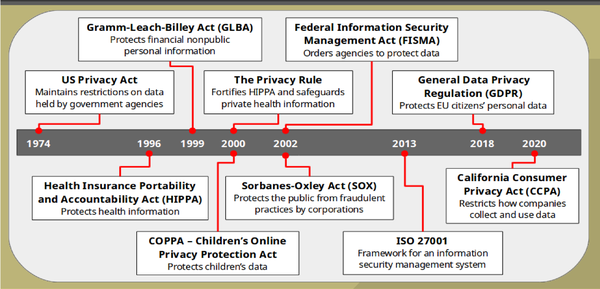
Helmut
Bierbaumer
IMS19

Machine Learning and Data Privacy

FH JOANNEUM
University of Applied Sciences



Motivation & Objectives

With the emergence of Big Data, the protection and privacy of personal data is becoming an increasingly important subject. Coinciding with the technological progress, many countries and associations have enacted data privacy regulations, of which the General Data Privacy Regulation (GDPR) is only the most prominent. The timeline lo the left gives an overview of some common laws in the US and the EU.
The power of sophisticated Machine Learning (ML) algorithms provides the necessary insight into the wealth of information. As such, the combination of Big Data and ML has already yielded numerous success stories that have led to significant improvements in areas such as healthcare, and customer service. Out of these circumstances, a field of tension between two opposing poles arises, which is addressed by this project work. On the one hand, there is the promising scientific field of artificial intelligence, for which data is indispensable as training material. On the other hand, there are legal restrictions on data protection and the legitimate concerns of individuals about the privacy of their sensitive information.

This leads to the central consideration of whether it is possible to build powerful ML models while still preserving data privacy. In particular, the aims of this project work can be summarized by the following two main research objectives:

(I) Evaluation of viable data protection techniques for different data types.

(II) Assessment of the impact on ML algorithms when trained with anonymized datasets.

Company	Type of Service	Year	Affected User Accounts [Millions]
Yahoo	Web	2013	3000
Sina Weibo	Social Media	2020	538
Marriott International	Hotel	2014	500
Friend Finder Networks	Web	2016	412
MySpace	Social Media	2013	360
NetEase	Email Provider	2015	235
Zynga	Mobile Games	2019	218
LinkedIn	Career Networking	2012	165
Dubsmash	Video Messaging	2018	162
Adobe	Software	2013	153

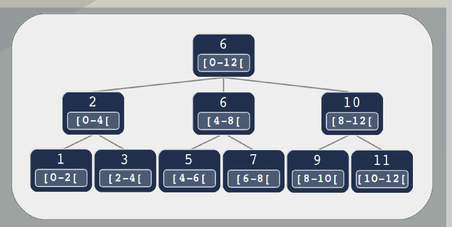
Data breaches that affect millions of users occur all to frequently. The table above provides a listing of the most devastating data breaches of the 21st century.

