A Privacy-Preserving Smart Body Scale with K-Means Anonymization towards GDPR-Compliant IoT

Abdurohman, Maman; Prabowo, Sidik; Putrada, Aji Gautama; Oktaviani, Ikke Dian; Nuha, Hilal Hudan; Jacob, Deden Witarsyah; Janssen, Marijn

DOI
10.1109/ICECCE61019.2023.10442797

Publication date
2023

Document Version
Final published version

Published in
4th International Conference on Electrical, Communication and Computer Engineering, ICECCE 2023

Proc. of the 4th International Conference on Electrical, Communication and Computer Engineering (ICECCE)
30-31 December 2023, Dubai, UAE

2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE) | 979-8-3503-6969-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICECCE61019.2023.10442797

A Privacy-Preserving Smart Body Scale with K-Means Anonymization towards GDPR-Compliant IoT

Maman Abdurohman
School of Computing
Telkom University
Bandung, Indonesia
abdurohman@telkomuniversity.ac.id

Sidik Prabowo
School of Computing
Telkom University
Bandung, Indonesia
prabowo@student.telkomuniversity.ac.id

Aji Gautama Putrada
School of Computing
Telkom University
Bandung, Indonesia
ajigautama@student.telkomuniversity.ac.id

Ikke Dian Oktaviani
School of Computing
Telkom University
Bandung, Indonesia
idoktaviani@student.telkomuniversity.ac.id

Hilal Hudan Nuha
School of Computing
Telkom University
Bandung, Indonesia
hilalnuha@telkomuniversity.ac.id

Deden Witarsyah Jacob
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
dedenw@telkomuniversity.ac.id

Marijn Janssen
Faculty of Technology Policy And Management
Delft University of Technology
Delft, Nethderlands
M.F.W.H.A.Janssen@tudelft.nl

***Abstract*—A smart weight scale, or smart scale, is an Internet of Things (IoT)-based scale that can measure metrics other than body weight using various sensors and send the information to the cloud. Meanwhile, the problem is that a person's weight is considered personally identifiable information (PII) and needs to be preserved to comply with general data protection regulations (GDPR). Our research aim is to use K-Means for anonymization so that a privacy-preserving smart body scale becomes GDPR-compliant. The first step is to form a novel privacy-preserving smart body scale framework. We obtained the cardiovascular disease dataset containing personal weights from Kaggle. We apply random noise perturbation and k-means clustering for anonymization. We apply cardiovascular disease classification using gradient boosting. Finally, we compared the performance of the three anonymization methods with several metrics, including information loss, entropy, and distortion. Test results show that our elbow method shows that the optimum number of clusters for body weight is six. This number has passed the k-anonymity assessment. Furthermore, comparisons show that the k-means generalization performs better than noise perturbation with distortion, information loss, and entropy values 71.1, 0.001, and 15.6, respectively.**

***Index Terms*—smart body scale, general data protection regulation, anonymization, k-means, generalization**

I. Introduction

A smart weight scale, or smart scale, is an Internet of Things (IoT)-based scale that can measure metrics other than body weight using various sensors and send the information to the cloud. [1]. On the other hand, information such as age, weight and height is needed in several studies to predict cardiovascular disease [2]. Meanwhile, the problem is that a person's weight is classified as privacy-sensitive data [3].

General Data Protection Regulation (GDPR) states that anonymous data is non-personal data that can be used, analyzed, shared, and monetized without compliance risk [4]. Anonymizing personal body weight data for smart body scales is a research opportunity. Several techniques in previous research have been used for anonymization. McDonald *et al.* [5] uses normalization as a writing style anonymization technique. The system they are promoting is called anonymous. Tran *et al.* [6] uses random noise perturbation for the anonymization of speech signals sent to the cloud. They claim that the method can be modified easily without retraining. Finally, Abbasi *et al.* [7] create anonymization in healthcare using k-means clustering. In addition, they use normal distribution to remove data

979-8-3503-6969-4/23/$31.00 ©2023 IEEE

that rarely appears. Comparing normalization, random noise perturbation, and k-means clustering with the anonymization of personal weight data is a research opportunity.

