EasyChair Preprint

№ 6677

Local Privacy Protection System Framework Based on Encryption Algorithm Library

Gu Yingcheng, Chen Yongqiu and Xu Mingsheng

September 24, 2021

Local Privacy Protection System Framework Based on Encryption Algorithm Library

Yingcheng Gu[1], Yongqiu Chen[2], Mingsheng Xu[3]

[1]State Grid Jiangsu Electric Power Co., Ltd. Information & Techcommunication Branch , Nanjing Jiangsu, China

[2]Jiangsu Electric Power Information Technology Co., Ltd., Nanjing Jiangsu, China

[3]Jiangsu Electric Power Information Technology Co., Ltd., Nanjing Jiangsu, China

Abstract: How to effectively protect the privacy of data, to establish a data center platform, solve the problem of deep learning vulnerable, has become a urgently need to solve the problem, in which the data is desensitization treatment is an effective way to avoid data privacy, this study puts forward a new solution, first identify sensitive data, then put the sensitive data from the original data. At the same time, the desensitization technology library of sensitive data is built, and then the sensitive data is desensitized. Finally, the data is transmitted to the model for training, so that the deep learning model is delivered for training without changing the original distribution of data, and the privacy leakage caused by the attack of the model is avoided.

Keywords: Encryption Algorithm Library, Privacy Protection, Data Center Platform, Deep Learning

0 Introduction

In the current era of big data, many fields involving the storage and use of personal privacy data inevitably need to face data security and compliance problems. In terms of government affairs, as government data platforms tend to grasp a large amount of extremely sensitive personal information such as identity information and household registration information. It is necessary to protect data privacy in the whole life cycle of data collection, transmission, application and archiving, and implement other data security protection means simultaneously. In key fields such as finance and telecommunications, data security protection technology is the first choice to achieve compliance because telecom customers' mobile phone numbers, call records, network traffic and other information and financial customers' personal account information, transaction records and other information are important and sensitive information, which face strict industry regulatory requirements. In the internet field where data is most widely used, a large amount of user behavior data that may involve personal privacy is used. From the perspective of avoiding additional costs caused by violations, data desensitization is an important prerequisite step when using sensitive data.

The existing methods to protect private data from being leaked can be roughly divided into two schools[4-5]. One is the method based on sensitive data encryption, and the other is the differential privacy protection technology based on disturbance[6-7]. The encryption algorithm of the former can be divided into multi-party secure computing[1] and homomorphic encryption[2-3]. According to the location of disturbance, the latter can be roughly divided into input disturbance[8-11], target disturbance[12], gradient disturbance[14] and output disturbance.

Fund Project Name: Research and Application of Data Security Protection Technology Based on Data Center
Fund Project No: 5210ED2100L

Compared with encryption algorithm, the differential privacy protection method is a method that has undergone strict mathematical proof[6] and has strong utility. However, the current model calculation method based on deep learning is particularly common, and how to desensitize the data so that the recognition accuracy of the model is less affected has become an important research target: there are a lot of people have long believed by gradient sharing strategy[15-17], the model in local training, to avoid the leakage of data privacy, now there are many ways to do this, then[18] proves that this method is also a safe method, the article said, in a known learning model, and real gradient under the condition of weight parameters. With only a few iterations, the pixel-level image and label can be inferred backwards. Therefore, the strategy of gradient sharing also appears to have some risks. At the same time, the paper also shows that the attack can be resisted by gradient disturbance method, target disturbance method or encryption method[14] shows that the standard sgd gradient descent method has a high variance in differential privacy, and can achieve good experimental results by restricting it. However, due to the disturbance of the gradient, the gradient descent is more effective for the function that is not non-convex, and it is easy to cause the problem of non-convergence[19-20]. Literature belief network is proposed aiming at the encoder to drink convolution depth to the polynomial approximation nonlinear objective function is expressed as parameters, disturbance, and then through the target training process meet the parameters of privacy protection, but this method is not suitable for the present various based on modular neural network model, at the same time, some of the other is based on the concentration difference privacy[21], zero-set differential privacy[22] and rainey differential privacy[23] are widely used in the privacy protection of deep learning. However, it is difficult for these methods to withstand attacks such as member reasoning, and it is easy to cause higher possibility of privacy leakage[24].

And comparison, based on the privacy protection mode of the encryption algorithm, may be able to better adapt to the local data privacy protection, however, encryption algorithm in the process of data encryption and decryption for data process, involving the huge computational overhead, making it difficult to fall to the ground, this paper proposes a kind of new train of thought, first identify sensitive data. Then, the sensitive data is extracted from the original data, and at the same time, the desensitization technology library of sensitive data is constructed. Then, the sensitive data is desensitized, and the desensitization process does not change the original distribution information of the data. Finally, the data is transmitted to the model for training.

1 Implementation plan

In order to establish a privacy protection data center platform, as shown in the Figure 1, this paper proposes the following system framework, which mainly includes sensitive data discovery, data extraction, data desensitization, data output functions, but also supports data source management, desensitization task management, algorithm configuration association and user rights management and other major functions.

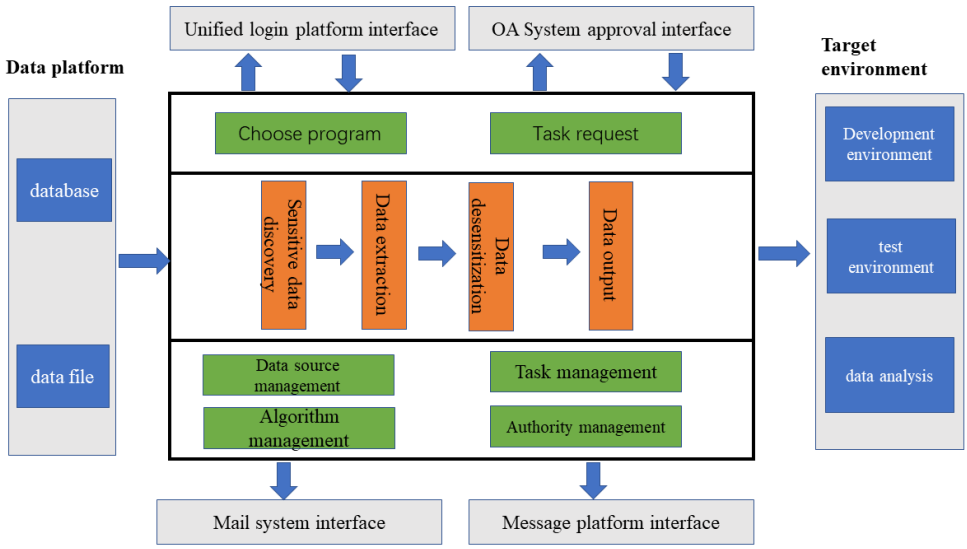

Figure 1 System framework

Sensitive data discovery and data extraction module: this module has the capability of sensitive data found rule management, more than 20 found built-in rules, primarily through regular expression custom find rules and data dictionary or custom fields dictionary found rules is given priority to, and the composite way custom found rule and other rule is complementary, used in the field information can press a split into multiple scenes of sensitive data. In addition, you can customize functions based on the service characteristics of field data to meet the requirements for discovering sensitive data. At the same time, the system also supports the selection of database schema and table, which can be used to discover the sensitive data when multiple sensitive fields appear simultaneously in a single table. In the aspect of sensitive data sorting, it has the function of sensitive field sorting and sensitive file sorting, which is mainly based on the manual assisted adjustment of data column and sensitive data relationship, so as to achieve more precise and sensitive data management.

Other sensitive data also support the rules found in the list field manual adjustment and verification, to support the list of sensitive data field note information to fill in, and support the list of sensitive data field is set to the sensitive field, contains settings and unified set alone, support the sensitive data list of export and import, export of sensitive data list can be restricted to edit and verify, verify the complete list of data can be imported into the system, the configuration rule strategy solve the sensitive data found the templated and external interface processing, sample data browsing, support for sensitive sample data in the database and file the source of more sensitive to sample data browsing, support tasks have been found in the data fields add, delete, change the status of the tips and correction. It is used to prompt and manually correct the status of the changed fields when they are rediscovered after being changed. In this way, users can only pay attention to the sensitive data of the changed fields for rule verification.

Data desensitization and desensitization management module: according to the characteristics of the different data using different desensitization algorithm, can be the common data such as name, id number, bank account, amount, date, address, telephone number, email address, license plate number, chassis number, name of the enterprise,

industrial and commercial registration number, organization code, taxpayer identification number to desensitization and other sensitive data, built-in desensitization algorithm has the following features:

(1) Synonymous replacement, the original sensitive data is replaced with data with the same meaning, such as the name is still meaningful after desensitization, and the address is still the address after desensitization.

(2) Partial data masking: part or all of the original data is replaced with characters such as "*" or "#" to cover part or all of the original text.

(3) Mixed shielding: the related columns are shielded as a group to ensure that the masked data in these related columns maintain the same relationship. For example, the city, province and postcode remain the same after shielding.

(4) Deterministic masking to ensure that repeatable masking value is generated after running masking.

You can ensure that specific values (e.g., customer number, id number, bank card number) are masked as the same value in all databases. For the management of the desensitization function, different desensitization schemes can be formulated according to various data application scenarios such as system development, functional testing, performance testing, data analysis, etc. The desensitization scheme for the development and test environment can guarantee the uniqueness and certainty of the data after desensitization, and the reducibility of the data after desensitization can be guaranteed for the data analysis scenario. Desensitization strategy is the rule of desensitization of sensitive data, the desensitization strategy includes the characteristics of sensitive data and the desensitization algorithm for this kind of data. For the same application scenario, users can combine several desensitization strategies to form a desensitization scheme suitable for this scenario. After the desensitization scheme is formulated, it can be reused to meet the desensitization requirements of different batches of data in this scenario. Support the configuration of cross-mode desensitization and source mode desensitization, cross-mode desensitization is used for source database to target database desensitization scenario, source mode desensitization is used for direct desensitization of data in the source database; Supports the configuration of a group dictionary, which is used in the desensitization scenario where multiple fields in a table serve as conditions and the desensitization field is associated with the condition field.

The desensitization task given can be carried out against the target database system or structured file. Through the desensitization task, the product is connected with the business system that provides the original data and the system that uses the desensitization data. The user can select the source of the desensitization data, the direction of the desensitization data and the most suitable data desensitization scheme within the task. The maintenance and management function of tasks is enabled. Tasks can be stopped, started, or restarted, and tasks can be concurrently implemented to fully utilize system resources and improve desensitization efficiency. The desensitization task can be compatible with exceptions encountered during the execution, and the task can continue to execute without abnormal data. On the other hand, it also supports the configuration of the database and file source desensitization scheme, and supports the desensitization data output for the database and file; Supports metadata configuration for defensiveness tasks, including the schema name or database name of the destination database, table space, table processing - delete table, empty

data, and append data; Support data increment configuration, increment mode, increment table, increment name, increment value; You can query the execution history of desensitization tasks in the last week, last month, month, last month, or a specified period. At the same time, it has the scheduled task management ability and provides a mechanism for automatic desensitization of scheduled tasks. Add edit, and delete scheduled tasks. Supports the configuration of discovery tasks, desensitization tasks, and scheduled file desensitization tasks. Periodic tasks can be configured by single task, daily task, weekly task, monthly task, and annual task. You can start and stop scheduled tasks.

2 Conclusion

This research for the data centralized platform construction, and the relevant privacy protection technology into the study, put forward the privacy protection technology framework, and respectively from sensitive data automatic identification task, building data desensitization algorithms library, and desensitization tasks for the idea, implements the deformation of the sensitive data and shielding, replace, randomization, encryption, so as to make the sensitive data into fictitious data, to hide the real privacy information, provide the basis for data security use, at the same time, after desensitization data can keep the characteristics and distribution of original data, without changing the corresponding business logic system, implements the low cost, high efficiency, the use of the safety production of privacy.

References

[1] Yao A C C. How to Generate and Exchange Secrets[C]//27th Annual Symposium on Foundations of Computer Science (sfcs 1986). IEEE, 1986: 162-167.

[2] Rivest R L, Adleman L, Dertouzos M L. On Data Banks and Privacy Homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[3] Gentry C. Fully Homomorphic Encryption Using Ideal Lattices[C]//Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. 2009: 169-178.

[4] Tan Compositions, Lianfu Zhang. Journal of Software,31(7):30.

[5] Junxu Liu, Xiaofeng Meng. Survey on Privacy-Preserving Machine Learning[J]. Journal of Computer Research and Development, 2020, 57(2): 346-362.

[6] Dwork C, McSherry F, Nissim K, et al. Calibrating Noise to Sensitivity in Private Data Analysis[C]//Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2006: 265-284.

[7] Dwork C. Differential Privacy: A Survey of Results[C]//International Conference on Theory and Applications of Models of Computation. Springer, Berlin, Heidelberg, 2008: 1-19.

[8] Duchi J C, Jordan M I, Wainwright M J. Local Privacy and Statistical Minimax Rates[C]//2013 IEEE 54th Annual Symposium on Foundations of Computer Science. IEEE, 2013: 429-438.

[9] Agrawal R, Srikant R. Privacy-Preserving Data Mining[C]//Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. 2000: 439-450.

[10] Ye Q, Hu H, Meng X, et al. PrivKV: Key-value Data Collection with Local Differential Privacy[C]//2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 317-331.

[11] Kasiviswanathan S P, Lee H K, Nissim K, et al. What can We Learn Privately[J]. SIAM Journal on Computing, 2011, 40(3): 793-826.

[12].Chaudhuri K, Monteleoni C. Privacy-Preserving Logistic Regression[C]//NIPS. 2008,

8:289-296.

[13] Zhang J, Zhang Z, Xiao X, et al. Functional Mechanism: Regression Analysis Under Differential Privacy[J]. ArXiv Preprint ArXiv:1208.0219, 2012.

[14] Song S, Chaudhuri K, Sarwate A D. Stochastic Gradient Descent with Differentially Private Updates[C]//2013 IEEE Global Conference on Signal and Information Processing. IEEE, 2013: 245-248.

[15] Fredrikson M, Jha S, Ristenpart T. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 1322-1333.

[16] Hitaj B, Ateniese G, Perez-Cruz F. Deep Models under The GAN: Information Leakage from Collaborative Deep Learning[C]//Proceedings of The 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 603-618.

[17] Melis L, Song C, De Cristofaro E, et al. Exploiting Unintended Feature Leakage In Collaborative Learning[C]//2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 691-706.

[18] Zhu L, Han S. Deep Leakage from Gradients[M]//Federated learning. Springer, Cham, 2020: 17-31.

[19] Phan N H, Wang Y, Wu X, et al. Differential Privacy Preservation for Deep Auto-encoders: An Application of Human Behavior Prediction[C]//Thirtieth AAAI Conference on Artificial Intelligence. 2016.

[20] Phan N H, Wu X, Dou D. Preserving Differential Privacy in Convolutional Deep Belief Networks[J]. Machine Learning, 2017, 106(9): 1681-1704.

[21] Dwork C, Rothblum G N. Concentrated Differential Privacy[J]. ArXiv PreprintarXiv:1603.01887, 2016.

[22] Bun M, Steinke T. Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds[C]//Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2016: 635-658.

[23] Mironov I. Rényi Differential Privacy[C]//2017 IEEE 30th Computer Security Foundations Symposium (CSF). IEEE, 2017: 263-275.

[24] Abadi M, Chu A, Goodfellow I, et al. Deep Learning with Differential Privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 308-318.