cross-entropy.

$$\mathrm{CrossEntropy}(y, y^\wedge) = -(y \cdot \log(y^\wedge) + (1 - y) \cdot \log(1 - y^\wedge))$$

  Where,
  - y represents the actual target value (0 or 1).
  - y^ represents the predicted probability of the positive class (output of the sigmoid activation function)
- Select an optimizer to update weights and reduce the loss function, such as Adam.

$$\mathrm{Loss} = -(y^\wedge \quad \cdot \log(y) + (1 - y) \cdot \log(1 - y))$$

  Where,
  - y is the actual target value (0 or 1).
  - $y^\wedge$ is the predicted probability of the positive class (output of the sigmoid activation function).
- Utilising the training dataset, train the model while employing backpropagation to change the weights.

Step 4: Data enhancement

- Apply transformations (rotations, flips, shifts) to training data to enhance dataset variety.
- By subjecting it to different data variations, you can avoid overfitting and improve model generalisation.

Step 5: Combat Training

- Create adversarial examples using methods like the Projected Gradient Descent (PGD) or the Fast Gradient Sign Method (FGSM).
- To increase the CNN model's resistance to attacks, train it on both neutral and adversarial samples.

Step 6: Transmission of Secure Data

- Utilise encryption and decryption techniques to safeguard data when it is being transmitted between Internet of Things devices and cloud servers.
- In order to strengthen data security against prospective assaults, use CNNs in encryption techniques.

Step 7: Detecting Intruders

- Train the CNN model to spot typical network behaviour patterns.
- Determine whether incoming data streams and network traffic are normal or suspicious by keeping an eye on them.

Step 8: Real-Time Monitoring and Alerting

- Use CNN-based anomaly detection to implement real-time monitoring of patient data and medical devices.
- Recognise any unexpected changes or anomalies that might be signs of security risks or equipment problems.
- Inform administrators or medical staff if any suspicious activity is found.

B. Performance Evaluation:

The percentage of accurately anticipated positive cases (true positives) compared to the total number of positive instances predicted is known as precision.

$$\text{Precision} = \frac{\text{Tp}}{\text{Tp} + \text{Fp}}$$

Recall determines the percentage of accurately foreseen positive situations (true positives) in relation to all positive instances overall.

$$\text{Recall (R)} = \frac{\text{Tp}}{\text{Tp} + \text{Fn}}$$

The average of recall and precision is represented by the F1-score. By accounting for both false positives and false negatives, it provides a fair assessment of a model's accuracy.

$$\text{F1} - \text{Score} = 2 \times \frac{(\text{P} + \text{R})}{(\text{P} \times \text{Rl})}$$

Instances accurately classified (including true positives and true negatives) as a percentage of all instances constitute accuracy.

$$\text{Accuracy} = \frac{\text{Tp} + \text{Tn}}{\text{Total Instances}}$$

V. RESULT AND DISCUSSION

The accuracy and different metrics of the various algorithms' diagnoses of chest diseases from X-ray pictures showed substantial differences shown in table 3. With a 97% accuracy rate and values for precision, recall, specificity, F1 score, and area under the curve (AUC) of 0.99, 0.98, 0.95, 0.97, and 0.98, respectively, the Convolutional Neural Network (CNN) demonstrated impressive accuracy. The accuracy of Random Forest (RF) was 89%, with reasonable precision, recall, specificity, F1 score, and AUC values of 0.98, 0.96, 0.91, 0.95, and 0.91. AUC of 0.96 and precision of 0.94, recall of 0.89, specificity of 0.86, F1 score of 0.94, and accuracy of 93% were all maintained via Logistic Regression (LR). Overall, these findings highlight how effective the CNN is at correctly identifying chest diseases from X-ray pictures, while the RF and LR models also displayed excellent performances, albeit with some changes in their precision, recall, and specificity measures.

Table 3: Evaluation parameter of different model on given dataset

Method	Model Accuracy	Model Precision	Model Recall	Model Specificity	Model F1 Score	Model AUC
CNN	0.97	0.99	0.98	0.95	0.97	0.98
RF	0.89	0.98	0.96	0.91	0.95	0.91
LR	0.93	0.94	0.89	0.86	0.94	0.96

The efficacy of various models in diagnosing chest disorders from X-ray pictures can be understood by comparing model precision, recall, and specificity. Out of all cases that are projected to be positive, precision is the percentage of correctly predicted positive cases. The model's accuracy in recognising positive situations without producing many false positives is indicated by a high precision. The ratio of accurately anticipated positive instances to all actual positive cases is calculated as recall, sometimes referred to as sensitivity or true positive rate. High recall indicates that a significant number of positive cases are successfully captured by the model. On the other hand, specificity gauges the percentage of cases that were accurately anticipated as negative out of all cases that were predicted to be negative. A high specificity shows how well the model can recognise negative cases without making many false negatives.

DOI: https://doi.org/10.17762/ijritcc.v11i8.7991
***Article Received**: 12 May 2023 **Revised**: 15 July 2023 **Accepted**: 05 August 2023*

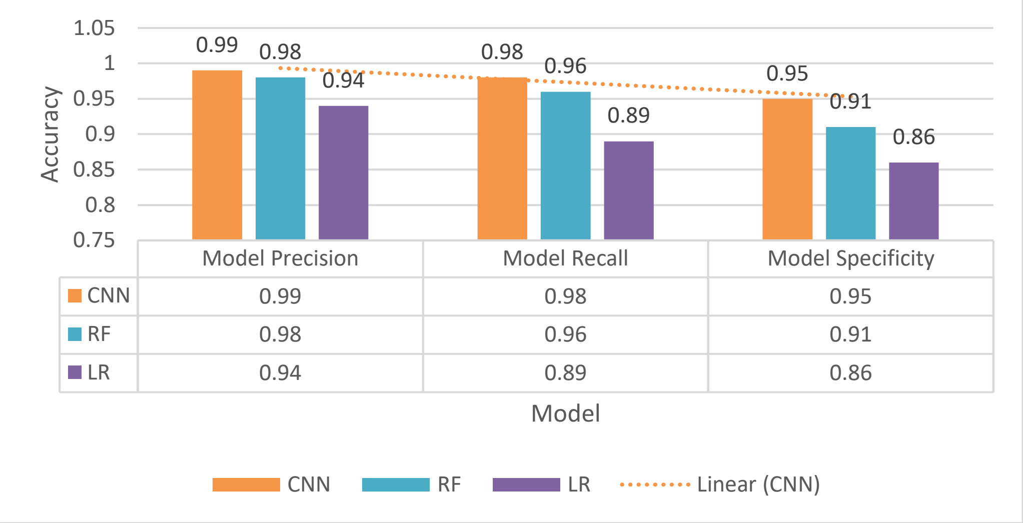

Figure 5: Comparison of Model precision, Recall and Specificity representation

The Convolutional Neural Network (CNN) clearly achieved the highest accuracy, recall, and specificity values in the comparison of model precision, recall, and specificity. This suggests that the CNN effectively collected a considerable number of true positive cases (high recall) while minimising false positives, in addition to correctly identifying positive cases (high precision). Additionally, as seen by its high specificity value, the CNN showed a noteworthy capacity for precisely identifying negative situations. Although the precision, recall, and specificity values of the Random Forest (RF) and Logistic Regression (LR) models can slightly differ, demonstrating their various trade-offs in accurately identifying positive and negative situations, these models also demonstrated reasonable performance in these metrics.

Table 4: Based on the user base, the proposed model's accuracy performance is estimated

No of User	Missed detection Rate	False rate
30	42.11	49.66
60	48.18	57.76
90	54.61	65.16
120	60.21	73.65
150	66.45	81.75
180	72.66	89.29
210	78.87	97.98

The information offered offers a quantitative assessment of a system's effectiveness based on the quantity of users, concentrating on missed detection rates and false rate. The percentage of instances where the system incorrectly missed detecting an event or condition is known as the missed detection rate. The false rate, on the other hand, is the proportion of times the system incorrectly recognised an event that didn't actually happen. The missed detection rate gradually increases with the number of users, rising from 42.11% with 30 users to 78.87% with 210 users.

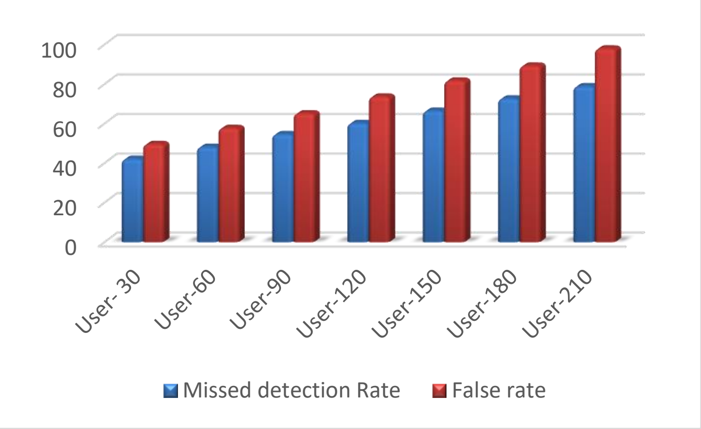

Figure 6: The proposed model's accuracy performance is estimated based on number of user data

This suggests that as the number of users increases, the system has a propensity to miss more real occurrences or situations, increasing the risk of missed detections. The difficulty in precisely finding pertinent patterns or anomalies may be related to the growing complexity of processing data from a larger user base.The false rate, on the other hand, displays a comparable growing pattern as the number of users rises. With 30 people, it starts at 49.66% and increases to 97.98% with 210 users. This means that when the system has more users, it is more likely to mistakenly identify events that didn't actually happen. The spike in false rates could be caused by variables in user behaviour, noise in the data, or a larger dataset, which could result in more instances of mistaken identifications.

***Article Received**: 12 May 2023 **Revised**: 15 July 2023 **Accepted**: 05 August 2023*

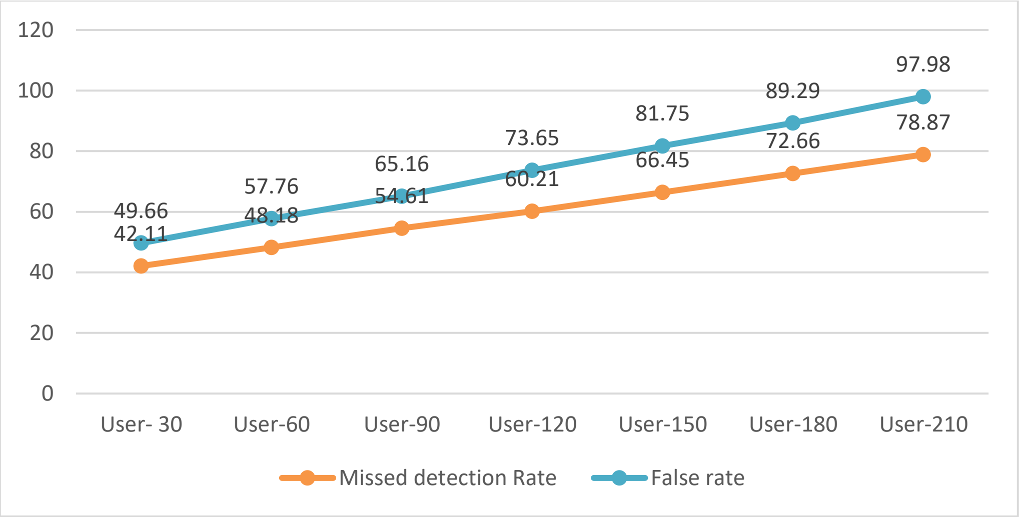

Figure 7: Comparison of False rate and Missed rate representation

Particularly in situations where detection and recognition are crucial, the comparison of false rate and missing rate offers insightful information about the effectiveness and dependability of a system. These metrics are crucial for assessing how well systems work in detecting and reacting to certain occurrences or conditions. Let's examine the importance and consequences of contrasting false rate and missing rate.The proportion of occasions where the system wrongly detects an event or condition that didn't actually happen is represented by the false rate, also known as the false positive rate. When a system raises alarms or initiates responses frequently even when there is no real reason to be concerned, this is known as a high false rate. This may undermine the system's credibility by resulting in pointless acts, resource waste, and a decline in trustworthiness.

The percentage of times the system misses a real event or condition that should have been picked up on is known as the missed rate, also known as the false negative rate. A larger missed rate suggests that the system is more likely to ignore real events, which could have serious repercussions in important applications. Missed detections may cause reaction delays, significant safety issues, and decreased overall effectiveness.It's important to balance these two variables when comparing false rate and missed rate. Often, decreasing one causes the other to rise. In building systems for purposes like security, healthcare, and anomaly detection, this trade-off is a frequent difficulty. Due to the inherent uncertainties and complexities of real-world circumstances, achieving the ideal balance may not always be possible.The ideal ratio of false rate to missed rate will vary depending on the application's needs and the particular circumstance.

