International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Privacy Preservation using Deep Learning Methods

Amreen Ayisha M[1], Ankit Kumar[2], Gasti Harshini[3], Keerthana S[4],Mrs. Samatha R Swamy[5]

[12345] *ayishaamreen78@gmail.com, ankit.astaim@gmail.com, harshinisweety61@gmail.com, twinklekee026@gmail.com, samatha-ise@dsatm.edu.in*

[1234]*Student, Department of Information Science and Engineering, DSATM, Bangalore-88, Karnataka*

[5]*Faculty, Department of Information Science and Engineering, DSATM, Bangalore-88, Karnataka*

Abstract- Heart disease is a major concern worldwide , and the analysis of heart disease - related data can provide valuable insights for healthcare professionals and researchers. However , sharing such data poses a significant risk to individuals' privacy , as personal information can be used to re-identify individuals. To address this issue, techniques as k-anonymization, randomization is employed in our project protecting individuals privacy and deriving meaningful analysis of data. We have created the random data using Faker library. Providing the specific attributes it randomly generates the values. We have generated 10000 rows for four columns. Privacy preserving techniques are applied to this data and which is shown in the background, We have also included the prediction of heart disease which is a website. This predicts the presence or absence of the disease based on realistic data. Our website also provides the information about heart disease. When the required data is entered by the user, that data can be viewed in encrypted form except the age all the other factors are encrypted for privacy concerns. This is to show how the data is encrypted. Our results show that k-anonymization and randomization techniques can be used together to achieve privacy-preserving analysis of heart related data , making it possible to derive valuable insights from such data without compromising individuals' privacy.

Keywords- K-anonymization, Randomization, Prediction, Encrypted data, Security, Faker library.

I. INTRODUCTION:

Privacy preservation methods like k-anonymization, randomization play a crucial part as safeguarding the sensitive information of individuals, particularly in the context of heart disease prediction. Also using these methods and allowing those dataset to be used for research [11]. Heart disease is a prevalent health concern globally, and predicting its occurrence can aid in early detection and intervention. However, accessing and analyzing personal health data introduces privacy risks. To mitigate these risks, privacy preservation techniques are employed [14]. A common technique for anonymizing data is called k-anonymization, which makes sure that each person's data cannot be distinguished from the information of at least k-1 other people. By grouping and generalizing data attributes, such as age ranges and medical conditions[20]. Randomization techniques add an additional layer of privacy preservation. They introduce noise pr perturbations to the data, making it harder for unauthorized users to identify specific individuals. Randomization helps prevent re-identification attacks and further enhances privacy preservation[2].

When applied to heart disease prediction, privacy preservation techniques enable researchers and healthcare professionals to work with anonymized data while maintaining .

the privacy rights of patients. By anonymizing and randomizing personal health information, the privacy risks associated with heart disease prediction are significantly reduced. [3],[15]. We have used Faker library to create a dataset. The dataset is preserved using K-anonymization and randomization. Along with the privacy preservation which is shown at the background, we have a website for prediction of heart disease presence or absence. Where users are allowed to enter required medical data values. These entered data are preserved using hash encryption method . These encrypted data can not be decrypted for further use, except the age parameter other medical information is hidden. With this we can analyse what age group people mostly uses our project[4].

II. METHODOLOGY

Let's analyze different algorithms used to protect sensitive data, including randomization, k-anonymization, and data encryption using hashing methods.

1. Randomization:

Randomization involves adding noise or perturbation to the original data to preserve privacy. The goal is to make it difficult for an attacker to identify specific individuals or sensitive information within the dataset. Randomization techniques include:

- Randomized Response: This method introduces random noise into survey responses, ensuring plausible deniability and preserving privacy.
- Differential Privacy: To secure individual privacy while keeping statistical accuracy, differential privacy introduces noise to the query results.
- Secure Multi-party Computation: It enables multiple parties to compute on their combined data without revealing their individual inputs.
- Deep learning methods can be used to develop randomization algorithms that generate synthetic data that approximates the original data distribution.

Here's a general framework for developing a randomization algorithm using deep learning:

1. Data preprocessing: Prepare the original dataset for training the deep learning model. This may involve standardizing features, handling missing values, and encoding categorical variables.
2. Synthetic data generation: Use the trained deep learning model to generate synthetic data points. This can be done by sampling from the learned latent space of the model or directly generating new data points.
3. Randomization mechanism: Apply a randomization mechanism to the synthetic data to introduce additional noise and privacy protection. This can involve techniques such as adding random noise, perturbing data points, or shuffling attributes while preserving certain statistical properties of the original data.
4. Evaluation: Assess the utility and privacy guarantees of the randomized data. Measure the similarity between the original and randomized data using metrics such as Jensen-Shannon divergence, Wasserstein distance, or classification accuracy. Additionally, evaluate the privacy protection achieved by analyzing the re-identification risk or information leakage.
5. It's worth noticing that the effectiveness for randomization method relies on the quality of the deep learning model and the randomness introduced during the randomization process. The exact needs of the data and the required level of privacy protection will determine the deep learning architecture, training approach, and randomization mechanism to use.

Furthermore, it's crucial to thoroughly evaluate the privacy guarantees of the randomized data and ensure that it cannot be easily re-identified or linked to individuals. Privacy risk assessments and validation against privacy attacks should be conducted to ensure performances of the randomization algorithm.

Overall, deep learning-based randomization algorithms have the potential to generate synthetic data that preserves privacy while maintaining data utility. When developing and putting such algorithms into practise, it's crucial to take the unique application and privacy requirements into account.

2. K-Anonymization:

K-anonymization is a technique that aims to anonymize data by grouping individuals into clusters (also known as equivalence classes) where each cluster contains at least k individuals. This prevents the identification of specific individuals. Common algorithms used for k-anonymization include:

- Generalization: Replacing specific values with more generalized ranges, such as replacing exact ages with age ranges.
- Suppression: Removing or suppressing certain attributes or values to prevent identification.
- Data Swapping: Swapping values between

individuals to preserve statistical properties while maintaining privacy.

2. Even while deep learning has been used to do a number of tasks, including image recognition and natural language processing, it is not commonly used directly for k-anonymization. Traditional k-anonymization algorithms, such as generalization and suppression-based methods, are more commonly employed due to their simplicity and effectiveness.

And, it can be utilized as a complementary technique to enhance the effectiveness of k-anonymization. Here's a general framework which combines k-anonymization and deep learning:

1. Preprocessing: Transform the raw data into a deep learning-friendly format. This could entail separating the data between training and validation sets, normalising numerical features, and encoding categorical variables.
2. Deep learning model training: Train a deep learning model on the dataset using techniques such as neural networks or convolutional neural networks (CNNs).
3. Feature extraction: Extract the learned features from the trained deep learning model. Either the output of an intermediary layer can be used, or dimensionality reduction methods like principal component analysis (PCA) or t-SNE can be used.
4. K-anonymization: Apply traditional k-anonymization techniques to the extracted features. To do this, the traits are often generalised and suppressed so that each individual cannot be distinguished from at least k-1 other individuals.
5. Evaluation: Assess the effectiveness of the k-anonymization process by measuring the information loss and the privacy guarantee achieved. This can be done using metrics such as entropy, information gain, or the average pairwise distance between records.

It's critical to understand that the success of this strategy depends on the quality and representativeness of the learned features. Additionally, the choice of deep learning architecture, training methodology, and k-anonymization technique will vary depending on the specific dataset and privacy requirements.

Overall, while deep learning can enhance the feature representation in the k-anonymization process, it is typically used in combination with traditional k-anonymization techniques rather than as a standalone algorithm.

3. Data Encryption using Hashing:

Data is converted into a fixed-length character string, known as a hash value or digest, using the one-way encryption technique of hashing. It is commonly used to protect sensitive data by securely storing passwords or validating data integrity. Some hashing algorithms include:

- Secure Hash Algorithm (SHA-2, SHA-3): Cryptographic hash functions that generate a unique fixed-size hash value for a given input, making it computationally infeasible to reverse-engineer the original data.
- Message Digest Algorithm (MD5): Although widely used, MD5 is considered weak for cryptographic purposes due to vulnerabilities. It is more suitable for checksum validation or non-security-related tasks.

It's important to note that while encryption using hashing provides data integrity and non-repudiation, it does not provide confidentiality. If confidentiality is required, symmetric or asymmetric encryption algorithms, such as AES or RSA, should be used.

The choice depends on the particular requirements of the use case as each of these algorithms has benefits and disadvantages, level of privacy required, and the potential threats faced. It is advisable to consult security professionals and adhere to industry best practices when implementing data protection techniques.

Here's a basic framework for using hashing as a privacy-preserving encryption method:

1. Data preprocessing: Prepare the data to be encrypted. This may involve converting the data into a suitable format, such as strings or byte arrays.
2. Hash function selection: Choose a suitable hash function for the encryption process.

Used hash functions include MD5, SHA-1, SHA-256, and bcrypt. It's important to select a hash function that provides a good balance between security and performance.

3. Hashing process: Apply the selected
4. hash function to the data. The hash function will generate a fixed-length hash value that represents the input data. This hash value is typically a non-reversible, unique representation of the original data.
5. Storage or transmission: Store or transmit the

generated hash value instead of the original data. This ensures that the sensitive information remains protected. For example, in the case of password storage, the password is hashed and only the hash value is stored in the database.

6. Verification: When it is necessary to verify the data, such as during user authentication utilizing the same hash algorithm, the input data is hashed, and the calculated hash value is compared to the previously calculated hash value. The data is regarded as legitimate if the two hash values coincide.

It's important to note that while hashing provides privacy protection by preventing the recovery of the original data from the hash value, it is susceptible to brute-force attacks and rainbow table attacks. Therefore, to enhance the security of hashed data, additional techniques such as salting and iterating the hash function multiple times (key stretching) can be applied.

Before hashing, the data is salted by adding a random string of characters (salt).. The salt is stored alongside the hash value. This prevents precomputed attacks (using rainbow tables) because the attacker needs to compute a new rainbow table for each unique salt.

Key stretching involves repeatedly hashing the data (with or without salt) for a certain number of iterations. This increases the computational cost of hashing, making it more difficult for attackers to guess the original data through brute-force or dictionary attacks.

It's crucial to consider the specific requirements and security considerations of your application when implementing hashing for privacy-preserving encryption. Hashing alone may not provide the same level of security as modern encryption algorithms, such as symmetric or asymmetric encryption. Therefore, it's important to assess the privacy and security requirements of your use case and consult security experts when necessary.

Since our project mainly focuses on predicting and securing the user's medical data, encryption using hashing method is considered as the best approach because the original data cannot be derived from the hash value and protects the sensitive data and it also cannot be used for further analysis and research whereas the data derived from K anonymization and randomization can used used to further analysis.

Hashing is primarily used for data integrity verification and password storage, while MLPs are employed for predictive modeling and pattern recognition tasks.

However, it is possible to combine encryption and predictive modeling in a broader system architecture where encryption is used to protect sensitive data, including input features, while the predictive model utilizes the encrypted data for analysis or inference. Here's a general outline:

1. Data preprocessing: Prepare the sensitive data for encryption and feature engineering. This may involve data cleaning, normalization, and encoding categorical variables.
2. Encryption using hashing: Apply a suitable hashing algorithm, such as MD5 or SHA-256, to the sensitive data, including the input features. This ensures that the data is securely transformed into irreversible hash values.
3. Predictive model training: Train an MLP neural network on data which is encrypted. The encrypted data acts as the input to the model, while the target labels are used for supervised learning. The MLP learns the underlying patterns and relationships within the encrypted data.
4. Predictive model deployment: Once the MLP model is trained, it can be deployed for inference on new, encrypted data. The input data is hashed, similar to the training process, and fed into the deployed MLP model for predictions or other analysis tasks.

It's important to note that during the inference phase, the MLP model operates on the hashed data, meaning it doesn't have access to the original sensitive information. Therefore, the predictive model's output is based solely on the patterns learned from the encrypted data.

The key advantage of this approach is that it offers a level in privacy protection for the sensitive data, as the original information is not directly exposed to the predictive model. However, it's important to consider the limitations and challenges that arise from working with encrypted data, such as the inability to interpret or understand the predictions in terms of the original data.

Furthermore, the encryption and hashing techniques used should be carefully chosen to ensure strong security and avoid vulnerabilities. Consulting with security and privacy experts and adhering to industry best practices are crucial when implementing such systems to protect sensitive data while utilizing predictive modeling capabilities.

III. CONCLUSION:

The "privacy preservation using deep learning methods" project was designed to develop a web application that predicts whether a user is a heart patient or not while ensuring the privacy of the user's health-related data. The project was divided into two modules - prediction and privacy and utilized deep learning techniques to train a model that achieved high accuracy in predicting heart disease. The project successfully implemented privacy-preserving measures by encrypting all user inputs, except for age, before storing them in the database. This ensured that user data remains confidential and cannot be accessed by unauthorized users. The results of the project demonstrate the importance of privacy preservation in health-related applications and the effectiveness of using deep learning methods to predict heart disease. The web application developed as part of the project was user-friendly and easy to use, providing accurate predictions of whether a user is a heart patient or not. The project can be extended to address other health-related prediction tasks and can be further improved by incorporating additional health-related factors.

IV. RESULT:

Using privacy preservation techniques like k-anonymization and randomization in the context of heart disease have been promising.

K-anonymization ensures that individual identities are preserved by grouping and generalizing data attributes. This anonymization technique prevents unauthorized identification of specific individuals, safeguarding their privacy rights. Where based on the attributes it replaces the first few letters of the word with asterisk symbol.

Reduced Re-identification Risk is reduced using Randomization techniques that introduces noise or perturbations into the data, making it more challenging to re-identify individuals. This mitigation significantly reduces the risk of re-identification attacks and unauthorized disclosure of personal health information.

Despite anonymization and randomization, the predictive utility of the data is maintained. Researchers and healthcare professionals can still extract meaningful insights from the anonymized dataset to develop accurate heart disease prediction models. By prioritizing privacy protection, organizations and institutions foster public trust in their handling of sensitive health information. Individuals are more likely to participate in heart disease research knowing that their privacy is being respected and protected. Where in our prediction website we ensure the users data are not used by anyone. The data entered by the users for predicting the presence or absence of disease are preserved using hash method where data is completely encrypted except the age.Thus ensuring the privacy of medical data of the users.

REFERENCES:

1. Agrawal, Shaashwat, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. "Federated learning for intrusion detection system: Concepts, challenges and future directions." Computer Communications(2022).
2. Singh, Saurabh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, and Byungun Yoon. "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology." Future Generation Computer Systems 129 (2022): 380-388.
3. Durrant, Aiden, Milan Markovic, David Matthews, David May, Jessica Enright, andGeorgios Leontidis. "The role of cross-silo federated learning in facilitating data sharing in the agri-food sector." Computers andElectronics in Agriculture 193 (2022): 106648.
4. Lee, Joon-Woo, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee et al. "Privacy- preserving machine learning with fully homomorphic encryption for deep neural network." IEEE Access 10 (2022): 30039- 30054
5. Dou, Qi, Tiffany Y. So, Meirui Jiang, Quande Liu, Varut Vardhanabhuti, Georgios Kaissis, Zeju Li et al. "Federated deep learning fordetecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study." NPJ digital medicine 4, no. 1 (2021):
6. Ali, Mansoor, Faisal Naeem, Muhammad Tariq, and Geroges Kaddoum. "Federatedlearning for privacy preservation in smart healthcare systems: A comprehensive survey." IEEE journal of biomedical and healthinformatics (2022).

