مروری بر روش‌های تشخیص نفوذ در پایگاه داده

جواد مرادی*[1] و مجید غیوری[2]

[1]دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین (ع)
jmoradi@ihu.ac.ir

[2] استادیار دانشگاه جامع امام حسین (ع)
ghayoori@ihu.ac.ir

چکیده

داده‌های رایانه‌ای یکی از ارزشمندترین دارایی‌ها در دنیای امروز است و در زندگی روزمره هر فرد و سازمان بزرگ استفاده می‌شود. به‌منظور بازیابی و نگهداری آسان و کارامد، داده‌ها را در یک پایگاه داده ذخیره می‌کنند. از آنجا که می‌توان یک پایگاه داده را با حملات تزریق اس کیو ال[1]، تهدیدات داخلی و حملات ناشناخته در معرض خطر قرار دارد، همواره نگرانی‌هایی مبنی بر ازدست‌رفتن یا تغییر داده‌ها توسط افراد غیرمجاز وجود دارد. برای غلبه بر این نگرانی‌ها چندین لایه امنیتی بین کاربر و داده در لایه شبکه، میزبان و پایگاه‌داده قرار می‌دهند. به‌عنوان‌مثال برای جلوگیری از نفوذ، سازوکارهای امنیتی ازجمله دیواره‌آتش، رمزنگاری داده‌ها، سامانه‌های تشخیص نفوذ و غیره استفاده می‌کنند. از سامانهٔ تشخیص نفوذ پایگاه داده[2] برای شناسایی ناهنجاری‌ها[3] با استفاده از روش‌های مختلف داده‌کاوی و تشخیص فعالیت‌های مخرب و مزاحم استفاده می‌کنند. در این مقاله ابتدا یک دسته‌بندی از روش‌های تشخیص نفوذ در پایگاه داده ارائه شده و سپس مروری بر الگوریتم‌های کلی در تشخیص نفوذ در پایگاه‌های داده ارائه شده است. از آنجا که روش‌های مبتنی بر امضا قدمت بیشتر و پیچیدگی و تنوع کمتری دارند، بنابراین تمرکز اصلی این مقاله بر روش‌های مبتنی بر رفتار است.

واژگان کلیدی: امنیت پایگاه داده، تشخیص نفوذ پایگاه داده، حملات پایگاه داده.

۱- مقدمه

امنیت همانند یک مثلث سه‌ضلعی است که اضلاع آن شامل محرمانگی[4]، جامعیت[5] و دسترس‌پذیری[6] است. به هرگونه اقدامی که تلاش دارد تا محرمانگی یا دسترس‌پذیری و یا یک‌پارچگی سامانه را از بین ببرد، نفوذ گفته می‌شود [۱]. اگر بنا به هر دلیلی نفوذگر بتواند اقدامات امنیتی مانند دیواره‌آتش[7]، رمزنگاری[8]، نهان‌نگاری[9]، سیاست‌های امنیتی[10] و غیره را دور بزند وظیفه سامانه تشخیص نفوذ است که این فعالیت‌های مخرب را شناسایی کند [۲]. درواقع سامانه‌های تشخیص نفوذ برای کمک به مدیران امنیتی در جهت کشف نفوذ و حمله به کار گرفته شده‌اند. هدف یک سامانهٔ تشخیص نفوذ جلوگیری از حمله نیست بلکه تنها کشف و به‌احتمال شناسایی حملات و تشخیص اشکالات امنیتی در سامانه است [۳]. به‌طورعمومی سامانه‌های تشخیص نفوذ در کنار دیواره‌های آتش به‌صورت مکمل امنیتی مورد استفاده قرار می‌گیرند. سامانهٔ تشخیص نفوذ فعالیت‌های کاربران و برنامه‌ها را رصد می‌کنند و درصورت تشخیص آن‌ها به‌عنوان فعالیت مخرب، به مدیر سامانه هشدار می‌دهد. از آنجا که از نظر تکنیکی ایجاد سامانه‌های رایانه‌ای (سخت‌افزار و نرم‌افزار) بدون نقاط ضعف و شکست امنیتی درعمل غیرممکن است [۴]، بنابراین در پژوهش‌های سامانه‌های رایانه‌ای مسألهٔ تشخیص نفوذ با اهمیت خاصی دنبال می‌شود؛ اما بیشتر پژوهش‌های انجام‌شده در زمینهٔ سامانه‌های تشخیص نفوذ، بر روی سامانه‌های تشخیص نفوذ در شبکه یا سیستم‌عامل تمرکز کرده‌اند؛ ولی سامانهٔ تشخیص نفوذ در شبکه یا سیستم‌عامل

1 SQL Injection
2 Database Intrusion Detection System
3 Anomaly
4 Confidentiality
5 Integrity
6 Availability
7 Firewall
8 Cryptography
9 Watermark
10 Security Policy

*نویسندهٔ مسؤول

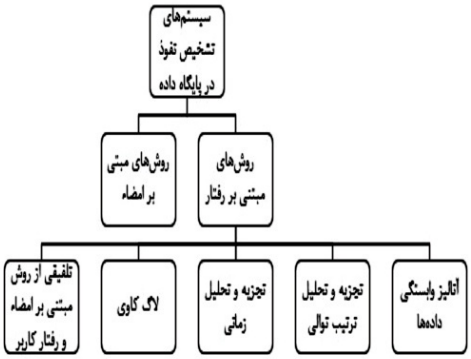
نمی‌تواند فعالیت‌های مخرب در پایگاه داده را تشخیص دهد؛ زیرا فعالیت‌های مخرب برای پایگاه داده به‌الزام برای شبکه و سیستم‌عامل مخرب نیست. از طرف دیگر حملات مخرب به پایگاه داده ممکن است، باعث نامعتبرشدن داده‌ها شود و این داده‌ها از طریق کاربران معتبر به سایر بخش‌های پایگاه داده سرایت کند [۵]. به همین دلیل وجود سامانه‌های تشخیص نفوذ در پایگاه داده امری حیاتی است؛ زیرا سازمان‌ها با استفاده از این سامانه‌ها در اسرع وقت تراکنش‌های مخرب پایگاه داده را تشخیص، و مانع از آسیب‌پذیری سایر بخش‌های پایگاه داده می‌شوند. با توجه به دلایل یادشده در بالا برای برقراری امنیت در سطح پایگاه داده نیاز است، تمام فعالیت‌هایی که قرار است بر روی پایگاه داده انجام شود، ابتدا وارد سامانهٔ تشخیص نفوذ به‌منظور بررسی مخرب یا عادی‌بودن تراکنش‌ها[1] شود و درصورت تشخیص مبنی بر عادی‌بودن تراکنش، اجازه اجرا داده شود [۶-۸].

۲- تشخیص نفوذ در پایگاه داده

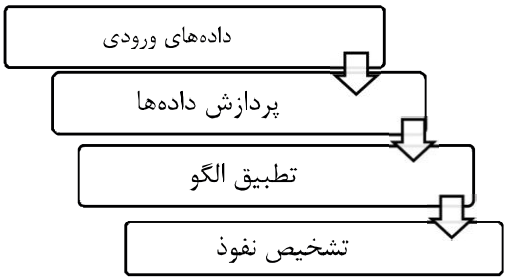
به‌طورکلی دو نوع حمله در پایگاه داده وجود دارد. حملات داخلی و حملات خارجی. حملات داخلی اقدامات مخرب عمدی است که توسط کاربران مجاز که امتیازات دسترسی به برنامه یا سامانه را دارند، مانند کارمندان ناراضی انجام می‌شود. حملات خارجی اقدامات غیرمجازی است که به‌صورت عمدی توسط نفوذگرهایی که حق دسترسی به سامانه را ندارند، به‌منظور سوءاستفاده از اطلاعات سازمان به کار می‌رود. سازوکارهای امنیتی مانند دیوارهٔ‌آتش و غیره که درقبل یاد شد، فقط قادر به تشخیص حملات خارجی هستند؛ اما برتری سامانهٔ تشخیص نفوذ این است که اگر به‌طور صحیح برنامه‌ریزی شود، توانایی تشخیص حملات داخلی را نیز دارد [۹]. همان‌طور که در شکل (۱) مشاهده می‌شود، رویکرد تشخیص نفوذ در پایگاه داده می‌تواند براساس سازوکارهای طبقه‌بندی نفوذ به دو دسته شامل رویکردهای مبتنی بر امضا[2] و رویکردهای مبتنی بر رفتار[3] طبقه‌بندی شود که رویکرد مبتی بر رفتار شامل روش‌های تحلیل وابستگی داده‌ها، تجزیه و تحلیل ترتیب توالی، تجزیه و تحلیل زمانی، لاگ‌کاوی و تلفیقی از روش مبتی بر امضا و رفتار کاربر است.

۳- روش تشخیص نفوذ مبتنی بر امضا

این روش بر پایه روش‌های تطبیق الگو است. این مدلِ سامانهٔ تشخیص نفوذ شامل یک پایگاه داده از امضاهای حملات شناخته شده است و تلاش می‌کند که این امضاها را با داده‌های آنالیزشده مطابقت دهد. هرگاه یک تطبیق یافت شود هشداری به مدیر سامانه به این منظور که تراکنش موردنظر ممکن است، مخرب باشد، ارسال می‌کند. از ویژگی‌های این مدلِ سامانهٔ تشخیص نفوذ، تشخیص سریع، مطمئن و با خطای کم است؛ اما ضعف آن در عدم تشخیص حملات جدید و همچنین نیازمند به‌روزرسانی مداوم پایگاه داده امضاها است. لی و همکارانش [۱۰] یک سامانهٔ تشخیص نفوذ پایگاه داده مبتنی بر امضا را ارائه کرده‌اند که حملات SQL را با نمونه‌های ثبت‌شده مقایسه می‌کند، اگر تطابق داشت آن را به‌عنوان حمله شناسایی می‌کند. در شکل (۲) سلسه‌مراتب روش تشخیص نفوذ مبتنی بر امضا مشاهده می‌شود.



(شکل-۱): دسته‌بندی روش‌های تشخیص نفوذ در پایگاه داده



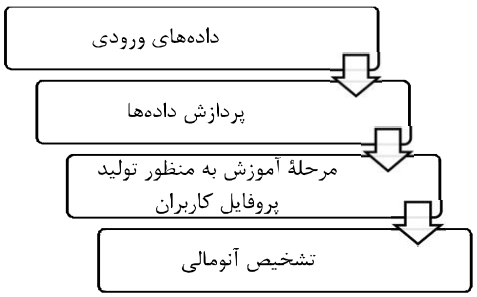
(شکل-۲): سامانهٔ تشخیص نفوذ مبتنی بر امضا

۴- تشخیص نفوذ مبتنی بر رفتار

بر اساس این روش، سامانهٔ تشخیص نفوذ ابتدا در بازهٔ زمانی مشخص شروع به یادگیری ترافیک عبوری پایگاه داده و با ایجاد الگوهای رفتار عادی کاربران، رفتار حملات را شناسایی می‌کند. این روش برای پیداکردن حملات ناشناخته در پایگاه داده مناسب ولی مشکل این روش بالابودن نرخ هشدارهای اشتباه و نیاز به داده‌ها و زمان آموزشی است [۱۱]. سامانه‌های تشخیص نفوذ پایگاه داده مبتنی بر رفتار به‌صورت کلی دارای دو مرحله هستند. الف) مرحلهٔ آموزش (پروفایل‌کردن) ب)

[1] Truncations
[2] Misuse Detection
[3] Anomaly Detection

مرحلهٔ تشخیص نفوذ. هدف مرحلهٔ یادگیری، ساختن پروفایلی دقیق از رفتار کاربران به‌وسیله کاویدن الگوی رفتار کاربران سامانه است. الگوی رفتاری، فعالیت‌هایی هستند که توسط کاربر در مرحلهٔ یادگیری تکرار می‌شوند و قابل‌استخراج از لاگ فعالیت‌های کاربر هستند؛ سپس در مرحلهٔ تشخیص نفوذ، فعالیت‌های کاربر که شامل توالی اجرای دستوراتش است با پروفایل مجاز کاربر که در مرحله قبل ساخته‌شده، تطبیق می‌دهد و درصورت مغایرت، تراکنش موردنظر را به‌عنوان تراکنش مخرب شناسایی کرده و به مدیر امنیتی سامانه هشدار می‌دهد در غیر این صورت تراکنش را مجاز دانسته و اجازه اجرا به آن می‌دهد [۱۲]. هرچند ممکن است، این سامانه‌ها بعضی از رفتارهای عادی را به‌عنوان حمله تشخیص دهد، اما برتری اصلی آن‌ها توانایی شناسایی حملات جدید است. برتینو و همکارانش [۱۳،۱۴] یک پایگاه داده مبتنی بر نقش برای دسترس‌پذیری ارائه داده‌اند (RBAK) که هر نقش یک پروفایل دارد. در شکل (۳) سلسه‌مراتب روش تشخیص نفوذ مبتنی بر رفتار مشاهده می‌شود.



(شکل-۳): سامانه تشخیص نفوذ مبتنی بر رفتار

۴-۱- تحلیل وابستگی داده‌ها

این روشِ تشخیص نفوذ، مبتنی بر وابستگی و تجزیه‌وتحلیل ارتباط‌های میان بخش‌های تراکنش به‌منظور مشخص‌شدن اینکه دستورهای کدام ستون‌ها، ردیف‌ها، جدول‌ها و غیره، به‌طورمعمول با یکدیگر صادر می‌شوند. در این رویکرد تشخیص نفوذ به‌طورمعمول از قوانین انجمنی به‌منظور پی‌بردن به وابستگی بین داده‌ها استفاده می‌کنند. هو و همکارانش [۱۵] برای تشخیص نفوذ، از ارتباط بین داده‌ها استفاده کرده‌اند. اگر تراکنش‌هایی که از هیچ‌کدام از قوانین وابستگی داده پیروی نکند به‌عنوان حمله شناسایی می‌شود. مشکل این روش این است که ویژگی‌هایی از داده‌ها را که خیلی تکرار می‌شوند، در نظر می‌گیرد که ممکن است، این داده‌ها حساس نباشند درواقع این رویکرد ایده‌ای برای داده‌های حساس ندارد. ممکن است، داده‌ای تعداد دسترسی‌های آن کم ولی تغییر آن داده‌ها بر روی پایگاه‌داده بسیار تأثیرگذار باشد. وانگ و همکارانش [۱۶] برای حل این مشکل یک وزن را برای این روابط در نظر می‌گیرند که این وزن نشان‌دهندهٔ چگالی بخش‌های موردنظر در آن تراکنش است.

۴-۲- تجزیه‌وتحلیل ترتیب توالی

ترتیب توالی به‌طور عمده در رویدادها مانند تراکنش‌ها، دستورها (Insert ،Delete ،Select ،Update) و عملیات (Read ،Write) رخ می‌دهد. DIDS[1] با استفاده از این نوع روش‌ها، به‌طورمعمول مجموعه‌ای از تکرارهای انجام‌شده را با طول قابل‌توجهی یاد می‌گیرند و درنهایت آن‌ها را به زیرمجموعه‌های کوچک‌تر تقسیم می‌کند تا این توالی‌ها و زیرمجموعه‌های آن را به‌عنوان رفتار کاربر نرمال دسته‌بندی کند. این روش بر این مبنا کار می‌کند که داده‌ای برای تغییر، دنباله‌ای از سه مجموعه عمل مقابل را در برمی‌گیرد. مجموعه نخست، مجموعه‌ای از ویژگی‌هایی که به‌دلیل به‌روزرسانی خوانده می‌شوند. مجموعه دوم، مجموعه‌ای از ویژگی‌هایی است که قبل از به‌روزرسانی نوشته می‌شوند و در آخر مجموعه‌ای از ویژگی‌هایی که بعد از به‌روزرسانی به‌عنوان نتیجه نوشته می‌شوند؛ سپس از این رویدادها که با نظم خاصی انجام می‌شوند، به‌عنوان رفتار کاربر نرمال دسته‌بندی می‌کنند. در مرحله تشخیص، هر دنباله‌ای از رویدادهای جدید با توجه به توالی‌های آموخته‌شده و زیرمجموعه‌های آن‌ها برای اندازه‌گیری بیشینه تفاوت آن‌ها برای ارزیابی احتمال وقوع نفوذ مقایسه می‌شود. راه‌حل ارائه‌شده در توالی از ویژگی‌های دسترسی، دستورها و جداول را برای ساخت پروفایل کاربر مشخص می‌کند. این ایده در پایگاه داده‌های مبتنی بر نقش کاربرد دارد. در مرحلهٔ یادگیری، مدل‌های توالی را با توجه به مقدار آستانه، برای تعیین بیشینه مقدار تفاوت ایجاد می‌کنند و در مرحله تشخیص نیز، از آستانه برای محاسبه بیشترین مقدار اختلاف بین توالی مورد آزمایش و مواردی که در مرحلهٔ یادگیری نگه‌داری و استفاده می‌شود تا توالی‌ها را به‌صورت معمول یا غیرطبیعی دسته‌بندی کنند. پس در روش تشخیص نفوذ مبتنی بر تجزیه‌وتحلیل مبتنی بر توالی، تعیین مقدار آستانه در تعیین درستی نرخ هشدار بسیار تأثیرگذار است. برای نمونه جداول زیر پس از تجزیه‌وتحلیل رفتار کاربران به‌دست آمده است که در جدول (۱)، الگو <r(6),w(5),w(4)> نشان می‌دهد که این داده‌ها در ۴۰% تراکنش‌های نرمال با یکدیگر مورد دسترسی قرار می‌گیرند. و در جدول (۲)، مجموعه‌ی دنباله‌های خواندن و نوشتن تولیدشده از الگوهای

[1] Database Intrusion Detection System

ترتیبی جدول (۱) را نشان می‌دهد؛ سپس قوانین خواندن و نوشتن استخراج‌شده از دنباله‌های خواندن و نوشتن جدول (۲)، در جدول (۳) نشان داده شده است [۱۷].

(جدول-۱): الگوهای ترتیبی استخراج شده [۱۷]

الگوهای ترتیبی پیداشده	پشتیبانی
r(3)	۳۰٪
w(6)	۴۰٪
r(1) ،w(4)	۳۰٪
r(2),w(2)	۳۰٪
r(2),r(7)	۳۰٪
r(4),w(4)	۳۰٪
r(5),w(4)	۳۰٪
r(5),w(5)	۳۰٪
r(6),r(5)	۳۰٪
r(6),w(5),w(4)	۴۰٪
r(7),r(6),r(1)	۳۰٪
r(7),r(6),w(4)	۳۰٪
r(7),r(6),w(5)	۳۰٪

(جدول-۲): مجموعه دنباله‌های خواندن و نوشتن [۱۷]

مجموعه دنباله‌های خواندن	مجموعه دنباله‌های نوشتن
r(1) ،w(4)	r(1) ،w(4)
r(2),w(2)	r(2),w(2)
r(2),r(7)	r(4),w(4)
r(4),w(4)	r(5),w(4)
r(5),w(4)	r(5),w(5)
r(5),w(5)	r(6),w(5),w(4)
r(6),r(5)	w(5),w(4)
r(6),w(5)	r(7),w(4)
r(6),w(4)	r(6),w(4)
r(7), r(6), r(1)	r(7), w(5)
r(7), r(6)	r(6), w(5)
r(7), r(6),w(4)	
r(7), r(6), w(5)	

(جدول-۳): قوانین وابستگی داده تولیدشده [۱۷]

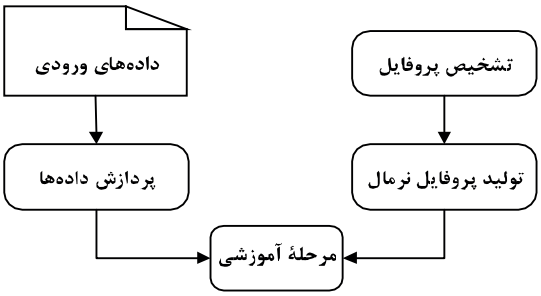
قوانین وابستگی داده	اطمینان
w(2)→r(2)	۱۰۰٪
w(5)→r(6)	۱۰۰٪
w(4)→r(6)	۸۳٪
w(5)→w(4)	۸۰٪
r(2)→w(2)	۷۵٪
r(7)→r(2)	۷۵٪
r(7)→w(4)	۷۵٪
r(7)→w(5)	۷۵٪

۴-۳- تجزیه‌وتحلیل زمانی

این روش بر ویژگی‌های زمانی مانند فاصله زمانی بین دستورهای کاربر و مدت‌زمان این اعمال (زمان پاسخ سرویس‌دهنده، به مشتری) تمرکز می‌کند. به‌عنوان‌مثال، به‌روزرسانی یک شیء دادهٔ زمانی می‌تواند یک قاعده را به‌وجود آورد که زمان به‌روزرسانی در مواقع خاص (برای مثال روزهای شنبه) و مدت زمان انجام این عمل مشخص باشد. سامانهٔ تشخیص نفوذ، تراکنشی را که قصد به‌روزرسانی داشته ولی عمل به‌روزرسانی در محدوده پیش‌بینی‌نشده باشد، به‌عنوان حمله تشخیص داده و به مدیر هشدار می‌دهد [۱۸،۱۹]. البته این روش کارایی چندانی ندارد؛ زیرا پارامترهایی مانند وضعیت اینترنت (سرعت، قطع‌بودن اینترنت و غیره) برای کاربران مختلف متفاوت است و همین دلیل باعث ایجاد هشدارهای اشتباه می‌شود.

۴-۴-تشخیص فعالیت‌های مخرب در پایگاه داده با رویکرد لاگ کاوی

در این مقاله [۲۰] داده‌کاوی را بر روی فایل لاگ به‌منظور شناسایی تراکنش‌های مخرب پایگاه داده انجام می‌دهند. در این رویکرد اگر آستانه پشتیبان[1] و اطمینان[2] به‌درستی انتخاب شود، با کاهش نرخ هشدارهای غلط و افزایش نرخ هشدارهای درست روبه‌رو خواهیم شد. ابتدا (در مرحلهٔ آموزشی) رفتار اشیای پایگاه داده را ضبط و سپس با استفاده از ممیزی فایل لاگ پایگاه داده، رفتار کاربران عادی را ایجاد می‌کند.



(شکل-۴): مرحلهٔ آموزشی درروش لاگ‌کاوی

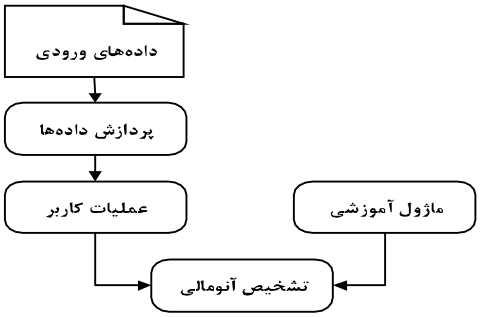
سپس در مرحلهٔ تشخص ورودی‌های کاربر را با پروفایل‌های ساخته‌شده از مرحله آموزشی مقایسه و درصورت مغایرت با آن‌ها، تراکنش موردنظر را به‌عنوان تراکنش مخرب شناسایی می‌کند.

۴-۵-تشخیص نفوذ با استفاده از امضای تراکنش‌ها و رفتار کاربران

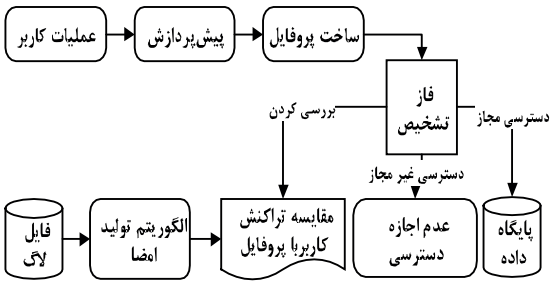
این رویکرد تلفیقی از روش تشخیص نفوذ مبتنی بر امضا و تشخیص مبتنی بر رفتار کاربر است. معماری این روش شامل سه قسمت است: الف) مرحلهٔ آموزشی ب) مرحلهٔ تولید امضا ج) مرحلهٔ تشخیص نفوذ. مرحلهٔ یک: این مرحله به‌عنوان مهم‌ترین مرحله است که شامل یادگیری و جمع‌آوری داده

[1] Support
[2] Confidence

است. در این مرحله باید رفتار عادی کاربر مدل شود. همان‌طور که در شکل (۵) نشان داده‌شده است فایل لاگ داده‌ها را به‌صورت آفلاین ذخیره و سپس با استفاده از الگوریتم تولید امضا تراکنش‌های قانونی را از فایل لاگ استخراج می‌کند که برای شناسایی رفتار معمول و قابل‌قبول تراکنش پایگاه داده است؛ سپس در پیش‌پردازش واژگان کلیدی مانند Select، Update، Insert و ... تراکنش کاربر را استخراج می‌کند و درنهایت در مرحلهٔ آخر با مقایسه تراکنش‌های ورودی با تراکنش‌های مجاز سامانه یک تراکنش را به‌عنوان مخرب یا عادی شناسایی می‌کند [۲۱].



(شکل-۵): فاز تشخیص در روش لاگ کاوی



(شکل-۶): معماری تشخیص نفوذ با استفاده از امضای تراکنش‌ها و رفتار کاربران

۵- کارهای آینده

با توجه حساسیت داده‌ها و اینکه سامانه‌های تشخیص نفوذ قادر به تشخیص تمامی حملات نیستند، در حال حاضر حوزهٔ تشخیص نفوذ پایگاه‌داده جذابیت قابل توجه‌ای از سوی جامعه پژوهشی و شرکت‌های تجاری دارد. پس پژوهش‌گران به‌عنوان پژوهش‌های آینده، به‌منظور بهبود عملکرد سامانه‌های تشخیص نفوذ پایگاه‌داده می‌توانند بر مسائل زیر تمرکز کنند. پژوهش‌گران می‌توانند به بررسی نقاط ضعف و قوتِ روش‌های تشخیص نفوذ بپردازند و استراتژی‌هایی را که در ادامه یاد می‌شود، مد نظر قرار دهند.

الف) افزایش دامنه تشخیص حملات مختلف

در بیش‌تر مقالاتی که به بررسی امنیت پایگاه داده می‌پردازند، به‌طور تخصصی به تحلیل حمله تزریق SQL می‌پردازند؛ اما با تأکید بر سایر حملات پایگاه‌داده مانند سو استفاده از امتیاز سطح دسترسی اجراکننده پرس‌وجو، سرریز بافر، انکار سرویس پایگاه‌داده و غیره می‌توان سطح امنیتی پایگاه‌داده را ارتقا داد.

ب) بهبود راه‌بردهای اعتبارسنجی روش‌های تشخیص نفوذ

ج) بهبود عملکرد سیستم‌های تشخیص نفوذ از طریق کاهش نرخ تشخیص اشتباه.

استفاده مناسب از روش‌های داده‌کاوی در تحلیل رفتارهای کاربران یا بروزرسانی مداوم فهرست امضاهای حمله پایگاه‌داده با استفاده از پایگاه‌های ثبت آسیب‌پذیری مانند exploit-db.com و cvedetails.com.

د) توسعه سامانه‌های تشخیص نفوذ مانند ارتباط هشدارهای سامانه با مدیر.

با استفاده از هوشمندسازی هشدارهای سامانه تشخیص نفوذ و عدم دخالت مستقیم با مدیر مگر در مواقع ضروری می‌تواند به‌عنوان یکی از زمینه‌های ادامه پژوهش‌های سامانه تشخیص نفوذ پایگاه‌داده مورد بررسی قرار گیرد.

ه) در کنارِ دقت بالای تشخیص، کاهش زمان تشخیص در سامانه‌های تشخیص نفوذ پایگاه‌داده می‌تواند مورد بررسی پژوهش‌گران این حوزه قرار گیرد.

۶- نتیجه‌گیری

با توجه به اینکه حساسیت داده‌ها در زندگی روزمره و سازمان‌ها روزبه‌روز افزایش می‌آبد حفظ امنیت این داده‌ها به امری حیاتی در دنیای امروز تبدیل شده است. سامانه‌های تشخیص نفوذ، می‌تواند سازوکار بسیار مناسبی به‌منظور حفظ امنیت این داده‌ها از طریق تشخیص حملات سایبری باشد. سامانه‌های تشخیص نفوذ در سه دسته، سامانه‌های تشخیص نفوذ مبتنی بر میزبان، سامانه‌های تشخیص نفوذ مبتنی بر شبکه و سامانه‌های تشخیص نفوذ پایگاه داده‌ها قرار می‌گیرند. با توجه به اینکه داده‌ها در پایگاه‌داده ذخیره می‌شود، پس پایگاه داده همواره هدف جذابی برای مهاجمان است؛ بنابراین تصمیم گرفتیم در این مقاله به بررسی سامانه‌های تشخیص نفوذ پایگاه داده‌ها بپردازیم. در این پژوهش، ما با بررسی ۲۱ مقاله در زمینه تشخیص نفوذ پایگاه داده یک مرور کلی از روش‌های تشخیص نفوذ در پایگاه‌داده ارائه و سپس این مقاله‌ها در دو دسته کلی مبتنی بر امضا و مبتنی بر رفتار طبقه‌بندی و سپس در دسته مبتنی بر رفتار براساس

ویژگی‌های، تحلیل وابستگی داده‌ها، تجزیه‌وتحلیل ترتیب توالی، تجزیه‌وتحلیل زمانی، تشخیص فعالیت‌های مخرب در پایگاه داده با رویکرد لاگ‌کاوی، تشخیص نفوذ با استفاده از امضای تراکنش‌ها و رفتار کاربران، مقاله‌ها را به پنج زیردسته طبقه‌بندی کردیم.

۷- مراجع

[1] J.Shelton, and I. Vorobyeva, *an Effective Log Mining Approach for Database Intrusion Detection*, 2018.

[2] T. Hamed, J.B. Ernst, and S. C. Kremer, "A Survey and Taxonomy of Classifiers of Intrusion Detection System," In *Computer and Network Security Essentials*, Springer. Cham, 2018, pp. 21-39.

[3] E.Kabir, J.Hu, H.Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," *Future Generation Computer Systems*, no.79, pp.303-318, 2018.

[4] F.Y.Leu, K. L Tsai, Y. T. Hsiao, and C.T. Yang, "An internal intrusion detection and protection system by using data mining and forensic techniques," *IEEE Systems Journal*, no.11 (2), pp.427-438.2017.

[5] A. L.Buczak, and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, No.18 (2), pp.1153-1176, 2016.

[6] G.RajeshKumar, N.Mangathayaru, and G. Narsimha, *Intrusion detection a text mining based approach*, arXiv preprint arXiv: 1603.03837, 2016.

[7] J.Peng, K.K.R. Choo, and H.Ashman, "User profiling in intrusion detection," A review, *Journal of Network and Computer Applications*, No.*72*, pp.14-27, 2016.

[8] R.Wankhede, and V. Chole, "Intrusion detection system using classification technique," *International Journal of Computer Applications*, vol.*139* (11), 2016.

[9] E.Vasilomanolakis, S.Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Computing Surveys (CSUR)*, Vol.*47* (4), No.55, 2015.

[10] A.Chakraborty, A.K.Majumdar, and S. Sural, "A column dependency-based approach for static and dynamic recovery of databases from malicious transactions," *International Journal of Information Security*, Vol.*9* (1), pp.51-67, 2010.

[11] C.Y. Chung, M.Gertz, and K. Levitt, "Demids: A misuse detection system for database systems," In *Integrity and Internal Control in Information Systems* , M.A. theses. pp. 159-178, Springer. Boston,.2000.

[12] S.Y. Lee, W.L. Low, and P.Y. Wong, "Learning fingerprints for a database intrusion detection system," In *European Symposium on Research in Computer Security* , Berlin: Springer. Heidelberg, 2002, pp. 264-279.

[13] A. Kamra, and E. Bertino, "Design and implementation of an intrusion response system for relational databases," *IEEE transactions on knowledge and data engineering*, Vol.*23* (6), pp.875-888, 2011.

[14] A. Kamra, E. Bertino,and E.Terzi, "Detecting Anomalous Access Patterns in Relational Databases," *Springer VLDB Journal,* No.17, 2008.

[15] A. Kundu, S. Sural, and A. K. Majumdar, "Database intrusion detection using sequence alignment," *International Journal of information security*, Vol.9(3), pp.179-191, 2010.

[16] S.Mathew, M.Petropoulos, H.Q. Ngo,and S.Upadhyaya, "A data-centric approach to insider attack detection in database systems," In *International Workshop on Recent Advances in Intrusion Detection* , Berlin: Springer, Heidelberg, 2010, pp. 382-401.

[17] ذبیح زاده خواجوی، داود و محمدرضا کنگاوری، ۱۳۸۴، تشخیص نفوذ در پایگاه داده با استفاده از تحلیل وابستگی بین داده ها، *یازدهمین کنفرانس سالانه انجمن کامپیوتر ایران*، تهران، انجمن کامپیوتر ایران، مرکز تحقیقات فیزیک نظری و مخابرات

[18] J.Ng, D.Joshi, and S.M. Banik , "Applying data mining techniques to intrusion detection," In *Information Technology-New Generations (ITNG), 2015 12th International Conference,*2015,pp. 800-801.

[19] L.M. brahim, D.T.Basheer, and M.S. Mahmod, "A comparison study for intrusion database (Kdd99, Nsl-Kdd) based on self organization map (SOM) artificial neural network," *Journal of Engineering Science and Technology*, Vol.*8*(1), pp.107-119, 2013.

[20] U.P. Rao, N.K. Singh, A.R. Amin, and K. Sahu, "Enhancing detection rate in database intrusion detection system," In *Science and Information Conference (SAI),* 2014, pp. 556-563, IEEE.

[21] R. J. Santos, J. Bernardino, and M. Vieira, "Approaches and challenges in database intrusion detection," *ACM SIGMOD Record*, Vol. 43(3), pp.36-47,2014.

جواد مرادی درجه کارشناسی خود را در سال ۱۳۹۴ از دانشگاه رازی کرمانشاه و درجه کارشناسی ارشد خود را در سال ۱۳۹۷ از دانشگاه جامع امام حسین (ع) اخذ کرد. سامانه‌های تشخیص نفوذ در پایگاه داده، سامانه‌های تشخیص نفوذ در شبکه‌های رایانه‌ای، امنیت و حریم خصوصی در وب از جمله زمینه‌های پژوهشی ایشان است.

مجید غیوری درجه دکترای خود را در دانشگاه علم و صنعت اخذ کرد. ایشان در حال حاضر دانشیار دانشکده فناوری اطلاعات و ارتباطات دانشگاه جامع امام حسین (ع) هستند. سامانه‌های تشخیص نفوذ در شبکه‌های رایانه‌ای، سامانه‌های تشخیص نفوذ در پایگاه داده، مدل‌سازی امنیت با استفاده از داده‌کاوی، بررسی مناقشات سایبری با استفاده از نظریه بازی‌ها از جمله زمینه‌های پژوهشی ایشان است.