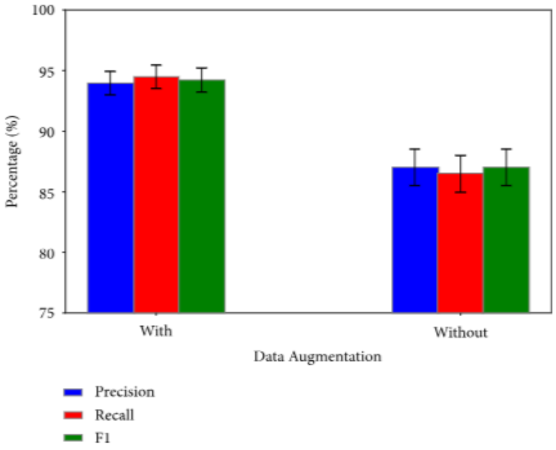

Figure 8: Estimating the suggested model's performance both with and without data augmentation

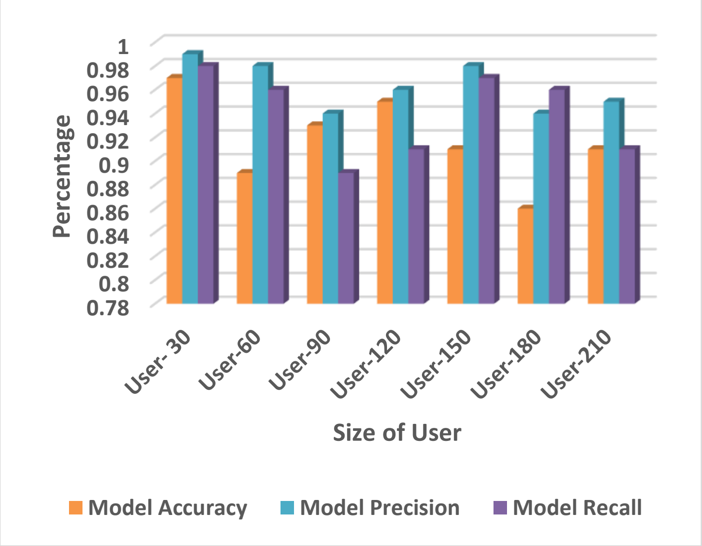

Figure 9: Estimating the proposed model's performance based on the number of participants.

For instance, security systems prioritise a lower false rate even if it means missing some real events in order to reduce unwanted alarms and replies. On the other hand, even if it results in a little higher false rate, a reduced missed rate in healthcare diagnostics is essential to guarantee that potential health risks are not missed.The comparison of the false rate and missing rate highlights the value of precision and recall in detecting systems, in the end. The correct balance must be struck carefully, taking into account the goals of the application as well as the potential repercussions of false positives and missing detections. For system performance to be optimised and accuracy to be at a level that corresponds to the intended results, a thorough grasp of these metrics is necessary.Figure 9 displays a graphical depiction that provides details on how the proposed model's performance estimation relates to the number of participants. This type of analysis is particularly pertinent in situations where user engagement levels have an impact on system efficacy. The graph probably illustrates how specific performance indicators, such accuracy, detection rates, or efficiency, change as the number of participants rises.The graph's y-axis displays the performance metric being assessed, while the x-axis shows the total number of participants. This measure could be anything from processing speed to detection accuracy, or it could be any other pertinent characteristic.

