Advancing Healthcare Anomaly Detection: Integrating GANs with Attention Mechanisms

Thakkalapally Preethi[1], Afsana Anjum[2], Dr Anjum Ara Ahmad[3], Dr. Chamandeep Kaur[4],
Dr. Vuda Sreenivasa Rao[5], Prof. Ts. Dr. Yousef A.Baker El-Ebiary[6], Ahmed I. Taloba[7]
Assistant Professor, Department of CSE-(CYS,DS) and AI&DS,
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India[1]
Lecturer, Dept.of Information Technology & Security, Jazan University Jazan, KSA[2]
Professor, Department of Mathematics & Statistics, Rizvi College of Arts,
Science & Commerce, Affiliated to University of Mumbai, Bandra West, Mumbai, Maharashtra, India[3]
Lecturer, Department of Computer Science, Jazan University, Jazan, Saudi Arabia[4]
Associate Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India[5]
Faculty of Informatics and Computing, UniSZA University, Malaysia[6]
Department of Computer Science, College of Computer and Information Sciences, Jouf University, Saudi Arabia[7]
Information System Department-Faculty of Computers and Information, Assiut University, Assiut, Egypt[7]

***Abstract*—Early illness diagnosis, treatment monitoring, and healthcare administration all depend heavily on the identification of abnormalities in medical data. This paper proposes a unique way to improve healthcare anomaly detection through the integration of attention mechanisms and Generative Adversarial Networks (GANs) for improved performance. By integrating GANs, artificial data that closely mimics the distributions of actual healthcare data may be produced, so, it is important to supplementing the dataset and strengthening the resilience of anomaly detection algorithms. Simultaneously, the Convolutional Block Attention Module (CBAM) facilitates the model's concentration on useful characteristics present in the data, thereby augmenting its capacity to identify minute deviations from the norm. The suggested method is assessed using a large dataset from healthcare settings that includes both typical and unusual cases. When compared to current techniques, the results show notable gains in anomaly detection performance. The model also shows resilience to noise, small abnormalities, and class imbalance, indicating its potential for practical clinical applications. The suggested strategy has the potential to improve clinical decision-making and patient care by giving doctors faster, more precise insights into anomalous health states. With an accuracy of around 99.12%, the suggested GAN-CBAM is implemented in Python software and outperforms other current techniques such as Gaussian Distribution Anomaly detection (GDA), Augmented Time Regularized (ATR-GAN), and Convolutional Long Short-Term Memory (ConvLSTM) by 2.97%. With potential benefits for bettering patient outcomes and the effectiveness of the healthcare system, the suggested strategy is a major step forward in the improvement of anomaly identification in the field of medicine.**

Keywords*—Generative Adversarial Networks (GANs); Convolutional Block Attention Module (CBAM); anomaly detection; attention mechanism; healthcare

I. INTRODUCTION

Advancements in anomaly detection methodologies hold significant promise for enhancing healthcare outcomes by enabling early identification of abnormal patterns or deviations in medical data [1]. Anomaly detection plays a pivotal role in various healthcare applications, including disease diagnosis, treatment monitoring, and patient management [2]. However, the complexity and heterogeneity of healthcare data pose significant challenges for traditional anomaly detection techniques. In recent years, the integration of advanced machine learning techniques has emerged as a promising approach to address these challenges and improve the accuracy and reliability of anomaly detection in healthcare settings [3]. In this context, this paper proposes a novel framework for advancing healthcare anomaly detection by integrating GANs with attention mechanisms to achieve enhanced performance [4].

GANs have garnered considerable attention in the ML community for their ability to generate synthetic data that closely resembles real-world data distributions [5]. By leveraging the adversarial training paradigm, GANs learn to generate high-fidelity samples that capture the underlying structure and complexity of the original data [6]. In the context of healthcare anomaly detection, GANs offer a promising avenue for data augmentation, enabling the generation of diverse and representative synthetic samples to augment limited or imbalanced datasets [7]. Furthermore, attention mechanisms have gained prominence for their ability to focus on relevant features or regions within the data, thereby enhancing the model's ability to capture salient information for anomaly detection. By integrating attention mechanisms into the anomaly detection framework, the proposed approach aims to improve the model's discriminative power and robustness to subtle deviations or anomalies in healthcare data [8].

The integration of GANs and attention mechanisms represents a novel and synergistic approach to advancing healthcare anomaly detection [9]. By harnessing the complementary strengths of these techniques, the proposed framework aims to overcome limitations associated with traditional anomaly detection methods, such as reliance on handcrafted features or susceptibility to class imbalance and noisy data [10]. Moreover, the proposed approach holds promise for facilitating interpretability and explainability in anomaly detection, enabling clinicians to better understand and trust the model's outputs. Overall, this paper contributes to the ongoing efforts in leveraging advanced machine learning techniques to enhance anomaly detection in healthcare, with potential applications in improving patient outcomes, clinical decision-making, and healthcare system efficiency [11].

Healthcare anomaly detection, a critical aspect of healthcare informatics, involves the identification of abnormal patterns, deviations, or outliers within healthcare data. This field plays a pivotal role in various healthcare applications, including disease diagnosis, treatment monitoring, patient safety, fraud detection, and resource optimization. Anomalies in healthcare data can manifest in diverse forms, such as unusual physiological measurements, unexpected variations in medical imaging findings, irregularities in billing records, or atypical patterns in patient health records. Detecting these anomalies is essential for ensuring early disease diagnosis, timely intervention, and effective healthcare management, ultimately leading to improved patient outcomes and healthcare system efficiency [12].

One of the primary objectives of healthcare anomaly detection is to enhance early disease diagnosis and treatment monitoring. By analyzing patient health records, medical imaging data, and physiological measurements, anomaly detection algorithms can identify subtle deviations from normal patterns that may indicate the presence of underlying health conditions [13]. For example, anomalies in ECG signals could signify cardiac arrhythmias or abnormalities, while anomalies in medical imaging scans such as CT or MRI could indicate the presence of tumors, lesions, or other pathological findings. Early detection of these anomalies enables healthcare practitioners to initiate timely interventions, implement appropriate treatment strategies, and monitor patient progress more effectively.

Furthermore, healthcare anomaly detection plays a crucial role in patient safety and quality of care. By flagging unusual medication prescriptions, treatment orders, or adverse drug reactions, anomaly detection systems help prevent medication errors, adverse events, and patient harm. Similarly, anomaly detection algorithms can identify anomalies in hospital admission records, discharge summaries, or surgical procedures, enabling healthcare providers to ensure compliance with clinical protocols, minimize risks, and enhance patient safety standards [14].

In addition to improving patient care and safety, healthcare anomaly detection contributes to healthcare system efficiency by optimizing resource allocation, streamlining administrative processes, and reducing operational costs. By identifying anomalies in healthcare supply chain data, inventory management systems, or staffing schedules, healthcare organizations can optimize resource utilization, mitigate supply chain disruptions, and improve workflow efficiency [15]. Moreover, anomaly detection algorithms can identify inefficiencies, bottlenecks, or deviations from established performance metrics within healthcare operations, enabling administrators to implement targeted interventions, process improvements, and quality assurance initiatives to enhance overall system performance.

The key contributions of the article are,

- The paper suggests a unique method to improve healthcare anomaly detection that combines GANs with attention processes, notably the CBAM. The model can now produce synthetic data that closely resembles actual healthcare distributions while concentrating on useful aspects seen in the data, which enhances the algorithm's capacity to spot minute departures from the norm.
- The work efficiently increases the dataset and improves the resilience of anomaly detection models by utilizing GANs for data augmentation. This augmentation leads to more dependable detection outcomes by addressing the restrictions caused by incomplete or unbalanced datasets that are frequently found in healthcare settings.
- The suggested methodology is assessed using an extensive dataset that includes both typical and unusual cases from medical environments.
- The study demonstrates how resilient the suggested paradigm is to problems like noise, class imbalance, and minute abnormalities seen in healthcare data. Because of its resilience, the model may be applied more effectively in actual clinical situations and gives doctors faster, more precise insights into diseases that deviate from the norm.

The remainder of the article includes related works, problem statement, methodology and results in Section II, III, IV and V. The paper and future scope are concluded in Section VI and Section VII respectively.

II. Related Works

Oluwasanmi et al. [16] explain that due to their involvement in several crucial and vital situations, computerized anomaly detection and detection have grown increasingly important in the modern age. It suggests three AI systems that use DL techniques to examine and identify abnormalities in human electrical impulses in order to achieve these objectives. Two of the three suggested methods are a restoration decoder with minimal remodeling losses and an attention automatic encoder that transfers the input information to a lower-dimensional latent representations with optimal features persistence. To identify the prominent responses in the encoded dispersion, the auto encoder incorporates a focus component at the bottlenecks. Furthermore, time-series sequencing data analysis and generating reconstructions have been developed for learning a Gaussian distribution through the use of a VAE and a network with LSTM. When identifying normal beating hearts from individuals suffering from acute congestive cardiac failure, the three suggested models shown exceptional capacity to identify abnormalities on the assessed ECG5000 data with an accuracy of 99% and 99.3% precise value.

Vaccari et al. [17] explains that AI and ML techniques are increasingly being used in the medical field for a variety of reasons, including systems for clinical decision-making, tracking patients, and the detection and prognosis of potential illnesses. In addition, because autonomous medical devices which fall under the IoMT umbrella allow ongoing surveillance and immediate utilization of data by medical professionals, their widespread adoption has made it easier to get information about patients. Nevertheless, the data gathered may not be accurate enough to apply accurate methods because of potential problems in real-world contexts, like connectivity failure, inconsistent use, abuse, or lax compliance to a surveillance programmed. To build artificial datasets big enough to train ML models, hence, methods to augment data can be applied. In this study, it uses the notion of GANs to supplement patient data collected by IoMT devices for the purpose of tracking COPD. By contrasting the artificial information with the actual data captured by the detectors, also use an understandable AI system to show how accurate the simulated information is. As confirmed using a unique ML-based technique, the outcomes show that data sets generated by an organized GAN are similar with a real database.

In the United States, heart disease is the primary cause of mortality. In order to preserve the lives of individuals, prompt medical attention is essential for the accurate identification of cardiac disease. The ECG is an extremely widely used tool used by doctors to evaluate heart electrical activity and identify potential abnormalities. Creating efficient mathematical models is necessary to fully utilize the ECG data for trustworthy heart disease diagnosis. Zekai Wang et al. [18] present a GAN-based two-level hierarchy structure to support ECG signal interpretation. A Made GAN makes up the first-level demonstrate, that attempts to distinguish anomalous signals from regular ECGs in order recognize anomalies. By combining the TL learning method used to on information from the first-level acquiring with the multi-branching design to deal with the data-lacking and unbalanced information problems, the second-level training aims at strong multi-class categorization for various arrhythmia recognition. It assesses how well the suggested architecture performs using actual ECG readings obtained from the MIT-BIH cardiac dataset. According to results from experiments, suggested model works better than the approaches that are already in widespread use in fact.

Said et al. [19] explains that False alarms have several detrimental consequences in important IoT application areas including the Defense Industry and Healthcare, including anxiety, interruption of emergency services, and wasted resources. As a result, an alert should only be delivered when the right thing happens. However, the accuracy of identifying events is impacted by intrusions into connected devices. In this study, an ADS is presented for a connected device in a smart healthcare facility to identify occurrences of interest related to the surroundings and health of patients while also looking for hacking attempts. It was demonstrated that supplying one platform for e-health assessment and network infrastructure supervision helps to optimize capabilities and uphold system dependability. As a result, choices about patient treatment and environmental modification are made with more accuracy. Because of an edge installation that enables processing near to data sources, minimal latency is guaranteed. The suggested ADS is put into practice and assessed utilizing the Contiki Cooja simulator, and an examination of an actual data set serves as the foundation for the e-health detection of events. The findings demonstrate a high rate of detection for both IoT network breaches and e-health-related incidents.

Li et al. [20] explains that Modern manufacturing has made extensive use of supervised ML approaches, like categorization models, for web-based anomaly detection. Since anomalous process states are uncommon in typical industrial environments, there's a chance that the data used to train the model is excessively unbalanced. This might lead to a large amount of training biases in supervised learning that would further reduce the accuracy of anomaly detection. It makes sense to use methods for data enhancement to provide useful fake data samples for the anomalous process states in order to lessen training bias. Unfortunately, the majority of data enhancement algorithms now in use do not adequately account for the temporal arrangement of the signal generated by sensors, and in need to achieve appropriate augmentation achievement, a significant number of real samples are often needed. This research created a unique data-driven approach called augmented temporal regularized ATR-GAN to overcome these constraints. ATR-GAN can provide simulated samples for models of supervised learning that are more successful by including a suggested enhanced generator. Three factors sum up this enhanced generator's originality in the suggested technique: 1) To recognize high-quality manufactured samples, an enhanced filter layer is added to the augmented the generator; 2) A new separation metric called TRH distance was created in the enhanced filter layer to accurately assess the similarities within accomplished artificial instances and actual instances. However, and 3) to make the most of the comparatively small amount of training data and better diversify the generated data, batching methods have been included in the suggested enhanced generator. Furthermore, cases from the real-world in additive production and computational modelling are used to verify the efficacy of the suggested ATR-GAN.

Ziyu Wang et al. [21] explains that EMR progress has been hampered by the dichotomy between the years of administrative oversight and the enormous rise in the need for health information privacy. This invention has the potential to encourage patient data independence at this historical juncture. In this work, researchers suggest a decentralized, effective, and secure Ethereum platform for sharing and protecting data privacy called Guard Health. When working with sensitive data, Guard Health oversees data exchange, security, authorization, and preservation. In order to ensure safe information preservation and transmission which forbids transmission of information without authorization it makes use of the Blockchain and smart contracts. The latest GNN for harmful node identification is implemented together with an authentication model to accurately manage user trust. The results of the test and safety assessment demonstrate that the suggested plan is suitable for smart healthcare system.

Massive amounts of statistics are generated by sensors, the foundation for sophisticated data technologies. The cloud may be utilized for storing this information for later analysis and effective use. Unusual information may be found in sensor information for a number of circumstances (e.g., node placement in hard locations, inadequately configured instruments, and malicious operations by attackers). In certain instances, such as data systems for forest fires, health care surveillance structures, along with other IoT structures, recognizing anomalies is essential. Dwivedi et al. [22] presents a machine-learning-supervised system of identifying anomalies for medical surveillance sensor clouds, which integrate many bodily sensors from various individuals with the internet. The method has its foundation on the Gaussian distribution. Python is used for executing this position. The suggested scheme's utilization of the Gaussian statistical framework enhances effectiveness, productivity, and accuracy. When contrasted with different controlled learning-based anomaly identification systems, GDA offers 98% effectiveness with 3% and 4% enhancements.

Astillo et al. [23] explains that in the field of medical treatment, implanted internet of things medical equipment, have caused a radical shift. It has enhanced the patient care that healthcare practitioners provide. Furthermore, it has assisted those with chronic illnesses in taking control of their own treatment. The majority of IoTMD's clients are individuals who have the condition, who need help keeping their blood sugar levels within acceptable bounds. Nevertheless, these technologies' security protection against possible cyber threats is still lacking. These kinds of hazards should not be disregarded as they may endanger the patients' life. In light of this, this study suggests a deep learning-based anomalous identification system made up of estimate and categorization algorithms that can be utilized to the diabetes administration management and control System, an area of healthcare organizations. While the categorization technique's goal is to identify aberrant points of information, the estimating technique was utilized to predict the individuals' blood sugar levels at each assessment period increment. For contrast, this article provides the multilayer perceptron and convolutional neural network techniques. Furthermore, in order to protect individual confidentiality regarding significant physiologic information contained in the information set, this work uses federated learning and independent training techniques. Moreover, simulations were transformed into their compact versions using the post-quantization reduction approach, which helped to get around the operationally taxing deep learning operations. The FL approach had a greater recall percentage than the IL technique, according to the trial data. Furthermore, the CNN-based anomalous identification system enhanced by FL outperforms the MLP-based method in terms of performance. The typical remember percentage for the first category was 99.24%, whereas the typical recall rate for the latter was just 98.69%. When the initial algorithms were changed to their compact form, the inferential latencies of the predictions were drastically lowered from in excess of three hundred ms to lower than several milliseconds, and all without compromising the value of recall.

Numerous studies demonstrate the importance of AI and ML in anomaly identification across a range of industries, particularly healthcare. With its high accuracy in detecting illnesses like heart disease using ECG data, artificial intelligence (AI) systems that use deep learning techniques are becoming more and more important for analyzing and recognizing irregularities in human electrical impulses. Furthermore, GANs are a useful tool for enhancing patient data to improve ML model training and enable more accurate tracking of illnesses like COPD. Novel techniques such as ATR-GAN, which tackles temporal arrangement and data imbalance, improve anomaly detection systems for smart industrial processes and healthcare facilities. Using blockchain technology and smart contracts, decentralized systems such as Guard Health guarantee safe data exchange and security in the healthcare industry. Moreover, deep learning-based systems for controlling chronic illnesses like diabetes and machine learning-supervised systems for medical monitoring sensor clouds show notable gains in anomaly identification and patient care. All things considered, anomaly detection and data security are changing as a result of AI and ML breakthroughs, improving the precision and dependability of many applications.

III. PROBLEM STATEMENT

Effectively identifying abnormalities in medical data, which are essential for early illness diagnosis, treatment monitoring, and healthcare management, is a major issue for the healthcare industry. Current anomaly detection techniques frequently encounter problems such as unequal class distribution, noisy data, and minute departures from typical patterns, which can result in less-than-ideal outcomes and possibly compromise patient safety [23]. Therefore, there is a pressing need to advance anomaly detection techniques in healthcare by integrating cutting-edge technologies such as GANs and attention mechanisms. This study aims to address these challenges by proposing a novel approach that combines GANs for data augmentation with attention mechanisms for feature selection, ultimately enhancing the performance of anomaly detection models in healthcare settings.

IV. PROPOSED GAN-CBAM FRAMEWORK FOR ANOMALY DETECTION

The research methodology entails several key steps. Firstly, information series is conducted to accumulate relevant datasets containing each regular and anomalous instances from healthcare settings. Subsequently, statistics preprocessing techniques, together with Min-Max normalization, are carried out to standardize the statistics and make sure consistency across extraordinary functions. Next, GANs are used for records augmentation, generating synthetic facts samples to decorate the training dataset and enhance the version's robustness. Attention mechanisms are protected in the ambiguity detection framework to beautify the version's overall performance by specializing in informative functions within the records. Finally, a performance assessment is performed to assess the effectiveness of the proposed method using appropriate metrics along with accuracy, precision, recollect, and F1-score, providing insights into the model's capability to efficiently hit upon anomalies in healthcare statistics. It is depicted in Fig. 1.

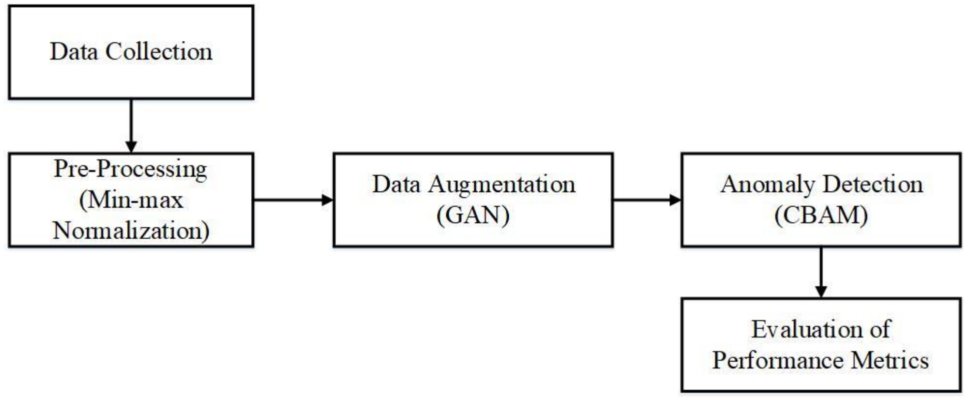

Fig. 1. Proposed methodology.

