بررسی سیستم‌های تشخیص نفوذ مبتنی بر تکنیک‌های داده‌کاوی

زینب لیرکی[۱]، ابراهیم بهروزیان نژاد[۲]

[۱]دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد علوم و تحقیقات خوزستان، گروه کامپیوتر، اهواز، ایران، z.liraki@khouzestan.srbiau.ac.ir

[۲]استادیار، دانشگاه آزاد اسلامی، واحد شوشتر، گروه کامپیوتر، شوشتر، ایران، E.Behrozian@iau-shoushtar.ac.ir

چکیده: با فراگیر شدن روزافزون فناوری اطلاعات و ارتباطات و گسترش شبکه‌های کامپیوتری متصل به اینترنت، حملات و نفوذهایی در اشکال مختلف به شبکه‌ها صورت می‌گیرد، لذا سیستم‌های تشخص نفوذ (IDS) جزء حیاتی در هر شبکه‌ای در دنیای اینترنت امروزی است. جهت تأمین امنیت شبکه‌های به هم پیوسته، سیستم‌های تشخیص نفوذ روش مؤثری برای شناسایی اشکال مختلف حملات نفوذی در شبکه‌ها هستند. کارایی سیستم‌های تشخیص نفوذ وابسته به نرخ تشخیصِ نفوذی با دقت بالا و کمترین نرخ هشدار غلط است. نتایج بسیاری از تحقیقات حاکی از این است که، در تجزیه و تحلیل و رویارویی با حجم بالایی از ترافیک شبکه، تکنیک‌های داده‌کاوی متفاوتی همانند: دسته‌بندی، خوشه‌بندی و یا روش‌هایی ترکیبی، عملکرد خوبی در سیستم‌های تشخیص نفوذ از خود نشان می‌دهند. در این مقاله مروری بر تکنیک‌های متفاوت داده‌کاوی ذکر شده در سیستم‌های تشخیص نفوذ، جهت شناسایی حملات شناخته شده و ناشناخته می‌شود.

واژگان کلیدی: امنیت شبکه، داده‌کاوی، سیستم تشخیص نفوذ، دسته‌بندی، خوشه‌بندی، روش یادگیری ترکیبی.

۱- مقدمه

با فراگیر شدن روزافزون فناوری اطلاعات و ارتباطات و گسترش شبکه‌های کامپیوتری متصل به اینترنت، به دلیل حملات و نفوذهایی که در اشکال مختلف به شبکه‌ها صورت می‌گیرد، لزوم حفظ امنیت اطلاعات و کارایی شبکه‌های کامپیوتری اهمیت ویژه ای دارد. از آنجایی که از نظر تکنیکی ایجاد سیستم‌های کامپیوتری سخت‌افزاری و نرم‌افزاریِ عاری از نقاط ضعف و شکست امنیتی عملاً غیر ممکن است، لذا تشخیص نفوذ در تحقیقات سیستم‌های کامپیوتری با اهمیت خاصی دنبال می‌شود. نفوذ به عملیاتی اطلاق می‌شود که تلاش می‌کند برای دسترسی غیر مجاز به شبکه یا سیستم‌های کامپیوتری از مکانیزم‌های امنیتی سیستم عبور کند [1]. این عملیات، توسط نفوذکنندگان داخلی و خارجی انجام می‌شود. نفوذگرها عموماً از عیوب نرم‌افزاری، شکستن کلمات رمز، استراق سمع، ترافیک شبکه و نقاط ضعف طراحی شبکه یا کامپیوترهای شبکه جهت نفوذ به سیستم‌ها و شبکه‌های کامپیوتری بهره می‌برند. استفاده از تکنیک‌های داده‌کاوی برای تشخیص نفوذ یکی از مسیرهای تحقیقاتی مهم در رابطه با امنیت شبکه است. سیستم‌های تشخیص نفوذ با استفاده از تکنیک‌های داده‌کاوی می‌توانند در میان حجم عظیمی از داده‌ها و بسته‌های اطلاعاتی شبکه، رفتارهای غیرنرمال و نفوذی را شناسایی کرده و عملکرد مناسب را اتخاذ کنند.

۱-۱- سیستم تشخیص نفوذ[۱]:

سیستم تشخیص نفوذ (IDS) یک سیستم دفاعی است که در حفظ امنیت شبکه‌های کامپیوتری در مقابل تهدیدات و نفوذهای کاربران داخلی و خارجی نقش مهمی را ایفا می‌کند [2]. سیستم تشخیص نفوذ وظیفه شناسایی و تشخیص هرگونه استفاده غیرمجاز، سوء استفاده و یا آسیب رساندن به منابع و سیستم‌های شبکه را بر عهده دارد. روشهای تشخیص مورد استفاده در IDSها به دو دسته تقسیم می‌شوند: تشخیص رفتار غیرعادی[۲] و تشخیص مبتنی بر امضاء[۳].

روش تشخیص رفتار غیرعادی براساس رفتار عادی سیستم بنا می‌شود. بدین گونه که رفتارهای عادی سیستم را شناسایی کرده و الگوهای خاصی برای آنها استخراج می‌کند و رفتارهایی که از این الگو پیروی نکند به‌عنوان رفتارهای غیرعادی تشخیص داده

می‌شوند. در تشخیص مبتنی بر امضاء نیز، الگوهای رفتاری هر نفوذ تحت عنوان امضای آن نفوذ در پایگاه داده‌ای ذخیره می‌شود. سیستم با بررسی ترافیک شبکه، اگر الگویی را مشابه با آنچه در این پایگاه داده وجود دارد بیابد، یک نفوذ به سیستم را تشخیص می‌دهد. از بین این دو روش تنها روش تشخیص رفتار غیرعادی قادر به تشخیص حملات ناشناخته هستند، زیرا روش تشخیص مبتنی بر امضاء تنها قادر به تشخیص نفوذهای شناخته شده است [3,4]. به طور کلی سیستم‌های تشخیص نفوذ به دو دسته عمده تقسیم می‌شود: سیستم تشخیص نفوذ مبتنی بر میزبان[۴] و سیستم تشخیص نفوذ مبتنی بر شبکه[۵].

IDSهای مبتنی بر میزبان در میزبان‌های نهایی مستقر شده و در سطح لایه کاربرد شبکه اقدام به فعالیت می‌کنند. و تمامی تقاضاهای ارسالی هر برنامه کاربردی را جهت شناسایی حملات بررسی می‌کنند. IDSهای مبتنی بر شبکه نیز در سطح لایه شبکه فعالیت می‌کنند و برای شناسایی حملات نفوذی، بر ترافیک‌های ارسالی و دریافتی شبکه نظارت می‌کنند.

۲-۱- داده‌کاوی

داده‌کاوی فرآیند استخراج دانش و معرفت از پایگاه داده‌ها جهت کشف الگوها و روابط نامعلوم در پایگاه داده‌ها است. به عبارتی دیگر داده‌کاوی یک مرحله ضروری از فرآیند بزرگتر کشف دانش و معرفت از پایگاه داده است.

امروزه داده‌کاوی نقش مهمی در سیستم‌های تشخیص نفوذ ایفا می‌کنند. تکنیک‌های داده‌کاوی مختلفی همانند دسته‌بندی و خوشه‌بندی جهت شناسایی عملیات نفوذی در سیستم‌های تشخیص نفوذ مورد استفاده قرار گرفته و کارایی آنها به اثبات رسیده است. روش‌های یادگیری ترکیبی مختلفی نیز با ترکیب روش‌های دسته‌بندی و خوشه‌بندی جهت دستیابی به نرخ تخیص بالا و نرخ هشدار غلط پایین مورد استفاده قرار گرفته‌اند.

در ادامه تعدادی از الگوریتم‌های مطرح شده با تکنیک‌های مختلف داده‌کاوی را در تشخیص نفوذ مورد بررسی قرار می‌دهیم.

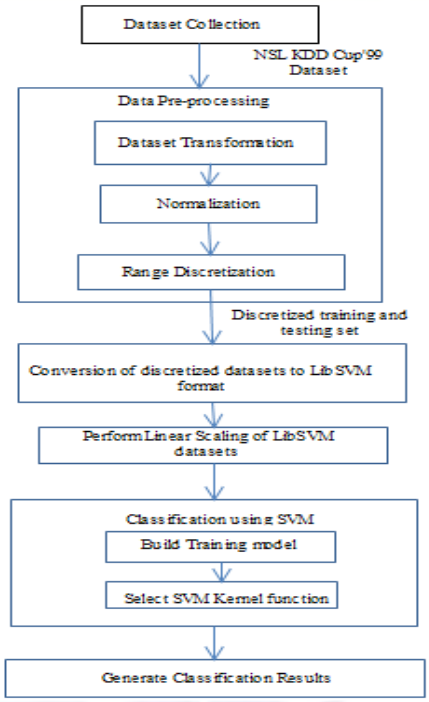
سازماندهی مقاله بدین صورت است که در بخش۲ متن اصلی مطرح می‌شود. که مروری بر روش‌های مطرح شده در سیستم‌های تشخیص نفوذ در زمینه‌های دسته‌بندی، خوشه‌بندی و روش‌های یادگیری ترکیبی است. بخش ۳ مربوط به نتیجه گیری کلی از مقاله اختصاص دارد. در این بخش پیشنهاداتی جهت کارهای آتی مطرح شده است.

۲- متن اصلی

۲-۱- دسته‌بندی[۶]

دسته‌بندی [3] یکی از تکنیک‌های داده‌کاوی است، که هر نمونه در مجموعه داده را به یک دسته خاص اختصاص می‌دهد. تکنیک دسته‌بندی مدل‌هایی را جهت تعریف کلاس‌های مهم داده استخراج می‌کند. هر نمونه مدل، یک دسته نامیده می‌شود. دسته-بندی مبتنی بر IDS ترافیک‌های شبکه را به دو دسته نرمال یا نفوذی دسته‌بندی می‌کنند. دسته‌بندی داده‌ها شامل دو گام است: گام نخست، یادگیری و گام دوم، دسته‌بندی است. در گام یادگیری، دسته‌ها ساخته می‌شوند و در گام دسته‌بندی، مدل‌ها جهت پیش‌بینی برچسب کلاس‌ها برای اخذ داده‌ها مورد استفاده قرار می‌گیرند. برای تجزیه و تحلیل دسته‌بندی، تحلیلگر می-بایست از چگونگی تعریف بسته‌ها اطلاع داشته باشد. دسته‌بندی یک مکانیزم یادگیری نظارت شده ماشین است که تنها از داده‌های برچسب‌دار حمایت می‌کند. لذا همین ویژگی موجب ضعف در عملکرد تشخیص نفوذ می‌شود، زیرا از داده‌های فاقد چسب حمایت نمی‌کند. در نتیجه عملکرد ضعیف‌تری نسبت به خوشه-بندی در تشخیص نفوذ به شبکه دارد.

مدل شبکه عصبی مصنوعی که جهت یادگیری رفتار سیستم در [5] ارائه شده است، نشان می‌دهد که کارایی بیشتری در IDSهای در حال توسعه دارند. استفاده از روش یادگیری ماشین در طراحی سیستم‌های تشخیص نفوذ و پیاده‌سازی این روش موجب می‌شود که سیستم، امکان انطباق با محیط جدید و تغییراتی که در محیط ایجاد می‌شود را داشته باشد. لذا این ویژگی امکان تشخیص حملات ناشناخته در سیستم را تسهیل می‌بخشد. در [13] یک سیستم تشخیص نفوذ مبتنی بر بهبود عملکرد تکنیک ماشین بردار پشتیبان[۷] (SVM) ارائه شده است. این روش بر نقطه ضعف SVM که زمان زیادی در ساخت مدل جهت دسته-بندی داده نیاز داشت، غلبه کرده است. لذا در این روش با پیش-پردازش صحیح مجموعه داده زمان مورد نیاز برای ساخت مدل SVM را کاهش یافت. مجموعه داده مورد استفاده در این مقاله برای بررسی عملکرد سیستم تشخیص نفوذ، نسخه پیشرفته ای از KDD Cup'99 است به نام NSL-KDD Cup'99 که مزایای بیشتری نسبت به ورژن قبلی دارد. طراحی این سیستم پیشنهادی در شکل(۱) نشان داده شده است.



شکل(۱) طراحی IDS با تکنیک SVM [13]

همانطور که در طراحی سیستم مشاهده می‌شود مجموعه داده NSL-KDD Cup'99 جهت ساخت ورودی SVM پیش‌پردازش می‌شود، که شامل مراحل: انتقال مجموعه داده، نرمال‌سازی مجموعه داده و گسسته‌سازی مجموعه داده است. سپس مجموعه‌های آموزشی و تستِ گسسته‌سازی شده به فرمت libSVM تبدیل می‌شوند، که ویژگی‌های دسته‌بندی شده به مقادیر عددی تبدیل می‌شود. و با توجه به دو کلاس هدف مشخص شده که کلاس صفر برای نمونه‌های نرمال و کلاس یک برای نمونه‌های غیرنرمال است، نمونه‌ها دسته‌بندی می‌شوند. سپس مجموعه داده libSVM جهت بهبود عملکرد دسته‌بندی SVM مقیاس‌بندی خطی شده و ذخیره‌سازی می‌شوند. در مرحله بعد، توسط الگوریتم SVM دسته‌بندی‌های مجموعه‌های آموزشی و تست انجام می‌شود. سپس تابع کرنل مناسب انتخاب شده و نتایج دسته‌بندی تولید می‌شود.نتایج آزمایش‌ها حاکی از این است که زمان مورد نیاز جهت ساخت مدل برای دسته‌بندی کاهش یافته و دقت تشخیص نفوذ هنگامی که از تابع کرنل گائوسی استفاده می‌شود افزایش می‌یابد.

۲-۲- خوشه‌بندی[۸]:

الگوریتم K-means [6] یک الگوریتم خوشه‌بندی ساده برای حل بهتر مشکل خوشه‌ها است. عملکرد این الگوریتم از یک روش ساده و آسان پیروی می‌کند، به این ترتیب که داده‌های مجموعه داده را بر اساس تعداد ثابتی از K خوشه که قبلاً تعیین شده است، خوشه‌بندی می‌کند.

الگوریتم K-means بهبودیافته [6] در عملکرد تشخیص نفوذ می‌تواند نویزها و نقاط جدا مانده از مجموعه داده را تشخیص داده و به این ترتیب اختلال در سیستم را کاهش دهد. این الگوریتم تعداد خوشه‌های مرکزی را با روش تقسیم و ادغام و همچنین استفاده از تراکم شعاع آن حوزه محاسبه می‌کند.

الگوریتم K-means پویای اصلاح شده‌ای به نام MDKM در [7] ارائه شده است. این الگوریتم از طریق حذف نویز و نقاط جدا مانده، اثرات مخرب در مجموعه داده را کاهش داده و سپس با پردازش‌های مکرر پویا با دقت بیشتری، تعداد K مرکز خوشه را مشخص می‌کند. لذا این مدل عملکرد بهتری در تشخیص نفوذ دارد.

الگوریتم CLDCGB [12] یک الگوریتم تشخیص نفوذ مبتنی بر گراف با استفاده از روش تشخیص داده‌های پرت که مبتنی بر ضریب انحراف محلی است. از جمله ویژگی‌های این الگوریتم می‌توان به این موارد اشاره کرد: این الگوریتم ضرورتی بر تعیین تعداد اولیه خوشه‌ها ندارد، توانایی بسیار بالایی در تشخیص داده‌های پرت دارد، علاوه بر توانایی تشخیص خوشه‌های دایره‌ای شکل توانایی تشخیص هر شکلی از خوشه‌ها را نیز دارد، نرخ پایداری در تشخیص حملات خاموش یا ناشناخته دارد و چون از روش مبتنی بر یادگیری ترکیبی استفاده می‌کند دقت بالایی در برچسب‌گذاری داده‌ها دارد.

الگوریتم CLDCGB به صورت زیر تعریف می‌شود:

گام ۱. پیاده‌سازی الگوریتم GB به منظور خوشه‌بندی داده‌ها در n خوشه C1, C2…Cn که به صورت نزولی مرتب و ذخیره‌سازی می‌شوند.

گام ۲. مقداردهی اولیه مجموعه های
CN= {φ}, CS= {φ}, CA= {φ}

گام ۳. برای i=1 تا n

اگر (C1.num+C2.num…Ci.num>λ1*M)

آنگاه CN={C1,C2…Ci-1} و

اگر (Cn+Cn-1..Cj+1 > λ 2*M)

آنگاه CA = {Cj+1 … Cn} .

خوشه‌های باقی‌مانده در خوشه {Ci…Cj} CS دسته‌بندی می‌شوند

انتهای حلقه.

گام ۴. محاسبه LDC به ازای هر شیء $p \in CS$ به وسیله معادله (۱) و (۲) و ذخیره آنها به صورت نزولی. اولین k رکورد در مجموعه CA و بقیه رکوردها در مجموعه CN دسته‌بندی می‌شوند.

$$LDC_{k(p)} = dis(p,p') \Big/ \left|N_{k-distance(p)}\right| \quad (1)$$

$$LDC_{k(p)} = \sum_{o \in N_{k-distance(p)}} LDR_{k(o)} \Big/ \left|N_{k-distance(p)}\right| \quad (2)$$

گام ۵. داده‌هایی که در مجموعه CN قرار دارند به عنوان داده‌های نرمال و داده‌هایی که در مجموعه CA قرار می‌گیرند، به عنوان داده‌های غیرنرمال برچسب‌گذاری می‌شوند. فرآیند برچسب‌گذاری بعد از برچسب‌گذاری تمامی داده‌ها به اتمام می‌رسد.

در این الگوریتم CN، CA و CS به ترتیب خوشه‌های نرمال، غیرنرمال و مشکوک هستند. در گام سوم M تعداد اعضای مجموعه داده و $\lambda 1$ و $\lambda 2$ به ترتیب نرخ نرمال و غیر نرمال را نشان میدهد به‌گونه‌ای که ($\lambda 1 + \lambda 2 = 1$) است.

در محاسبه عملکرد الگوریتمCLDCGB روی مجموعه داده KDD cpu99 در مقایسه با الگوریتم‌های K-means و FCM نتایج حاکی از این است که الگوریتمCLDCGB در مقایسه با الگوریتم‌های مذکور نرخ تشخیص بالاتری دارد و همچنین نرخ تشخیص بالا و نسبتاً پایداری در حملات ناشناخته دارد. و توانایی تشخیص هر شکل خوشه‌ای را نیز دارد.

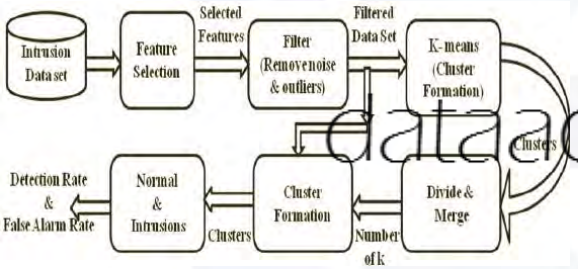
۲-۳- روش‌های یادگیری ترکیبی[9]

یک روش یادگیری ترکیبی در [8] ارائه شده است. این روش ترکیبی از روش‌های خوشه‌بندی K-means و دسته‌بندی ساده بیز است. روش کار به این صورت که همه داده‌ها را در گروه‌های مربوطه قبل از اعمال یک دسته‌بند برای دسته‌بندی، داده‌ها را خوشه‌بندی می‌کند.

یک سیستم تشخیص نفوذ با ترکیب خوشه‌بندی optigrid و یادگیری مبتنی بر گرید در [9] ارائه شده است. خوشه‌بندی optigrid قابلیت بالایی در داده‌های چند بُعدی دارد و می‌تواند بر نقاط ضعف خوشه‌بندی K-means غلبه کند. الگوریتم برچسب‌گذاری، ویژگی‌ها را به گریدهایی تقسیم‌بندی کرده و سپس خوشه‌ها را با استفاده از تراکم گریدها برچسب‌گذاری می‌کند. لذا این سیستم ترکیبی امکان استخراج دقیق داده‌ها و دسته‌بندی صحیح آنها در دسته داده‌های نرمال و نفوذی را امکان‌پذیر می‌کند.

یک سیستم تشخیص نفوذ با ترکیب الگوریتم K-means و دو الگوریتم دسته‌بندی k-نزدیکترین همسایه و الگوریتم بیز ساده در [10] ارائه شده است. در این روش انتخاب ویژگی از مجموعه داده سیستم تشخیص نفوذ با استفاده از الگوریتم انتخاب ویژگی مبتنی بر آنتروپی، که ویژگی‌های مهم را انتخاب و ویژگی‌های زائد را حذف می‌کند اجرا می‌کند. گام بعدی خوشه‌بندی با الگوریتم K-means است و سپس دسته‌بندی بهتر آنها توسط یک دسته‌بندی ترکیبی انجام می‌شود.

در [11] برای تشخیص نفوذ، یک روش ترکیبی مبتنی بر الگوریتم خوشه‌بندی K-means و تجزیه و تحلیل خوشه‌ها جهت غلبه بر نقاط ضعف الگوریتم K-means ارائه شده است. معماری این سیستم تشخیص نفوذ در شکل(۲) نشان داده شده است. مراحل تشخیص نفوذ در این روش ترکیبی پیشنهادی شامل: انتخاب ویژگی، فیلترینگ، خوشه‌بندی، تقسیم و ادغام، خوشه‌بندی مجموعه‌ها[10] و تشخیص حالات داده‌ای نرمال و نفوذی است.



شکل ۲: معماری سیستم تشخیص نفوذ در [11]

در مرحله انتخاب ویژگی، خصوصیات مهم از هر مجموعه داده انتخاب می‌شود. در مرحله فیلترینگ به ازای تمامی نقاط مجموعه داده، مجموع فواصل هر نقطه از سایر نقاط داده‌ای و همچنین مجموع میانگین فواصل محاسبه می‌شود و به ازای هر نقطه اگر مجموع فواصل آن بزرگتر از میانگین فواصل باشد، آن نقطه به‌عنوان نقطه پرت قلمداد شده و از مجموعه داده حذف می‌شود. به این ترتیب در مرحله فیلترینگ نقاط پرت از مجموعه داده حذف می‌شوند. در مرحله بعد خوشه‌بندی توسط الگوریتم K-means انجام می‌شود. خوشه های تولید شده در مرحله بعدی تقسیم‌بندی و ادغام می‌شوند و تعداد k مرکز خوشه محاسبه می‌شود. در این مرحله همچنین تراکم تمامی نقاط در مجموعه داده محاسبه شده و به صورت نزولی مرتب و ذخیره‌سازی می‌شود. سپس k نقطه با بیشترین تراکم به‌عنوان مراکز اولیه انتخاب می‌شوند. در مرحله بعد بر اساس تعداد k مرکز خوشه محاسبه شده، مجدداً داده‌ها خوشه‌بندی می‌شوند. به این ترتیب با مجموعه‌بندی خوشه‌ها از

طریق تغییر تعداد k مرکز خوشه در مرحله بعد توانست داده‌های نرمال و نفوذی را با نرخ تشخیصی با دقت بالا و کمترین هشدار غلط تشخیص دهد.

۳- نتیجه‌گیری

در این مقاله تعدادی از تکنیک‌های مختلف داده‌کاوی که در سیستم‌های تشخیص نفوذ به کار برده شده است مورد بررسی قرار گرفت. با استفاده از تکنیک‌های داده‌کاوی در سیستم‌های تشخیص نفوذ می‌توان ترافیک‌های نرمال و غیرنرمال را در شبکه شناسایی کرد. این مقاله تکنیک‌های داده‌کاوی متفاوتی که در سیستم‌های تشخیص نفوذ مورد استفاده قرار گرفته است همانند: تکنیک‌های دسته‌بندی، خوشه‌بندی و روش‌های یادگیری ترکیبی را مورد بررسی قرار داد. خوشه‌بندی یک تکنیک یادگیریِ بدون نظارت است که داده‌های بدون برچسب مثل حملات ناشناخته را تشخیص می‌دهد. درحالی که دسته‌بندی یک تکنیک یادگیری نظارت شده است که تنها داده‌های برچسب‌دار مثل حملات شناخته شده را تشخیص می‌دهد. نتایج به‌دست آمده از مقالات مختلف نشان می‌دهد، خوشه‌بندی نسبت به دسته‌بندی در زمینه تشخیص نفوذ برای دستیابی به نرخ تشخیص بالا و نرخ هشدار غلط پایین، مناسب‌تر عمل می‌کند. همچنین مشاهده می‌شود سیستم‌های تشخیص نفوذ مبتنی بر روش‌های یادگیریِ ترکیبی عملکرد بسیار خوبی در سیستم‌های تشخیص نفوذ دارند.

مراجع

[1] S. Forrest ,S.A.Hofmeyr, "Intrusion Detection using SequencesofSystem Calls, in Computer & Communication Sciences Journal of Computer Security, vol. 6, no. 3, pp:151-180, 1998.

[2] V. K. Pachghare, Parag Kulkarni, Deven M. Nikam, “Intrusion Detection System Using Self Organizing Maps”, In Proceedings of IAMA 2009, IEEE, 2009.

[3] Deepthy K Denatious, Anita John, “Survey on Data Mining Techniques to Enhance Intrusion Detection” In Proceedings of International Conference on Computer Communication and Informatics (ICCCI - 2012), Jan. 10 – 12, 2012, Coimbatore, INDIA, IEEE, 2012.

[4] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, “Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification”, In Proceedings of 7th International Conference on IT in Asia (CITA), IEEE, 2011.

[5] Sufyan T. Faraj Al-Janabi, Hadeel Amjed Saeed, “A Neural Network Based Anomaly Intrusion Detection System”, 2011 Developments in Esystems Engineering, IEEE, 2011, pp.221-226.

[6] LI Han, “Research and Implementation of an Anomaly Detection Model Based on Clustering Analysis”, In Proceedings of International Symposium on Intelligence Information Processing and Trusted Computing (IPTC 2010), IEEE, HuangGang, China, 2010, pp.458-462.

[7] LI Han, “Using A Dynamic K-means Algorithm to Detect Anomaly Activities”, In the Proceedings of Seventh International Conference on Computational Intelligence and Security, IEEE, 2011, pp.1049-1052.

[8] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, “Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification”, In Proceedings of 7th International Conference on IT in Asia (CITA), IEEE, 2011.

[9] Moriteru Ishida, Hiroki Takakura, Yasuo Okabe, “High-Performance Intrusion Detection Using OptiGrid Clustering and Grid-based Labelling”, In Proceedings of 2011 IEEE/IPSJ International Symposium on Applications and the Internet, IEEE, 2011, pp.11-19.

[10] Hari Om, Aritra Kundu, “A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System”, In Proceedings of 1st Int’l Conf. on Recent Advances in Information Technology (RAIT- 2012),IEEE, 2012.

[11] Kapil Wankhade, Sadia Patka, Ravindra Thool, “An Efficient Approach for Intrusion Detection Using Data Mining Methods” , International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 2013.

[12] Zhou Mingqiang, Huang Hui, Wang Qian, “A Graph-based Clustering Algorithm for Anomaly Intrusion Detection”, The 7th International Conference on Computer Science & Education (ICCSE 2012), IEEE, July 14-17, 2012. Melbourne, Australia.

[13] Yogita B. Bhavsar, Kalyani C.Waghmare, “ Intrusion Detection System Using Data Mining Technique: Support Vector Machine”, International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459), March 2013.

[1] Intrusion Detection System
[2] anomaly detection
[3] misuse detection
[4] Host IDS
[5] Network IDS
[6] Classification
[7] Support Vector Machine
[8] Clustering
[9] Hybrid Learning Approaches
[10] clustering ensemble