On the Soundness and Security of Privacy-Preserving SVM for Outsourcing Data Classification

ABSTRACT

Support vector machine (SVM) is a widely-used and power tool for data classification, and it has been applied in scientific and engineering problems, such as text classification, time series prediction, MAC protocol identification, fault diagnosis. Generally, SVM classification consists of two stages: training stage and testing stage. The training stage uses labeled samples to gain the classification parameters. Then, testing stage utilizes the classification parameters to predict the class label for any unlabeled sample.

EXISTING SYSTEM

We analyzed the privacy preserving SVM classification scheme recently and pointed out that their core protocol (i.e., a secure protocol to determine encrypted numbers' sign) suffers from soundness problem or security leakage.

Disadvantages

- It suffers from soundness problem or security leakage.
- SVM classifier are his private data and the server has cost much time, money and other resources to gain them.

PROPOSED SYSTEM

We proposed a new approach to correctly and securely determine encrypted numbers' sign, which can be utilized to support privacy-preserving SVM classification. Theoretical analysis shows our proposed protocol can fix all the flaws. Additionally, evaluation results indicate our scheme can achieve higher efficiency than the existing one.

Advantages

- It avoids soundness problem or security leakage.
- It can avoid the overflow error.

SOFTWARE REQUIREMENTS

Front-end : JSP

Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB