پایان‌نامه‌ی کارشناسی ارشد: حمید براتی گلشیخی، ۱۳۹۸

تشخیص حملات سرقت اینترنتی مبتنی بر شبکه عصبی مصنوعی و الگوریتم ژنتیک

امروزه حجم زیادی از تبادلات مالی از طریق شبکه جهانی اینترنت انجام می¬شود و کاربران مختلفی از آن استفاده می¬نمایند. امنیت شبکه اینترنت برای فعالیتهای مالی یک چالش بزرگ و اساسی محسوب می¬شود. سرقت اطلاعات یا فیشینگ توسط سایتهای جعلی یکی از چالش¬های اصلی شبکه جهانی اینترنت در نظر گرفته می¬شود که می¬تواند زیان فراوانی را به کاربران و بخش¬های مالی وارد نماید. در سرقت اطلاعات آنلاین یک سایت جعلی تلاش می¬کند تا اعتماد کاربران را به خود جلب نموده و اطلاعات با ارزش آنها نظیر نام کاربری و کمله عبور را مورد سرقت قرار دهد. حملات سرقت اینترنتی می¬تواند شماره حساب بانکی و کلمه عبور آنها را نیز مورد سرقت قرار دهد و از این نظر آسیب¬رسانی این حملات به کاربران قابل توجه است. حملات فیشینگ دارای الگوی¬های پنهانی می¬باشند که تشخیص الگوهای مورد نظر می¬تواند آثار این حملات را کاهش دهد. روش¬های جدیدی برای تشخیص حملات فیشینگ بر اساس تکنیک-های داده¬کاوی و یادگیری ماشین ارایه می¬شود که می¬تواند با دقت مناسبی این حملات را تشخیص دهد. در این پژوهش برای شناسایی حملات فیشینگ یک روش جدید مبتنی بر شبکه عصبی مصنوعی و الگوریتم ژنتیک استفاده شده است تا ویژگی¬های مهم شبکه عصبی نظیر اوزان و آستانه¬ها به صورت بهینه¬تری انتخاب شوند و دقت طبقه¬بندی حملات فیشینگ افزایش یابد. در روش پیشنهادی ابتدا با تشکیل یک راه حل اولیه ساختار کرومزومهای الگوریتم ژنتیک بدست آمده و پس از محاسبه بهینگی و با تشکیل حالتها در شبکه عصبی میتوان میزان حمله یا جعل اطلاعات را بهبود بخشید.نتایج آزمایشات و شبیه¬سازی ما بر روی مجموعه داده حملات فیشنگ موجود در پایگاه داده UCI نشان می¬دهد که روش پیشنهادی به ازای جمعیتی به اندازه 30 و تعداد تکرار 100 به طور متوسط دارای دقت، حساسیت و تشخیص به ترتیب در حدود 92.74%، 92.28% و 88.63% در تشخیص حملات فیشینگ می¬باشد.. افزایش دقت و حساسیت روش پیشنهادی را می¬توان به دلایلی مانند انتخاب بهینه¬تر اوزان و آستانه¬های شبکه عصبی مصنوعی توسط الگوریتم ژنتیک در نظر گرفت.

کلیدواژه‌ها: سرقت اطلاعات، فیشینگ، حملات آنلاین، شبکه عصبی مصنوعی، الگوریتم ژنتیک

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۱۰۹۷۲۰۰۶
تاریخ دفاع: ۱۳۹۸/۰۶/۱۷
رشته‌ی تحصیلی: مهندسی فناوری اطلاعات - شبکه‌های کامپیوتری
دانشکده: فنی و مهندسی
استاد راهنما: دکتر یاسر علمی‌سولا

استاد مشاور: مهندس حسام حسن‌پور

M.A. Thesis:

Proposing a new approach for Detecting Phishing Attacks based on Artificial Neural Network and Genetic algorithm

The large volume of transactions via the World Wide Web is conducted and various users will use it. Internet security is a big challenge and essential for financial activities. Information theft or phishing by fake sites is considered one of the main challenges the world wide web which can cause much damage to users and the financial sector. on a online information steal(phishing) one fraudulent site attempts to attract users trust. and their valuable information such as usernames and passwords to be stolen. phishing attacks also can steal bank account numbers and passwords. in this respect these attacks is significant harm to users. phishing attacks have hidden patterns that can detect patterns to reduce the effects of the attacks.new methods for detecting phishing attacks based on data mining and machine learning techniques is presented that can accurately recognize the right of the attacks.. in this study have been used a new method to identify phishing attacks based on artificial neural networks and genetic algorithms to be selected important features of neural network such as weights and thresholds for a more efficient and increase classification accuracy of phishing attacks. the results of simulations and experiments on data sets phishing attacks contained in UCI database that has 30 different features web pages show that the proposed method are detected with high sensitivity and accurately 97.24% and
94.43% respectively of the attacks.