Dynamic-Differential Privacy based on Feature Selection with Improved Usability and Security

Sun-Jin Lee[a], Hye-Yeon Shim[b], Jung-Hwa Rye[c] and Il-Gu Lee[d]
Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, Korea, Republic of

Keywords: Differential Privacy, Feature Selection, Machine Learning, Security, Usability.

Abstract: With the advent of the digital transformation era, the introduction of machine learning (ML) in all industries has accelerated. ML is highly utilized because it can provide various services, such as prediction and classification. However, because the data used in the learning process contain personal information, innumerable people could be harmed if the data are leaked. Differential privacy (DP) techniques have been studied to improve data security. They are improved by adding noise from the data. However, owing to the reduced classification performance of legitimate users, they are difficult to apply in areas that require accurate prediction. This study proposes the dynamic DP based on feature selection (D-DPFS) model. D-DPFS can improve usability and security by applying DP only to privacy-related features. Experiment results indicate that D-DPFS increases the prediction accuracy to 96.37% from a usability perspective. Additionally, for users who have predefined data to prevent information leakage, security was improved by adjusting the number of features to which DP was applied according to the number of privacy features.

1 INTRODUCTION

With the development of computing technology, machine learning (ML) types and utilization have been diversified. ML has been actively utilized to address various healthcare-related issues, such as predicting patient diseases (Uddin et al., 2019; Mohan et al., 2019), medical treatment for rare diseases, and classifying positron emission tomography-computed tomography (PET-CT) images (Garg & Mago, 2021). The financial sector also uses ML technology to provide services like credit card fraud detection (Aleskerov et al., 1997), stock price prediction, and customized financial product recommendations (Rundo et al., 2019). ML is recognized as a powerful tool for analyzing and predicting data and is widely distributed across all industries. Fortune Business Insight predicts that the ML market will grow at an average annual rate of 38.8%, from $15.44 billion in 2021 to $209.91 billion in 2029 (Machine learning market size, share, growth: Trends [2030] website).

An extensive dataset is required to improve ML performance in learning and evaluation. However, this dataset consists of extensive user information and thus has privacy issues (Kanwal et al., 2021). Medical or financial datasets are at high risk because once leaked, they can pose a threat to users or cause financial damage (Iwendi et al., 2020). Most countries aware of this problem take measures to distribute datasets by applying de-identification technologies. However, it is difficult to fully anonymize an individual's information, which reduces the usability of the data.

Differential privacy (DP) algorithms have been proposed as another method to increase data security (Kaissis et al., 2020). DP is a technique for protecting personal information by introducing randomness, such as by adding noise to data or transforming data (Lecuyer et al., 2019), which addresses the problem of information leakage in ML. However, applying DP is time-consuming, and applying a strong DP to all features results in a tradeoff problem that improves security but reduces data usability, which can be

[a] https://orcid.org/0000-0001-9114-2992
[b] https://orcid.org/0000-0009-4978-2553
[c] https://orcid.org/0009-0008-0134-6771
[d] https://orcid.org/0000-0002-5777-4029

Lee, S.-J., Shim, H.-Y., Rye, J.-H. and Lee, I.-G.
Dynamic-Differential Privacy based on Feature Selection with Improved Usability and Security.
DOI: 10.5220/0013117100003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 141-149
ISBN: 978-989-758-735-1; ISSN: 2184-4356

measured by prediction accuracy (Ouadrhiri & Abdelhadi, 2022).

This study proposes a dynamic-differential privacy based on feature selection (D-DPFS) model that combines feature selection (FS) and DP. The D-DPFS model does not apply DP to all features but only those where privacy is essential, simultaneously improving usability and security for legitimate users.

Thus, the contributions of this study are as follows:

- DP is applied only to privacy-related features to improve usability and security.
- Memory efficiency and latency are improved through FS.
- In addition to predictive performance from the perspective of general users, it quantitatively confirms user security in special situations where personal information protection is important.

The remainder of this paper is organized as follows. Section 2 analyzes the contributions and limitations of previous studies. Section 3 describes the framework and mechanism of the proposed D-DPFS. Section 4 describes the environment and performance indicators that were evaluated, and Section 5 analyzes the results. Finally, Section 6 concludes the study.

2 RELATED WORK

Various studies have been conducted to solve the tradeoff between accuracy, usability, and privacy issues in ML. FS is a representative method for improving accuracy and usability, and DP is a method to resolve privacy issues.