VI. CONCLUSION

Internet of Things (IoT) device integration has resulted in revolutionary improvements in the field of healthcare technology. Convolutional neural networks (CNNs) have tremendous potential for improving security in IoT-healthcare applications. CNNs, which are well-known for their effectiveness in a variety of fields, can be crucial in preserving private patient information and protecting sensitive medical data.The detection of deviations from established patterns is made possible by CNNs, which find useful applications in this field. This is crucial for identifying possible security lapses or unauthorised data access. By spotting tampering and guaranteeing the accuracy of diagnostic pictures, CNNs also excel at medical image security. Only authorised people are allowed access to sensitive patient data thanks to the application of CNNs in biometric authentication, which provides safe access control. CNNs allow for real-time monitoring of IoT-healthcare networks and can notify stakeholders of irregularities. The CNN-based edge processing of medical data further protects patient privacy by lowering the likelihood that sensitive information would be revealed while being transmitted. Through the use of encryption and decryption methods, CNNs can further improve the security of data transmission.The performance differences between different models are revealed by comparing model precision, recall, specificity, and other metrics. For choosing the best model for certain healthcare applications, these insights are quite helpful. The relationship between system performance and scalability is further demonstrated by the analysis based on participant count. The implementation and design of the model must be optimised using these insights.Ultimately, CNNs prove to be a crucial instrument for increasing the security architecture of IoT-Healthcare applications. They are prepared to revolutionise patient data protection thanks to their expertise in anomaly detection, medical picture security, secure access management, intrusion detection, and privacy preservation. Stakeholders can decide how to best use the system by analysing participation counts and model performance data. In order to meet the growing difficulties of security and privacy in IoT-Healthcare applications, CNN integration offers a comprehensive solution as the healthcare industry continues to change.

REFERENCES

[1] O. Keskes and R. Noumeir, “Vision-based fall detection using st-gcn,” IEEE Access, vol. 9, pp. 28224–28236, 2021.

[2] J. de Batlle, M. Massip, E. Vargiu et al., “Implementing mobile health–enabled integrated care for complex chronic patients: intervention effectiveness and cost-effectiveness study,” JMIR mHealth and uHealth, vol. 9, no. 1, article e22135, 2021.

[3] H. Bolhasani, M. Mohseni, and A. M. Rahmani, “Deep learning applications for IoT in health care: a systematic review,” Informatics in Medicine Unlocked, vol. 23, article 100550, 2021.

[4] Y. Yang, X. Liu, and R. H. Deng, “Lightweight break-glass access control system for healthcare Internet-of-Things,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3610–3617, 2018.

[5] J. Liu, H. Tang, R. Sun, X. Du, and M. Guizani, “Lightweight and privacy-preserving medical services access for healthcare cloud,” IEEE Access, vol. 7, pp. 106951–106961, 2019.

[6] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, “Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications,” IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 457–468, 2019.

[7] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.

[8] B. Jang, and J. W. Kim, “Collaborative Ehealth privacy and security: an access control with attribute revocation based on OBDD access structure,” IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 10, pp. 2960–2972, 2020.

[9] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, and R. H. Deng, “Lightweight and privacy-aware fine-grained access control

for IoT-oriented smart health," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6566–6575, 2020.

[10] K. Fan, Q. Pan, K. Zhang et al., "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5826–5835, 2020.

[11] F. Al-Turjman and B. Deebak, "Privacy-aware energy-efficient frame-work using the Internet of Medical Things for COVID-19," IEEE Internet of Things Magazine, vol. 3, no. 3, pp. 64–68, 2020.

[12] M. Shariq, K. Singh, M. Y. Bajuri, A. A. Pantelous, A. Ahmadian, and M. Salimi, "A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario," Sustainable Cities and Society, vol. 75, article 103354, 2021.

[13] G. S. Gunanidhi, "Extensive analysis of Internet of Things based health care surveillance system using Rfid assisted lightweight cryptographic methodology," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 10, pp. 6391–6398, 2021.

[14] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, ''Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks,'' IEEE Trans. Ind. Informat., vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[15] H. Yeh, T. Chen, P. Liu, T. Kim, and H. Wei, ''A secured authentication protocol for wireless sensor networks using elliptic curves cryptography,'' Sensors, vol. 11, no. 5, pp. 4767–4779, May 2011

[16] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2951

[17] A. Agarwal, R. Singh, M. Vatsa, and N. Ratha, ''Are image-agnostic universal adversarial perturbations for face recognition difficult to detect?'' in Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Oct. 2018, pp. 1–7

[18] Z. Yahya, M. Hassan, S. Younis, and M. Shafique, ''Probabilistic analysis of targeted attacks using transform-domain adversarial examples,'' IEEE Access, vol. 8, pp. 33855–33869, 2020.

[19] W. Zhang, ''Generating adversarial examples in one shot with imageto-image translation GAN,'' IEEE Access, vol. 7, pp. 151103–151119, 2019.

