PrEGAN: Privacy Enhanced Clinical EMR Generation: Leveraging GAN Model for Customer De-Identification

Syed Thouheed Ahmed, R Sivakami, Vinoth Kumar V, *Member, IEEE,* Mahesh T R, *Senior Member, IEEE,* Surbhi Bhatia Khan*, *Senior Member, IEEE,* Arwa Mashat and Ahlam Almusharraf

***Abstract*— Privacy in medical records while data sharing is a major concern for distributed learning models. The dataset generated and shared via Electronic Medical Records (EMR) consist of sensitive medical information such as patient identify and experts' recommendations, and causes setbacks in training larger models, dataset augmentation and polluting datasets with recursive attributes. The information processing and de-identification is proposed in this article to preserve and enhance the privacy of EMR. The proposed technique is termed as PrEGAN (i.e.) Privacy Enhanced Generative Adversarial Network (GAN) for EMR data training and realistic mapping. The proposed model generates and discriminates the ground truth with generated mask via a computation of loss function for de-identification or removal of personal linked/connected data in the records networks. The objective is to generate the mask of EMR, which is realistic and similar to the ground truth. The model is trained and validated with two distinguished discriminators, the CNN based discriminator is used for medical images, whereas Neural Networks are used for textural data generator. The experimental results demonstrate a higher degree of data privacy and de-identification in EMR with 88.32% accuracy in predicting and eliminating via RoI and loss function.**

***Index Terms*— Privacy Enhanced GAN, PrEGAN, Generative Adversarial Networks (GAN), biomedical GAN, data privacy, de-identification, EMR, Electronic Health Records**

I. INTRODUCTION

Generative Adversarial Networks (GANs), also known as Generative Models, have become a focal point in the field of machine learning, particularly following the seminal work of I. J. Goodfellow and his team [1]. Their groundbreaking proposal introduced a transformative paradigm involving the integration of a generator and a discriminator within a model, ushering in a novel approach for reliable decision support. This departure from the conventional reliance on probability distribution in deep learning models has had profound implications. In the landscape of traditional computational and machine learning models, intricate layers of data processing have long been the norm, giving rise to complex network architectures. The advent of GAN architecture represents a departure from this norm, replacing traditional deep learning models. This shift is particularly noteworthy in applications such as computer vision, advanced image processing, natural language processing, and semi-supervised learning models.

This research endeavors to make significant strides in the realm of safeguarding user (patient) privacy within the context of Electronic Medical Records (EMR), also recognized as Electronic Health Records (EHR). The primary goal is to leverage Generative Adversarial Network (GAN) models to enhance and refine privacy measures in the handling of sensitive medical information. This includes, but is not limited to, safeguarding patient-sensitive details, preserving the confidentiality of disease treatments and expert (doctor) recommendations, and securing the integrity of patient history. The backdrop for this research is the inherent limitation of medical datasets, which often poses challenges in conventional machine learning approaches. Augmentation methods employed in these approaches frequently resort to data replication, a practice that involves duplicating existing attributes and features. Unfortunately, such methodologies, while augmenting datasets, compromise the privacy of medical data and records.

Essentially, this research strives to contribute to the development of a sophisticated framework that not only addresses the limitations posed by restricted medical datasets but also places a significant emphasis on preserving data privacy and integrity. The ultimate goal is to enhance the decision-making capabilities and reliability of machine learning models in the critical domain of medical data management. Therefore, this manuscript presents a detailed overview of the GAN architecture proposed as the "Privacy Enhancing Clinical EMR Generative (PrEGAN)" model. The PrEGAN model incorporates a dual discriminator architecture to efficiently process and customize user de-identification. The manuscript is structured with an introduction and literature reviews in sections I and II, followed by the presentation of the problem statement in section III. Section IV discusses the PrEGAN architecture and associated methodology, while

Syed Thouheed Ahmed is is currently associated with School of Computing and Information Technology, REVA University, India. Syed.edu.in@gmail.com

R Sivakami is working as Associate Professor in the Department of Computer Science and Engineering, Sona College of Technology, Salem - 636005 E-mail: shivasona07@gmail.com

Vinoth Kumar V is working with School of Information Technology and Engineering, Vellore Institute of Technology University, Vellore 632014, India; drvinothkumar03@gmail.com

Mahesh T R is working with the Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bengaluru, 562112, India. trmahesh.1978@gmail.com

Surbhi Bhatia Khan is [5]Department of Data Science, School of Science Engineering and Environment, University of Salford, Manchester United Kingdom; s.khan138@salford.ac.uk

Arwa Mashat is working with the Faculty of computing and information technology, king Abdulaziz university, Saudi Arabia, asmashat@kau.edu.sa

Ahlam Almusharraf is working with the Department of Business Administration, College of Business and Administration, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia. Aalmusharraf@pnu.edu.sa

*Correspondence: Surbhi Bhatia Khan (s.khan138@salford.ac.uk)

sections V, VI, and VII provide a detailed mathematical modeling of GAN. The study's observations and results are outlined in section VIII, with the conclusion in section IX highlighting the PrEGAN model's importance in the user de-identification process.

II. LITERATURE REVIEWS

In the contemporary landscape of research, scholars have dedicated their efforts to proposing and refining a variety of supportive approaches and techniques aimed at fostering the development of sustainable and reliable Generative Adversarial Network (GAN) models [1]. This endeavor is particularly pertinent when dealing with datasets of a sensitive nature, as encountered in medical applications and autonomous navigation systems. In the context of this survey, our focus is specifically directed towards understanding the evolutionary trajectory of GAN models, with a keen emphasis on their applications and influencing parameters within the realm of medical studies. A critical facet of comprehending GAN models lies in the elucidation of their mathematical foundations, and the work presented in [2] delves into this aspect, offering a detailed exploration of the mathematical underpinnings that form the bedrock of GAN models. This contribution not only enhances theoretical understanding but also serves as a valuable resource for those engaged in the practical development of applications utilizing GAN models [3-6].

Expanding on this theme, both [7] and [8] delve into the synthesis of medical data, emphasizing the capability of GAN models to transform data from one type to another. This approach is instrumental in scenarios where data of a specific modality needs to be converted or augmented, enhancing the versatility of medical datasets. However, a notable concern arising from these approaches is the potential compromise of sensitive patient information during the data synthesis process. To address this privacy challenge, [9] introduces a privacy-enabled GAN, referred to as pGAN, specifically tailored for the synthesis of Electronic Medical Records (EMR). The objective is to produce synthetic EMR instances that closely resemble existing records while obfuscating any traces of private or sensitive data. This nuanced approach ensures that the privacy considerations inherent in medical data are upheld, mitigating the risk of unintended information disclosure. In the forefront of recent advancements, [10] introduces the concept of Local Differential Privacy (LDP) as an innovative strategy to preserve EMR data privacy. LDP is designed to protect against malicious attacks that may attempt to extract sensitive information from the synthesized data. This represents a cutting-edge contribution to the ongoing discourse on balancing the imperative of data synthesis with the critical need to uphold privacy standards, particularly in the intricate landscape of medical data management.

In [11], a cutting-edge machine learning model operating within the federated learning framework is presented, specifically tailored for the standardization of medical Electronic Health Records (EHRs). This approach not only delves into the current landscape of EHR and EHR processing but also anticipates and discusses potential future developments in biomedical datasets and data types. The proposed model represents a forward-looking solution that accommodates the evolving nature of medical data in EHR and EMR systems. In a parallel study, the HealthGAN model [12] is introduced with the primary goal of establishing a secure environment for the synthesis of medical data. This initiative acknowledges the paramount importance of safeguarding the integrity and privacy of medical information during the data synthesis process.

In addition to these advancements, several techniques have emerged to tailor Generative Adversarial Network (GAN) frameworks with a specific focus on enhancing privacy parameters. The Anonymization through Data Synthesis GAN (ADS-GAN) technique [13], GAN models rooted in the Internet of Medical Things (IoMT) [14], and the Privacy Protected GAN [15] each present dedicated methodologies and approaches to reinforce the GAN framework against potential privacy concerns. These customized techniques underscore a commitment to refining the GAN framework to align with the stringent privacy requirements inherent in medical data processing and synthesis [16]. This survey offers a comprehensive exploration of the evolution of GAN models, elucidating their mathematical foundations and the influential parameters governing their effectiveness. The incorporation of GAN models into application frameworks, as advocated by recent research, signifies a collective effort to address the nuanced demands of sensitive datasets, especially within the critical domain of medical studies [17] and further a simplified audio and noise controlled based NN model is discussed in [18] to support the biomedical signal based de-identification. The paper proposed boundary guided semantic learning network by enhancing the segmentation results [19].

III. METHODOLOGY AND MATERIALS

The proposed technique is defined to extract the vulnerable attribute in the medical dataset (D_X) under electronic medical records (EMR).

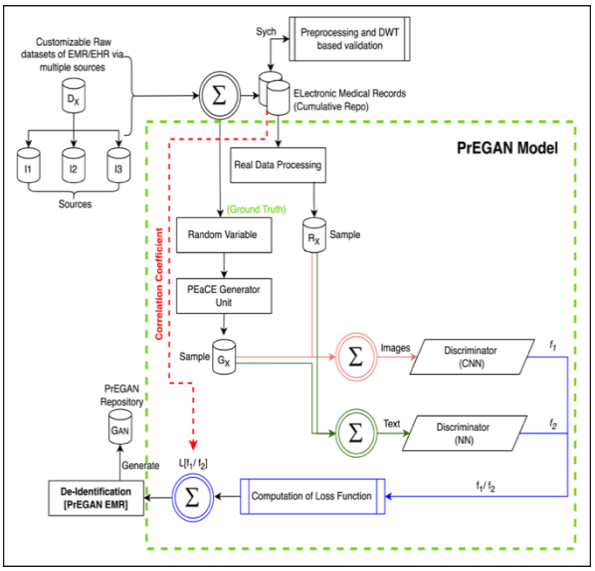

Fig 1. Architecture diagram of proposed PrEGAN model

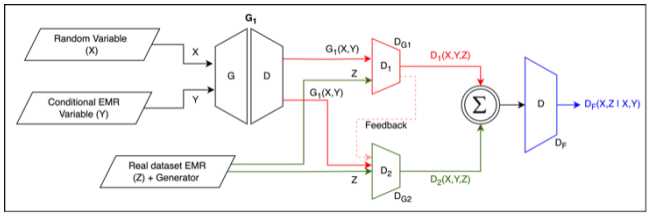

Fig 2. GAN based PrEGAN proposed model schematic representation and function computation.

Typically, the view of de-identification of privacy data or confidential information is termed as extraction of vulnerable variable such as patient_name, age, geographical data, medical linkage and patient_identity_remarks, EMR-Dates and record_indexes etc. The objective of the proposed technique is to identify and evaluate these attributes and variables via Generative Adversarial Networks (GAN) models. The dataset is calibrated from various EMR repositories for a generic medical images and records. These are of global data type such as MRI, CT, PET and X-ray and much more.

To keep the process agnostic, we have considered generic medical image representation as (I_{Gen}) for mathematical modeling under the dataset (D_X), where $(D_X = \{D_{X1}, D_{X2}, D_{X3}....\} \Rightarrow (\sum D_{Xi}))$ such that, (D_{Xi}) is agnostic of EMR repository.

The (D_{Xi}) is further compared under a preprocessing and discrete wavelet transformer (DWT) for segmentation of datasets and attribute extraction. The primary attributes (P_X) and vulnerable attribute (P_Y) are customized in this phase. The proposed GAN model is termed as "Privacy Enhanced Clinical GAN" or "PrEGAN", is a combination of multiple discriminator setup with uni-generator. The customization is demonstrated in Fig. 1, the architectural representation further discusses on the detailed PrEGAN model representation in Fig. 2. The inception random variable (X) and conditional variable termed as vulnerable variable (Y) under a PrEGAN generator for alike variable generation with $G(X,Y)$ and further processed with dual discriminators (D_1, D_2) where (D_1) is subject for CNN and (D_2) is subjected under NN for textual data processing.

The proposed setup of PrEGAN model on clinical dataset (D_X) is further demonstrated in the classification diagram (Fig. 3) where the process is evaluated in four prominent steps. The primary is "customable RAW EMR dataset (D_X)", the second step is "Generator Unit", and the third and

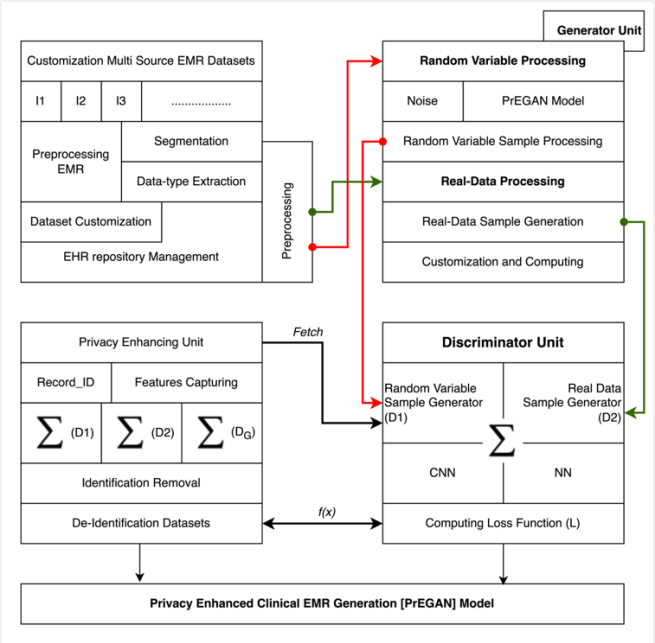

Fig 3. Classification and flow control representation of proposed PrEGAN framework for privacy enhancing and user de-identification on EMR dataset

fourth steps are interconnected via "Discriminator Unit and Privacy enhancing unit". The outcome of this proposed PrEGAN model is to generate/simulate medical and clinical records for efficient decision making by removing the confidential cum privacy data from the EMR's. Thus the PrEGAN repository generated is agnostic of data variable and medical data type for processing and customization. The PrEGAN model is defined on loss function (L) with minimal discrimination losses generated from real-dataset (D_R) with respect to the processed dataset (D_X).

IV. CUSTOMIZABLE RAW EMR DATASET

Consider the evaluation repositories of medical dataset (D_X) such as UCL repository, MIMIC-III, genomic-dataset and Cancer Image Archives (CIA) as $(D_X \Rightarrow \{D_1, D_2, D_3.....D_n\})$ where $(\sum D_X \Rightarrow \wp(A, f))$ and $(D_X \in \wp)$ at given interval of time (t). Since GAN models are time bound and are subjected to change with respect to time (t). The evaluating parameters of $\wp(A, f)$ where (A) is an attribute and (f) is a feature under function $(\wp)$. Thus if $(\wp(A_i, f_i) \Rightarrow D_X)$ then $(\forall D_X \subseteq D)$ where (D) is agnostic dataset of computation. Thus, according to GAN requirements, the supervised learning model datasets are to be aligned and subject under a uniform domain, (i.e.) time or frequency, for evaluation ease, PrEGAN

considers time domain computation. Hence $\left(\forall \wp\left(A_i, f_i\right)_t \Rightarrow \sum D_X\right)$ and further justified in Eq. 1.

$$\lim_{n\to\infty}\left(\wp\right)_t = \sum_{i=1}^{n} \log \wp\left(A_i, f_i\right) \oplus \prod_{k}^{\infty} \log\left(\wp_k\right) \quad (1)$$

Where according to Eq. 1, the function $\left(\wp\right)$ is subjected to the computation of $\left(A_i, f_i\right)$ with $\left(\forall A_i \subseteq f_i\right)$ and $\left(A_i \notin D_\infty\right)$, where $\left(D_\infty\right)$ the excluded dataset repository under supersized learning model's training generation is. The $\left(k\right)$ is the secondary computation variable to enrich the $\wp\left(A_i, f_i\right)$ at time $\left(t+1\right)$. Thus the customization of dataset and attributes array is represented as shown in Eq. 2.

$$\wp\left(A_i, f_i\right) = \lim_{n\to\infty}\left\{\left[\sum_{i=1}^{n}\sum_{k=i+1}^{n}\left(\frac{\delta\left(A_i\right)_k \oplus \delta\left(F_i\right)_k}{\delta t}\right)\right] \oplus \left[\log\left(\wp_k\right)_1^n\right]\right\} \quad (2)$$

$$\therefore \wp\left(A_i, f_i\right)_{t+1} = \arg\min\left(\theta_{GAN}\right) \oplus \wp\left(A_i, f_i\right)_t \quad (3)$$

Thus, according to Eq. 2, the computational variables of $\wp\left(A_i, f_i\right)$ are independent with $\left(t\right)$ and changes with $\left(t+1\right)$ as shown in Eq. 3. According to the setup, the variable $\left(\left(A_i, f_i\right) \Rightarrow A_i\right)$ and are classified as primary variables $\left(P_X\right)$ and hence the Eq. 3 can be realigned as

$$\Rightarrow \wp\left(A_i, f_i\right)_{t+1} = \wp\left(P_X\right)_{t+1} \Rightarrow \arg\min\left(\theta_G\right) \oplus \wp\left(P_X\right)_t \quad (4)$$

$$\therefore \wp\left(P_X\right)_{t+1} \Rightarrow \int_0^{\arg\max\left(\theta_G\right)} \wp\left(P_X\right)_t \oplus \log\left(P - P_X\right)_t \quad (5)$$

Thus according to Eq. 4, the $\left(P_X\right)$ variables are subjected to the customization of values in generating a supervised model for EMR dataset under $\left(\theta_G\right)$ model rules. Typically, the representation is customized as shown in Eq. 5. The attributes and features are resulting to a primary variable $\left(P_X\right)$ and thus $\forall\left(P - P_X\right)_t \Rightarrow \sum\left(P_Y\right)$ for a given time instance $\left(t+1\right)$ and thus shown in Eq. 6.

$$\therefore \wp\left(P_X\right)_{t+1} \Rightarrow \int_0^{\arg\max\left(\theta_G\right)} \wp\left(P_X\right)_t \oplus \log\left(P_Y\right)_{t+1} \quad (6)$$

$$\therefore \wp\left(P_X\right)_{t+1} \Rightarrow \begin{cases} \int_0^{\arg\min\left(\theta_G\right)} \left(\frac{\delta\left[\wp\left(P_X\right)_t\right]}{\delta t}\right) \oplus \log\left(P\right) \\ \int_{a\arg\min\left(\theta_G\right)}^{\arg\max\left(\theta_G\right)} \left(\frac{\delta\left[\wp\left(P_Y\right)_t\right]}{\delta t}\right) \oplus \log\left(P\right) \end{cases} \quad (7)$$

$$\therefore \wp\left(P_X\right)_{t+1} \Rightarrow \begin{cases} \int_0^{\arg\min\left(\theta_G\right)} \sum\left(\Delta P_X\right)_i\}_{i=1}^{\infty} \\ \int_{a\arg\min\left(\theta_G\right)}^{\arg\max\left(\theta_G\right)} \sum\left(\Delta P_Y\right)_i\}_{i=1}^{\infty} \end{cases} \quad (8)$$

The rational differences of $\left(\Delta P_X\right)$ and $\left(\Delta P_Y\right)$ is the primary segregation of attributes with respect to vulnerable variable $\left(\Delta P_Y\right)$ and non-vulnerable variable $\left(\Delta P_X\right)$ such that, $\left(\Delta P_X \cup \Delta P_Y = 0\right)$ and $\left(\Delta P_X \not\subset \Delta P_Y\right)$ at the given time $\left(t\right)$ interval. Hence, the extracted variables of $\left(\Delta P_Y\right)$ are subjected to occurrence between the argmin $\left(\theta_G\right)$ and argmax $\left(\theta_G\right)$. For instance, the minimum space represents the computational value and regional scope represents the maximum computational values of a given attribute $\left(A_i\right)$. Hence summarizing the EMR dataset customization and repository management in Eq. 9 and 10 respectively.

$$\left(D_X\right)_{EMR} = \theta_G \oplus \left[\frac{\arg\min\left(P_X\right)}{t} \bigcup \frac{\arg\max\left(P_Y\right)}{t+1}\right] \quad (9)$$

$$\therefore \left(D_X\right)_{EMR} = \theta_G \oplus \left[\frac{\delta\left(\arg\min\left(P_X\right)\right) \otimes \delta\left(\arg\max\left(P_Y\right)\right)}{\delta\left(t\right)}\right] \quad (10)$$

Where, $\left(\theta_G\right)$ is the backbone supervised model executed in the pattern identification and customization with respect to $\left(\Delta P_X\right)$ and $\left(\Delta P\right)$ as shown in Eq. 10.

V. PRIVACY ENHANCED CLINICAL EMR GENERATOR: PEACE GENERATOR

The generator unit, termed as PEaCE generator, generates the random and customized variables for decision making as shown in classification diagram (Fig. 3). The approach of generator is to customize the random variables (i.e.) primary variables $\left(P_X\right)$ processing and real variable based cloning $\left(\overrightarrow{P_X}\right)$ such that $\left(P_X \Rightarrow \overrightarrow{P_X}\right)$ and $\left(\overrightarrow{P_X} \in D_X\right)$, where $\left(D_X\right)$ is the dataset pool of variables. Typically, the customization random data $\left(P_X\right)$ and aligned data $\left(\overrightarrow{P_X}\right)$ is processed under PrEGAN model as demonstrated in Fig. 2. The variation of PEaCE generator is shown in Eq. 11, where $\left(G\left(\theta_{\max}\right)\right)$ is agnostic generator for $\left(D_X\right)$ dataset such that $\left(\forall D_X = \left(P_X, P_Y\right)\right)$ and $\forall\left(P_X \notin P_Y\right)$ at given $\left(t\right)$ instances.

$$G\left(\theta_{\max}\right) \Rightarrow \arg\min_{\theta\in n}\left[\sum_i f\left(\delta\left(P_X\right)_i\right) \oplus \sum_j f\left(\delta\left(P_Y\right)_j\right)\right] \quad (11)$$

$$\therefore G\left(\theta_{\max}\right) \Rightarrow \arg\min_{\theta\in n}\left[\sum_i\sum_j \left\{\frac{\left(\delta\left(P_X\right)_i\right) \cup \left(\delta\left(P_Y\right)_j\right)}{\delta\left(t\right)}\right\} \times \left(\theta_G\right)\right] \quad (12)$$

Thus according to Eq. 12, the variable $\left(P_X\right)$ and $\left(P_Y\right)$ are subjected to the nominal attribution of data attribute patterns generated as that of $\left(P_X \rightarrow \overrightarrow{P_X}\right)$, then $\left(\forall\left(P_X\right)_i \in \forall\left(\overrightarrow{P_X}\right)_i\right)$

such that, $\left(P_X \Rightarrow D_X \Rightarrow \overrightarrow{P_X}\right)$ at given instance (t). The variable decomposition of (ΔP_X) features (i.e.) $\left(f(\Delta P_X) \cong f\left(\overrightarrow{\Delta P_X}\right)\right)$ is approximately equivalent to $\left(\overrightarrow{\Delta P_X}\right)$. For instance, the primary feature (f_1) in (ΔP_X) is aligned with secondary feature (f_2) in $\left(\overrightarrow{\Delta P_X}\right)$ as the generated attribute values from single origin source (D_X). The attribute values of (ΔP_X) and $\left(\overrightarrow{\Delta P_X}\right)$ alikeness can be bounded under a single representation of Eq. 12 as shown in Eq. 13.

$$\therefore G(\theta_{\max}) \Rightarrow \left\{\left[\left\{\frac{\delta(\Delta P_X)_i}{\delta t} \square \frac{\delta\left(\overrightarrow{\Delta P_X}\right)_j}{\delta t}\right\} \oplus \left\{\arg\min_{\theta \in n}(\Delta P_Y)\right\}\right](\theta_G)\right\} \quad (13)$$

$$\therefore G(\theta_{\max}) \Rightarrow (\theta_G) \cup \left\{\left[\arg\min\left[\left(\Delta P_X \cup \overrightarrow{\Delta P_X}\right)\right] \cap \left\{\arg\min(\Delta P_Y)\right\}\right]\right\} \quad (14)$$

$$\therefore G(\theta_{\max}) \Rightarrow \begin{cases} \arg\min\left[\left((\Delta P_X)_i \cup \left(\overrightarrow{\Delta P_X}\right)_j\right)\right]_{(i,j)} \times (\theta_G) \\ \arg\max\left[(\Delta P_Y)_k\right]_{(k \subseteq [i,j])} \end{cases} \quad (15)$$

Therefore, the fundamental customization variables $\left[G(\theta_{\max})\right]$ as a generator has extracted two series of dataset attributes, where (ΔP_X) and $\left(\overrightarrow{\Delta P_X}\right)$ are from primary, non-vulnerable attributes and (ΔP_Y) are termed as vulnerable attributes. The attribute (ΔP) in general consist of images such as CT, MRI, PER, Xray etc and textural medical data/information from EMR or Electronic Health Records (EHR). The generator (G) in Eq. 15 has discussed the customization and freezing of attribute generated from the generator. The proposed PrEGAN model has considered a single generator unit for attribute customization as shown in Fig. 2 and Fig. 3 respectively. The noise variant of the generator is default associated with (ΔP_X) variables generated in the process. Typically, the series of labels (L_Z) is added on each of (ΔP) variable extracted to segment the attribute as image or textural representation. Such that $(\forall \Delta P_X \Rightarrow L_Z)$ and $(L_Z \neq NULL)$ at (D_X) dataset variables.

A. *Privacy Enhancing Unit (PEU)*

Under this privacy enhancing unit, the generated model $\left[G(\theta_{\max})\right]$ is customized and evaluated with respect to record_id, capturing feature labeling and identification removal. The process of record_id identification is associated with attribute values (ΔP_X) and $\left(\overrightarrow{\Delta P_X}\right)$ at consistent intervals of time. The approach of fundamental processing and customization (C_G) is governed with assignment of attribute values (A_{VAL}) and Indexing (θ_{IND}) such that $\left(\forall \theta_{IND} = \{\theta_1, \theta_2, \theta_3 ....\}\right)$ where (θ_i) are the independent labels associated with one particular attribute function. Using (θ_{IND}) the label values (A_{VAL}) is assigned as $(\theta_{IND} \exists A_{VAL} \,/\, A_{VAL} \subseteq P_X)$ and thus on association, the (A_{VAL}) attributes are further dependent on $\left(\overrightarrow{\Delta P_X}\right)$ occurrence with respect to changing time as shown in Eq. 16.

$$C_G = \lim_{n \to \infty}\left(\int_{\theta_{IND}}^{\infty} \frac{\delta(A_{VAL})}{\delta(P_X)} \cap \frac{\delta\left(\overrightarrow{P_X}\right)}{\delta(A_{VAL})}\right) \quad (16)$$

On customization representation, the $\delta(A_{VAL})$ value is subjected to fundamental time changes (i.e.) $\delta(t) \to \delta(t+1)$ then $\left[\delta(A_{VAL}) \Rightarrow \delta\left(\overrightarrow{A_{VAL}}\right)\right]$ at rational variation of values associated with time series such that $\left[(\Delta t \to \Delta t + 1) \Rightarrow \Delta \overrightarrow{P_X}\right]$. This association is reflected and customized with changing time and thus the representation is shown in Eq. 17.

$$C_G = \lim_{n \to \infty}\left(\log_n\left(\delta(A_{VAL})\right) \oplus \int_{\theta_{IND}}^{\infty} \frac{\delta(P_X) \to \delta\left(\overrightarrow{P_X}\right)}{\delta(t)}\right) \quad (17)$$

$$C_G = \lim_{n \to \infty}\left(\sum_i^{\infty}\left\{\log_n\left(\delta(A_{VAL})_i\right) \oplus \int_{\theta_{IND}}^{\infty} \frac{\delta(P_X)_i \to \delta\left(\overrightarrow{P_X}\right)_{i+1}}{\delta(t)}\right\}\right) \quad (18)$$

Thus according to the representation, the (C_G) customization is bounded with respect to $\log_n\left(\delta(A_{VAL})\right)$ value as the changing (A_{VAL}) is impacted directly on the customization process of (ΔP_X). The associations of (ΔP_X) attributes are alike with $\left(\overrightarrow{\Delta P_X}\right)$ attribute and thus the summarization is as shown in Eq. 19 for value attribute extraction.

$$C_G = \lim_{n \to \infty}\left(\sum_i^{\infty}\left\{\log_n\left(\delta(A_{VAL})_i\right) \oplus \int_{\theta_{IND}}^{\infty} \frac{\delta^2(P_X)_i}{\delta(t)^2}\right\}\right) \quad (19)$$

The value on (C_G) is a robust variable approach for extracting and customizing the privacy value and adding a label index on identifying the vulnerability attribute in (ΔP_X). Such that $(\Delta P_Y \subseteq \Delta P_X)$ and $(\Delta P_X \in \square_d)$ as $(\square_d)$ variable at random instance is associated with (ΔP_X) and

$\left(\Delta P_X \rightarrow \Delta P_Y \Rightarrow \square_{d}\right)$ in instance resolving of vulnerable attributes as shown in Eq. 20.

$$\Delta P_Y \Rightarrow \begin{cases} if\left[A_{VAL} < C_G\right]: label\left(P_X\right) \\ f\left[A_{VAL} \geq C_G \,||\, P_X\right]: label\left(\overrightarrow{P_X}\right) \\ else[\ ]: label\left(P_Y\right) \end{cases} \tag{20}$$

From the Eq. 20, a demonstrative representation of fundamental $\left(A_{VAL}\right)$ classification with respect to $\left(\Delta P_Y\right)$ extraction. The overall view, $\left(\Delta P_Y\right)$ attributes are eliminated from $\left(\Delta P_X\right)$ and $\left(\overrightarrow{\Delta P_X}\right)$ attributes. Such that $\left(\Delta P_Y\right)$ the vulnerable attributes are extracted from $\left(C_G\right)$ process. Typically, the privacy enhancing unit (PEU) is aligned with terms to the PEaCE generator unit for vulnerable attribute identification and computing. The processed $\left(\Delta P_Y\right)$ in $\left(C_G\right)$ is feed as a discriminator function to identify the alikeness of sensitive variable location in medical cloning process.

B. EMR GAN Discriminator Unit

The discriminator unit is to justify the computation reliability and similarity with respect to original (Real) and random variable as demonstrated in Fig. 2. The further evaluation of discriminator $\left(D_{GAN}\right)$ is implemented in $\left(D_{GAN} \rightarrow \left[P_X \bigcap P_Y\right]\right)$ such that $\left(\forall P_X \in C_G\right)$ and $\left[C_G \subseteq G\left(\theta_{MAX}\right)\right]$ at given rational instances. Typically, the fundamental unit of evaluating a discriminator $\left(D_{GAN}\right)$ is based on effectiveness in identifying the vulnerable variables $\left(\Delta P_Y\right)$ and thus eliminating $\left(\Delta P_Y\right)$ in dataset cloning process under GAN model. The $\left(D_{GAN} \not\subset G\left(\theta_{MAX}\right)\right)$ on a direct corelationship mapping and assures the functioning of $\left(D_{GAN}\right)$ in an independent phase. The primary data type in medical/clinical is images and textural data and hence a discriminator independently processes the images under a defined convolutional neural networking (CNN) and textural data in neural networking model as shown in Fig. 1. The Computation of loss function $\left(\gamma\right)$ is shown in Eq. 21.

$$\gamma = \begin{cases} \forall \gamma_1 : \lim\limits_{n\to\infty}\left[\dfrac{\delta\left(P_Y\right)}{\delta t} \oplus \left(A_{VAL}\right)_{C_G}\right] \\ \forall \gamma_2 : \lim\limits_{n\to\infty}\left[\dfrac{\delta\left(P_Y\right)}{\delta t} \oplus \left[G\left(\theta_{MAX}\right)\right]\right] \end{cases} \tag{21}$$

$$\therefore \gamma = \begin{cases} \forall \gamma_1 : [CNN]: \left\{\dfrac{\partial^2\left(P_Y\right)}{\partial t^2} \oplus \log\left[A_{VAL}\right] \times e^{C_G}\right\} \\ \forall \gamma_2 : [NN]: \left\{\dfrac{\partial^2\left(P_Y\right)}{\partial t^2} \oplus \left(-\log\left[A_{VAL}\right] \times e^{C_G}\right)\right\} \end{cases} \tag{22}$$

$$\therefore \gamma \Rightarrow \left[\left(\gamma_2 - \gamma_1\right) \times e^{C_G}\right] \tag{23}$$

Thus according to Eq. 23, the loss function $\left(\gamma\right)$ and its associated values from $\left(C_G\right)$ is dependent factor for decision making and discriminator computation. Thus, $\left[\gamma_1 \leq C_G \leq CNN\left(\Delta \mathrm{T}\right)\right]$ then compute a function of image discrimination else compute textural data discriminator, here $\left(\Delta \mathrm{T}\right)$ is the threshold value fixed for the neural networking computation to surpass the evaluation phase of the dataset.

VI. RESULTS AND OBSERVATIONS

The computational representation of the proposed technique is based on the de-identification process of the user information from the Electronic Medical Records (EMR). The objective is to extract the vulnerable attributes via Region of Interest (RoI) identification within the sampling range of the datasets $\left(D_X\right)$. The evaluation process of the proposed PrEGAN model is supported with a dedicated EMR datasets from UCL repository, MIMIC-III and CHD. These dataset repositories include various sequels of biomedical data-types such as MRI images, CT images, X-Ray images and textural files with expert recommendation and treatment history. The dataset is acuminated in a common DRIVE portal for processing and customization. This includes a preprocessing and data segmentation operations. Typically, the image input data (medical) is resized with 512*512 pixel. The CNN model based discriminator provides a de-convolutional filter patterns for image RoI extraction with respect to $\left(\Delta P_X\right)$ and $\left(\overrightarrow{\Delta P_X}\right)$ image attributes. The representation of pattern extracted and elevated under the training and testing model for various epochs is represented in Table. 1. The model is implemented on NVIDIA A5000 RTX GPU units under kubeADM cluster (local) nodes for centralized dataset $\left(D_X\right)$ storage.

According to Table. 1, the instances of $\left(\overrightarrow{\Delta P_X}\right)$ is dependent on the RoI of $\left(\Delta P_X\right)$ with respect to the range loss computed during the process of RoI extraction. The evaluated pattern of $\left(\overrightarrow{\Delta P_X}\right)$ similarity is bound to the loss function $\left(\gamma\right)$ computation and the interfacing attribute thresholding ratio from the neural networking model. The influence is bounded on internal occurrence of the vulnerable attribute amid of primary and non-vulnerable attributes. The training and validating represented is shown in Fig. 4. The training is processed on 200 epochs for RoI extraction in $\left(\Delta P_X\right)$ such

that, the further detailed analysis on epoch 100, 150 and 200 is represented in Fig. 5.

The split representation previews the learning curve of proposed PrEGAN model under training and testing phase with respect to (D_X) datasets. Whereas the detailed representation on internal loss at individual epoch is demonstrated in Fig. 6. The moving average of the training and testing curve is analyzed and represented for an individual model based (ΔP_X) attribute extraction and learning. The PrEGAN model is subjected to be evaluated under NN and CNN for independent data type mapping and further (NN+CNN) model with PrEGAN rules are aligned for generative learning. The detailed representation is shown in Fig. 7.

Table. 1: $(\overrightarrow{\Delta P_X})$ similarity score mapping and extraction via dependency rule of (ΔP_X) variables on a dataset (D_X)

Epoch	(ΔP_X) extracted variables	$(\overrightarrow{\Delta P_X})$ extracted variables	ROI probability (%)	Range Loss (%)	$(\overrightarrow{\Delta P_X})$ similarity (%)
50	39	37	85.32	33.21	89.61
75	39	38	85.93	30.32	89.91
100	40	40	85.99	31.03	90.31
125	40	40	84.32	30.42	89.24
150	40	40	86.12	28.42	90.18
175	40	40	86.41	28.94	90.21
200	40	40	86.88	28.03	90.47

Fig. 4. Training and testing loss computation over the primary vulnerable attribute training model

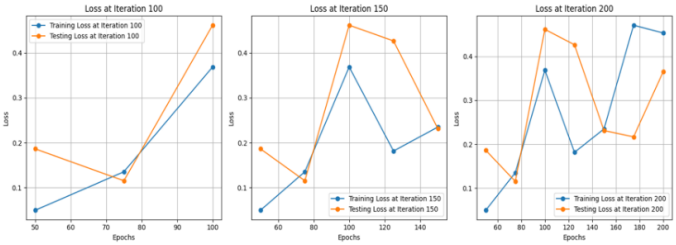

Fig. 5: Representation of losses (γ) incurred under primary attribute (ΔP_X) extraction

The (NN+CNN+PrEGAN) representation in Fig. 7, demonstrates the training and testing phases of individual and collective model, as per the proposed system, the defined model is subjected to extract vulnerable attributes i.e. (ΔP_Y). Since the early phase of GAN model is to summarize the learning parameters in dataset (D_X), hence the individual process of evaluating losses from the similar and vulnerable attributes are computed in Eq. 23 and further represented in Fig. 8. The collective summarization of the performance matrix from the proposed system is summarized in Fig. 9. The accuracy of PrEGAN is evaluated at 88.32%, compared to CNN and NN, the PrEGAN is a hybrid approach for customizing the attributes via Generative Learning (GL) and hence the process of computing and training is relatively unbound to that of CNN and NN. Hence, the loss computation of PrEGAN is relativity lower compared to the NN and CNN models in an individual state.

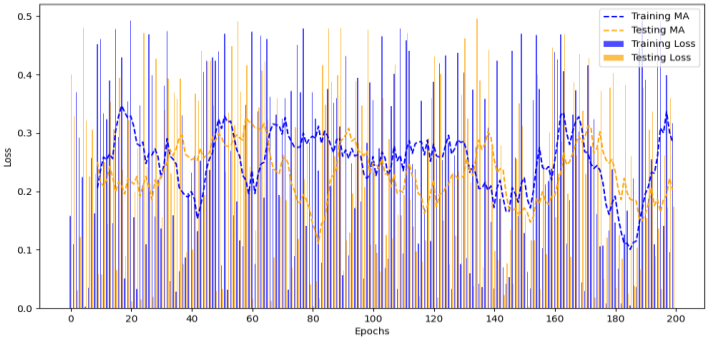

Fig. 6: Representation of training and testing loss under single iterative model training of PrEGAN model and supporting moving average of learning curve.

VII. CONCLUSION

The Privacy Enhanced Clinical Electronic Medical Record Generation Model (PrEGAN) is proposed with the primary objective of advancing the de-identification process applied to electronic medical records (EMR). At its core, PrEGAN utilizes a dual discriminator approach, a sophisticated technique designed to discern between vulnerable and non-vulnerable attributes within the EMR dataset. PrEGAN, is able to precisely delineate the areas within the EMR that require heightened privacy considerations, contributing to a more refined and targeted de-identification process.

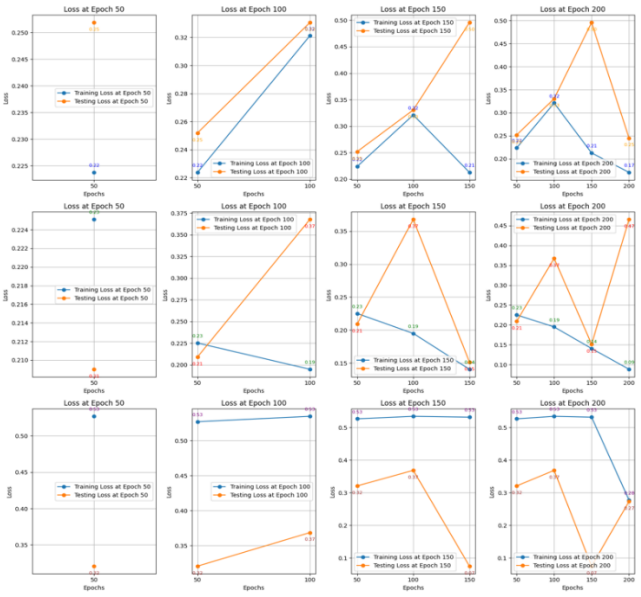

Fig. 7: A collective representation of training and testing loss function (γ) computation with (top row) representing the computation via NN model for (ΔP_X) evaluation, (middle row) representing the computation via CNN model for (ΔP_X) evaluation and (last row) representing the computation of proposed PrEGAN model computation of (ΔP_X).

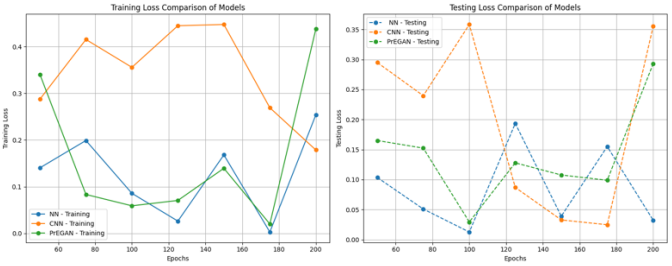

Fig. 8: Comparative representation of proposed PrEGAN model performance in training and testing with reference to CNN, NN and PrEGAN

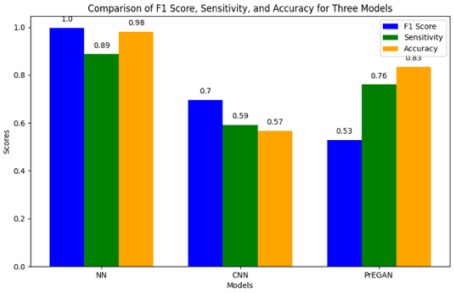

Fig. 9: Performance comparison and computation matrix representation with respect to NN, CNN and PrEGAN models.

A significant accomplishment of the PrEGAN model is its successful elimination of dependencies on specific attributes within the EMR. This multifaceted approach enables the model to effectively analyze diverse types of information within the EMR, enhancing its overall performance. In rigorous evaluations, PrEGAN demonstrates a remarkable accuracy rate of 88.32% in identifying vulnerable attributes within the EMR. This attests to the efficacy of the model in ensuring the robust protection of sensitive information during the de-identification process.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R432), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

REFERENCES

1. I. Goodfellow et al., "Generative adversarial nets," *Adv. Neural Inf. Process. Syst.*, vol. 27, 2014.
2. Y. Wang, 2020, "A mathematical introduction to generative adversarial nets (GAN)," *arXiv Preprint ArXiv:2009.00169*.
3. M. Durgadevi, "Generative adversarial network (gan): A general review on different variants of gan and applications" in 6th International Conference on Communication and Electronics Systems (ICCES), vol. 2021. IEEE, 2021, Jul., pp. 1-8.
4. T. Zhou et al., "GAN review: Models and medical image fusion applications," *Inf. Fusion*, vol. 91, pp. 134-148, 2023 [doi:10.1016/j.inffus.2022.10.017].
5. A. You et al., "Application of generative adversarial networks (GAN) for ophthalmology image domains: A survey," *Eye Vis. (Lond)*, vol. 9, no. 1, pp. 6, 2022 [doi:10.1186/s40662-022-00277-3].
6. M. Abedi et al., "GAN-based approaches for generating structured data in the medical domain," *Appl. Sci.*, vol. 12, no. 14, p. 7075, 2022 [doi:10.3390/app12147075].
7. M. Krithika alias Anbu Devi and K. Suganthi, "Review of medical image synthesis using GAN techniques" in *ITM Web Conf.* EDP Sciences, vol. 37, 2021 [doi:10.1051/itmconf/20213701005].
8. M. Frid-Adar et al., "GAN-based synthetic medical image augmentation for increased CNN performance in liver lesion classification," *Neurocomputing*, vol. 321, pp. 321-331, 2018 [doi:10.1016/j.neucom.2018.09.013].
9. R. Venugopal et al., "Privacy preserving generative adversarial networks to model electronic health records," *Neural Netw.*, vol. 153, pp. 339-348, 2022 [doi:10.1016/j.neunet.2022.06.022].
10. H. Gwon et al., "LDP-GAN: Generative adversarial networks with local differential privacy for patient medical records synthesis," *Comput. Biol. Med.*, vol. 168, p. 107738, 2024 [doi:10.1016/j.compbiomed.2023.107738].
11. D. K. Heyland et al., "Procalcitonin for reduced antibiotic exposure in the critical care setting: A systematic review and an economic evaluation," *Crit. Care Med.*, vol. 39, no. 7, pp. 1792-1799, 2011 [doi:10.1097/CCM.0b013e31821201a5] [PMID:21358400].
12. A. S. Fathima et al., "Federated learning based futuristic biomedical big-data analysis and standardization," *PLOS ONE*, vol. 18, no. 10, p. e0291631, 2023 [doi:10.1371/journal.pone.0291631].
13. A. Yale et al., "Generation and evaluation of privacy preserving synthetic health data," Neurocomputing, vol. 416, pp. 244-255, 2020 [doi:10.1016/j.neucom.2019.12.136].
14. J. Yoon et al., "Anonymization through data synthesis using generative adversarial networks (ads-gan)," IEEE J. Biomed. Health Inform., vol. 24, no. 8, pp. 2378-2388, 2020 [doi:10.1109/JBHI.2020.2980262].
15. I. Vaccari et al., "A generative adversarial network (gan) technique for internet of medical things data," Sensors (Basel), vol. 21, no. 11, p. 3726, 2021 [doi:10.3390/s21113726].
16. Y. He, X. Jin, Q. Jiang, Z. Cheng, P. Wang, and W. Zhou, "LKAT-GAN: A GAN for Thermal Infrared Image Colorization Based on Large Kernel and AttentionUNet-Transformer," IEEE Transactions on Consumer Electronics, vol. 69, no. 3, pp. 478–489, Aug. 2023, doi: 10.1109/tce.2023.3280165.
17. H. Yan, H. Zhang, J. Shi, J. Ma and X. Xu, "Inspiration Transfer for Intelligent Design: A Generative Adversarial Network With Fashion Attributes Disentanglement," in *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 1152-1163, Nov. 2023, doi: 10.1109/TCE.2023.3255831
18. S. Xu, X. Xu, H. Gao and F. Xiao, "TLS-WGAN-GP: A Generative Adversarial Network Model for Data-Driven Fault Root Cause Location," in *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 850-861, Nov. 2023, doi: 10.1109/TCE.2023.3300442

19. R. Cong et al., "Boundary Guided Semantic Learning for Real-Time COVID-19 Lung Infection Segmentation System," in IEEE Transactions on Consumer Electronics, vol. 68, no. 4, pp. 376-386, Nov. 2022, doi: 10.1109/TCE.2022.3205376.