Our research aim is to use K-Means for anonymization so that a privacy-preserving smart body scale becomes GDPR-compliant. The first step is to form a novel framework of privacy-preserving smart body scale. We got a cardiovascular disease dataset containing personal weights from Kaggle. We apply normalization, random noise perturbation, and k-means clustering for anonymization. We apply cardiovascular disease classification using gradient boosting. Finally, we compared the performance of the three anonymization methods with several metrics, including data utility, entropy, and distortion.

To the best of our knowledge, there has never been any research that makes a privacy-preserving smart body scale with k-means anonymization for IoT that is GDPR-compliant. Here are our research contributions:

1) A discussion of privacy concerns on smart body scales as part of smart healthcare and wearable sensors
2) A novel smart body scale implementation with K-Means anonymization.
3) An IoT framework that is GDPR-compliant, specifically for data minimization, anonymization, purpose limitation, and documentation.

Readers can find the remainder of this paper arranged in the following systematic manner: Chapter II discusses papers related to anonymization and smart body scales. Chapter III explains the steps in our research and the theory involved. Chapter IV shows the test results and discusses our research contributions. Lastly, Chapter V is our declaration of conclusion.

II. Related Works

Several studies have discussed advances in the smart body scale. Johannessen *et al.* [8] researched how to collect weight data for research using IoT-connected household scales. This research investigates trends in changes in fat, muscle mass, and visceral fat data over a period of several years. Research from Turicchi *et al.* [9] focused on imputation data in body weight data originating from smart scales. The big goal was to diagnose body weight patterns to prevent the risk of diabetes or disease.

Several studies have discussed the sensitivity of some personal data in healthcare and wearable devices. Stojkov *et al.* [10] said in his research that IoT in smart healthcare threatens personal data leakage. The research carried out simple mitigation in some of the cases they identified. Dincelli *et al.* [11] discussed privacy on wearable sensors, which is increasingly worrying, considering wearable sensors are increasingly ubiquitous. Discussing the sensitivity of personal data on the smart body scale is a research opportunity.

Several studies, such as Ghate *et al.* [12], used k-means for anonymization. Ashkouti *et al.* [13] uses k-means for anonymization and uses Apache Spark. Information loss from this method is a decrease in accuracy of around 0.01 to 0.02. K-means clustering in the research of Logesware *et al.* [14] is intended for anonymization of personal health records. Using k-means clustering for anonymizing weight data in a smart body scale is a research opportunity. Table I shows the relationship of our paper to state-of-the-art papers in smart body scales and anonymization.

TABLE I
Related Works on Smart Body Scale Privacy-Preserving with Anonymization

Reference	Smart Body Scale	Privacy-Preserving	K-Means	Anonymization
[8]	✓	✗	✗	✗
[9]	✓	✗	✗	✗
[10]	✗	✓	✗	✗
[11]	✗	✓	✗	✗
[12]	✗	✓	✓	✓
[13]	✗	✓	✓	✓
[14]	✗	✓	✓	✓
Proposed Method	✓	✓	✓	✓

III. Proposed Method

We designed a methodology to achieve our research objectives. The first step is to form a novel framework of privacy-preserving smart body scale. We got a cardiovascular disease dataset containing personal weights from Kaggle. We apply normalization, random noise perturbation, and k-means clustering for anonymization. We apply cardiovascular disease classification using gradient boosting. Finally, we compared the performance of the three anonymization methods with several metrics, including data utility, entropy, and distortion. Fig. 1 makes it easier to explain our methodology by presenting it in diagram form.

A. The Privacy-Preserving Smart Scale Framework

Anonymization is key in safeguarding personal data and ensuring compliance with GDPR [15]. GDPR demands that personal data be stored in a way that ensures confidentiality and security. The task of anonymization is to remove or change identifying information from data so that mapping the data back to the original data becomes impossible or difficult [16]. With anonymization, personal data can still be used for

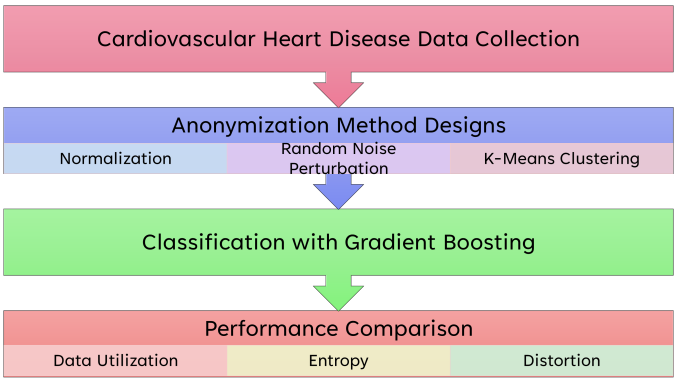


Fig. 1: Our Proposed Methodology

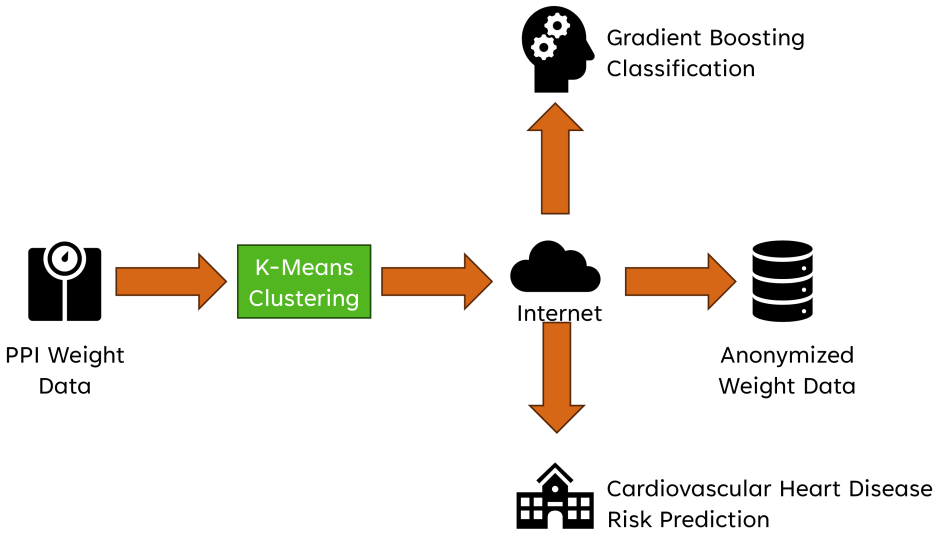


Fig. 2: The PPSBS model.

purposes such as machine learning training while maintaining the privacy of the people whose data is used [17].

Here, we propose a generalization type of anonymization, namely a type of anonymization, by replacing a value in the dataset with a more general representation [18]. K-anonymity is a generalization assessment that ensures that each value represented cannot be distinguished from k-1 other data [19]. K-means clustering is one step in achieving k-anonymity [20].

We propose a novel privacy-preserving Smart Body Scale Framework. Fig. 2 shows the privacy-preserving smart body scale (PPSBS) framework design. The original weight data is considered personal identifiable information (PII), namely any information attached to a personal [21]. To maintain the anonymity of the data when the data is about to go through the machine learning training process for cardiovascular heart disease risk prediction, we first perform k-means clustering on the data. After going through k-means clustering, the data has become a cluster. This new data has two characteristics: Firstly, the data cannot be recognized as PII anymore, and secondly, this data minimizes loss of data utility. Algorithm 1 explains the anonymization process using k-means.

