****

|  |
| --- |
| **دانشگاه شهید بهشتی****دانشکده مهندسی و علوم کامپیوتر****اطلاعیه دفاع** |

|  |  |
| --- | --- |
| **نام استاد راهنما:**جناب دکتر فریدون شمس علیئی | **نام دانشجو:**رضا فتوحی سلاله |
| **مقطع:**دکتری | **گرایش**: نرم افزار | **رشته**:مهندسی کامپیوتر |
| **تاریخ:**19/10/1400 | **نوع دفاع:*** **دفاع پروپوزال■**
* **دفاع پایان نامه □**
* **دفاع رساله دکترا□**
 |
| **ساعت:**11 الی 13 |
| **مکان:**طبقه دوم دانشکده، اتاق شماره 200 |
| **عنوان:**ارائه مدلی سبک‌وزن جهت حفظ حریم خصوصی داده‌های سازمان هوشمند |
| **داوران داخلی:**جناب دکتر علیرضا شاملیجناب دکتر اسلام ناظمی | **داوران خارجی:**جناب دکتر مرتضی امینیجناب دکتر مهدی آبادی |
| **چکیده:**افزایش روزبه‌روز حجم داده‌ها و تغییرات سریع محیطی، نیازمند تجزیه، تحلیل و کسب بینش مناسب از داده‌ها است. امروزه سازمان‌های پیشرو از فناوری‌های جدیدی برای ارتقاء دانش سازمانی خود استفاده می‌کنند. این فناوری‌ها به رهبران سازمان‌ها کمک می‌کند تا به‌راحتی به تحلیل عمیق داده‌ها بپردازند. مهم‌ترین دلایل نیاز به فناوری‌های جدید، وجود کلان‌داده‌ها است که دارای ویژگی‌های حجم زیاد، تنوع زیاد و شدت تولید بالا هستند. در واقع امروزه داده‌ها به منبع حیات سازمان‌ها تبدیل شده‌اند اما به‌صورت خام برای تضمین موفقیت کسب‌وکارها کافی نیستند. اگر سازمان‌ها از فناوری‌های جدید استفاده نکنند محکوم به شکست خواهند بود. از سوی دیگر در سازمان‌های امروزی علاوه بر تبدیل داده‌ها به بینش و بینش به عمل، نیازمند مدلی هستند تا حریم خصوصی داده‌ها را حفظ کنند؛ بنابراین حفظ حریم خصوصی داده‌ها یکی از دغدغه‌های کلیدی در سازمان‌های امروزی است. حریم خصوصی نه‌تنها محدود به داده‌های مربوط به دارایی‌های سازمان نیست بلکه شامل داده‌های کاربران، تیم‌ها، گروه‌ها، مجموعه ذی‌نفعان، داده‌های مربوط به سازمان من‌جمله داده‌های اینترنت اشیاء سازمان‌ها است و در صورت نقض حریم خصوصی ممکن است کل هویت سازمان زیر سؤال برود. از طرفی چون در رویکردهای معمولی داده‌ها یکجا بر روی سرویس‌دهنده مرکزی جمع‌آوری می‌شوند تا مدل‌هاییادگیری ماشین بر روی آنها آموزش داده شود، همین کار نقض حریم خصوصی داده‌ها را در پی خواهد داشت. باتوجه‌به به‌کارگیری فناوری‌های پیشرفته در سازمان‌های امروزی و افزایش روزبه‌روز داد‌ه‌ها و گرایش به سمت کلان‌داده، بحث سازمان هوشمند مطرح می‌شود. ازاین‌رو؛ هدف این پیشنهاد پژوهشی، ارائه مدلی برای حفظ حریم خصوصی داده‌های سازمان هوشمند است. این کار با استفاده از یادگیری مشارکتی، طرح شناسایی مدل‌های محلیصادق، شبکه گمنامی و حریم خصوصی تفاضلی در قالب دو فاز اصلی انجام می‌شود تا داده‌های سازمان در مقابل سه نوع حمله مسمومیت داده‌ها، استنتاج داده‌ها و نشت بصیرت ایمن باشد؛ بدین صورت که در فاز اول از یادگیری مشارکتی، در لایه ابری مدل اولیه با داده‌های محدودی که در اختیار دارد ساخته شده؛ به دنبال آن توسط لایه میان‌افزار به‌صورت ناشناس در اختیار دستگاه‌های محلی قرار می‌گیرد تا توسط نفوذگران قابل ردیابی نباشند. در لایه دستگاه آموزش مدل‌های محلی با استفاده از داده‌های سازمان‌های کوچک و متوسط انجام می‌شود. در ادامه بر روی متغیرهای مدل آموزش‌دیده شده، روش حریم خصوصی تفاضلی اعمال می‌شود. بدین ترتیب با تزریق نویز در متغیرها آشفتگی ایجاد می‌شود. بعد متغیرها از طریق شبکه گمنامی به لایه ابری ارسال می‌شود تا متغیرها در یک محیط باز استنتاج نشوند. در فاز دوم و در لایه ابری با استفاده از لایه میان‌افزار مدل‌های محلی به‌روزرسانی شده دریافت شده و از حالت نویز خارج می‌شوند تا با استفاده از طرحCMDشناسایی مدل‌های محلی صادق انجام می‌شود. نهایتا تجمیع این مدل‌های صادق به‌منظور به‌روزرسانی مدل سراسری نهایی انجام می‌شود. قبل از ارسال مدل سراسری نهایی به لایه دستگاه، با استفاده از حریم خصوصی تفاضلی با تزریق نویز آشفتگی ایجاد خواهد شد سپس با استفاده از شبکه گمنامی و به‌صورت ناشناس به سمت لایه دستگاه برگردانده می‌شود تا سازمان‌ها با استفاده از این مدل بتوانند پیش‌بینی‌هایی را انجام دهند. این فرایند تکرار می‌شود تا مدل همگرا شود. بدین ترتیب مدلی مناسب برای سازمان هوشمند استخراج می‌شود که علاوه بر اینکه نگرانی‌های حریم خصوصی را برطرف می‌کند دارای ویژگی‌های سبک‌وزنی می‌باشد. ازاین‌جهت که میزان ارتباطات، هزینه محاسبات و میزان سخت‌افزار موردنیاز برای اجرای این مدل به نسبت به حالتی که از این مدل استفاده نمی‌شود، کمتر است. مدل پیشنهادی در محیط پایتون پیاده‌سازی می‌شود و عملکرد سامانه از لحاظ کارایی و امنیت در قالب سناریوها و مجموعه‌های داده مختلف با مدل‌های مرتبط قبلی مقایسه و ارزیابی خواهد شد.**کلمات کلیدی:** سازمان هوشمند، حفظ حریم خصوصی، کلان‌داده، یادگیری مشارکتی، حریم خصوصی تفاضلی |