Data & Knowledge Engineering 79–80 (2012) 40–61

Contents lists available at SciVerse ScienceDirect

Data & Knowledge Engineering

journal homepage: www.elsevier.com/locate/datak

Privacy-preserving back-propagation and extreme learning machine algorithms

Saeed Samet [a,*], Ali Miri [b]

[a] eHealth Research Unit, Faculty of Medicine, Memorial University of Newfoundland, 300 Prince Philip Drive, St. John's, NL, Canada A1B3V6
[b] Department of Computer Science, Ryerson University, 245 Church Street Toronto, ON, Canada M5B2K3

ARTICLE INFO

Article history:
Received 15 November 2010
Received in revised form 19 June 2012
Accepted 24 June 2012
Available online 30 June 2012

Keywords:
Privacy preserving data mining
Neural networks
Machine learning
Back-propagation
Extreme learning machine
Distributed data structures

ABSTRACT

Neural network systems are highly capable of deriving knowledge from complex data, and they are used to extract patterns and trends which are otherwise hidden in many applications. Preserving the privacy of sensitive data and individuals' information is a major challenge in many of these applications. One of the most popular algorithms in neural network learning systems is the *back-propagation* (BP) algorithm, which is designed for single-layer and multi-layer models and can be applied to continuous data and differentiable activation functions. Another recently introduced learning technique is the *extreme learning machine* (ELM) algorithm. Although it works only on single-layer models, ELM can out-perform the BP algorithm by reducing the communication required between parties in the learning phase. In this paper, we present new privacy-preserving protocols for both the BP and ELM algorithms when data is horizontally and vertically partitioned among several parties. These new protocols, which preserve the privacy of both the input data and the constructed learning model, can be applied to online incoming records and/or batch learning. Furthermore, the final model is securely shared among all parties, who can use it jointly to predict the corresponding output for their target data.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

The design of privacy-preserving protocols has become a very important and challenging issue in data mining and machine learning methods ever since they have been applied to areas requiring data privacy, particularly distributed and collaborative learning [1]. Several protocols are proposed for each method, including decision trees [2–4], association rule mining [5–8], clustering [9–13], secure join [14], k-anonymity [15], Random Forests classification [16], and support vector machines [17,18]. Some techniques, such as [2], use a cryptographic approach to preserve the privacy of sensitive data, while others like [3] employ an additive perturbation approach. Adaptable perturbation models [19] and multiplicative perturbation [20] have also been used in some privacy-preserving techniques, and random data projection, in which data is projected into a random subspace [21], is another approach. In Ref. [22] a general and flexible framework has been proposed by mapping the original dataset into a new anonymized dataset, in which the perturbed data will match the features of the source data.

Neural networks are widely used for learning systems and knowledge representation, and they are applied in different fields, including medical diagnosis, pattern recognition, homeland security, fraud detection and other knowledge discovery systems.

Healthcare systems are among the most demanding areas, due to the critical need to maintain the privacy of individuals' health information. Different privacy laws are enforced in various countries, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the Freedom of Information and Protection of Privacy Act (FIPPA) in Canada, and the Data Protection Directive in Europe. Therefore, protocols used in health applications must assure the client that sensitive and private information will not be revealed to un-authorized parties at any stage of data processing and knowledge discovery.

[*] Corresponding author. Tel.: +1 709 777 8607; fax: +1 709 777 8838.
E-mail addresses: ssamet@mun.ca (S. Samet), samiri@scs.ryerson.ca (A. Miri).

0169-023X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.datak.2012.06.001

Though health clinics, physicians and hospitals have great volumes of patients' health data, much of which could be helpful to researchers, privacy legislation prevents the data from simply being released.

In another scenario, consider the situation when two or more nations wish to combat fraud and money laundering in their respective countries through collaborative processes that require using each other's databases. Access to such databases is often restricted and governed by diverse privacy laws in different jurisdictions. Thus, secure protocols that can run jointly on private information to obtain aggregate knowledge without revealing raw or sensitive data are essential. Neural network learning systems are one of the methods that can be used to manage such issues.

The *back-propagation* (BP) algorithm is a commonly used method in neural network learning systems. It was designed for both single and multi-layer models, and can be applied to continuous data and differentiable activation functions. Another recently introduced method for creating neural network learning systems is the *extreme learning machine* (ELM) [23]. This method is limited to single-layer models, but it is faster than the BP method in neural network learning construction. This improved efficiency can be important to overall performance when the algorithm is applied to a distributed environment involving two or more parties creating a neural network that uses their data. In our work, we consider both of these methods to address single and multi-layer models, and users can choose whichever best suits their model structure and performance requirements.

This paper proposes two new privacy-preserving protocols for BP and ELM algorithms. In both cases, we consider environments in which the training data is horizontally or vertically distributed among several parties, and the final distributed model is used securely to predict the correct output for the target data. Note that the network can have more than one output, and the solutions provided here could also be applied to multiple output nodes. However, for simplicity, and to maintain generality, we consider only single outputs in the proposed protocols. The protocols can be applied to online data (i.e. single record and/or batch learning).

A potential scenario for utilizing our proposed protocols could be the following: A data holder wants to use the trained network for scoring previously unseen data. They can securely distribute the data horizontally or vertically among the parties, who would then send the final output shares back to be aggregated and to determine the final weight vector values.

For these protocols, secure building blocks should be used to preserve the privacy of the parties involved (e.g. secure addition and multiplication and *secure dot product* (SDP)). Some of these secure building blocks can be found in the literature. For example, in Ref. [24] building blocks such as secure sum and secure dot product are introduced as a toolkit. In Ref. [25] a cryptographic privacy-preserving protocol is presented for addition using average computation. Another sub-protocol for secure dot product, using a cryptographic approach, is proposed in Ref. [26]. We chose to use this secure dot building block in our paper, due to its level of security and efficiency. However, for secure addition and multiplication we used our own building blocks, in order to provide secure distribution of the final results to all parties; each party receives a portion of the final results and does not know or learn about others' shares. The advantage of these building blocks is that they are secure against collusion attacks, and can be used over public channels. In our protocols, we assume that the parties are only semi-honest, meaning that they correctly follow the steps of the protocols, but might use the intermediate or final outputs to learn about others' private data. It has been shown in Ref. [27] that zero-knowledge proofs can be applied to force malicious parties to properly follow a protocol and provide correct information.

Our main objectives in this work are:

- To introduce privacy-preserving protocols for both back-propagation and extreme learning machine, giving users the option of selecting whichever best meets their requirements. The activation function used to illustrate the use of the proposed secure building blocks in this paper is a *sigmoid* function. A brief discussion of how this can be extended to other activation functions is presented later in the paper.
- To show our protocols can address both vertical and horizontal data distribution among the parties.
- To show that the final results using our protocols will be securely distributed among the parties. This reduces opportunities to access other parties' private inputs using intermediate and final outputs. The shares could also be sent to a third party to use as test data. For example, health researchers could receive the final model jointly created by the clinics and hospitals to perform their research, without having access to any individual's private data.
- To show the proposed protocols will not only preserve privacy, but will also be resistant to collusion attacks, and can be run over public channels.
- To show that using different datasets, both non-privacy-preserving and privacy-preserving protocols will be compared in terms of accuracy of results and time performance.

The content of this paper is as follows: Related work is reviewed in Section 2. In Section 3, neural networks, the BP algorithm and the ELM method are explained. New protocols for horizontally and vertically partitioned data for the BP algorithm are proposed in Section 4, and new protocols for a privacy-preserving ELM with the same data configurations are presented in Section 5, along with security and complexity analysis. Conclusions and future work are discussed in Section 6.

2. Related work

In this section, we review the existing work on privacy-preserving protocols for different neural networks, and highlight the major differences in our work in terms of the number of parties involved, initial assumptions, and distribution of the intermediate and final results. Barni et al. [28] presented an asymmetric protocol for privacy-preserving neural networks. In this protocol, two parties are involved: a client or data owner who wants their data processed, and a server or neural network owner who is able to process data. Both parties wish to keep their information private. The protocol assumes that the learning model already exists,

Download English Version:

https://daneshyari.com/en/article/378835

Download Persian Version:

https://daneshyari.com/article/378835

Daneshyari.com