A. Data Collection

CT (Computed Tomography) scientific pix had been sourced from Kaggle, a famous platform for web hosting and sharing datasets. These images, obtained through Kaggle's repositories, constitute a treasured useful resource for scientific studies and diagnostic purposes. CT imaging performs an important position in healthcare, imparting distinctive move-sectional images of inner systems within the frame. The availability of CT images on Kaggle allows get admission to various datasets encompassing various anatomical regions, pathologies, and patient demographics. Researchers and clinical professionals utilize these datasets for obligations inclusive of disease diagnosis, treatment making plans, and clinical education. Moreover, the collaborative nature of Kaggle permits the sharing of knowledge, algorithms, and insights, fostering collaboration and innovation in medical imaging research [24]. Overall, the CT medical images sourced from Kaggle function a precious useful resource for advancing scientific imaging strategies, enhancing patient care, and furthering our understanding of complicated medical conditions**.**

B. Preprocessing using Min-Max Normalization

Preprocessing of the CT scientific images received from Kaggle includes several steps, with Min-Max normalization being an essential method to standardize the pixel depth values throughout the images. In this system, each pixel intensity price is scaled to fall within a particular variety, typically among 0 and 1, primarily based at the minimal and most intensity values found inside the dataset. This normalization step ensures that the pixel values are similar across exclusive images and prevents any biases brought by using versions in pixel intensity distributions. By scaling the pixel values to a common variety, Min-Max normalization allows in enhancing the convergence and stability of subsequent machine studying algorithms applied to the dataset. Min-max normalization is given in Eq. (1).

$$X_{Normalized} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

The implementation of Min-Max normalization for the CT images includes iterating through every pixel in every image and making use of the normalization components, which calculates the scaled pixel value based totally on the authentic depth value, the minimal intensity fee found within the dataset, and the most depth price located in the dataset. This process is computationally positive and may be without difficulty included into present image processing pipelines. Additionally, Min-Max normalization preserves the relative relationships among pixel intensities within each image whilst making sure consistency and comparison across the whole dataset. Overall, by preprocessing the CT scientific images the usage of Min-Max normalization, the dataset is ready for subsequent evaluation, which includes responsibilities which include feature extraction, image segmentation, and machine mastering-based category or detection algorithms.

C. GAN for Data Augmentation

GANs are applied for data augmentation in various domain names, inclusive of medical imaging. In the context of CT images sourced from Kaggle, GANs play a critical function in expanding the dataset size and variety by producing artificial images that intently resemble real CT images. GANs consist of neural networks, a generator and a discriminator, which can be educated adversarial to generate sensible images while distinguishing among real and artificial ones. By leveraging GANs for information augmentation, researchers can conquer limitations posed by using the availability of restrained or unbalanced datasets, improving the robustness and generalization capabilities of device studying models skilled on those datasets. The artificial images generated by GANs seize the underlying distribution of the unique facts, allowing more powerful education of deep mastering trends for duties consisting of ailment category, segmentation, and anomaly detection in medical imaging packages. Additionally, GAN-based totally facts augmentation helps the exploration of rare or pathological instances, supplying treasured insights for enhancing diagnostic accuracy and clinical decision-making in healthcare settings.

1) GAN initialization: The discriminator D and the generator G contain specific class understanding, in contrast to the autoencoder. G is instructed to create photos for various classes throughout the adversarial training, and D is tasked to decide whether to identifier the images as bogus or with a problem-specific classification c. By initializing G with the weights included in the decoder Δ and one of the layers of a discriminator D_e with the values of the encoder E, the autoencoder information is transmitted between the GAN components at the point of GAN initialization. The highest layer of the discriminator $Dd\ produces$ the final discriminant output. It is an intense layer with an activation function based on softmax. The final layer's values are learned throughout adversarial training and are first initialized at randomly.

The discriminator's initialization is just utilized to provide significant properties to D that aid in image classification. There is a deeper purpose to the generator's startup. The generator G is equal to the decoder Δ whenever adversarial instruction begins. As a result, the latent vector Z supplied to generators G is equal to a position in the autoencoder's hidden space; that is, Z may be seen as either the input of Δ or the output of E. As a result, the encoder E converts actual pictures into the latent area that G is using. Before beginning adversarial training, it takes use of this feature to acquire a decent class conditioned thinking, that is, determining the appearance of a latent vector Zc for a class c image.

The transformation of the prior probability distribution $D(x)$ and $G(z)$ of GAN into the related probability distribution subsequent to $D(x \mid c)$ and $G(z \mid c)$ can be represented as follows:

$$min_G max_D V(D,G) = E_{x\sim p_{data}(x)}[logD(x \mid c)] + E_{z\sim p_z(z)} [log(1 - D(G(z \mid c)))] \quad (2)$$

In this equation, min_G denotes the minimization with respect to the generator G. max_D denotes the maximization with respect to the discriminator D. $V(D,G)$ represents the value function. $E_{x\sim p_{data}(x)}[logD(x \mid c)]$ denotes the expectation over real data samples x drawn from the data distribution $p_{data}(x)$. $E_{z\sim p_z(z)}\left[log\left(1 - D\left(G(z \mid c)\right)\right)\right]$ denotes the expectation over generated samples $G(z \mid c)$ drawn from the generator's distribution $p_z(z)$. The GAN training methodology is based on the same process as GAN. To maximize the loss values generated by the discriminator and minimize the loss values of the generator unless they both stabilize, the optimizer performs the highest and lowest operations during alternating rounds of adversarial training.

With median vector μc and a matrix of covariance Σc, it represents a class within the space of latent variables with a normal distribution of multiple variables $Nc = N\,(\mu c, \Sigma c)$. It calculates μc and Σc for every class c in the training dataset, taking into account all real images Xc of class c that are accessible, in order to approximate the distribution of $Zc = E(Xc)$. It uses these distributions of probabilities to initialize the class-conditional hidden vector power source, which is a random process that accepts a class label c as input and outputs a randomly selected residual vector Zc from Nc. The probabilistic distributions of Nc are regarded as immutable while undergoing adversarial training, preventing the generation algorithm from deviating from the original class encoded in the space of latent values.

2) Adversarial training: Data goes via the generator G and discriminator D in groups throughout the training process, and the weights they assign are adjusted to maximize the loss values. An input image is classified by the discriminator as either phoney or matching to a single of the *n* problem-specific classes. It gives $1/\,(n\,+\,1)$ of the number of images for every batch; that is, it offers the best feasible balancing for the fictitious class. The result of G, which receives dormant vectors Zc that are taken from the class-conditional dormant vector generators as inputs, is bogus data. The evenly spaced class labels c, or the fictitious images that are uniformly dispersed among the problem-specific groups, are then fed into the category-conditional dormant vector encoder. It optimizes the sparsely categories cross entropy loss function in order to correspond to the category labels for genuine images and the false label for created ones while trained the discriminant D.

The generator G learns batches of identical size for each batch that the discriminant learns. In order to accomplish this, a standard distribution is applied to the labels c, resulting in the randomized drawing of an entire set of conditionally residual vectors Zc. The generator processes these vectors, while the discriminant receives the resultant pictures. The discriminator's chosen labels and the labels c that were utilized to create the images are matched by the settings in G.

D. Employing Attention Mechanism for Enhanced Anomaly Detection

Employing attention mechanisms for stronger anomaly detection involves integrating mechanisms that permit trends to focus on applicable capabilities or areas inside the input statistics, thereby enhancing the detection of irregularities or anomalies. By dynamically weighting one-of-a-kind components of the facts, interest mechanisms enable the version to prioritize informative functions even as suppressing noise or irrelevant statistics. This selective attention enhances the model's potential to figure subtle deviations from normal styles, leading to extra accurate anomaly detection. Additionally, attention mechanisms facilitate interpretability with the aid of highlighting the capabilities contributing maximum to anomaly detection selections, permitting higher expertise and validation of detected anomalies. Overall, incorporating attention mechanisms enhances anomaly detection systems' performance, robustness, and interpretability, making them greater powerful in numerous real-world programs, inclusive of healthcare, cybersecurity, and fraud detection.

1) Attention mechanism: The attention mechanism is going to be implemented on the framework using the Convolutional Block Attention Module (CBAM) and the system for attention. After going via CBAM, the characteristic maps created by the next encoder convolutional layer that follows will yield a more detailed feature map for the next encoder convolutional layer. A more accurate characteristic map for the hidden representational space is then produced by passing the improved features map via the encoder layer of convolution and CBAM using the same process. Significantly this idea, it's possible to see that the latent shape space improves with learning about the characteristics of this information and provides us with improved outcomes. Because the attention mechanism suggested by the attention compute block feeds in the encoder's intermediate results and adds them to the encoder's final result to produce an equivalent weight.

Subsequently, the autoencoder's bottlenecks layer receives the improved intermediate outcomes from the encoder due to their comparable value. Through doing this, the abnormal input is suppressed and the bottleneck layer is able to identify the regular input by learning from the improved feature maps.

2) Baseline deep autoencoder: The encoder is composed of five Conv2D blocks, every one of which has an activation layer with a slope that is negative of 0.2, a 2D batch normalization layer, and a 2D convolutional layer. The graphic displays the convolutional layers' total amount of input methods, amount of output methods, and kernel size. Four FC layers make up the bottle neck layer, and a ReLU activating layer sits behind them. The flattening size of the encoder's output, or 4 * 4 * 128 = 2048, is the quantity of inputs. It is used for acquiring the features that are taken from the encoder; it might be conceptualized as a space that contains the inputs' hidden representations. Five 2D inverted convolutional (DConv2D) blocks make up the decoder. Identical to the Conv2D blocks, the DConv2D blocks contain the identical information; however, because they are performing opposite operations, the input and output channels of each block are inverted. To preserve the reconstruction values, the batch normalization layer and activating layer are deleted from the final DConv2D block. The two attention-based approaches that are presented in the current endeavor are both applied to the basal algorithm's encoder to improve the model's ability to focus on and learn form the more representational aspects of the input.

3) CBAM-based deep autoencoder: The subsequent Conv2D block's result will pass via CBAM Block 1 to provide improved output. The encoder's deep layer receives the improved output after that. After obtaining the characteristic maps of the final Conv2D block, the CBAM Block 2 refines its results once more. In order for the final Conv2D block to learn regarding featured-emphasized outputs, twice-refined map features will be fed into the latent image space. The model should do reconstructions better and have a higher learning result. Since the CBAM block requires the smallest amount of setting for CNN systems, it's possible that no significant gains are seen. The model should do reconstructions better and have a higher learning result. Since the CBAM block requires the smallest amount of setting for CNN systems, it's possible that no significant gains are seen. It is depicted in Fig. 2.

4) Attention-based deep autoencoder: Separated and input into attention blocks 1, and 2, respectively, are the results of the subsequent and fourth Conv2D blocks. The layers wherever the global maps of features will be used to improve the intermediary feature maps are wherever the focus of calculation takes place. The result is combined and sent into the layer that represents the bottleneck after that. Wherein a comparison matrix is initially created by adding the intermediary feature maps to the global map of features. The intermediary feature maps are subsequently amplified by the matrix of features to highlight the pertinent ones and prevent the irrelevant ones. This widens the distinction among pertinent and unimportant data and aids in the autoencoder's rebuilding of regular information and unusual input that has been detected by computing the restoration.

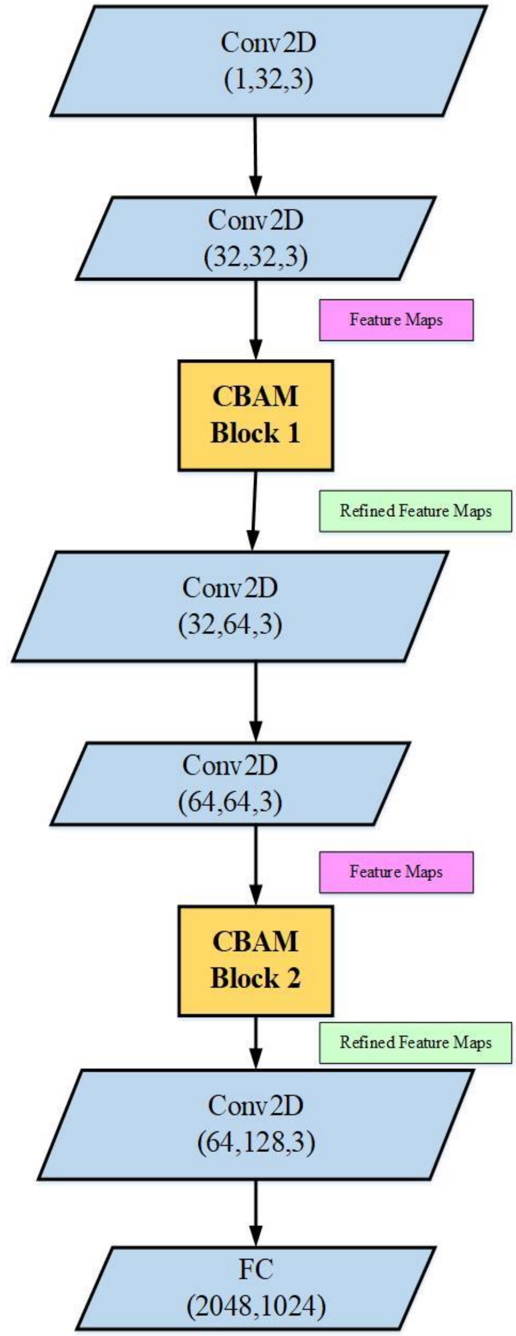

Fig. 2. CBAM-based deep autoencoder.

V. Results and Discussion

There are various important phases in the research approach. First, information series are run in order to compile pertinent datasets from healthcare settings that include both typical and unusual cases. Then, to standardize the data and ensure consistency among remarkable functions, preprocessing techniques for statistics are applied, including Min-Max normalization. GANs are then applied to records augmentation, producing fake fact samples to adorn the training dataset and improve the resilience of the version. The ambiguity detection framework incorporates attention methods that enhance the version's overall performance by focusing on informational functions inside the records. Lastly, performance evaluation is carried out to evaluate the efficacy of the suggested approach utilizing relevant measures in addition to accuracy, precision, recall, and F1-score, offering insights into the model's capacity to effectively identify abnormalities.

A. Model Accuracy

Model accuracy, inside the context of device gaining knowledge of and statistical modeling, refers to the proportion of effectively categorized times or predictions made by means of a model out of the full quantity of times in the dataset. It is a fundamental evaluation metric used to assess the overall performance of a predictive version, indicating how nicely the version's predictions align with the surface fact labels or effects. Model accuracy is calculated because the ratio of the number of efficaciously expected times to the overall number of instances, usually expressed as a percent. A higher accuracy fee means that the model is making more correct predictions, even as a decrease accuracy indicates a better price of misclassifications. It is depicted in Fig. 3.

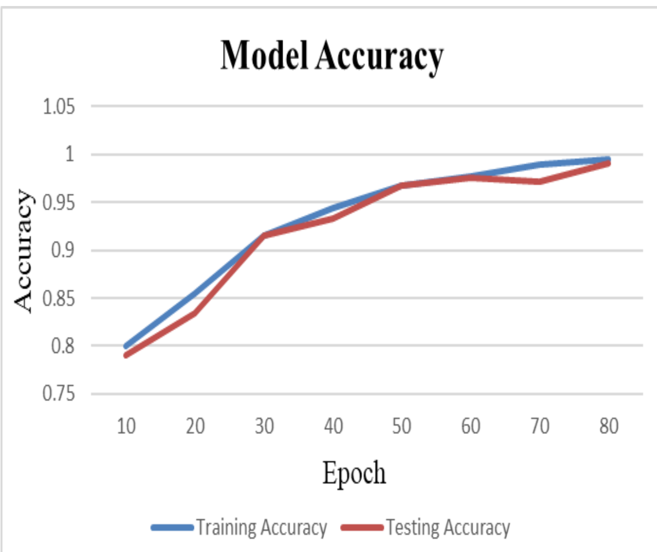

Fig. 3. Model accuracy.

B. Model Loss

Model loss, inside the context of ML, refers to a measure of the discrepancy among the actual outcomes and the predictions made by means of a model all through the learning procedure. It quantifies how nicely the version's predictions align with the real labels or goals for the given dataset. The intention of gaining knowledge of version is to limit its loss feature, thereby enhancing the model's capability to as it should be predicting effects. Commonly used loss features consist of MSE for regression duties and specific entropy for type duties. As the model iteratively learns from the education data, its loss regularly decreases, indicating advanced overall performance and better alignment with the ground reality. It is depicted in Fig. 4.

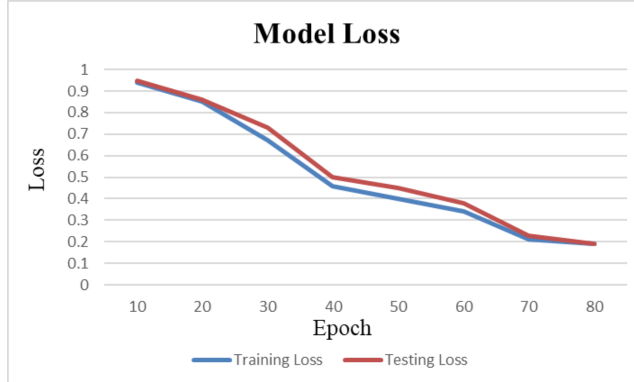

Fig. 4. Model loss.

C. ROC

Receiver Operating Characteristic (ROC) is a graphical representation of the performance of a binary class model throughout different discrimination thresholds. It plots the genuine nice charge (sensitivity) in opposition to the false high-quality rate (1 - specificity) at various threshold values, wherein sensitivity is the proportion of actual positives efficiently recognized by the version, and specificity is the proportion of real negatives efficiently recognized by way of the model. The ROC curve visually illustrates the trade-off between sensitivity and specificity and gives insights into the model's potential to discriminate among the advantageous and terrible classes. A higher vicinity below the ROC curve suggests higher discrimination overall performance, with values in the direction of suggesting a extra effective classifier. ROC analysis is extensively utilized in evaluating the performance of type models and determining the most fulfilling threshold for making predictions. It is depicted in Fig. 5.

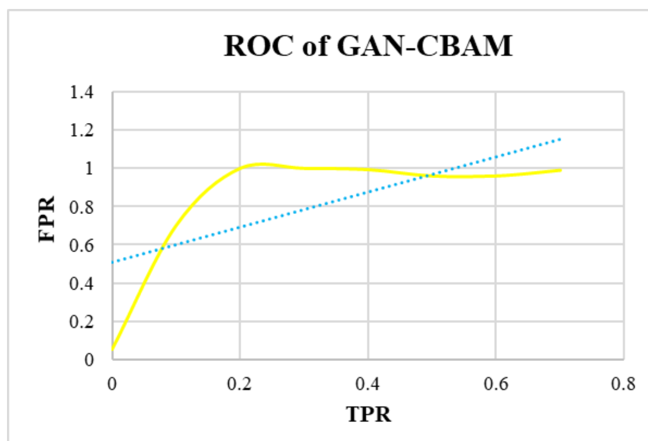

Fig. 5. ROC of GAN-CBAM.

D. Detection Time

Detection time refers to the length taken through device or set of rules to identify and flag anomalies inside a dataset. In the context of anomaly detection, detection time is a crucial performance metric that measures the performance and responsiveness of the detection manner. It encompasses the time elapsed from the moment an anomaly happens or enters the gadget to the factor at which it's miles detected and flagged for further action or research. A shorter detection time is applicable as it permits for timely responses to anomalies, minimizing capacity dangers or damages related to anomalous events. Detection time is mainly crucial in time-touchy applications such as cybersecurity, fraud detection, and actual-time tracking systems in which spark off identification of anomalies is important for powerful chance mitigation and selection-making. It is depicted in Fig. 6.