2.1 Feature Selection

FS is the process of extracting useful information from the data, which can reduce the complexity of the model and prevent overfitting by removing unnecessary features (Khaire & Dhanalakshmi, 2022). With FS, the time required for the DP application process can be significantly reduced by selecting the necessary features before applying the DP and after applying DP.

Chiew et al. (2019) proposed HEFS, a feature selection framework for an ML-based phishing detection system. We demonstrated improved accuracy using Support Vec-tor Machine (SVM), Naive Bayes, Random Forest (RF), and several classifiers when constructing the top-n feature subsets based on the cumulative distribution function gradient (CDF-g) algorithm. In addition, an optimal accuracy of 94.6% was achieved when the IG methodology was integrated with a random forest classifier based on entropy. However, in constructing the basic feature set for the entire feature set, there is a limitation in that the feature importance cannot be considered as a chi-square, and information gain and symmetric uncertainty are selected as filter measurements.

Kou et al. (2020) proposed a multi-criteria decision-making (MCDM) method to overcome the limitations of small samples and large dimensions in the text classification process. This methodology calculates the presence or absence of terms in a document set using IG and various filter-based feature selection methods, determines the contribution of terms according to the calculated ratio, and shows the prediction accuracy. However, there is a limit to optimal methodologies that have yet to be considered other than TOPSIS, VIKOR, GRA, Weighted sum method (WSM), and PROMOTHEE methodologies.

Rehman et al. (2020) proposed CbFNN, a new deep-learning-based method for detecting microscopic brain tumors and classifying tumor types. After performing feature extraction with VGG19, a pre-trained convolution neural network (CNN) model, the best features were selected based on the entropy and information gain methodology. The methodology achieved high accuracies of 98.32, 96.97%, and 92.67 % for the BraTS datasets for 2015, 2017, and 2018, respectively. However, training a pre-trained model with extracted tumor images increases the classification accuracy of tumor-type classification. Still, it has a limitation in that the time cost is high because the classification time increases compared to the pre-trained model trained with the original magnetic resonance imaging (MRI) scan.

2.2 Differential Privacy

DP achieves privacy by adding noise. Because sensitive information can be protected through the application of DP, the security of the data can be improved.

Liu (2019) proposed a generalized Gaussian (GG) mechanism that integrates the Laplace and Gaussian mechanisms, the primary DP methodologies. The theoretical requirements for the proposed mechanism to reach DP at prespecified privacy parameters were explored. The prediction accuracy and statistical usefulness of the Laplace, Gaussian-pDP, and Gaussian-aDP methodologies were compared to the changes in epsilon and delta values. However, since the range of epsilon values on the abscissa axis is limited from 0.5 to 2, it is difficult to check the changing trend according to the epsilon value. In addition, there is a limitation in that there is bias owing to noise and disturbed results caused by integrating the two mechanisms.

Xue et al. (2022) proposed Acies, a method for indirectly controlling information leakage in training data by perturbing the adaptive feature selection. This methodology has a higher recognition rate than conventional models, even with the same epsilon value. In addition, the time consumption and RAM cost were analyzed simultaneously to identify optimization points and improve memory usage. However, it does not specify which feature selection method was applied in the Acies methodology, and it shows limitations in that the accuracy performance is not measured. In addition, the proposed method can slow down a reconstruction attack, which is an attack that can occur at the edge but has a limitation in that it does not provide a complete solution.

Desfontaines et al. (2019) proposed a method to realistically model an attacker's uncertainty in a DP application situation and provide mathematical proof. By defining an attacker with partial knowledge as a passive or active attacker, a method for quantifying privacy guarantees in a realistic home situation was demonstrated. However, in the DP application process, the privacy parameter epsilon value was considered, whereas the delta value, which indicates the probability of information leakage by mistake, was not considered.

2.3 Differential Privacy and Feature Selection

In this section, the DP framework with feature selection is reviewed.

Alishahi et al. (2022) proposed a local DP (LDP)-FS framework that applies an FS using LDP. This concept satisfies differential privacy in a local setting to eliminate the need for a trusted third party. Through experiments, it was shown that irrelevant features could be selected in a data-protected situation by identifying factors such as the size of the dataset and the number of features that affect LDP-FS performance. However, because the characteristics targeted in this thesis are independent variables, applying this methodology to diverse environments is necessary.

Zhang et al. (2020) proposed removing data correlations, increasing data usability, and protecting data by applying DP and feature selection techniques. DP-based FS was performed by adding Laplace noise according to feature importance and then performing normalization. However, it takes a long time to perform feature selection because the feature set with the highest accuracy is found after reviewing all the features. In addition, there is a limitation in that only data usability indicators exist, and data privacy-related performance indicators do not.

Conventional studies have not resolved the DP applications' tradeoff relationship between utility and privacy. Security is improved because sensitive information can be protected through DP; however, actual data utilization decreases as epsilons (noise) are added. DP is in the limelight because it protects sensitive information; however, owing to this tradeoff relationship, only a limited range of high epsilon is applied, and the technology is being used (Wilson et al., 2019). The proposed methodology compensates for the decrease in utility due to the DP application by applying DP after performing feature selection considering privacy to compensate for these limitations.

3 PROPOSED FRAMEWORK

In this study, a D-DPFS model is proposed to prevent attackers from acquiring information from legitimate users while ensuring the classification performance of legitimate users. The proposed framework is illustrated in Fig. 1.

The D-DPFS comprises a feature selection module, a differential privacy module, a privacy feature selector, and a data processing module. In the feature selection module, IG, a representative FS technique, is used to select features of high importance from the dataset input for data processing. The privacy feature selector selects the privacy feature the user wants to protect. Finally, the DP algorithm is applied to the chosen features through the privacy feature selector and feature selection modules in the differential privacy module. At this time, it is assumed that the user corresponds to a legitimate user requesting data analysis for the D-DPFS. Users can also select several privacy-enhancing features for enhanced security.

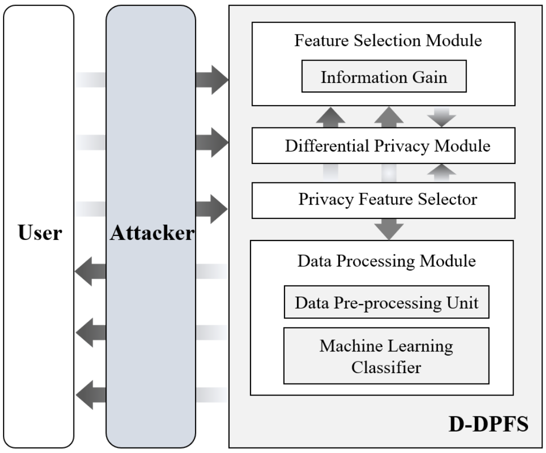

Figure 1: Structure of D-DPFS.

The flowchart of D-DPFS is shown in Fig. 2.

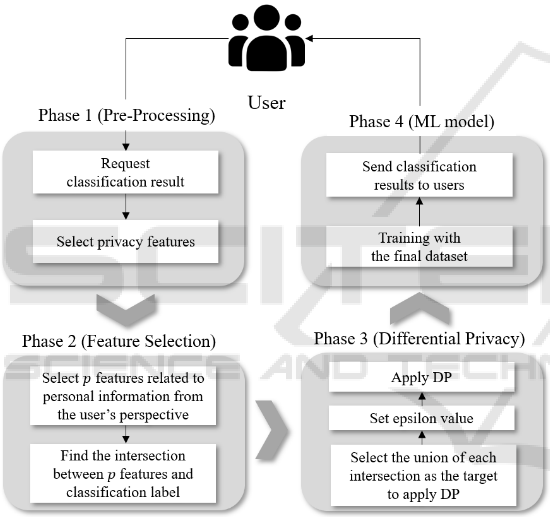
User
Phase 1 (Pre-Processing)
Request classification result
Select privacy features
Phase 4 (ML model)
Send classification results to users
Training with the final dataset
Phase 2 (Feature Selection)
Select p features related to personal information from the user's perspective
Find the intersection between p features and classification label
Phase 3 (Differential Privacy)
Apply DP
Set epsilon value
Select the union of each intersection as the target to apply DP

Figure 2: Flowchart of D-DPFS.

When a user requests classification for a specific dataset, D-DPFS identifies privacy-related features for protection in the dataset used for classification and data preprocessing. At this time, privacy-related features are for primary security and refers to a feature to which DP is applied by default even without the user setting it. Representative examples include gender and phone number. Subsequently, in Phase 2, two types of different feature selection are performed. The first type of feature selection was performed to select features for the classification requested by the user, and then the second type of feature selection was performed to select features for privacy-related features. In the second type of feature selection, the user may select p personal information related features. Among the feature selection results for the class requested by the user, the feature selection results for each p privacy feature are obtained. Then, the feature corresponding to the intersection of one feature out of p and the feature selection result for the class requested by the user is obtained. When p intersections are created, find the union of the p intersections. The method of finding the union of intersections for each privacy feature is as shown in Fig. 3.

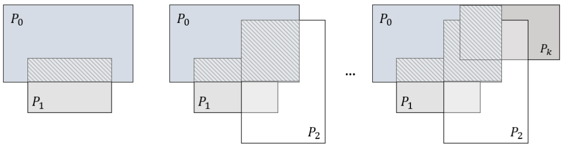

Figure 3: Feature selection method applying DP in D-DPFS.

DP is then applied according to the epsilon value set by the user in advance. Finally, in Phase 4, the user class classification dataset with DP is trained and evaluated, and the final result is delivered to the user.

When the class the user wants to classify is called P_0 and the privacy feature additionally defined by the user is defined as $P_{1,2,..,k}$, the privacy feature to which differential privacy will be applied is as shown in equation (1). P can be obtained by adding up all the features corresponding to the intersection between P_0 and the remaining $P_{1,2,..,k}$.

$$P = (P_0 \cap P_1) \cup (P_0 \cap P_2) \cup \cdots \cup (P_0 \cap P_k) = \bigcup_{i=1}^{k} (P_0 \cap P_i) \qquad (1)$$

The Laplace mechanism (ℓ) for applying differential privacy is given by equation (2). Noise is generated through Laplace Distribution based on scale b. b is the variance of distribution, and in differential privacy it follows $b = \frac{\Delta f}{\varepsilon}$ (Dwork & Roth, 2013). Epsilon ε is a privacy parameter. The sensitivity Δf represents the effect that a change in a dataset can have on query results. x is the dataset.

$$\ell(b, x) = \frac{1}{2b} exp\left(-\frac{|x|}{b}\right) \qquad (2)$$

Mutual information gain is used to select features that have a significant impact on classification among features, and weights are defined based on this. Assume $f_j \in P$ and $0 < IG_{normalization}^{f_j} \leq 1$. At this time, the reason $0 < IG_{normalization}^{f_j} \leq 1$ is because the classification method used in D-DPFS is binary classification, and when multiple classification is used, the entropy value can increase up to ∞.

The weight formula can be expressed as equation (3), where $n(P)$ means the number of privacy features. The weight ω is multiplied by the information gain value of f_j, and the impact of each privacy feature on classification accuracy can be confirmed.

$$\omega = \prod_{j=1}^{n(P)} IG_{normalization}^{f_j} \tag{3}$$

The objective function of D-DPFS can be constructed according to equations (1) to (3), which is the same as equation (4).

$$O(k, \mathcal{E}) = \min\left(\frac{n(\bigcup_{i=1}^{k}(P_0 \cap P_i))\omega}{N} \times \ell\left(\frac{\Delta f}{\varepsilon}, P\right)\right) \tag{4}$$

DP is applied only to the features corresponding to $n(P)$ among the total N pieces of data, and at this time, a weight ω is added. Specifically, the higher the ω value, the greater the impact on classification performance and the lower the accuracy. Additionally, the Laplace function $\ell\left(\frac{\Delta f}{\varepsilon}, P\right)$ for DP application is defined, and the k and $\mathcal{E}$ values are adjusted in D-DPFS. In other words, the objective function improves accuracy by minimizing the overall value (applying DP only to some features). Then, security is maximized by applying DP to features related to the k privacy features.

4 EXPERIMENTAL ENVIRONMENTS

4.1 Experimental Datasets and Packages

To evaluate the performance of the D-DPFS, the Behavioral Risk Factor Surveillance System (BRFSS) dataset (Centers for Disease Control and Prevention website), which includes users' personal information, was used. The BRFSS dataset was created as a collaboarative project between all US states and the Centers for Disease Control. It collects information on health abnormalities and disease states related to human mortality, disease, and disability. The BRFSS dataset has 279 features, ranging from race and sex to disease information such as blood pressure, diabetes, and obesity. In this experiment, the user predicts the likelihood of heart disease, and the personal information characteristics to be protected are assumed to be race when p=1 and race and age when p=2.

Logistic regression (LR) is a model that improves classification performance by predicting data with a value between 0 and 1 using a sigmoid function and classifying it with a high probability based on probability. The LR model is primarily used for classification and prediction in medicine and communication. A multiclass LR model (Logisticregression website) was used for learning and evaluation.

The mutual-information gain package (Mutual_info_classif website) provided by Sklearn was used as the FS algorithm. Additionally, the FS rate was fixed at 5%. For the DP algorithm, the Laplace mechanism in Diffprivlib (IBM website; Holohan et al., 2019) developed by IBM was used to verify the experiment.

4.2 Comparison Models

To objectively verify the performance of D-DPFS, four comparative models were selected. These models are listed in Table 1.

Table 1: Types of comparison models.

Model name	Feature selection	Differential Privacy	Function
Non-DPFS (Speiser et al., 2019)	X	X	-
FS (Sneha & Gangil 2019)	O	X	-
DP (Liu, 2019)	X	O	Static DP
S-DPFS (Zhang et al., 2020)	O	O	Static DP
D-DPFS (Our Model)	O	O	Dynamic DP

The non-DPFS model (Speiser et al., 2019) refers to a general ML classifier to which neither DP nor FS is applied. The FS model (Sneha & Gangil, 2019) only performs feature selection and does not apply DP. It has the advantage of fast performance but is limited in that it cannot protect users' personal information. The DP model (Liu, 2019) applies differential privacy to all the features. When DP is used for all features, security is improved. Still, legitimate users' usability is also reduced, and applying DP to all features takes time. The Static-Differential Privacy based on Feature Selection (S-DPFS) model (Zhang et al., 2020) applies DP only to features selected through feature selection. Although the range of features to which DP is applied is reduced, the required time is also reduced; however, noise is added to all the features used, limiting usability.

The proposed D-DPFS model takes longer than the FS model for the two feature selections. However, it can optimize memory usage through FS and is the most improved model in terms of security and usability through dynamic DP applications.

4.3 Evaluation Metrics

Four evaluation indicators were selected from performance, cost, and security perspectives to compare the proposed and conventional models. The classification accuracy of the LR model according to the change in epsilon (ε) was used to measure performance. Epsilon refers to privacy parameters that can be controlled to balance the accuracy of the analysis of data with security. In this experiment, ε-differential privacy was used to implement the pure DP algorithm (Aitsam, 2022). The epsilon was tested in 0.0001, 0.01, 1, 100, and 10,000 environments, and the accuracy was measured using equation (5).

$$Accuracy(\%) = \frac{Number\ of\ data\ accurately\ predicted}{Total\ number\ of\ data} \times 100 \quad (5)$$

Memory usage and latency were used to compare the performance of the proposed and conventional models in terms of cost. Memory usage was measured using a memory profiler (Memory-profiler website). Memory Profiler is a Python memory measurement package based on psutil that monitors the memory consumption of processes. Latency measures the time spent executing each model using a time module.

In addition, this study proposes a new methodology for measuring security. A previous DP study used the epsilon value as a security index (Xue et al., 2022). However, security can be abstractly confirmed by using the epsilon value, but it is difficult to confirm with quantitative values. Therefore, to clearly understand the security of the proposed model, classification performance was measured from the perspective of general users and general users for whom security is important. Legitimate users identify information with standard labels, and in environments where security is important, several privacy features are selected and delivered to the system, providing strong security for the features.

5 EXPERIMENTAL RESULTS AND ANALYSIS

Experiments were conducted regarding the classification accuracy from the perspective of legitimate users and the classification accuracy of the proposed model according to the number of privacy features, latency, and memory usage.

5.1 Classification Accuracy of Legitimate User

The classification accuracy was measured using four comparatives and the proposed models. Fig. 4 shows the classification accuracy of each model according to the increase in epsilon.

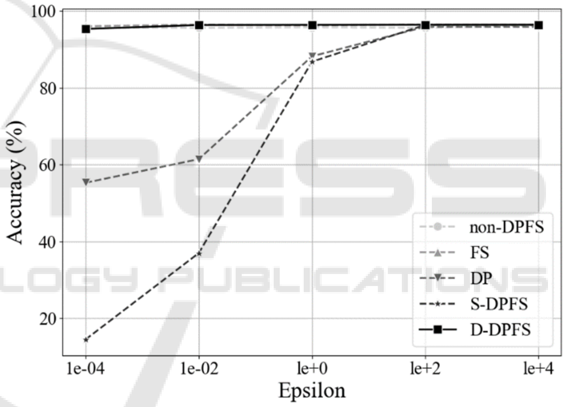

Figure 4: Classification accuracy in each model.

The non-DPFS, FS, and proposed models all showed 95–96% accuracy regardless of epsilon changes. The classification accuracy of the S-DPFS model was at least 15% and up to 95%, showing up to 80% lower performance than the other methods owing to changes in epsilon. Even the DP-only models showed at least 55% accuracy, higher performance than S-DPFS, but up to 40% lower accuracy than the proposed method.

The proposed D-DPFS model applies DP only to privacy-related features to classify legitimate users. Therefore, unlike the S-DPFS model with 5% feature selection DP, it can have the same high performance as the non-DPFS and FS models, regardless of epsilon.

5.2 Classification Accuracy According to Number of Privacy Features

Fig. 5 shows the classification accuracy results of general users and users with defined privacy features.

Among the BRFSS datasets, it is assumed that general users (n(p)=0) classify heart diseases within the BRFSS dataset by setting them as labels. If the privacy feature was selected (n(p)>0), FS between the privacy feature and the heart disease label was applied, then the intersection was selected as the target for DP application, p intersection sets were created, and DP was applied by combining them.

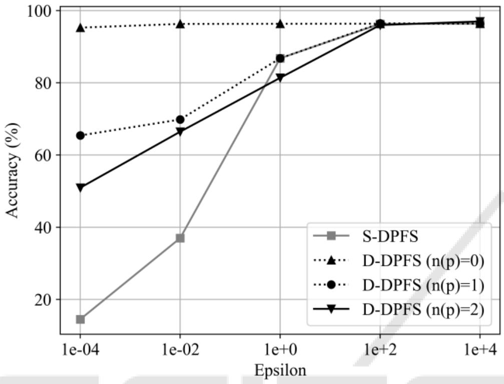

Figure 5: Accuracy according to $n(p)$.

In the situation where $n(p) = 0$, no additional security experiments related to the privacy feature were conducted, so only DP for the pre-set security column was applied. At $n(p) = 1$, features are applied to both the intersection of the FS results for race and the FS results for general classification labels, resulting in a 1.15 times reduction in classification accuracy compared to $n(p) = 0$. However, it has improved accuracy compared to the S-DPFS model, which applies DP to all features of FS. Even in the case of $n(p) = 2$, it is lower than $n(p) = 0$, but shows improved accuracy than the S-DPFS model. In other words, using D-DPFS can increase user usability compared to S-DPFS while effectively protecting features linked to privacy.

5.3 Classification Accuracy According to Number of Privacy Features

Fig. 6 shows the average latency and memory usage measured by repeating the classification of the comparative model and the proposed model 1,000 times. Data preprocessing was not included at this time because it was performed in all models.

Regarding latency, non-DPFS without going on had the lowest, followed by the FS, S-DPFS, D-DPFS, and DP models. The latency of the proposed model was approximately 26 s, which is approximately 36 s lower than that of the DP model, which had the highest latency of 62 s. Compared to S-DPFS, a model that performs both FS and DP, there was a slight difference of approximately 6 s, approximately 24 s higher than that of non-DPFS, which has the minimum latency.

Therefore, it is significant that the proposed model has less latency than when DP is applied to all data and does not differ significantly from S-DPFS. Other non-DPFSs with a latency of 2 s or FSs with a latency of 15 s have a small latency; however, unlike the proposed model, DP does not exist, and thus privacy cannot be maintained. Therefore, among the methods that can protect privacy, the proposed model has a great advantage while increasing the time required. It also improves usability while protecting the privacy features of general users as much as possible.

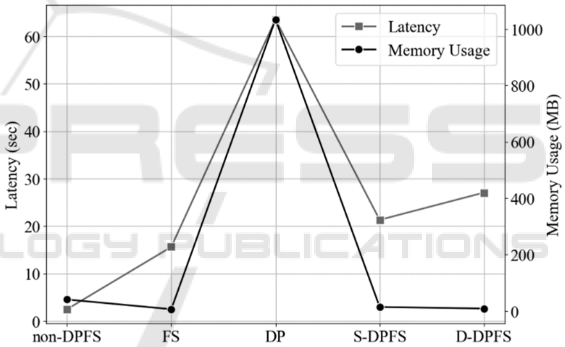

Figure 6: Training latency and memory usages in each model.

Regarding memory usage, the DP model had a significant memory usage of ap-proximately 1,035 MB compared to the other methods, and most other methods had a memory usage of less than 50 MB. The proposed D-DPFS used approximately 9 MB of memory, which was 1,026 MB lower than the DP model and 5 MB less memory than the S-DPFS method, which performs FS and DP. In addition, the proposed model showed lower memory usage than the other methods, except for the FS single method, and had a slight difference of approximately 3 MB from the FS method.

Therefore, we experimentally showed that the proposed model can achieve high performance with lower memory usage than other methods.

6 CONCLUSION

ML solves various problems in all industries; however, personal information leakage can occur, and the damage is significant in the medical and financial sectors. DP is a technology used for data protection that can solve information leakage problems in ML. However, conventional DP techniques lack prediction accuracy and require significant time and cost. To address these challenges, this study proposes a D-DPFS model that combines the DP technology for privacy protection in ML with the FS technology for data analysis.

The experiment used four models to compare the proposed and conventional models' performance, cost, and security. The performance measures the classification accuracy of the LR model according to the change in epsilon, and the cost is compared based on memory usage and latency. Additionally, to measure security in detail, we measured classification performance for general users and users who selected privacy features.

The D-DPFS model proposed through experiments guarantees a high classification performance of 95% for general users and adopts a method of applying additional DP when general users select the feature they want to protect, preventing attackers from stealing personal information, can be prevented. Therefore, it has been proven that the D-DPFS method is suitable for protecting user privacy in ML situations.

In this study, the D-DPFS model was evaluated only using the BRFSS dataset; however, in future studies, the model's performance will be verified in various dataset environments, and the privacy feature selection algorithm will be specified.

ACKNOWLEDGEMENTS

This work is supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry (RS-2024-00415520) supervised by the Korea Institute for Advancement of Technology (KIAT), and the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2022-RS-2022-00156310) and Information Security Core Technology Development (RS-2024-00437252) supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

REFERENCES

Aitsam, M. (2022). Differential Privacy Made Easy. *2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)*, *17*, 1–7. https://doi.org/10.1109/etecte55893.2022.10007322

Aleskerov, E., Freisleben, B., & Rao, B. (1997). CARDWATCH: A Neural Network based database mining system for credit card fraud detection. *Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr)*. https://doi.org/10.1109/cifer.1997.618940

Alishahi, M., Moghtadaiee, V., & Navidan, H. (2022). Add noise to remove noise: Local Differential Privacy for Feature Selection. *Computers &amp; Security*, *123*, 102934. https://doi.org/10.1016/j.cose.2022.102934

Centers for Disease Control and Prevention. (2024, August 28). *CDC - BRFSS Annual Survey Data*. Centers for Disease Control and Prevention. https://www.cdc.gov/brfss/annual_data/annual_data.htm

Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S. C., & Tiong, W. K. (2019). A New Hybrid Ensemble Feature Selection Framework for Machine Learning-based phishing detection system. Information Sciences, 484, 153–166. https://doi.org/10.1016/j.ins.2019.01.064

Desfontaines, D., Mohammadi, E., Krahmer, E., & Basin, D. (2019). Differential privacy with partial knowledge. *arXiv preprint arXiv:1905.00650*.

Dwork, C., & Roth, A. (2013). *The Algorithmic Foundations of Differential Privacy*. https://doi.org/10.1561/9781601988195

Garg, A., & Mago, V. (2021). Role of machine learning in Medical Research: A survey. *Computer Science Review*, *40*, 100370. https://doi.org/10.1016/j.cosrev.2021.100370

Holohan, N., Braghin, S., Mac Aonghusa, P., & Levacher, K. (2019). Diffprivlib: the IBM differential privacy library. *arXiv preprint arXiv:1907.02444*.

Ibm. (n.d.). *IBM/differential-privacy-library: Diffprivlib: The IBM Differential Privacy Library*. GitHub. https://github.com/IBM/differential-privacy-library

Iwendi, C., Moqurrab, S. A., Anjum, A., Khan, S., Mohan, S., & Srivastava, G. (2020). N-Sanitization: A semantic privacy-preserving framework for unstructured medical datasets. *Computer Communications*, *161*, 160–171. https://doi.org/10.1016/j.comcom.2020.07.032

Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and Federated Machine Learning in medical imaging. *Nature Machine Intelligence*, *2*(6), 305–311. https://doi.org/10.1038/s42256-020-0186-1

Kanwal, T., Anjum, A., Malik, S. U. R., Sajjad, H., Khan, A., Manzoor, U., & Asheralieva, A. (2021). A robust privacy preserving approach for electronic health records using multiple dataset with multiple sensitive attributes. *Computers &amp; Security*, *105*, 102224. https://doi.org/10.1016/j.cose.2021.102224

Khaire, U. M., & Dhanalakshmi, R. (2022). Stability of Feature Selection Algorithm: A Review. *Journal of*

King Saud University - Computer and Information Sciences, *34*(4), 1060–1073. https://doi.org/10.1016/j.jksuci.2019.06.012

Kou, G., Yang, P., Peng, Y., Xiao, F., Chen, Y., & Alsaadi, F. E. (2020). Evaluation of feature selection methods for text classification with small datasets using multiple criteria decision-making methods. *Applied Soft Computing*, *86*, 105836. https://doi.org/10.1016/j.asoc.2019.105836

Lecuyer, M., Atlidakis, V., Geambasu, R., Hsu, D., & Jana, S. (2019). Certified robustness to adversarial examples with differential privacy. *2019 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp.2019.00044

Liu, F. (2019). Generalized gaussian mechanism for differential privacy. IEEE Transactions on Knowledge and Data Engineering, 31(4), 747–756. https://doi.org/10.1109/tkde.2018.2845388

Logisticregression. scikit. (n.d.). https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LogisticRegression.html

Machine learning market size, share, growth: Trends [2030]. Machine Learning Market Size, Share, Growth | Trends [2030]. (n.d.). https://www.fortunebusinessinsights.com/machine-learning-market-102226

Memory-profiler. PyPI. (n.d.). https://pypi.org/project/memory-profiler/

Mohan, S., Thirumalai, C., & Srivastava, G. (2019). Effective heart disease prediction using hybrid machine learning techniques. *IEEE Access*, *7*, 81542–81554. https://doi.org/10.1109/access.2019.2923707

Mutual_info_classif. scikit. (n.d.-b). https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.mutual_info_classif.html

Ouadrhiri, A. E., & Abdelhadi, A. (2022). Differential privacy for deep and federated learning: A survey. IEEE Access, 10, 22359–22380. https://doi.org/10.1109/access.2022.3151670

Rehman, A., Khan, M. A., Saba, T., Mehmood, Z., Tariq, U., & Ayesha, N. (2020). Microscopic brain tumor detection and classification using 3d cnn and feature selection architecture. *Microscopy Research and Technique*, *84*(1), 133–149. https://doi.org/10.1002/jemt.23597

Rundo, F., Trenta, F., di Stallo, A. L., & Battiato, S. (2019). Machine Learning for Quantitative Finance Applications: A survey. *Applied Sciences*, *9*(24), 5574. https://doi.org/10.3390/app9245574

Sneha, N., & Gangil, T. (2019). Analysis of diabetes mellitus for early prediction using optimal features selection. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0175-6

Speiser, J. L., Miller, M. E., Tooze, J., & Ip, E. (2019). A comparison of random forest variable selection methods for classification prediction modeling. *Expert Systems with Applications*, *134*, 93–101. https://doi.org/10.1016/j.eswa.2019.05.028

Uddin, S., Khan, A., Hossain, M. E., & Moni, M. A. (2019). Comparing different supervised machine learning algorithms for disease prediction. *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-019-1004-8

Wilson, R. J., Zhang, C. Y., Lam, W., Desfontaines, D., Simmons-Marengo, D., & Gipson, B. (2019). Differentially private sql with bounded user contribution. *arXiv preprint arXiv:1909.01917*.

Xue, W., Shen, Y., Luo, C., Xu, W., Hu, W., & Seneviratne, A. (2022). A differential privacy-based classification system for Edge Computing in IOT. *Computer Communications*, *182*, 117–128. https://doi.org/10.1016/j.comcom.2021.10.038

Zhang, T., Zhu, T., Xiong, P., Huo, H., Tari, Z., & Zhou, W. (2020). Correlated differential privacy: Feature selection in Machine Learning. *IEEE Transactions on Industrial Informatics*, *16*(3), 2115–2124. https://doi.org/10.1109/tii.2019.2936825.