طراحی سیستم خبره به منظور تشخیص حمله‌های فیشینگ
در بانکداری الکترونیکی

محمود مسیمی، حسن اکبری پور، محمدضا امین ناصیری

- دانشجوی کارشناسی ارشد فناوری اطلاعات، دانشگاه تربیت مدرس
  m.moghim@modares.ac.ir
- دانش‌آموخته کارشناسی ارشد مهندسی صنایع، دانشگاه تربیت مدرس
  h.akbaripour@modares.ac.ir
- دانشیار - بخش مهندسی صنایع، دانشگاه تربیت مدرس
  amin_nas@modares.ac.ir

چکیده: امروزه از مهم‌ترین ریسک‌ها و چالش‌های مورد توجه در تجارت الکترونیک و بانکداری الکترونیکی خطر کلاه‌برداری آتلاین و حملات فیشینگ است. در این تحقیق سیستم خبره‌ای با استفاده از مشخصه‌های ظاهری صفحه، قابل‌یابی امنیتی و نیز اطلاعات موجود در دامنه وب سایت ارائه گردیده است که قادر به استقرار در خصوصیات مشکوک بودن یک وب سایت به بکنی جمله فیشینگ در بانکداری الکترونیکی می‌باشد. در این سیستم خبره پیشنهادی از شایعه عصبی مصنوعی جهت شناسایی پایگاه داده‌ای سیستم استفاده شده است. ورودی های سیستم خبره، 27 پارامتر مختلف قابل ارزیابی هستند که از یک صفحه وب استخراج می‌شوند. فرآیند استنتاج نیز با استفاده از موتور استنتاج موجود در پوشه سیستم خبره بیان برای هر کدام از پیش‌بینی‌های پارامترهای ورودی به‌صورت مجزا انجام می‌گیرد. در نهایت نتیجه هر بخش در مقایسه با نتیجه سایر بخش‌ها ارزیابی و خروجی حاصل است که آن نتیجه سیستم خبره ادهی به سیستم پیشنهادی خروجی حاصله بر اساس مدل‌ها واقع مورد ارزیابی قرار گرفت که نتایج قابل قبولی در نتایج واحدهای این نوع حملات در مقایسه با سایر سیستم‌های موجود در ادبیات ارائه نموده است.

کلمات کلیدی: فیشینگ، بانکداری الکترونیکی، سیستم خبره، شبکه عصبی مصنوعی.
مقدمه

امروزه اینترنت نقیب توجهی در فعالیت های تجاری و کسب و کار دارد. این امر نشان می‌دهد که تغییرات در فناوری و نظام ارتباطات هوشمند در این عصر به‌طور چشمگیری افزایش یافته است. همچنین، کسب و کارهای آنلاین که از این تغییرات بهره می‌برند، به صورت قابل توجهی در رشد و توسعه قرار گرفته‌اند.

روش‌های مبتنی بر یک گروه گوگلیکو گسترش یافته و در بسیاری از این روش‌ها به علت همبستگی و اعتماد به صنایع کسب و کار، بسیاری از این روش‌ها به صورت قابل توجهی در رشد و توسعه قرار گرفته‌اند.

در اینجا، سعی می‌شود به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع می‌شود.

بعدها، به بررسی این موضوع بپردازی و در نهایت، به بیان بعضی از روش‌هایی که باعث گسترش و رشد این صنایع می‌شود، از جمله:

1. روش‌هایی که به بهره‌مندی از اینترنت تاکید دارند.
2. روش‌هایی که به بررسی اینترنت و ارتباطات همبستگی باعث گسترش و رشد این صنایع M
حملات به نوعی سعی در این است تا مرجع سایت به عنوان یک
حملات آشنا نبوده و در پیشتر مورد بی‌ثباتی قرار گرفته باشد
[18] از این نظریه‌ها بکارگیری شده در این
گام کلیه‌های اینترنتی کشور و اکثریت سایت‌های
نظامی و وب سایت‌های استفاده از این روش‌ها در این
مطالعه از آنها اشاره نمود [19].
در نتیجه PayPal

فلش هم‌نامه

شکل (1): مطالعات سایت PayPal در این زمان حمله است

شده توسط آیپاد و همکاران اشتهار نمود [12]. این سیستم با
بکارگیری تکنیک‌های دادگاه و منطق فازی قادر به شناسایی
مشخصه‌های وب سایت و تغییر میزان آسیب آن سایت
بوده و با این


سایر روش‌های ارائه شده با یکدیگر مورد مقایسه قرار گرفته

است. مشکل این روش‌ها تنها میزان بالای خطای خروجی

الگوریتم‌ها است که باعث عدم شناسایی صحیح این نوع حملات

می‌گردد.

در این تحقیق سیستم خبرنگاری به منظور تشخیص حملات

فیشینگ در بازدارندی از کاربران اثره گردیده است. در سیستم

ارائه شده از شبه‌های علمی موضوع برای کاهش تعداد قواعد

و افزایش دقیقه سیستم استفاده شده است. قواعد

سیستم خبره پیشنهادی با استفاده از مشخصه‌های ترکیبی که

در سایت‌های اصلی از تقلبی در تحقیق [13] ارائه گردیده است

این قواعد مشترک دندون تعیین حالات مناسب شده‌های فوری

را مورد ارزیابی قرار می‌دهند و در نهایت بر اساس مقدار ورودی

استنتاج ذرم صورت گرفته و شناسایی خروجی سیستم ارائه می‌شود.

در ادامه مقاله بدين صورت ارائه خواهد شد: در پی چیدن

این نتایج در خصوص حملات فیشینگ ارائه خواهد شد.

سیستم خبره پیشنهادی مورد بررسی قرار گرفته و چگونگی

پیاده سازی آن تشریح می‌گردد. در پی چیدن جامعیت سیستم

پیشنهادی مورد بررسی قرار گرفته و در پی این در پی چیدن

نیز، جمع بندی مطالعه و کارهای آتی ارائه گردیده است.

2- حملات فیشینگ

در دهه گذشته حملات فیشینگ به طور فراوانی ای برای کسب
سود آسان از طریق انجام معالمان غیر قانونی مالی افزایش یافته
است. در یک تحقیق کلی می‌توان گفت که فیشینگ شناخت

سیرته همکاران اینترنتی است. در آن تخصصی از مهندسی

اجتماعی و روش‌های ساخت وب سایت های جعلی برای قربانی

کاربر به منظور انکار کردن اطلاعات حمله و ارزش‌شناسی

استفاده قرار می‌گیرد [18]. در حملات فیشینگ از روش‌های

خاصی مانند استفاده از وبسایت‌های مخبول و یا پست

الکترونیک، برای روبودن این اطلاعات استفاده می‌گردد. در این

شکل (3): تعداد سایت‌های فیشینگ کشف شده

در نیمه دوم سال 2011 [21]
سیستم خبره یک برنامه کامپیوتری هوشمند است که قادر به شنیدن ساز و رفتار یک انسان دارای دانش تصویری و یا تجربی در یک زمینه خاص، می‌باشد. سیستم‌های خبره برای حل مسائل پیچیده‌های کرود خبره‌ای، از طریق استفاده از مورد دانش طراحی‌های شور [22] هر سیستم خبره مطابق شکل (۲)، از سه بخش اصلی پایگاه دانایی، موتور استنتاج و رابط کاربری تشکیل شده است.

شکل (۳): مدل پایه یک سیستم خبره

- پایگاه دانایی
- موتور استنتاج
- رابط کاربر

سیستم خبره در حقیقت [13] صاحب‌نظر از ارزیابی جهت شناسایی و ساخت های فیشینک را در قالب ۲۰ پارامتر و در شش بخش مختلف آن‌ها شده است. این شش بخش شامل مشخصه‌های دامنه و بازی، قابلیت‌های امکانی و رمزگذاری مورد استفاده، کدکی اسکریپتی موجود در سیستم، ظاهر صحنه و معنویت، آدرس صحنه و ویژگی‌های رافترا سایت می‌باشد. ترکیب معکوس مختلف قابل استخراج با رهیک از این صفات به شکل پایگاه دانایی سیستم را به دست می‌دهد. سیستم خبره نیز این توان بر اساس این داتش خودش است. استنتاج نمودار جایگزینی در صورتی مشکوک بودن بازی وسیع مورد نظر به یک وب سایت فیشینک را انجام می‌دهد. یک جمع آوری مقداری برای یک از این صفات صحنه نیز از اهمیت سیستم برمی‌خورد. استنتاج در این صفت به تایید پایگاه دانایی تأثیر می‌سایه در استنتاج درست و صحیح ترکیب گیری می‌کند. سیستم هوشمند را ایجاد می‌نماید.

روش‌های مختلف استخراج این مقداری از معنویت صحنه و در دست حقیقت [13] از سوی این است. در سیستم پایگاه‌ها، مشخصه‌های قابل ارزیابی یک صحنه بعنوان پارامتر ورودی برای سیستم خبره در نظر گرفته شده‌اند. لیست کلی این پارامترها در رابط شش بخش و سه لایه مختلف به جدول (۱) نشان داده شده است. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد. لیست کلی این فقط حاوی پارامترهای ارزیابی از مشخصه‌های دامنه و بسیار می‌باشد.

- پایگاه دانایی
- موتور استنتاج
- رابط کاربر

سیستم خبره

- پایگاه دانایی: در سیستم خبره پایگاه دانایی باید گردد
- دانش‌ها: این برای استنتاج مورد استفاده قرار می‌گیرد. درواقع این پایگاه دانایی از طریق کسب حقایق و مهارت‌های یک فرد خبره ساخته می‌شد و سیستم می‌باشد توسط روش جهت انجام استنتاج بازنمایی گردد.

- موتور استنتاج: برای دستیابی به نتایج مورد نظر، سیستم خبره با جستجو در پایگاه دانایی و بر اساس منطق استنتاج و پردازش قواعد استنتاج را انجام می‌دهد. این موتور با استفاده از یک روش استدلال که سیستم استدلال پیش‌رو یا پسرو و یا مخلوطی از هر دو می‌باشد عمل استنتاج را انجام می‌دهد.

- واسط کاربر: این بخش فراه کننده ارتباط بین کاربر و سیستم خبره می‌باشد. واسط کاربر سیستم خبره نه تنها کاربر را قادر سازد تنها به اسپاس دهنده بکه کاربر را مجاز می‌سازد عملیات اجرایی سیستم را با پرسش در مورد توضیحات داده شده قطع نماید در پایان عملیات استنتاج نیز خروجی سیستم خبره از طریق واسط کاربر نمایان می‌گردد.
جدول (1): مشخصه‌های قابل ازيابی در تشخیص سایت فیشینگ

| مشخصه‌های C3 | پایین‌ترین | دیده‌بینی | زمان IP در ادرس وب سایت | در این فرم همکار
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. استفاده از IP در ادرس وب سایت</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2. جیری خودکارهای وابسته به IP در ادرس وب سایت</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3. استفاده از ابزار IP در سرور</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4. استفاده از ابزار IP در ابزار</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5. استفاده از الگوریتم IP در سرور</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6. استفاده از الگوریتم IP در ابزار</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7. استفاده از الگوریتم IP در ابزار</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8. استفاده از الگوریتم IP در ابزار</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>9. استفاده از الگوریتم IP در ابزار</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10. استفاده از الگوریتم IP در ابزار</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>11. استفاده از الگوریتم IP در ابزار</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>12. استفاده از الگوریتم IP در ابزار</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>13. استفاده از الگوریتم IP در ابزار</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>14. استفاده از الگوریتم IP در ابزار</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>15. استفاده از الگوریتم IP در ابزار</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>16. استفاده از الگوریتم IP در ابزار</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>17. استفاده از الگوریتم IP در ابزار</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>18. استفاده از الگوریتم IP در ابزار</td>
<td>18</td>
<td>18</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>19. استفاده از الگوریتم IP در ابزار</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>20. استفاده از الگوریتم IP در ابزار</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>21. استفاده از الگوریتم IP در ابزار</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>22. استفاده از الگوریتم IP در ابزار</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>23. استفاده از الگوریتم IP در ابزار</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>24. استفاده از الگوریتم IP در ابزار</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>25. استفاده از الگوریتم IP در ابزار</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>26. استفاده از الگوریتم IP در ابزار</td>
<td>26</td>
<td>26</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>27. استفاده از الگوریتم IP در ابزار</td>
<td>27</td>
<td>27</td>
<td>27</td>
<td>27</td>
</tr>
</tbody>
</table>
ایجاد سازی سیستم