E. Accuracy

A performance parameter called accuracy is used to evaluate a model's overall prediction accuracy in machine learning and classification applications. The ratio of accurately predicted instances to all occurrences in the dataset is used to calculate it. Analyzing a model's accuracy measure is a simple and straightforward way to assess how well it performs in forecasting outcomes for each class. Even while it provides a rapid evaluation of overall performance, it might not be adequate in situations when there is an uneven distribution of courses. Eq. (3) expresses accuracy.

$$Accuracy = \frac{T_{Pos} + T_{Neg}}{T_{Pos} + T_{Neg} + F_{Pos} + F_{Neg}} \quad (3)$$

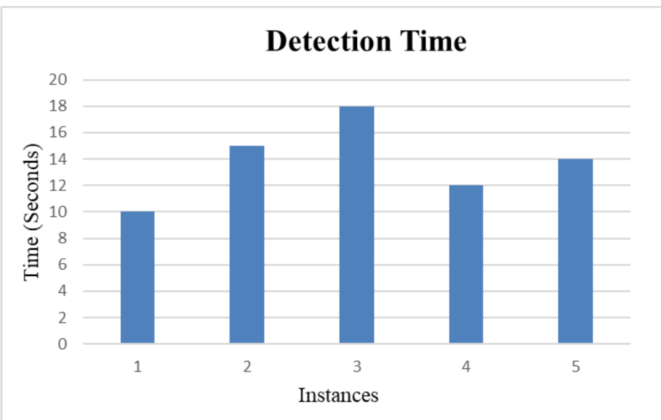

Fig. 6. Detection time.

F. Precision

Precision is a machine learning performance indicator that measures how well a model predicts the future. It is computed as the ratio of correctly predicted positive outcomes to the total of correctly predicted positive and false positive outcomes. One may calculate precision using Eq. (4).

$$P = \frac{T_{Pos}}{T_{Pos} + F_{Pos}} \quad (4)$$

G. Recall

A performance parameter called recall assesses how well a model can identify and pinpoint each and every pertinent instance of a particular class. It goes by the names true positive rate and sensitivity as well. The ratio of true positive predictions to the total of true positives and false negatives is used to compute it. It appears in Eq. (5).

$$R = \frac{T_{Pos}}{T_{Pos} + F_{Neg}} \quad (5)$$

H. F1-Score

The F1 score is a machine learning performance statistic that sums together recall and accuracy into a single figure. It provides a fair metric that takes into account both false negatives and false positives. It is computed using the harmonic mean of accuracy and recall. Eq. (6) represents it.

$$F1 - score = \frac{2 \times precision \times recall}{precision + recall} \quad (6)$$

The contrast of performance metrics across distinctive anomaly detection methods, as provided in Table I, exhibits the effectiveness of the proposed GAN-CBAM method in advancing healthcare anomaly detection. The outcomes demonstrate that the proposed approach achieves superior overall performance throughout all metrics compared to existing strategies, including GDA, ATR-GAN, and ConvLSTM. With an impressive accuracy of 99.12%, the precision of 97.32%, consider of 98.11%, and F1-Score 98.45%, the GAN-CBAM model showcases its capability to correctly perceive anomalies in healthcare information even as minimizing false positives and false negatives which is shown in Fig. 7. The integration of GANs for facts era and interest mechanisms for feature selection lets in the version to awareness on relevant records and effectively discriminate among regular and anomalous times. These findings highlight the capacity of the proposed approach to enhance anomaly detection in healthcare settings, enabling more correct and reliable detection of abnormalities for advanced affected person care and medical selection-making.

TABLE I. COMPARISON OF PERFORMANCE METRICS

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
GDA [22]	93.78	92.89	91.23	96.77
ATR-GAN [20]	98.11	93.78	94.99	97.89
ConvLSTM [15]	96.89	91.67	93.89	93.89
Proposed GAN-CBAM	99.12	97.32	98.11	98.45

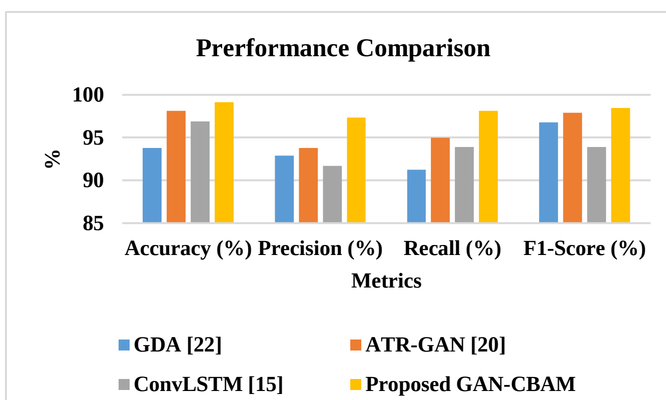

Fig. 7. Comparison of metrics.

I. Discussion

The suggested collection of GANs with CBAM improves the robustness and accuracy of detecting irregularities in medical data, which represents a breakthrough in healthcare anomaly identification. Data scarcity and class imbalance are addressed by using GANs to create generated data that closely resembles actual healthcare data, strengthening the robustness of anomaly detection systems. By improving the model's capacity to concentrate on pertinent features, the CBAM improves the identification of small abnormalities. With an accuracy of 99.12%, the analysis conducted on a large healthcare dataset demonstrates that the GAN-CBAM approach performs noticeably better than other conventional methods like GDA [22], ATR-GAN [20], and ConvLSTM [15]. This enhancement highlights the potential of the technique for useful clinical applications by providing quicker and more accurate insights that can support treatment monitoring, early sickness identification, and overall patient care.

The suggested approach, however, is not without its difficulties and restrictions. When GANs and attention mechanisms are combined, the computational complexity rises, necessitating a significant investment of time and resources for training and deployment. This may restrict the method's scalability and accessibility, especially in healthcare settings with limited resources. The challenges of the proposed method include handling data imbalance, noise resilience, identifying minute abnormalities, and ensuring practical clinical applicability. The proposed method may face limitations in computational complexity and scalability for large-scale healthcare datasets. Furthermore, more validation is needed to assess the method's efficacy in a wide range of real-world settings with different kinds of anomalies, even if it demonstrates robustness to noise and minor irregularities. Reliance on massive datasets for training might also be problematic when access to such data is restricted or unavailable due to privacy issues. Notwithstanding these drawbacks, the suggested GAN-CBAM technique is a promising advancement in improving anomaly detection efficiency in the medical field, with the potential to greatly enhance patient outcomes and clinical decision-making.

