یک چارچوب کنترل دسترسی برای سامانه‌های بر پایه پایگاه داده

پیام محمودی نصر

دانشگاه مازندران، دانشکده مهندسی و فناوری، گروه مهندسی کامپیوتر و فناوری اطلاعات

چکیده

حمله به پایگاه داده در یک سامانه نرم‌افزاری می‌تواند آسیب‌های جبران‌ناپذیر به‌همراه داشته‌باشد. این حمله ممکن است در اشکال متفاوتی مانند سرقت داده، جعل داده و یا نقض حریم خصوصی نمایان شود. گستردگی این حمله، با توجه به کاربرد داده ذخیره‌شده، می‌تواند منجر به ایجاد خسارت‌های جانی و مالی فراوانی حتی در سطح ملی شود. از آنجایی که کاربران قانونی نقش کلیدی در تأمین امنیت پایگاه داده دارند، یکی از تهدیدهای خطرناک پایگاه داده حمله کاربران قانونی است. این حمله هنگامی به‌وجود می‌آید که کاربر خودی با سوءاستفاده از مجوزهای قانونی تلاش برای استفاده غیرمجاز از داده‌ها داشته‌باشد. در این مقاله یک چارچوب کنترل دسترسی بر پایه کارایی برای کاهش تهدید کاربران خودی ارائه‌شده است. در این چارچوب سطح دسترسی کاربر به جدول پایگاه داده با توجه به مقدار کارایی وی و سطح حساسیت جدول تعیین می‌شود. مقدار کارایی کاربر در فواصل زمانی معین و یا هنگام تشخیص سوءاستفاده به‌روزرسانی می‌شود. نتایج شبیه‌سازی با به‌کارگیری داده‌های واقعی از یک سامانهٔ اطلاعات بیمارستانی نشان می‌دهد که چارچوب پیشنهادی از کارایی مناسبی برخوردار است.

واژگان کلیدی: امنیت سایبری، پایگاه داده، تهدید خودی، دیده‌بانی، کنترل دسترسی.

An Access Control Framework for Database Systems

Payam Mahmoudi-Nasr

Department of Computer Engineering and Information Technology, University of Mazandaran, Mazandaran, Iran

Abstract

The use of database-based systems has expanded to all kinds of software systems. The range of database usage can be expressed from critical infrastructures such as power systems to application software on mobile phones. In a database system, attacking data can cause severe damage. The attack may carried out in various ways, such as data theft, damaging data, and privacy breach. According to the sensitivity of the stored data, database attack could lead to significant financial losses even at the national level. Since legitimate operator plays a key role in a database system, his/her threat is one of the most dangerous threats to the security and integrity of a database system. This type of cyber-attack occurs when an insider operator abuses his/her legal permissions in order to access unauthorized data. In this paper, a new performance-based access control framework has been presented which is able to reduce the potential of insider threat in the database system. In the proposed framework, the access permission of the operator to a database table is determined using his/her performance and the level of sensitivity of the table. The operator's past performance is also used to calculate his/her current performance value. In addition, if the operator makes an unintentional mistake, he/she is given the opportunity to compensate. The operator's performance is calculated based on his ability to use and not abuse the permissions. The value of the operator performance is updated at periodic intervals or when an abuse is detected. The sensitivity level of each permission is proportional to the type of request and the sensitivity level of the table for which the permission is assigned. Simulation results, using real dataset from a hospital information system, indicate that the proposed framework has effective performance for mitigating insider threats.

Keywords: Access control, cyber security, database system, insider threat.

* **Corresponding author**

* نویسندهٔ عهده‌دار مکاتبات

• **تاریخ ارسال مقاله:** ۱۳۹۹/۵/۲۳ • **تاریخ پذیرش:** ۱۴۰۰/۹/۲۰ • **تاریخ انتشار:** ۱۴۰۱/۱۲/۲۹ • **نوع مطالعه:** پژوهشی

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]

۱- مقدمه

داده‌ها و به طبع آن پایگاه داده‌ها نقش عمده‌ای در زندگی امروز نوع بشر ایفا می‌کنند. این نقش به حدی پراهمیت است که کمتر برنامه کاربردی را می‌توان پیدا کرد که از پایگاه داده استفاده نکند. گستره به‌کارگیری سامانه‌های برپایه پایگاه داده در انواع سامانه‌های نرم‌افزاری؛ از زیرساخت‌های حیاتی مانند صنایع برق، نفت، گاز گرفته تا برنامه‌های کاربردی بر روی گوشی همراه؛ گواه بر جایگاه کلیدی پایگاه داده است.

حمله به یک پایگاه داده در یک سامانه نرم‌افزاری، با توجه به درجه محرمانگی داده‌های ذخیره‌شده در آن، ممکن است منجر به ایجاد خسارت‌های جبران‌ناپذیر شود [1] (برای نمونه حمله به سامانه‌های بانکی). از این روی تأمین امنیت سایبری سامانه‌های نرم‌افزاری بر پایه پایگاه داده نقش عمده‌ای در تأمین امنیت ملی هر کشوری خواهد داشت. این در حالی است که شاهد رشد روزافزون تعداد و انواع حملات سایبری بر روی سامانه‌های نرم‌افزاری هستیم.

یکی از تهدیدهای خطرناک در سامانه‌های نرم‌افزاری، تهدید کاربران خودی[1] است. این تهدید زمانی به‌وجود می‌آید که کاربر قانونی، با سوءاستفاده از مجوزهایی که در اختیار دارد موجب ایجاد نتیجه‌ای غیرقانونی در سامانه می‌گردد. بنا بر گزارش [2] در سال ۲۰۱۳، حملات خودی سهم ۳۴ ٪ را در بین انواع حملات به خود اختصاص داده‌اند. این در حالی است که جلوگیری و تشخیص حملات خودی نسبت به حملات بیگانه[2] بسیار مشکل‌تر است[3].

یکی از انواع تهدیدهای خودی در یک سامانه نرم‌افزاری بر پایه پایگاه داده که از کنترل دسترسی نقش مبنا[3] برای دسترسی به داده‌ها استفاده می‌کند، سوءاستفاده از مجوزها برای دسترسی به داده‌های حساس است[4]. هنگامی که مدیر سامانه نقش یک کاربر را در سامانه تعیین می‌کند، مجوزهای دسترسی به داده‌ها برای وی فراهم می‌گردد. اما نکته دارای اهمیت از نظر امنیت سایبری آن است که تمامی کاربرانی که دارای یک نقش هستند دارای عملکرد و کارایی[4] یکسان نمی‌باشند [5]. این اختلاف کارایی می‌تواند به‌دلایل گوناگونی باشد از جمله سطح تحصیلات، تجربه کاری، میزان علاقه، اختلاف سنی،... و حتی تفاوت‌های شخصیتی. از آنجایی که تعداد نقش‌ها در یک سامانه نرم‌افزاری محدود است و مدیر سامانه نمی‌تواند با توجه به خصوصیات فردی هر کاربر نقش جدیدی برای وی تعریف کند؛ لذا همواره این اختلاف کارایی در بین کاربرانی که دارای یک نقش هستند وجود خواهد داشت. در چنین شرایطی این احتمال همواره وجود دارد که کاربر با کارایی کمتر با ارسال دستور قانونی اشتباه *(غیرعمدی)* وظایف خود را به‌درستی انجام نداده و در پی دسترسی به برخی از داده‌های حساس باشد. همچنین، این در حالی است که امکان *سوءاستفاده عمدی* از مجوزها نیز برای دسترسی به داده‌های حساس همواره برای تمامی کاربران وجود دارد.

در این مقاله یک چارچوب کنترل دسترسی برپایه کارایی کاربر به‌منظور کاهش تهدیدهای خودی در سامانه‌های نرم‌افزاری بر پایه پایگاه داده ارائه‌شده است. در این چارچوب فرض بر آن است که با تعیین سطح کارایی کاربر در استفاده مجاز از منابع پایگاه داده، از میزان تهدیدهای خودی کاسته خواهد شد. بدین ترتیب که هرچه سطح کارایی کاربر بیشتر باشد اجازه به‌کارگیری مجوزهای دسترسیِ بیشتری (در محدوده نقشی که به وی اختصاص داده شده) برای وی فراهم می‌گردد. چنانچه کاربر با سوءاستفاده از مجوزها به داده‌های حساس دسترسی پیدا کند، چارچوب پیشنهادی متناسب با مقدار سوءاستفاده کاربر از دسترسی وی به مجوزهای قانونی در محدوده نقش اختصاص داده‌شده به وی جلوگیری به‌عمل می‌آورد. در این چارچوب برای هر یک از جداول پایگاه داده یک درجه حساسیت، به‌عنوان حد آستانه برای دسترسی به داده‌های آن جدول، محاسبه و تعیین می‌گردد. کاربر به شرطی به داده‌های یک جدول دسترسی خواهد داشت که سطح کارایی وی از سطح حساسیت جدول بیشتر باشد.

برای محاسبه درجه حساسیت جدول از ویژگی‌های آن، و برای محاسبه سطح کارایی کاربر، از میزان سوءاستفاده وی به‌عنوان یک مقدار منفی استفاده شده‌است. سطح کارایی کاربر در فواصل زمانی مشخص (به‌عنوان بازرسی) و یا درمواقع اضطراری (هنگام شناسایی سوءاستفاده)، به‌روزرسانی می‌شود. به‌اختصار نوآوری این مقاله عبارت است از:

۱- ارائه راه‌کاری کارآمد برای تعیین درجه حساسیت جداول در یک پایگاه داده.

[1] Insider threat
[3] Outsider attack
[4] Role Base Access Control (RBAC)
[4] Performance

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]
[DOI: 10.61186/jsdp.19.4.61]

۲- ارائه روشی جدید برای محاسبه کارایی کاربر در یک سامانه نرم‌افزاری بر پایه پایگاه داده.

۳- ارائه یک چارچوب کنترل دسترسی برای کاهش تهدیدهای خودی در سامانه‌های نرم‌افزاری بر پایه پایگاه داده بر پایه سطح کارایی کاربر و درجه حساسیت منابع پایگاه داده. در این مقاله برای نخستین‌بار از مقدار کارایی کاربر و درجه حساسیت جداول برای تعیین مجوزهای دسترسی به جداول پایگاه داده استفاده‌شده است.

این مقاله به‌صورت زیر ادامه داده‌می‌شود. بخش دوم مقاله به‌مرور پژوهش‌های پیشین می‌پردازد. در بخش سوم بحث‌های مقدماتی شامل مدل کنترل دسترسی نقش مبنا و تهدیدهای خودی بررسی‌شده‌اند. چارچوب پیشنهادی برای کنترل دسترسی کاربر پایگاه داده در بخش چهارم ارائه می‌شود. بخش پنجم نحوه ارزیابی و نتایج شبیه‌سازی را نشان‌می‌دهد. در بخش ششم نتایج حاصل از این مقاله آورده شده‌است.

۲- پژوهش‌های پیشین

ایوان هومولیاک و همکاران در [6] پس از ارائه تعریفی دقیق از حملات خودی، انواع آن را از منظر محل حمله، علت حمله، زمان حمله، مورد حمله، و مهاجم مورد بررسی قرار داده‌اند. آنها همچنین مجموعه داده‌های رایج برای استفاده در پژوهش‌های مربوط به حملات خودی را معرفی و مورد ارزیابی قرار داده و سپس مهاجمان را به‌لحاظ رفتاری، روان‌شناسی فردی، و روان‌شناسی اجتماعی مورد آنالیز و تجزیه و تحلیل قرارداده‌اند. لیو لیو و همکاران [7] مقاله‌ای مروری بر روی پژوهش‌هایی که تاکنون برای شناسایی و جلوگیری از تهدیدهای خودی انجام‌شده ارائه کرده‌اند. کیوجیانگ و همکاران در [8] روش‌های شناسایی تهدیدهای خودی را به پنج گروه دسته‌بندی کرده‌اند: ۱) مدل‌های بر پایه قصد و نیت، ۲) مدل‌های بر پایه رفتار کاربر، ۳) مدل‌های بر پایه رفتار نقش کاربر، ۴) مدل‌های بر پایه توانایی کاربر، و ۵) مدل‌های ترکیبی. از بین این پنج گروه تمرکز اصلی بر روی روش‌های مبتنی بر رفتار کاربر و نقش کاربر است. در روش مبتنی بر رفتار کاربر، ابتدا ویژگی‌های رفتار عادی کاربر شناسایی شده تا بدین وسیله هرگونه تخطی از رفتار عادی به‌عنوان تهدید شناسایی شود. برای نمونه پراتیک چاتوپاتریاک و همکاران در [9] یک روش بر پایه یادگیری ماشین برای شناسایی تهدیدهای خودی ارائه کرده‌اند. در این روش ابتدا ویژگی‌های رفتاری کاربر با به‌کارگیری داده‌های موجود در فایل ثبت وقایع و الگوریتم‌های سری زمانی استخراج شده و سپس با به‌کارگیری شبکه‌های عصبی دسته‌بندی می‌شوند. نویسندگان در این مقاله نشان داده‌اند که روش پیشنهادی آنها می‌تواند نسبت به الگوریتم دسته‌بندی جنگل تصادفی بهتر عمل کند.

در مدل‌های بر پایه رفتار نقش کاربر، تلاش برای به‌دست‌آوردن الگوی رفتاری کاربرانی است که همگی دارای یک نقش هستند. بدین ترتیب هرگونه رفتاری خارج از الگوی گروهی به‌عنوان تهدید شناسایی می‌شود. پژوهش‌هایی که در این زمینه انجام شده نسبت به الگوی قبلی از تعداد کمتری برخوردار است. بری مثال اسلام و همکاران [10] با به‌کارگیری مدل مارکوف مخفی روش برای شناسایی تهدیدهای خودی در پایگاه داده‌های رابطه‌ای ارائه کرده‌اند.

در روش‌های بر پایه قصد و نیت کاربر، درحقیقت به‌جای توجه به شخصیت کاربر به چرایی و علت درخواست کاربر توجه کرده می‌شود. عبدالعزیز المهمادی و همکاران [11] روشی نقش مبنا بر پایه قصد و نیت کاربر برای جلوگیری از تهدیدهای خودی ارائه کرده‌اند. در این روش نیت کاربر با به‌کارگیری آنالیز سیگنال‌های مغزی و یک پایگاه دانش استخراج می‌شود. از آنجایی که شرایط آنالیز سیگنال‌های مغزی کاربر در همه شرایط امکان‌پذیر نیست؛ لذا روش پیشنهادی در موارد محدودی قابل استفاده است.

به‌کارگیری روش‌های کنترل دسترسی روشی مناسب برای جلوگیری از تهدیدهای خودی است. از این روی پژوهش‌های فراوانی برای به‌کارگیری مدل‌های کنترل دسترسی در زمینه‌های مختلف تاکنون انجام شده‌است. برای نمونه لوسیانو آرگنتو و همکاران یک مدل کنترل دسترسی تطبیقی در [12] ارائه کرده‌اند. این مدل قوانین کنترل دسترسی موجود در سامانه را (که برپایه ویژگی‌های کاربران و منابع است) بر اساس الگوریتم‌های یادگیری ماشین پالایش می‌کند. امینی و همکاران [13] یک مدل کنترل دسترسی پویا با حفظ حریم خصوصی و قابلیت وکالت دسترسی در حوزه سلامت الکترونیک ارائه کرده‌اند. در این مدل موارد مختلفی از جمله دسترسی پزشک به پرونده بیمار با توجه به موقعیت فیزیکی وی، شرایط اضطراری و اعطای حقوق دسترسی موقتی به پزشک حاضر، حفظ حریم خصوصی بیمار، و اعطای وکالت دسترسی به پزشک دیگر مورد مطالعه قرار گرفته است. محمودی و همکاران [14] یک سامانه مدیریت دسترسی

