PRIVACY PRESERVING MACHINE LEARNING CHALLENGES AND SOLUTION APPROACH FOR TRAINING DATA IN ERP SYSTEMS

Mithun Gaur
B.Tech (IT), PGDM (Marketing & IT),
BIMM- BIMM Balaji Institute of Modern Management, Pune, India

ABSTRACT
The digital transformation is ubiquitous and pushing the case further for ERP companies to incorporate more machine learning algorithms in order to drive intelligent real-time decision-making capabilities. ERP systems have started incorporating machine learning use cases powered by the huge enterprise data, cloud and compute capabilities. However, privacy of data remains a challenge. Data privacy is at the core of a machine learning model that is trained on sensitive information. Not just for profit businesses, but even academic endeavors in the field of medicine cannot progress if they can’t access sensitive medical information in a privacy preserved format. Ramifications of applying a ML model without even fully understanding what is happening inside its hidden layers can be disastrous and the resulting perils can lead to legal consequences. Therefore, Privacy preserving AI techniques started evolving in last few years. The privacy preserving AI field is still growing and there is an understanding gap in organizations and individuals, which makes privacy breach or compromise a pervasive business challenge. This paper focuses on what are key challenges for ERP companies as far as Training machine learning models on their enterprise data is concerned. And how can these challenges be overcome by applying data anonymization and differential privacy techniques.

Key words: Machine learning, Privacy Preserving, ERP, Differential privacy, k anonymity, SAP HANA

http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=11&IType=4

1. INTRODUCTION
Personal Information is collected by a business when providing goods or services that are personalized for a user to add more value to the goods/services. This information collected could be aggregate, biometric- physiological, biological or behavioral characteristics including DNA, that can be used, singly or in combination with each other or with other
identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a face-print, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information[1] can be extracted. This information can help companies identify valuable customers, predict future behaviors, and enable insight-driven decisions which goes beyond what is possible from decision support systems. With the advent in compute and storage capabilities along with the vast increase in data, companies starting using Artificial intelligence mainly machine learning techniques that use complex algorithms trained on past data and understand the hidden relationships to build models that can be applied by companies to predict business outcomes. Use of ML algorithms has gained lot of traction in recent years to uncover newer business opportunities and business models to such an extent that the privacy of the user’s personal information, which is at core, started being compromised. This led to formulation of various regulations such as GDPR(Europe), CCPA(California) and some other privacy legislations which are forcing organizations to take security and privacy seriously over their vested interests. This resulted in Privacy preserving AI/ML models. The need to protect personal privacy in the "era of big data", and the potential to do so successfully in the future, with techniques that allow computation over encrypted data, are widely acknowledged[3]. The privacy preserving AI field is still growing and there is an understanding gap in organizations and individuals, which makes privacy breach or compromise a pervasive business challenge. Today digital transformation is forcing companies to adopt machine learning technologies[2] in various enterprise systems and ERP systems are no exception[9], most ERP systems have started providing machine learning capabilities[12], but privacy preserving is still catching up. Machine learning methods like differential privacy and k-anonymization have gained some traction but their implementation is in nascent stage in ERP systems.

2. RELATED BACKGROUND

Data privacy is at the core of a machine learning model that is trained on sensitive information. Not just for profit businesses, but even academic endeavors in the field of medicine cannot progress if they can’t access sensitive medical information in a privacy preserved format. Ramifications of applying a ML model without even fully understanding what is happening inside its hidden layers can be disastrous and the resulting perils can lead to legal consequences.

A starting point for preserving privacy is data-anonymization in the training set which removes all personally identifiable information. Netflix hosted a Million-Dollar Challenge[4] for the data science community that involved anonymous movie reviews 500,000 by anonymous users for 17,770 movies. However, Arvind Narayanan and Vitaly Shmatikov demonstrated a robust De-anonymization Technique[5] using publicly available Internet Movie Database (IMDB) data and successfully identified Netflix records of known users and other potentially sensitive information.

C. Dwork ‘s[3][6] research on Differential privacy suggests that it is a notion of privacy tailored to private data analysis, where the goal is to learn information about the population as a whole, while protecting the privacy of each individual, differential privacy ensures that the system will behave in essentially the same fashion, independent of whether any individual opts in to, or out of, the database[6]. Intuitively, this captures the idea that no individual's data has a large effect on the output distribution of the mechanism. Organizations that are tasked with custody of personal information, be it patient health or other data, are skeptical of their ability to engage in machine learning (ML), partly due to lack of clarity on policies governing...
use of such data, and partly due to the fear of unknowingly violating the privacy of individuals that may occur in the process of mining such information[7].

3. CHALLENGES IN PRIVACY PRESERVING MACHINE LEARNING IN ERP SYSTEMS
There are numerous challenges in transforming a machine learning model into privacy preserving AI model such as :-

- Training data reverse engineering
- Model weight or hyperparameter stealing
- Model stealing
- Backdoor memorization

However, in ERP systems the later 3 namely- Model weight or hyperparameter stealing, Model stealing and back door memorization are less significant as compared to training data reverse engineering because ERP systems are the IT backbone of any organization[14] where proprietary data- transactional or master data is stored[11][12][13][14]. And any customer data which contains sensitive information, that can uniquely identify a customer need privacy preserving.

4. TRAINING DATA REVERSE ENGINEERING
Training Data itself can be reverse engineered to decode sensitive personal data for e.g. Arvind Narayanan and Vitaly Shmatikov[5] demonstrated a robust De-anonymization Technique using and successfully identified Netflix records of known users and other potentially sensitive information. Model weights, hyperparameters can be reverse engineered to re-construct training data and reverse-engineering models is not as huge challenge as one would think it to be. Users’ input data can be observed by the model creator and output of a model is also visible to others along with the user whose data is being inferred upon. Any model can leak information in unexpected ways and unintentional memorization. Model can memorize training data which happens in early stages and prevails further, no matter how rarely the specific information occurs as proved by Carlini and Wagner[7]. When a model gives 100% accuracy on training data but perform poorly on test data we can infer that it has memorized the random training data. To combat training data challenges, there are different privacy preserving training data preserving methods, which can be broadly divided as :-

- Anonymization methods like k-anonymization, data masking
- Differential privacy methods

5. TRAINING DATA PRESERVATION IN ERP
Before looking at how an ERP system should handle training data privacy preservation let’s look at what does these technique mean:-

5.1. Anonymization
The technique of anonymizing data by removing private details or replacing them with random values like phone numbers and zip codes is highly insufficient and the privacy it provides quickly degrades as adversaries obtain auxiliary information about the individuals represented in the dataset.

In ERP systems like SAP S/4 HANA[16] which has in memory HANA database, is the first vendor to include anonymization methods in its core SAP HANA system [8] data anonymization happens at the view level and the data in the table level remains unchanged. SAP HANA offers two different anonymization methods: k-anonymity and data masking.
Additionally, we can also add custom definition of anonymization views, access reporting views, and make use of the integration in the authorization framework[8]. Therefore, SAP HANA anonymization methods provides following invaluable business benefits to companies:-

- SAP HANA data anonymization enables customers to utilize personal data without inferring the privacy of individuals.
- Helps in analytics and machine learning scenarios of anonymized personal data possible.
- Enhances customer’s ROI by leveraging the value of enterprise data
- Real-time analytics on anonymized data helps in deriving insights from data that could not be leveraged beforehand

SAP HANA data masking is another technique that help in anonymizing data and it helps in:-

- Hiding sensitive information from DBAs and power users with broader access.
- Display/hide sensitive information depending on the user role for example – restricted view for call center employees.

### 5.2. Differential Privacy

Differential Privacy [6], is a privacy preserving ML mathematical model in which noise is added and randomness is introduced to the dataset without affecting the distribution of the sample, retaining the plausible deniability so that the individuals cannot be uniquely singled out in the data set and the results are not dependent on any individual data point.

For example, SAP HANA uses the Laplace mechanism. It draws noise from a Laplace distribution such that the multiplicative guarantee holds, and requires the definition of the sensitivity, that is the maximum impact an individual can have on the data set with respect to the query results.[15] Choosing the correct sensitivity is necessary to guarantee differential privacy if the sensitivity is too higher than necessary, it will reduce the quality of the anonymized data.[15].

Differential Privacy-Everyone gets same privacy as that of removing their data points from the sample. The denoising function can help us in retrieving original data back. Differential privacy has some key properties that make it a rich and promising framework[6] like:

- Quantification of privacy loss-Privacy loss is denoted by epsilon \( \epsilon \) and is inversely proportional to privacy protection. It is a measure for comparisons among different techniques. Less Privacy loss means better privacy protection. Privacy loss can be controlled to ensures a trade-off between privacy loss and the accuracy.
- Composition-The quantification of loss permits analysis and control of cumulative privacy loss over multiple computations. Understanding the behavior of differentially private mechanisms under composition enables the design and analysis of complex differentially private algorithms from simpler differentially private building blocks.
- Group Privacy-Differential Privacy permits the analysis and control of privacy loss incurred by groups, such as families.
- Closure Under Post-Processing- Differential Privacy is immune to post processing i.e.an adversary , without additional knowledge about the private database, cannot compute a function of the output of a differentially private algorithm and make it less differentially private.
However, if someone observes the data for a long time and deciphers the function using which the noise is added, then differential privacy can be breached. Example of differential privacy methods are - Differential Private Stochastic Gradient decent, GAN’s creating synthetic data.

6. CONCLUSION
Digital transformation has made ERP systems more agile and intelligent. However, there are numerous challenges that need to be addressed and requirements that need to be met[10] upfront before utilizing sensitive data and leveraging its value. Last but not the least, machine learning models form the core product & IP of many companies, so having a model, or training data or hyperparameters/weights stolen is a severe threat and can have significant negative business implications and credibility damage. There are many choices as far as privacy preserving techniques are concerned; however, which techniques to bundle differs from one use case to another. And the ability to club these different methods to guarantee privacy preservation is maximized, is what will differentiate a successful organization from an unsuccessful organization.

FUTURE RESEARCH
This research article aims at training data privacy preserving challenges and solution approach from ERP perspective, future research can include other aspects like model or hyperparameter theft.

REFERENCES
[1] https://www.oag.ca.gov/privacy/ccpa
Privacy Preserving Machine Learning Challenges and Solution Approach for Training Data in ERP Systems