7. Nguyen, Tham, Naveen Karunanayake, Sicong Wang, Suranga Seneviratne, and Peizhao Hu. "Privacy-preserving spam filtering using homomorphic and functional encryption." Computer Communications 197(2023): 230-241.
8. Shorten, Connor, Taghi M. Khoshgoftaar, and Borko Furht. "Deep Learning applications for COVID-19." Journal of big Data 8, no. 1 (2021): 1-54.
9. Alguliyev, Rasim M., Ramiz M. Aliguliyev, and Fargana J. Abdullayeva. "Privacy- preserving deep learning algorithm for big personal data analysis." *Journal of Industrial Information Integration* 15 (2019): 1-14.
10. Alkhelaiwi, Munirah, Wadii Boulila, Jawad Ahmad, Anis Koubaa, and Maha Driss. "An efficient approach based on privacy-preserving deep learning for satellite image classification." *Remote Sensing* 13, no. 11 (2021): 2221.
11. Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, and Gautam Srivastava. "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot." IEEE Transactions on Industrial Informatics 18, no. 9(2022): 6358-6367.
12. Huang, Qi-Xian, Wai Leong Yap, Min-Yi Chiu,and Hung-Min Sun. "Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images." IEEE Access 10 (2022): 66345-66355.
13. Popescu, Andreea Bianca, Ioana Antonia Taca, Anamaria Vizitiu, Cosmin Ioan Nita, Constantin Suciu, Lucian Mihai Itu, and Alexandru Scafa-Udriste. "Obfuscation Algorithm for Privacy-Preserving Deep Learning-Based Medical Image Analysis." Applied Sciences 12, no. 8 (2022): 3997.
14. Gupta, Deepti, Smriti Bhatt, Paras Bhatt, Maanak Gupta, and Ali Saman Tosun. "Game Theory Based Privacy Preserving Approach for Collaborative Deep Learning in IoT." In Deep Learning for Security and Privacy Preservation in IoT, pp. 127-149. Singapore: Springer Singapore, 2022.
15. Dash, Bibhu, Pawankumar Sharma, and Azad Ali. "Federated Learning for Privacy- Preserving: A Review of PII Data Analysis in Fintech." *International Journal of Software Engineering & Applications (IJSEA)* 13, no. 4 (2022).
16. Ali, Mansoor, Faisal Naeem, Muhammad Tariq, and Geroges Kaddoum. "Federatedlearning for privacy preservation in smart healthcare systems: A comprehensive survey." IEEE journal of biomedical and health informatics (2022).
17. Han, Gang, Tiantian Zhang, Yinghui Zhang, Guowen Xu, Jianfei Sun, and Jin Cao. "Verifiable and privacy preserving federated learning without fully trusted centers." Journal of Ambient Intelligence and Humanized Computing (2022): 1-11.
18. Tsouvalas, Vasileios, Tanir Ozcelebi, and Nirvana Meratnia. "Privacy-preserving speech emotion recognition through semi-supervised federated learning." In 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp.359-364. IEEE, 2022.
19. Yadav, Santosh Kumar, Siva Sai, Akshay Gundewar, Heena Rathore, Kamlesh Tiwari, Hari Mohan Pandey, and Mohit Mathur. "CSITime: Privacy-preserving human activity recognition using WiFi channel state information." Neural Networks 146 (2022): 11-21.
20. Liu, Shengheng, Chong Zheng, Yongming Huang, and Tony QS Quek. "Distributed reinforcement learning for privacy-preserving dynamic edge caching." IEEE Journal on Selected Areas in Communications 40, no. 3 (2022): 749-760.
21. R. Parekh et al., "GeFL: Gradient Encryption- Aided Privacy Preserved Federated Learning for Autonomous Vehicles," in IEEE Access, vol. 11, pp. 1825-1839, 2023, doi: 10.1109/ACCESS.2023.3233983.
22. Rasim M. Alguliyev, Ramiz M. Aliguliyev, Fargana J. Abdullayeva, Privacy-preserving deep learning algorithm for big personal data analysis,Journal of Industrial Information.