中国科学院软件研究所学术年会’2019
暨计算机科学国家重点实验室开放周

学术论文

面向医疗信息系统隐私保护的风险自适应访问控制
Privacy-Aware Risk-Adaptive Access Control in Health Information Systems using Topic Models

张文夕, 李昊(lihao@iscas.ac.cn), 张敏, 吕志泉

The ACM Symposium on Access Control Models and Technologies (SACMAT 2018)

研究背景

在许多信息系统中，为了不影响业务往往都未严格遵循“Need to know”原则，而是授予用户过量甚至全部的权限。该问题在医疗信息系统中更为普遍。主要原因包括两方面：

（1）安全管理员缺乏足够的领域知识进行授权管理；

（2）数据规模大，且增长迅速提高了人工授权管理的难度。

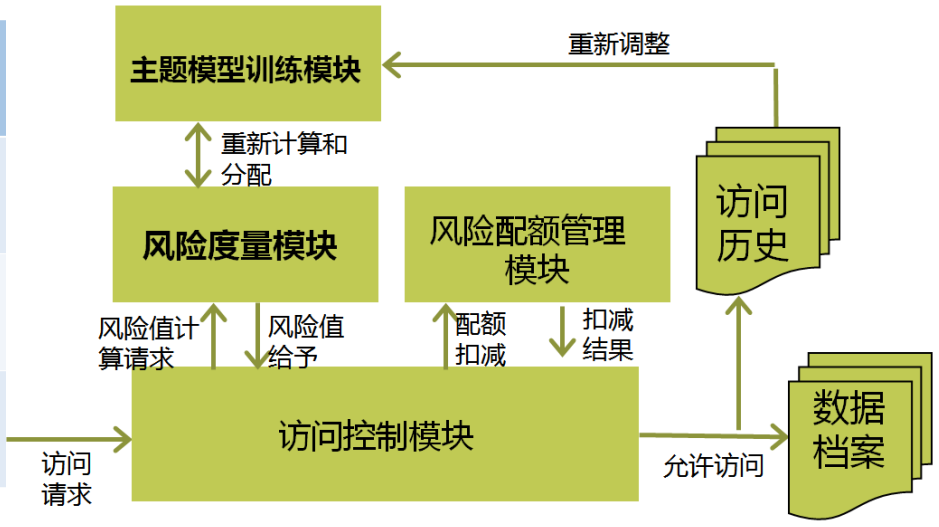
因此，亟需自动化、自适应的授权管理技术来解决此类授权管理困难问题。

主要方法

基于LDA算法构建所有医生的访问行为画像

医生 doctor k 的访问记录	一篇文章 W
打上标签的一条医疗数据	一个单词
潜在的访问数据的主题	文章的主题
doctor k 在这些主题上的偏好	文章 W 在不同主题上的权重

度量医生行为与基准之间的异常作为风险值实施访问控制



实验结果

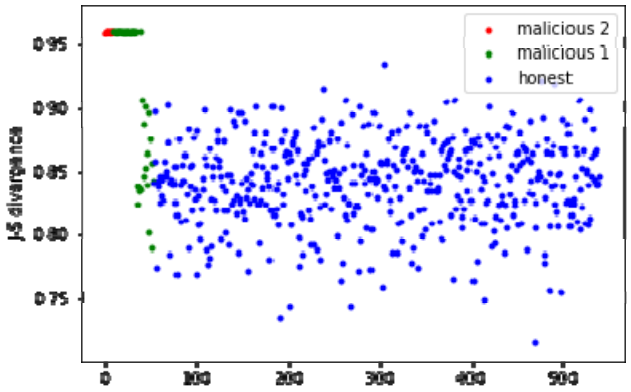


图1 所有医生的风险值分布

表1 异常医生的识别效果

Measure	Doctor Group	Top k results				
		Top 10	Top 20	Top 30	Top 40	Top 50
P	Both groups	1.00	1.00	1.00	0.90	0.74
	Malicious	0.70	0.65	0.73	0.65	0.54
	Concealed	0.30	0.30	0.23	0.25	0.20
R	Both groups	0.19	0.37	0.56	0.67	0.70
	Malicious	0.16	0.30	0.50	0.59	0.61
	Concealed	0.30	0.60	0.70	1.00	1.00
F1	Both groups	0.31	0.54	0.71	0.77	0.73
	Malicious	0.26	0.41	0.59	0.62	0.57
	Concealed	0.30	0.40	0.35	0.40	0.33