Comprehensive Study of Differentially Private Deep Learning Mechanism

Mohammad Faheem
Department of Computer Science
Cambridge Institute of Technology
Bangalore, India

Sujith A
Department of Computer Science
Cambridge Institute of Technology
Bangalore, India

Sharika L
Department of Computer Science
Cambridge Institute of Technology
Bangalore, India

Suresh N
Department of Computer Science
Cambridge Institute of Technology
Bangalore, India

***Abstract* - Privacy is the prioritized concern in the current scenario of big data analytics. A breach in data is a potential threat which gives an impact on an individual's life without control on their own data. Many algorithms have been implemented to preserve privacy in the field of big data. Differential privacy mechanism is the current technology which is used by many companies such as Netflix, Snapchat, and Uber to protect the data. A filter in differential privacy collects and shares the overall aggregate information by maintaining individual's private data. The paper discusses how the trend is working on privacy and big data. This paper gives a comprehensive review in literature survey of recent papers dealing with differential privacy algorithms.**

Keywords - Differential privacy, Deep Learning, Artificial Neural Network and Big Data.

I. INTRODUCTION

Privacy is the factor which deals with the information related to an individual's private data. The domain of privacy is a subset of security in data which can be subjected to inappropriate use by an intruder. Use of any sensitive information in order to develop the business tool is the main cause for privacy loss in the recent past. This paper reviews the literature survey of differential privacy strategy that preserves privacy of data by adding noise to it. The approach is based on a probability that the amount of information acquired about an individual before and after analysis is the same according to the survey. Deep learning algorithms are highly flexible which can directly learn from raw data and increase their accuracy prediction [8]. Differential privacy is the key factor which involves the study of privacy in the upcoming trend of Big Data analytics [7]. Big data is the transforming technology which gives access to tools in various sectors [15]. Utilization of such tools can envision real outcomes by improving the quality of the algorithm. Big data gives prominent knowledge on differential privacy to automate future technologies in the field of machine learning and artificial intelligence.

II. BACKGROUND STUDY

A. *Deep Learning*

Deep learning is a part of machine learning where artificial neural [13] network algorithms are stimulated with the guide of the human brain that gain from enormous measure of data. Deep learning tackles convoluted issues in any event, when the use of a data set that is unstructured, diverse and between associated [13], [7].

B. *Differential privacy*

Definition 1: A mechanism f is a random function that outputs a random variable f (D) where it takes a dataset D as input [5].

Example, suppose D is a COVID dataset, then the output of the function is the number of patients in D and noise from the standard normal distribution.

Definition 2: The minimum number of sample changes that are required to change D into D′ is denoted by the distance of two datasets, d (D, D′) [5].

Example, if the difference between D and D′ is one, that is d (D, D′) = 1.

The differential privacy defines as neighbors datasets which 'differ by at most one'.

Definition 3: A (ε, δ)-differential privacy for two non-negative numbers δ and ε iff for all neighbors d (D, D′) = 1 is satisfied by a mechanism f [5].

$$P\,(f\,(D) \in S) \leq \delta + e^{\varepsilon}\,P\,(f\,(D') \in S) \;[14] \qquad (1)$$

When ε applied to a dataset and any one of its neighbors, the mechanism's output varies by more than a factor of e^{ε}. A smaller value of ε increases the standard for privacy protection and a lower value of Ɛ shows greater confidence. The protection is stronger when value of Ɛ and δ are smaller.

The Ɛ-differential privacy is simplified from (Ɛ, 0)-differential privacy. In (Ɛ, 0)-differential privacy, there is a small chance that some information is leaked when Ɛ > 0. The guarantee is not probabilistic When δ = 0. The Ɛ-differential privacy is stronger than (Ɛ, δ)-differential privacy. The number Ɛ is also called the privacy budget in differential privacy.

III. RESEARCH DIRECTION

From privacy protection for standard datasets to prepare datasets in profound learning, differential privacy [2], [5] wants to be progressed to coordinate numerous cycles of high dimensional information in profound learning. A few practices can be taken [2] envelop increasingly exact privacy spending assignments or unwinding strategies to increment its reasonableness. The security of differential privacy is [2] basically dependent on exacting scientific verification, but because of loss of intuitionist interpretability, it is frequently addressed [2], [7]. In latest years, the privacy of preparing tests are under danger. Under differential privacy it is trying to decide the specific danger of an attacker recreating or re-distinguishing information [2], [8]. The dangers that profound learning faces in [2] sensible applications are complex, they have the normal component, focusing on overfitting profound learning. One of the significant explanations behind privacy spillage in AI models are overfitting. It is a key issue in AI that restricts the speculation capacity and prediction precision of the model [2], [7]. There is evidence that enormous informational indexes in differential privacy can even prevent overfitting to lessen prediction blunders [2].

IV. RELATED WORK

A lot of recent active research has been done on privacy preserving analytics using differential privacy.

1) *Jingwen Zhao, "Differential Privacy Preservation into Deep Learning"* [2]. Differential insurance is commonly seen in a large portion of customary circumstances for its numerical affirmation. Regardless, it's questionable to work reasonably in the profound learning structure [2]. It presents the security attacks facing the profound taking in model and presents them from three edges, they are participation induction, model extricating, and preparing information extraction [2]. Assessing some basic speculation about differential protection [2] and its ideas in profound learning circumstances [2]. In order to look at the current works and that combine differential protection and profound learning [2], it is ordered by the layers of components in differential security as [2] input layer, hidden layer, and output layer.

2) *Reza Skokri, "Privacy Preserving Deep Learning"* [9]. Utilization of a viable framework that enables various individuals to commonly become familiar with a precise [9] neural-arrange model for a given objective by not sharing their data datasets. Enhancement calculations utilized in present profound adapting to be specific, stochastic gradient descent, [9] can be parallelized and executed nonconcurrently. This framework leaves individuals to adapt autonomously all be datasets and specifically send little subsets of the framework key limits during the preparation [9]. It gives an engaging point in the security trade off space. Individuals shield the security on their particular information while as yet profiting by relevant parts and therefore increasing the learning precision past which is reachable exclusively on the information sources [9].

3) *Martin Abadi, "Deep Learning with Differential Privacy"* [10]. It joins the [10] cutting edge of AI strategies with higher protection saving framework, preparing neural system frameworks inside an unobtrusive security spending plan [10]. Remunerating the design like non-arched objectives, a few layers and a few hundreds to a colossal number of boundaries [10]. Latest Algorithms for understanding and refined examination of security prize within the structure of [10] differential protection. The usage shows that train [10] profound neural system frameworks with non-arched goals, under an unassuming security, financial plan and at a sensible expense in programming multifaceted nature, training efficiency and model quality [10].

4) *Nhathai Phan, "Differential Privacy Preservation in Deep Learning"*. In this paper, it focuses around building up a novel component which is an instrument to store differential insurance in profound neural system systems[11], with the ultimate objective of protection spending use is totally free of the amount of preparing steps [11]. It can adaptively implant noise into highlights endless supply of every one of the yield and it can be pasted in a wide scope of [11] profound neural system frameworks. For achieving, a way to deal with disturbing relative changes of neurons is found and misfortune capacities utilized in profound neural systems [11]. What's more, the system intentionally remembers more commotion for the features which are "less critical" to the model yield or the reverse way around [11].

5) *Yuichi Sei, "Privacy Preserving Publication of Deep Neural Networks"* [12]. Here, it adjusts ε-differential security for AI, it suggests three systems [12] for making protection saved DNNs reliant on the changed [12] ε - differential protection which foretell delicate attribute values, for instance, the compensation and maladies of people dependent on characteristic incentive considering the reality. DNNs are made from fragile property estimations [12], we can't provide them transparently without the express assent of the individuals whose data are used for the DNNs [12]. In recent years, ε - differential security [12] has been created as a genuine protection metric. The proposed approaches are tentatively assessed utilizing a genuine informational index, and it shows that the methodologies can secure individual personal attributes while keeping up the precision of the DNNs [12].

Paper	Technique/ Mechanism	Advantages	Challenges	Research Direction
[2] Jingwe Zhao, “Differential Privacy Preservation into Deep Learning”.	• Input layer. • Hidden layer. • Output layer.	• Adding noise to gradient Dataset.	• Determining the exact risk of an attacker reconstructing data.	• Robust security assurance system is relied upon to ensure a wide range of profound learning task [2].
[9] Reza Shokri, Vitaly Shmatikov, “Privacy Preserving Deep Learning".	• Distributed stochastic gradient descent (DSGD). • [9] Selective Stochastic Gradient Descent (SSGD). • Sparse vector mechanism.	• Accuracy of DSSGD is better [9].	• Estimating the real sensitivity of SGD [9].	• Expect that worldwide affectability [9] assessments can be altogether diminished. • Oblivious parameter server.
[10] Martín Abadi, “Deep Learning with Differential Privacy”.	• Gaussian mechanism. • Additive-noise mechanism. • Differentially private stochastic gradient descent.	• Able to adjust numerous other traditional and later first-order enhancement [10] techniques.	• For each step bounding the value αMt (λ) [10].	• Considering other classes in deep networks [10]. • Applying this techniques to LSTMs. • Additional improvements in accuracy.
[11] Nhathai Phan, “Differential Privacy Preservation in Deep Learning”.	• Adaptive Laplace Mechanism.	• Has an ability to redistribute the noise insertion. • Completely independent of the quantity of training epochs.	• Conducts both sensitivity examination and commotion inclusion on profound neural systems [11].	• Reallocation of ε1, ε2, and ε3 could further improve the utility.
[12] Yuichi Sei, “Privacy-Preserving of Deep Neural Networks”.	• 3 approaches are Anonymizing First, Learning First, Anonymized Learning.	• High estimation accuracy. • Ɛ-differential privacy is the encouraged protection metric [12].	• When ε is less, then accuracy [12] of Anonymizing First and Anonymized Learning are higher.	• Applying to other ML Algorithms [12].

V. CONCLUSION

Differential security [2] gives a superior protection ensure and has been acknowledged the protection model for as far back as years [2], [6]. At present, the investigation of differential security [1] in the field of profound learning is still in its start. Existing differentially private mechanisms or components are executed utilizing global differential privacy.

Picking the fitting protection boundary epsilon [6] is consistently the key in this procedure as there is an exchange off between information security and information utility. Through examinations we attempted to characterize diverse protection levels and ascertain the information utility [6] by the reference from information owners. The corresponding algorithmic executions are generally direct and straightforward in the interactive scenario and combined with procedures and techniques [6].

REFERENCES

[1] L. Deng and D. Yu, ‘‘Deep learning: Methods and applications,’’ Found. Trends Signal Process, vol. 7, nos. 3–4, pp. 197–387, Jun. 2014.

[2] Jingwen Zhao, Yunfang Chen, Wei Zhang. "Differential Privacy Preservation in Deep Learning: Challenges, Opportunities and Solutions", IEEE Access, 2019

[3] Cynthia Dwork, Aaron Roth “The Algorithmic Foundations of Differential Privacy” 2014

[4] Zhanglong Ji, Zachary C. Lipton, Charles Elkan, “Differential Privacy and Machine Learning

[5] B. Perozzi, R. Al-Rfou, and S. Skiena, ‘‘DeepWalk: Online learning of social representations,’’ in Proc. Int. Conf. Knowl. Discovery Data Mining (KDD), 2014, pp

[6] Yennun Huang, "Overview of Taiwan information security center and its research on privacy"

[7] Manasi Gyanchandani and Nilay Khare, “Differential privacy: its technological prespective using big data”, 2018

[8] Xue-Wen Chen and Xiaotong Lin, “Big Data Deep Learning: Challenges and Perspectives”,vol. 2,Jan. 2014

[9] Reza Shokri, Vitaly Shmatikov. "Privacy-Preserving Deep Learning", Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15, 2015

[10] Martin Abadi, Andy Chu, Ian Goodfellow, “Deep Learning with Differential Privacy” 2016

[11] Nhathai Phan, Xintao Wu, Han Hu “Differential Privacy Preservation in Deep Learning”

[12] Yuichi Sei, Hiroshi Okumura, Akihiko Ohsuga. "PrivacyPreserving Publication of Deep Neural Networks", 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016

[13] Patrik Eliardsson, Peter Stenumgaard. "Artificial Intelligence for Automatic Classification of Unintentional Electromagnetic Interference in Air Traffic Control Communications", 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, 2019

[14] J. Andrew, J. Karthikeyan, Jeffy Jebastin. "Privacy Preserving Big Data Publication On Cloud Using Mondrian Anonymization Techniques and Deep Neural Networks", 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019

[15] Parameshachari B D et. al “Epileptic Seizure Detection Using Machine Learning,” 1st International Conference on Emerging Trends in Engineering, Innovative Science and Management (ICETEISM-2019), 2019.