Case Studies

Multi-Class Categorization

Privacy Protection

k-Anonymity

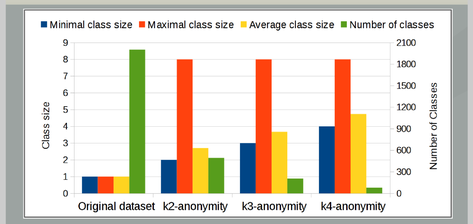


Generalization via hierarchical structures

Binary Classification

Privacy Protection

k-Anonymity with l-Diversity

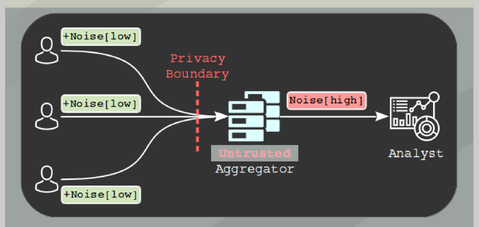


Mapping onto equivalent classes

Clustering and Segmentation

Privacy Protection

Differential Privacy

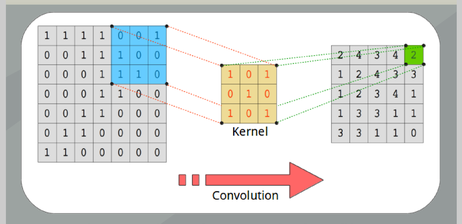


Adding random noise

Image Classification

Privacy Protection

Blurring and Pixelization

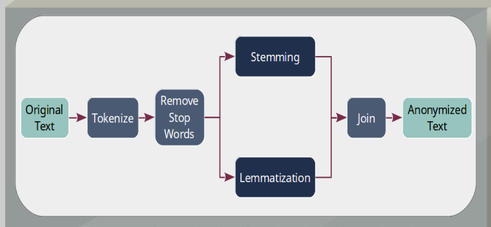


Obscuration via convolution filters

Text Classification

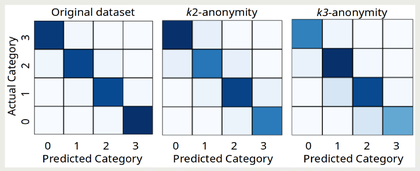
Privacy Protection

Stemming and Lemmatization

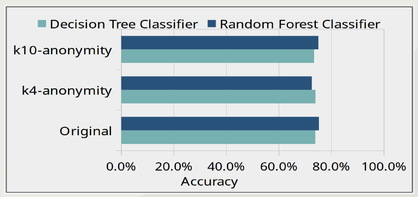


Processing chain for textual content

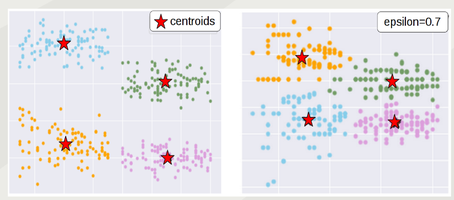
Results



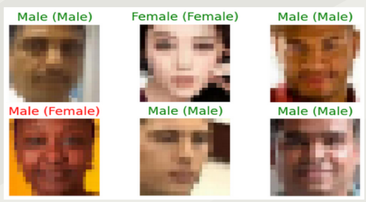
Confusion matrices on original and anonymized datasets



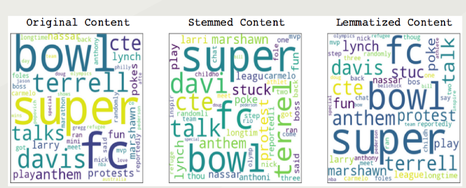
Comparison of the achieved accuracy rates



Obtained segmentation clusters for original and anonymized data points



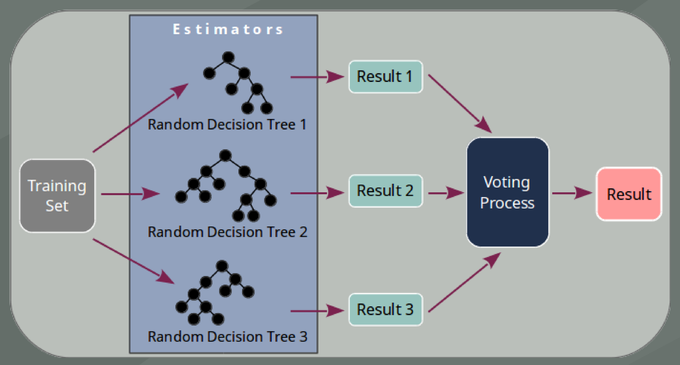
Gender classification on pixelated images

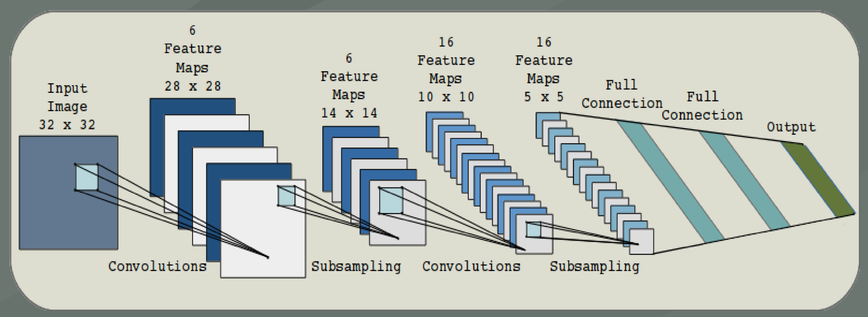


Generated word clouds from original and sanitized text segments

Machine Learning Algorithms & Models

- Logistic Regression
- k-Nearest Neighbor
- Support Vector Machines
- Naive Bayes
- Decision Trees
- Random Forest
- Convolutional Neural Networks
- k-Means





Conclusion

As the overall finding of the conducted research, it can be stated that in all of the investigated use cases, anonymized data were absolutely sufficient to achieve the desired goal for the different types of ML tasks. Regarding the various types of ML models, the results showed that there are indeed measurable differences between the compared algorithms and approaches. While the selection of the applied ML model has an impact on the overall quality of the achievable results, data anonymization has very limited influence on the effectiveness and performance of the implemented algorithm.

This project work demonstrated the possibilities and potential of combining ML and data privacy protection. Moreover, the evaluations have also shown that anonymization techniques can even lead to better performing systems. This convincing outcome has been observed by the training of models for text classification tasks on generalized data which ultimately achieved higher accuracy rates compared to the original dataset. As a summary from the findings of the five case studies, it can be concluded that it is indeed feasible to build highly accurate and well-functioning models for ML algorithms while still complying with privacy regulations.

References

ISBN: 9783319161099 G. Livraga: Protecting Privacy in Data Release
ISBN: 9781784392888 L. Coelho: Building Machine Learning Systems with Python
ISBN: 9783319084695 S. Zeadally: Privacy in a Digital, Networked World

Supervisor
DI Johannes Feiner

Contact
helmut.bierbaumer@edu.fh-joanneum.at