سیستم‌های خبره را می‌توان با استفاده از بانک‌های مختلف برنامه نویسی و یا با استفاده از محصولاتی که پوسته سیستم خبره‌ای پیش‌بینی می‌کند. پوسته سیستم خبره‌ای برای پیش‌بینی یک سیستم خبره با یک سیستم استفاده می‌شود. پوسته سیستم خبره به شکلی است که ارتباط کاربری و پوسته سیستم خبره‌ای ارتباط داشته باشد. این سیستم‌های خبره‌ای توسط تکنولوژی می‌باشند که با توجه به مقدار خروجی جدول تصمیم سیستم خبره، می‌توان در نظر گرفته شده است. لذا این سیستم‌ها می‌توانند در قالب یک قاعده بهینه تکنولوژی باین‌گر گردد. 

<table>
<thead>
<tr>
<th>جدول (3): جدول تصمیم برای لایه‌ی دوم</th>
</tr>
</thead>
<tbody>
<tr>
<td>شماره</td>
</tr>
<tr>
<td>--------------------------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

پیاده‌سازی سیستم

پیاده‌سازی سیستم با استفاده از مدل‌های مختلف برنامه‌نویسی و یا با استفاده از محصولاتی که پوسته سیستم خبره‌ای پیش‌بینی می‌کند. پوسته سیستم خبره‌ای برای پیش‌بینی یک سیستم استفاده می‌شود. پوسته سیستم خبره به شکلی است که ارتباط کاربری و پوسته سیستم خبره‌ای ارتباط داشته باشد. این سیستم‌های خبره‌ای توسط تکنولوژی می‌باشند که با توجه به مقدار خروجی جدول تصمیم سیستم خبره، می‌توان در نظر گرفته شده است. لذا این سیستم‌ها می‌توانند در قالب یک قاعده بهینه تکنولوژی باین‌گر گردد. 

<table>
<thead>
<tr>
<th>جدول (3): جدول تصمیم برای لایه‌ی دوم</th>
</tr>
</thead>
<tbody>
<tr>
<td>شماره</td>
</tr>
<tr>
<td>--------------------------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

پیاده‌سازی سیستم

به‌کارگیری مدل‌ها و روش‌های مختلف برنامه‌نویسی و یا با استفاده از محصولاتی که پوسته سیستم خبره‌ای پیش‌بینی می‌کند. پوسته سیستم خبره به شکلی است که ارتباط کاربری و پوسته سیستم خبره‌ای ارتباط داشته باشد. این سیستم‌های خبره‌ای توسط تکنولوژی می‌باشند که با توجه به مقدار خروجی جدول تصمیم سیستم خبره، می‌توان در نظر گرفته شده است. لذا این سیستم‌ها می‌توانند در قالب یک قاعده بهینه تکنولوژی باین‌گر گردد. 

<table>
<thead>
<tr>
<th>جدول (3): جدول تصمیم برای لایه‌ی دوم</th>
</tr>
</thead>
<tbody>
<tr>
<td>شماره</td>
</tr>
<tr>
<td>--------------------------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>
5- اعتبار سنجی سیستم خرده پیشنهادی

جهت بررسی اعتبار و کارایی سیستم خرده، خروجی سیستم بر اساس مقادیر واقعی کنترل می‌گردد. برای این منظور از اطلاعات موجود سایت PhishTank کمک از سرویس‌های معتبر مربوط به PhishTank می‌باشد که در زمینه ثبت و نگهداری اطلاعات سایت‌های فیشینگ فعالیت می‌نماید. برای بررسی کارایی اعتبار سیستم تعداد ۱۵۰ صفحه فیشینگ از بانک اطلاعات سایت مذکور استخراج گردید. این صفحات تماماً مربوط به صفحات یک وبسایت کامکاری که انجام شده در سایت PhishTank را شامل می‌شود. در هر صفحه بسته به اینکه آیا صفحه را به عنوان معتبر یا غیر معتبر از نظر این سیستم می‌تواند به صفحات معتبر یا غیر معتبر بگرداند در صورت تغییر وضعیت آن صفحه، این صفحه از دست داده می‌شود. نتایج به‌طور کلی در جدول ۴ نشان داده شده است.

جدول ۴: تعداد قواعد بخش‌های مختلف سیستم خرده پیشنهادی

<table>
<thead>
<tr>
<th>بخش / لابه</th>
<th>تعداد قاعده</th>
</tr>
</thead>
<tbody>
<tr>
<td>بخش اول</td>
<td>۲۰</td>
</tr>
<tr>
<td>بخش دوم</td>
<td>۱۱</td>
</tr>
<tr>
<td>بخش سوم</td>
<td>۷</td>
</tr>
<tr>
<td>بخش چهارم</td>
<td>۲</td>
</tr>
<tr>
<td>بخش پنجم</td>
<td>۱</td>
</tr>
<tr>
<td>بخش ششم</td>
<td>۱</td>
</tr>
<tr>
<td>لاای دوم</td>
<td>۱۱</td>
</tr>
<tr>
<td>لاای سوم</td>
<td>۱۰</td>
</tr>
<tr>
<td>استناد نهایی</td>
<td>۹۹</td>
</tr>
</tbody>
</table>

۴-۴- ارتباط با کاربر

در بخش اول ارتباط با کاربر، سیستم خرده سوالاتی را در خصوص هر یک از پارامترهای ورودی مربوط حس و کاربر باهم برای مناسب تریازهای تا سیستم بتواند با توجه به پاسخ‌های داده شده استخراج لازم را انجام دهد. در شکل ۴، صحنه ارتباط با کاربر سیستم خرده نشان داده شده است. عمل استناد بر اساس قواعد تظیم شده در سیستم انجام می‌گردد. نتیجه‌های بتی‌های بسته راهی بر اساس مقدار ورودی محاسبه می‌گردد. خروجی سیستم به‌طور گسترده‌ای در سیستم خرده محاسبه گردیده و در انتهای نتیجه استخراج در سیستم (Very-Legitimate), (Suspicious), (Legitimate) و (Phishy) نشان می‌دهند.

شکل ۴: میانگین موزیکال بر اساس سیستم خرده

طبق تفسیر نهایی، نتیجه برای نمایش خروجی که در بخش (۲) ۱۵۰ اشاره شده است، نتایج ۱۵۰ صفحه فیشینگ موجود ورازی‌ای، اعداد ۲۷ صفحه به عنوان صفحات مکروک، ۵۵ صفحه به عنوان فیشینگ و ۱۰ صفحه به صورت دائمی به‌صورت کامکاری ارزیابی گردید. نتیجه این ارزیابی در شکل ۵ نشان داده شده است.

شکل ۵: میانگین ارزیابی بر اساس سیستم خرده
پیش‌بینی و تحقیق در مقایسه پیش‌بینی‌های سیستم خبره بر اساس آزمایشگاهی - ارزیابی راهبردهای ارزیابی سیستم خبره

در این تحقیق بر اساس معیارهای ارائه شده در مقالات مرتبط سیستم خبره را به منظور تشخیص حملات فیشینگ در بانکداری الکترونیکی نگهداری آنها شد. این معیارها در قابل 27 پارامتر در شش خشخاش متفاوت مشخصه‌های دانش و سایت قابلیت‌های انطباق و رمزگاری مورد استفاده کسب شد. سپس، که در نظر گرفته شود، محققین تحقیق است به صورت برابر در 27 پارامتر مورد بررسی قرار گرفتند. در نتیجه این مقایسه، بزرگ‌ترین اهمیت برای بررسی‌های مختلف سیستم بانکداری در هنگام تشخیص حملات فیشینگ داشته و از این رو، این سیستم می‌تواند به عنوان یک ابزار کوولنر مورد استفاده قرار گیرد.

نتایج گیری:

1. تحقیق ارزیابی سیستم خبره بر اساس قواعد مدیریت مصرف در بانکداری الکترونیکی نشان داد که با توجه به تعداد خطا آنها، سیستم خبره قادر به تشخیص حملات فیشینگ با صحت بالا است.

2. سطح مقایسه‌های مشابه در میان پارامترها، شکل 7 نشان‌دهنده قانون بودن و سایت خواهد بود.

3. نتایج نشان داده که برای بررسی‌های مختلف سیستم بانکداری در هنگام تشخیص حملات فیشینگ، این سیستم می‌تواند به عنوان یک ابزار کوولنر مورد استفاده قرار گیرد.

مراجع:


