

## عنوان مقاله:

بهبود تشخیص وبگاه های جعل شده با استفاده از طبقه بندی کننده شبکه عصبی مصنوعی چند لایه با الگوریتم بهینه سازی شیرمورچه

## محل انتشار:

دوفصلنامه فناوری اطلاعات و ارتباطات ایران، دوره 15، شماره 55 (سال: 1402)

تعداد صفحات اصل مقاله: 12

## نویسنده:

مهشید صادقی باجگیران - موسسه آموزش عالی اشراق

## خلاصه مقاله:

در حملات فیشینگ یک وبگاه جعلی از روی وبگاه اصلی جعل میگردد که ظاهر بسیار شبیه به وبگاه اصلی دارد. فیشر یا سارق آنلاین برای هدایت کاربران به این وبگاهها، معمولاً لینکهای جعلی را در ایمیل قرار داده و برای قربانیان خود ارسال نموده و با روشهای مهندسی اجتماعی سعی در فریب کاربران و مجاب نمودن آنها برای کلیک روی لینکهای جعلی دارد. حملات فیشینگ زیان مالی قابل توجهی دارند و بیشتر روی بانکها و درگاههای مالی متمرکز هستند. روشهای یادگیری ماشین یک روش موثر برای تشخیص حملات فیشینگ است اما این مشروط به انتخاب بهینه ویژگی است. انتخاب ویژگی باعث میشود فقط ویژگیهای مهم به عنوان ورودی یادگیری در نظر گرفته شوند و خطای تشخیص حملات فیشینگ کاهش داده شود. در روش پیشنهادی برای کاهش دادن خطای تشخیص حملات فیشینگ یک طبقه بندی کننده شبکه عصبی مصنوعی چند لایه استفاده شده که فاز انتخاب ویژگی آن با الگوریتم بهینه سازی شیرمورچه انجام میشود. ارزیابی و آزمایشها روی مجموعه داده Rami که مرتبط با فیشینگ است نشان میدهد روش پیشنهادی دارای دقتی در حدود ۹۸.۵۳% است و نسبت به شبکه عصبی مصنوعی چند لایه خطای کمتری دارد. روش پیشنهادی در تشخیص حملات فیشینگ از روشهای یادگیری RF، C۴.۵، NB، SVM، BPNN و kNN با سازوکار انتخاب ویژگی توسط الگوریتم PSO دقت بیشتری دارد.

## کلمات کلیدی:

حملات فیشینگ، انتخاب ویژگی، الگوریتم بهینه سازی شیر مورچه، صفحات جعلی، لینکهای جعلی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1858777>