[20] J. Jia, A. Salem, M. Backes, Y. Zhang, and N. Z. Gong, ''MemGuard: Defending against black-box membership inference attacks via adversarial examples,'' in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2019, pp. 259–274.

[21] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, ''Securing CNN model and biometric template using blockchain,'' in Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Sep. 2019, pp. 1–7

[22] Z. Xu, F. Yu, and X. Chen, ''LanCe: A comprehensive and lightweight CNN defense methodology against physical adversarial attacks on embedded multimedia applications,'' in Proc. 25th Asia South Pacific Design Autom. Conf. (ASP-DAC), Jan. 2020, pp. 470–475.

[23]] A. Simonet-Boulogne, A. Solberg, A. Sinaeepourfard, D. Roman, F. Perales, G. Ledakis, I. Plakas, and S. Sengupta, ''Toward blockchainbased fog and edge computing for privacy-preserving smart cities,'' Frontiers Sustain. Cities, vol. 4, p. 136, Sep. 2022

[24] A. Kurakin, I. J. Goodfellow, and S. Bengio, ''Adversarial examples in the physical world,'' in Artificial Intelligence Safety and Security. London, U.K.: Chapman & Hall/CRC, 2018, pp. 99–112.

[25] X. Yuan, P. He, Q. Zhu, and X. Li, ''Adversarial examples: Attacks and defenses for deep learning,'' IEEE Trans. Neural Netw. Learn. Syst., vol. 30, no. 9, pp. 2805–2824, Sep. 2019.

[26] U. Shaham, Y. Yamada, and S. Negahban, ''Understanding adversarial training: Increasing local stability of supervised models through robust optimization,'' Neurocomputing, vol. 307, pp. 195–204, Sep. 2018.

[27] H. Shu, R. Shi, Q. Jia, H. Zhu, and Z. Chen, ''MFI-PSO: A flexible and effective method in adversarial image generation for deep neural networks,'' 2020, arXiv:2006.03243

[28] G. Goswami, A. Agarwal, N. Ratha, R. Singh, and M. Vatsa, ''Detecting and mitigating adversarial perturbations for robust face recognition,'' Int. J. Comput. Vis., vol. 127, nos. 6–7, pp. 719–742, 2019

[29] A. Agarwal, R. Singh, M. Vatsa, and N. Ratha, ''Are image-agnostic universal adversarial perturbations for face recognition difficult to detect?'' in Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Oct. 2018, pp. 1–7

[30] K. Kansal, P. S. Krishna, P. B. Jain, S. R, P. Honnavalli, and S. Eswaran, ''Defending against adversarial attacks on COVID-19 classifier: A denoiser-based approach,'' Heliyon, vol. 8, no. 10, Oct. 2022, Art. no. e11209.

[31] X. Ma, Y. Niu, L. Gu, Y. Wang, Y. Zhao, J. Bailey, and F. Lu, ''Understanding adversarial attacks on deep learning based medical image analysis systems,'' Pattern Recognit., vol. 110, Feb. 2021, Art. no. 107332.

[32] Z. Yahya, M. Hassan, S. Younis, and M. Shafique, ''Probabilistic analysis of targeted attacks using transform-domain adversarial examples,'' IEEE Access, vol. 8, pp. 33855–33869, 2020.

[33] W. Zhang, ''Generating adversarial examples in one shot with imageto-image translation GAN,'' IEEE Access, vol. 7, pp. 151103–151119, 2019.

[34] M. Nassar, K. Salah, M. H. urRehman, and D. Svetinovic, ''Blockchain for explainable and trustworthy artificial intelligence,'' WIREs Data Mining Knowl. Discovery, vol. 10, no. 1, Jan. 2020, Art. no. e1340.

[35] Z. Xu, F. Yu, and X. Chen, ''LanCe: A comprehensive and lightweight CNN defense methodology against physical adversarial attacks on embedded multimedia applications,'' in Proc. 25th Asia South Pacific Design Autom. Conf. (ASP-DAC), Jan. 2020, pp. 470–475

[36] J. Jia, A. Salem, M. Backes, Y. Zhang, and N. Z. Gong, ''MemGuard: Defending against black-box membership inference attacks via adversarial examples,'' in Proc. ACM

SIGSAC Conf. Comput. Commun. Secur., Nov. 2019, pp. 259–274

[37] Chest X Ray Dataset: https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia