# نقش داده کاوی در سیستم‌های تشخیص نفوذ

مؤلفان:

هادی بارانی برواتی

اطهره حاجی زاده مطلق

| | | |
|---|---|---|
| سرشناسه | : | بارانی برواتی، هادی، ۱۳۶۰- |
| عنوان و نام پدیدآور | : | نقش داده‌کاوی در سیستم‌های تشخیص نفوذ/ مولفان هادی بارانی‌برواتی، اطهره حاجی‌زاده‌مطلق. |
| مشخصات نشر | : | تهران: انتشارات راه دکتری: سنجش و دانش، ۱۳۹۸. |
| مشخصات ظاهری | : | ۹۸ص. |
| شابک | : | 978-622-241-305-7 |
| وضعیت فهرست نویسی | : | فیپا |
| موضوع | : | سامانه‌های تشخیص نفوذ (ایمن‌سازی کامپیوتر) -- ایران -- نمونه‌پژوهی |
| موضوع | : | Intrusion detection systems (Computer security) -- Iran -- Case studies |
| موضوع | : | شبکه‌های کامپیوتری -- ایران -- تدابیر ایمنی -- نمونه‌پژوهی |
| موضوع | : | Computer networks -- Iran -- Security measures -- Case studies |
| موضوع | : | داده‌کاوی -- نمونه‌پژوهی |
| موضوع | : | Data mining -- Case studies |
| شناسه افزوده | : | حاجی‌زاده مطلق، اطهره، ۱۳۶۲- |
| رده بندی کنگره | : | ۵۹/۸۰۵TK |
| رده بندی دیویی | : | ۸/۰۰۵ |
| شماره کتابشناسی ملی | : | ۵۸۸۸۴۶۷ |





سنجش و دانش

www.sanjesh.ir

عنوان: **نقش داده‌کاوی در سیستم‌های تشخیص نفوذ**

مولفان: هادی بارانی‌برواتی، اطهره حاجی‌زاده‌مطلق

ناشر: انتشارات سنجش و دانش

نوبت چاپ: اول ۱۳۹۸

تیراژ: ، ۵۰۰ نسخه

بهاء : ۳۰۰۰۰۰ ریال

**مرکز پخش : تهران ، خیابان انقلاب ، خیابان دانشگاه ، پلاک ۱۲۶**

**تلفن تماس: ۶۱۲۶-۰۲۱**

## پیشگفتار

در این کتاب یک رویکرد برخط برای مدیریت هشدارهای تولیدشده توسط سیستم‌های تشخیص نفوذ پیشنهاد می‌شود. همزمان با پیشرفت و گسترش روزافزون اینترنت و کاربردهای مبتنی بر آن، بر تعداد و پیچیدگی حملات سایبری نیز افزوده می‌شود. بنابراین، استفاده از ابزارهای مختلف امنیتی برای حفاظت از سیستم‌ها و شبکه‌های کامپیوتری به یک نیاز حیاتی تبدیل شده است. در میان این ابزارها، سیستم‌های تشخیص نفوذ از مؤلفه‌های ضروری دفاع در عمق می‌باشند. یکی از بزرگ‌ترین مشکلات سیستم‌های تشخیص نفوذ، تولید سیلی از هشدارهاست؛ هشدارهایی که اغلب آن‌ها هشدارهای غلط، تکراری، و بی‌اهمیت هستند. در میان رویکردهای مختلف برای حل این مشکل، روش‌های داده‌کاوی از سوی بسیاری از محققان پیشنهاد شده است. با این حال، بسیاری از روش‌های قبلی نتوانسته‌اند مشکلات را به طور کامل حل کنند. به علاوه، اغلب روش‌های پیشین، از مشکلاتی نظیر وابستگی به نیروی انسانی و برون‌خط بودن رنج می‌برند. رویکرد پیشنهادی، قابلیت دریافت هشدارهایی از چندین سیستم تشخیص نفوذ را داراست. ارزیابی‌های انجام شده نشان می‌دهد که راهکار ارائه شده با کاهش حجم هشدارها به میزان ۹۴.۳۲٪، می‌تواند تأثیر بسزایی در مدیریت هشدارها داشته باشد. این رهیافت، به دلیل استفاده از رویکرد تجمعی داده‌کاوی و به‌کارگیری الگوریتم‌های بهینه، می‌تواند متخصص امنیت شبکه را به صورت برخط از وضعیت شبکه‌ی تحت نظارت، آگاه سازد.

## فهرست مطالب

صفحه

عنوان