Algorithm 1: K-Means Anonymization Algorithm

Data: Dataset
Result: Anonymous Dataset
1 Select Quasi-Identifiers;
2 Run and Apply K-Means Clustering;
3 Apply Perturbation on Attributes;
4 Run K-Anonymity Assessment;
5 Replace Original Data with Perturbed Data;
6 Run Machine Learning Training;
7 Run Anonymity Testing Metrics;

Apart from the generalization method, there are other anonymization methods, including random noise addition. Random noise addition in anonymization refers to adding random noise to the original data with a known distribution property to maintain privacy while keeping parameter estimation efficient and consistent [22]. The random noise addition formula that we use in this research is as follows:

$$x'_n = 2x_n + \mathcal{N}(2, 20), n \in N \tag{1}$$

where $\mathcal{N}(2, 20)$ is a random number from the normal distribution with $\mu = 2$ and $\delta = 20$.

B. Cardiovascular Heart Disease Risk Prediction with Gradient Boosting

We obtained the cardiovascular heart disease dataset from Kaggle. This dataset was originally uploaded by Kuzak Demspy in 2021. This cardiovascular heart disease dataset comprises 13 features, 70,000 data items, and two labels. The labels are 0 for people indicated to have cardiovascular heart disease and 1 for those not indicated. Of the 13 features, we took one feature called "weight" from the smart body scale via the IoT architecture.

We use gradient boosting to classify cardiovascular heart disease. Gradient boosting is a type of ensemble learning that uses the boosting concept, namely a concept where several weak learners are arranged serially [23], where the weak learners are in the form of a decision tree. In this serial arrangement, the next weak learner in the sequence improves the performance of the previous weak learner by reducing the estimated error based on the gradient function. The final result of the weak learners' ensemble is the result of aggregation with majority voting.

We adopt several measurement metrics from several related studies to compare the performance of our three anonymization methods: information loss, entropy, and distortion. Information loss in anonymization is the reduction in the level of information in data due to the anonymization process [24].

Anonymization does hide sensitive privacy information, but on the other hand, information that is useful for machine learning training, for example, is also reduced. We calculate information loss with the following formula:

$$L = Acc - Acc' \tag{2}$$

where L is the information loss, Acc is the accuracy of the machine learning model using the original dataset, and Acc' is the accuracy of the machine learning model using the anonymous dataset. The smaller the information loss value, the better the measurable anonymization method.

Entropy in anonymization is a metric to quantify the degree of anonymity of an anonymization method [25]. In a more general definition, entropy in machine learning measures the randomness of a feature. The lower the entropy, the feature is less random. The formula for the entropy of a feature x ($H(x)$) is as follows:

$$H(x) = -\sum_{v \in V} p(x_v) log_2(p(x_v)) \tag{3}$$

where V is the number of unique values in a feature, then $p(x_v)$ is the probability of v appearing in the feature.

Finally, distortion measures the data modified in the anonymization process to protect privacy without reducing data utility [26]. We use mean absolute error (MAE) for the distortion metric. Here is the formula:

$$\text{MAE} = \frac{1}{N} \sum_{n \in N} |x_n - x'_n| \tag{4}$$

C. GDPR Compliance

An IoT system that involves personal data must comply with GDPR. Here are some of the GDPRs our system is considered:

- (**R1**) Data Minimization (Art. 5(1)(c)): Although the body scale produces data, only the weight data is sent to the cloud for processing by machine learning, which is included in data minimization
- (**R2**) Anonymization and Pseudonymization (Recital 26, Art.4(5)): Anonymization is also regulated by the GDPR
- (**R3**) Purpose Limitation (Art. 5(1)(b)): The weight data sent is only used for cardiovascular disease detection, not for anything else.
- (**R4**) Documentation (Art. 30): A log monitors the data that is processed, retained, and collected.

IV. Results and Discussion

A. Results

The first step in performing k-means clustering is conducting elbow method analysis. We run the elbow method for 1 cluster to 14 clusters. Fig. 3 shows the elbow method curve. We choose six clusters in ordinary k-means clustering with a curve like the graphic observation results. However, the number of clusters must meet k-anonymity. We carried out a k-anonymity assessment for 1 cluster to 14 clusters.

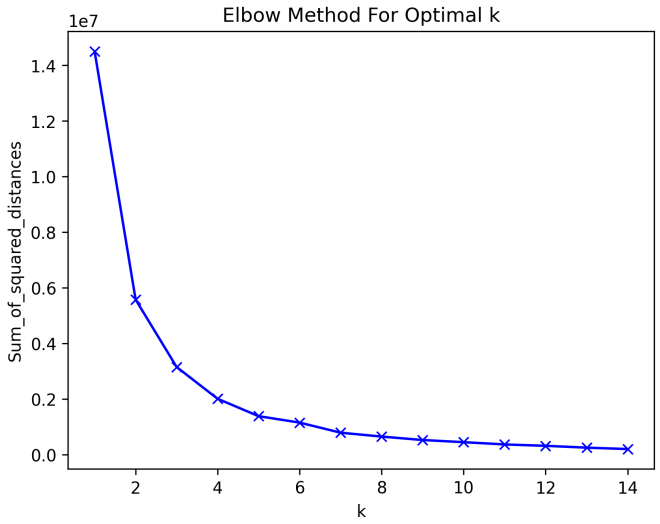


Fig. 3: The elbow method on determining the optimum k in k-Means.

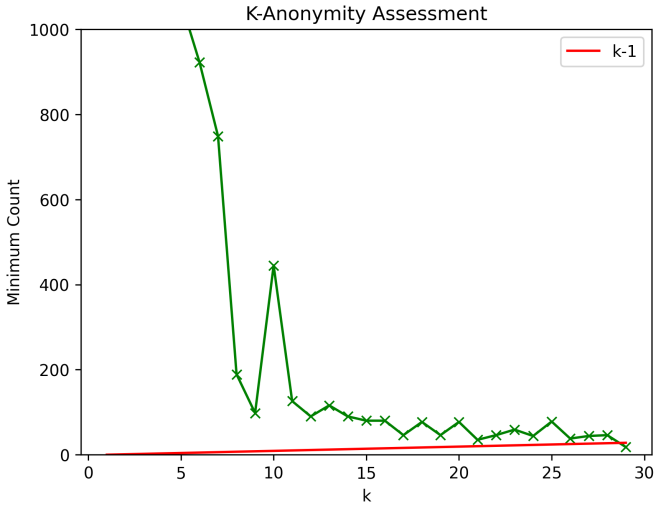
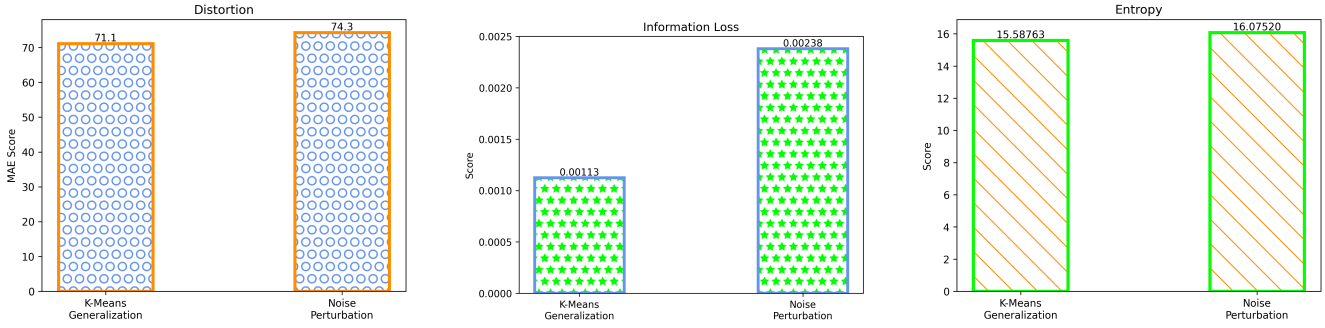


Fig. 4: The k-anonymity assessment

K-anonymity assessment requires that one generalization result value cannot be distinguished from at least k-1 values from another result. In other words, the number of labels resulting from k-means clustering cannot be smaller than k-1. Fig. 4 shows the results of our k-anonymity assessment. The first line describes the smallest number of labels from k-means clustering with k clusters. The second line is the k-1 value. Tests show that the smallest number of labels from k-means clustering is smaller than k-1 after k = 29. The conclusion is that the labels resulting from k-means clustering with k = 6 can be used for anonymization.

In the next step, we build four gradient-boosting models for cardiovascular heart disease risk prediction. Each uses four different datasets as follows:

1) Original dataset



(a) (b) (c)

Fig. 5: Performance comparison of k-means generalization and noise perturbation: (a) Distortion (b) Information Loss (c) Entropy.

2) Dataset with anonymous weights from k-means clustering
3) Dataset with anonymous weight resulting from random noise addition

Table II shows the performance of gradient boosting with the original dataset. Because there is no imbalance problem in the dataset, the model's performance can be represented by an accuracy value, namely 0.74.

We compare the two anonymization methods' information loss, entropy, and distortion to find the most optimal method. Fig. 5 shows the comparison. The test results show that k-means generalization has a smaller distortion, meaning the value is more similar to the original value than noise perturbation. Then, k-means generalization also has smaller information loss, meaning the gradient boosting model's accuracy reduction due to anonymization is smaller than noise perturbation. Finally, k-means generalization shows lower entropy, meaning that the randomness value of k-means generalization is lower than noise perturbation.

B. Discussion

In Subsection III-C, we have discussed how our system complies with several GDPRs. We compared our IoT system with several state-of-the-art IoT systems regarding how compliant our system is with GDPR. Badii *et al.* [27] is research on smart cities that are GDPR-compliant. The focus of the paper includes two, namely anonymization and documentation. Koutli *et al.* [28] is research into GDPR-compliant e-health. The focus of this research is compliance with documentation. Alamri *et al.* [29] is research that applies blockchain to GDPR-compliant personal health records (PHR). The focus of the research was anonymization. Barati *et al.* [30] is GDPR verification for IoT. The focus of this research is data minimization. Our research contribution is an IoT framework that is GDPR-compliant, specifically for data minimization, anonymization, purpose limitation, and documentation.

TABLE II
THE PERFORMANCE OF THE CARDIOVASCULAR HEART DISEASE RISK PREDICTION ON THE ORIGINAL DATASET

	Precision	Recall	F1-Score	Support
Label 0	0.72	0.77	0.75	11506
Label 1	0.76	0.7	0.73	11594
Accuracy			0.74	23100
Macro Avg.	0.74	0.74	0.74	23100
Weighted Avg.	0.74	0.74	0.74	23100

TABLE III
STATE-OF-THE-ART GDPR-COMPLIANT IOT FRAMEWORKS

Reference	Data Minimization	Anonymization	Purpose Limitation	Documentation
[27]	✗	✓	✗	✓
[28]	✗	✗	✗	✓
[29]	✗	✓	✗	✗
[30]	✓	✗	✗	✗
Proposed Model	✓	✓	✓	✓

Several studies have discussed advances in the smart body scale, such as the paper [8], [9]. On the other hand, several healthcare system researchers have discussed their privacy concerns, such as the paper [10], [11]. However, no research has focused on privacy-preserving body weight data classified as PII. Our research contribution is a smart body scale that pays attention to how the PII weight data from the tool can be preserved.

Several studies, such as Ghate *et al.* [12], use k-means for anonymization. Ashkouti *et al.* [13] uses k-means for anonymization and uses Apache Spark. Information loss from this method is a decrease in accuracy of around 0.01 to 0.02. K-means clustering in the research of Logesware *et al.* [14] is intended for anonymization of personal health records. However, no one has implemented k-means anonymization for smart body scales. Our research contribution is a smart body scale that applies k-means anonymization.

V. CONCLUSION

This research succeeded in implementing a cardiovascular disease detection model that uses body weight data that has gone through an anonymization process. Anonymization in this research uses k-means clustering. We have analyzed the

k-anonymity of our k-means clustering process. Test results show that our elbow method shows that the optimum number of clusters for body weight is six. This number has passed the k-anonymity assessment. Furthermore, through comparisons, we show that the k-means generalization performs better than noise perturbation with distortion, information loss, and entropy values 71.1, 0.001, and 15.6, respectively.

ACKNOWLEDGMENT

We thank the Research and Community Service (PPM) Directorate of Telkom University for funding our research. We also thank Kuzak Demspy for making the cardiovascular disease risk dataset available online and open access. It deepens our understanding of data privacy and GDPR compliance.

REFERENCES

[1] L. Zhang, P. Sun, and H. Lu, "Research on application and measurement of body scale," in *2022 International Seminar on Computer Science and Engineering Technology (SCSET)*, pp. 376–379, IEEE, 2022.

[2] E. Seto, R. Gravina, J. Kim, S. Lin, G. Ferrara, and J. Hua, "Prediction of personal cardiovascular risk using machine learning for smartphone applications," in *2020 IEEE International Conference on Human-Machine Systems (ICHMS)*, pp. 1–6, IEEE, 2020.

[3] N. D. Pham, T. K. Phan, A. Abuadbba, D. Nguyen, and N. Chilamkurti, "Split learning without local weight sharing to enhance client-side data privacy," *arXiv preprint arXiv:2212.00250*, 2022.

[4] N. Senavirathne and V. Torra, "On the role of data anonymization in machine learning privacy," in *2020 IEEE 19th International conference on trust, security and privacy in computing and communications (TrustCom)*, pp. 664–675, IEEE, 2020.

[5] A. W. McDonald, S. Afroz, A. Caliskan, A. Stolerman, and R. Greenstadt, "Use fewer instances of the letter "i": Toward writing style anonymization," in *Privacy Enhancing Technologies: 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012. Proceedings 12*, pp. 299–318, Springer, 2012.

[6] M. Tran and M. Soleymani, "A speech representation anonymization framework via selective noise perturbation," in *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1–5, IEEE, 2023.

[7] A. Abbasi and B. Mohammadi, "A clustering-based anonymization approach for privacy-preserving in the healthcare cloud," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 1, p. e6487, 2022.

[8] E. Johannessen, J. Johansson, G. Hartvigsen, A. Horsch, E. Årsand, and A. Henriksen, "Collecting health-related research data using consumer-based wireless smart scales," *International Journal of Medical Informatics*, vol. 173, p. 105043, 2023.

[9] J. Turicchi, R. O'Driscoll, G. Finlayson, C. Duarte, A. L. Palmeira, S. C. Larsen, B. L. Heitmann, R. J. Stubbs, *et al.*, "Data imputation and body weight variability calculation using linear and nonlinear methods in data collected from digital smart scales: simulation and validation study," *JMIR mHealth and uHealth*, vol. 8, no. 9, p. e17977, 2020.

[10] M. Stojkov, G. Sladić, B. Milosavljević, M. Zarić, and M. Simić, "Privacy concerns in iot smart healthcare system," in *International Conference on Information Science and Technology (ICIST), Kopaonik: Society for information systems and computer networks*, pp. 62–65, 2019.

[11] E. Dincelli, X. Zhou, A. Yayla, and H. Jafarian, "Wearable devices and privacy concerns: Data collection, analysis, and interpretation," in *Privacy Concerns Surrounding Personal Information Sharing on Health and Fitness Mobile Apps*, pp. 83–111, IGI Global, 2021.

[12] R. B. Ghate and R. Ingle, "Clustering based anonymization for privacy preservation," in *2015 International Conference on Pervasive Computing (ICPC)*, pp. 1–3, IEEE, 2015.

[13] F. Ashkouti, K. Khamforoosh, A. Sheikhahmadi, and H. Khamfroush, "Dhkmeans-diversity: distributed hierarchical k-means for satisfaction of the -diversity privacy model using apache spark," *The Journal of Supercomputing*, vol. 78, no. 2, pp. 2616–2650, 2022.

[14] G. Logeswari, D. Sangeetha, and V. Vaidehi, "A cost effective clustering based anonymization approach for storing phr's in cloud," in *2014 International conference on recent trends in information technology*, pp. 1–5, IEEE, 2014.

[15] M. Oleksy, N. Ropiak, and T. Walkowiak, "Automated anonymization of text documents in polish," *Procedia Computer Science*, vol. 192, pp. 1323–1333, 2021.

[16] I. E. Olatunji, J. Rauch, M. Katzensteiner, and M. Khosla, "A review of anonymization for healthcare data," *Big data*, 2022.

[17] J. Domingo-Ferrer, "Personal big data, gdpr and anonymization," in *Flexible Query Answering Systems: 13th International Conference, FQAS 2019, Amantea, Italy, July 2–5, 2019, Proceedings 13*, pp. 7–10, Springer, 2019.

[18] B. Hore, R. Jammalamadaka, S. Mehrotra, and A. D'Ascanio, "Contrained generalization for data anonymization-a systematic search based approach," *arXiv preprint arXiv:2108.04897*, 2021.

[19] H. Kaur, N. Hooda, and H. Singh, "k-anonymization of social network data using neural network and svm: K-neurosvm," *Journal of Information Security and Applications*, vol. 72, p. 103382, 2023.

[20] A. Arutyunova and M. Schmidt, "Achieving anonymity via weak lower bound constraints for k-median and k-means," *arXiv preprint arXiv:2009.03078*, 2020.

[21] Z. Song, H. Ma, S. Sun, Y. Xin, and R. Zhang, "Rainbow: reliable personally identifiable information retrieval across multi-cloud," *Cybersecurity*, vol. 6, no. 1, p. 19, 2023.

[22] H. Goldstein and N. Shlomo, "A probabilistic procedure for anonymisation, for assessing the risk of re-identification and for the analysis of perturbed data sets," *Journal of Official Statistics*, vol. 36, no. 1, pp. 89–115, 2020.

[23] S. F. Pane, A. G. Putrada, N. Alamsyah, and M. N. Fauzan, "A psogbr solution for association rule optimization on supermarket sales," in *2022 Seventh International Conference on Informatics and Computing (ICIC)*, pp. 1–6, IEEE, 2022.

[24] M. Hashimoto, R. Morishima, and H. Nishi, "Low-information-loss anonymization of trajectory data considering map information," in *2020 IEEE 29th International Symposium on Industrial Electronics (ISIE)*, pp. 499–504, IEEE, 2020.

[25] S. Arca and R. Hewett, "Is entropy enough for measuring privacy?," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1335–1340, IEEE, 2020.

[26] V. Primault, S. B. Mokhtar, C. Lauradoux, and L. Brunie, "Time distortion anonymization for the publication of mobility data with high utility," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 539–546, IEEE, 2015.

[27] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart city iot platform respecting gdpr privacy and security aspects," *IEEE Access*, vol. 8, pp. 23601–23623, 2020.

[28] M. Koutli, N. Theologou, A. Tryferidis, D. Tzovaras, A. Kagkini, D. Zandes, K. Karkaletsis, K. Kaggelides, J. A. Miralles, V. Oravec, *et al.*, "Secure iot e-health applications using vicinity framework and gdpr guidelines," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 263–270, IEEE, 2019.

[29] B. Alamri, I. T. Javed, and T. Margaria, "A gdpr-compliant framework for iot-based personal health records using blockchain," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, IEEE, 2021.

[30] M. Barati, O. Rana, I. Petri, and G. Theodorakopoulos, "Gdpr compliance verification in internet of things," *IEEE access*, vol. 8, pp. 119697–119709, 2020.