VI. Conclusion

The research shows how generative adversarial networks (GANs) and attention processes may be used to improve healthcare anomaly detection. In comparison to current techniques, the suggested GAN-CBAM model performs better, achieving greater accuracy, precision, recall, and F1-score. The model successfully identifies pertinent patterns and deviations in healthcare data by utilizing GANs for data augmentation and attention mechanisms for feature selection. This results in anomaly detection outputs that are more accurate and dependable. The results highlight how important it is to implement cutting-edge machine learning strategies that are customized to the particular qualities of healthcare datasets. The suggested method has the potential to improve clinical decision-making and patient care by giving medical professionals faster and more accurate insights on aberrant health conditions. Several directions for further study are worthwhile to pursue in the future.

VII. Future Scope

Further research into the model's predictability can shed light on the underlying causes of anomalies and improve physicians' comprehension and confidence in the model. Its application across other medical domains and contexts can also be expanded by investigating the scalability of the suggested technique to bigger and more diversified healthcare datasets. Further improving the model's performance and applicability in actual clinical settings is possible by the incorporation of domain-specific information or professional advice into the anomaly detection framework. Deploying the model in a variety of healthcare applications might also be facilitated by investigating the possibilities of transfer learning approaches to modify the model for various healthcare contexts or domains. The model's comprehension of intricate healthcare settings may be enhanced and anomaly detection performance can be enhanced by looking into the integration of other data modalities, such as textual or temporal data. The efficiency of the healthcare system and patient outcomes may both be greatly enhanced by ongoing research into developing anomaly detection techniques in the field of medicine.

References

[1] "A Data-Driven Heart Disease Prediction Model Through K-Means Clustering-Based Anomaly Detection | SN Computer Science." Accessed: Feb. 23, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s42979-021-00518-7

[2] "ANNet: A Lightweight Neural Network for ECG Anomaly Detection in IoT Edge Sensors | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9669005

[3] "Big Data-Driven Abnormal Behavior Detection in Healthcare Based on Association Rules | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9139506

[4] "Clustering-based anomaly detection in multivariate time series data - ScienceDirect." Accessed: Feb. 23, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1568494620308577

[5] V. Huynh, K. Vo, P. Phan, M. Elhoseny, and D.-N. Le, "Deep Learning based Optimal Multimodal Fusion Framework for Intrusion Detection Systems for Healthcare Data," Computers, Materials and Continua, vol. 66, pp. 2555–2571, Jun. 2021, doi: 10.32604/cmc.2021.012941.

[6] "ECG signal processing and KNN classifier-based abnormality detection by VH-doctor for remote cardiac healthcare monitoring | Soft Computing." Accessed: Feb. 23, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s00500-020-05191-1

[7] "Electronics | Free Full-Text | An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks." Accessed: Feb. 23, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/10/21/2562

[8] "Electronics | Free Full-Text | Security of Things Intrusion Detection System for Smart Healthcare." Accessed: Feb. 23, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/10/12/1375

[9] "Healthcare and anomaly detection: using machine learning to predict anomalies in heart rate data | AI & SOCIETY." Accessed: Feb. 23, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s00146-020-00985-1

[10] "Lightweight Photoplethysmography Quality Assessment for Real-time IoT-based Health Monitoring using Unsupervised Anomaly Detection - ScienceDirect." Accessed: Feb. 23, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921006499

[11] "Unsupervised Deep Anomaly Detection for Multi-Sensor Time-Series Signals | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 23,

2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9507359

[12] "Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9154698

[13] "Random Histogram Forest for Unsupervised Anomaly Detection | IEEE Conference Publication | IEEE Xplore." Accessed: Feb. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9338384

[14] J. Lee, H. Cha, S. Rathore, and J. Park, "M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT," Computers, Materials & Continua, vol. 67, pp. 1537–1553, Jan. 2021, doi: 10.32604/cmc.2021.014774.

[15] T. Tayeh, S. Aburakhia, R. Myers, and A. Shami, "An Attention-Based ConvLSTM Autoencoder with Dynamic Thresholding for Unsupervised Anomaly Detection in Multivariate Time Series," Machine Learning and Knowledge Extraction, vol. 4, no. 2, Art. no. 2, Jun. 2022, doi: 10.3390/make4020015.

[16] A. Oluwasanmi, M. U. Aftab, E. Baagyere, Z. Qin, M. Ahmad, and M. Mazzara, "Attention Autoencoder for Generative Latent Representational Learning in Anomaly Detection," Sensors, vol. 22, no. 1, Art. no. 1, Jan. 2022, doi: 10.3390/s22010123.

[17] I. Vaccari, V. Orani, A. Paglialonga, E. Cambiaso, and M. Mongelli, "A Generative Adversarial Network (GAN) Technique for Internet of Medical Things Data," Sensors, vol. 21, no. 11, Art. no. 11, Jan. 2021, doi: 10.3390/s21113726.

[18] Z. Wang, S. Stavrakis, and B. Yao, "Hierarchical deep learning with Generative Adversarial Network for automatic cardiac diagnosis from ECG signals," Computers in Biology and Medicine, vol. 155, p. 106641, Mar. 2023, doi: 10.1016/j.compbiomed.2023.106641.

[19] A. M. Said, A. Yahyaoui, and T. Abdellatif, "Efficient Anomaly Detection for Smart Hospital IoT Systems," Sensors, vol. 21, no. 4, Art. no. 4, Jan. 2021, doi: 10.3390/s21041026.

[20] Y. Li, Z. Shi, C. Liu, W. Tian, Z. Kong, and C. B. Williams, "Augmented Time Regularized Generative Adversarial Network (ATR-GAN) for Data Augmentation in Online Process Anomaly Detection," IEEE Transactions on Automation Science and Engineering, vol. 19, no. 4, pp. 3338–3355, Oct. 2022, doi: 10.1109/TASE.2021.3118635.

[21] Z. Wang, N. Luo, and P. Zhou, "GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare," Journal of Parallel and Distributed Computing, vol. 142, pp. 1–12, Aug. 2020, doi: 10.1016/j.jpdc.2020.03.004.

[22] R. K. Dwivedi, R. Kumar, and R. Buyya, "Gaussian Distribution-Based Machine Learning Scheme for Anomaly Detection in Healthcare Sensor Cloud," IJCAC, vol. 11, no. 1, pp. 52–72, Jan. 2021, doi: 10.4018/IJCAC.2021010103.

[23] P. V. Astillo, D. G. Duguma, H. Park, J. Kim, B. Kim, and I. You, "Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System," Future Generation Computer Systems, vol. 128, pp. 395–405, Mar. 2022, doi: 10.1016/j.future.2021.10.023.

[24] "CT Medical Images." Accessed: Feb. 23, 2024. [Online]. Available: https://www.kaggle.com/datasets/kmader/siim-medical-images