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]

را برای کاهش حملات خودی که منجر به تهدیدهای عملیاتی در سامانه اسکادا می‌شوند، ارائه کرده‌اند. در این سامانه حقوق دسترسی کاربران خودی متناسب با عملکرد عملیاتی در شبکه قدرت تنظیم می‌شود. چنانچه کاربر با ارسال دستور اشتباه عمدی یا غیرعمدی منجر به ایجاد نتیجه اشتباه در شبکه شود، از دسترسی وی به تجهیزات شبکه کاسته می‌شود. مناچای و همکاران [15] یک مدل کنترل دسترسی بر پایه اعتماد در محاسبات فراگیر ارائه کرده‌اند. در این پژوهش نویسندگان مقدار اعتماد اپراتور را بر اساس پارامترهای مشخصات فردی، میزان تجربه، و توصیه نامه‌های اپراتور محاسبه کرده‌اند. از آنجایی که تنها میزان تجربیات اپراتور در طول زمان تغییر می‌کند؛ لذا پویایی مقدار اعتماد محاسبه‌شده تنها وابسته به مقدار تجربه اپراتور است و دو پارامتر دیگر به‌صورت ایستا عمل می کنند. باراکالدو و همکاران [16] یک چارچوب کنترل دسترسی مبتنی بر مدیریت ریسک و اعتماد اپراتور برای کاهش تهدیدهای خودی ارائه کرده‌اند. در این چارچوب برای هر یک از مجوزها و اپراتورها به‌ترتیب مقداری از ریسک و اعتماد محاسبه می‌شود. در ادامه هر اپراتور تنها نقشی را می‌تواند فعال کند که حد آستانه ریسک آن از اعتماد کاربر کمتر باشد. حد آستانه ریسک یک نقش از مجموع ریسک مجوزهای نقش محاسبه می‌شود. اگر کاربر بتواند برای دسترسی به مجوزها از نقش‌های متفاوتی استفاده کند، در این‌صورت نقشی که کمترین ریسک را دارد، برای وی انتخاب خواهد شد.

۳- پیش‌زمینه

۳-۱-کنترل دسترسی نقش مبنا

در مدل کنترل دسترسی نقش مبنا [17]، نقش‌ها به کاربران، و مجوزهای دسترسی به نقش‌ها نسبت داده می‌شوند. بدین ترتیب هر کاربر می‌تواند دارای چندین نقش و هر نقش می‌تواند شامل چندین مجوز باشد. هر کاربر می‌تواند در هر جلسه کاری[1] تعدادی از نقش‌هایی که پیشتر به وی اختصاص داده شده را فعال نماید.

در مدل کنترل دسترسی نقش مبنا، نقش‌ها می‌توانند به‌صورت سلسله‌مراتبی تعریف شوند. در این صورت نقش‌ها مجوزهای دسترسی را از یکدیگر ارث‌بری می‌کنند. در این مدل کاربران نمی‌توانند مجوزهای دسترسی خود را با صلاحدید خود به دیگران منتقل کنند.

۳-۲- تهدیدهای خودی

تهدیدهای هر سامانه‌های نرم‌افزاری را می‌توان به دو دسته تهدیدهای غیرخودی (بیگانه) و خودی (داخلی) تقسیم کرد. تهدیدهای غیرخودی توسط کاربران خارج از سامانه (مانند تهدید هکرها) و به‌طور غیرمجاز انجام‌می‌شود. تهدیدهای خودی با سوءاستفاده از مجوزهای قانونی و توسط کاربران داخل سامانه انجام‌می‌شود [18]. اگرچه ممکن است تعداد تهدیدهای خودی کمتر از تعداد تهدیدهای غیرخودی باشد اما میزان موفقیت و آسیب آن‌ها به‌مراتب جدی‌تر و بیشتر از تهدیدهای غیرخودی است [19]. این امر به‌دلیل آن است که کاربران خودی (۱) از سامانه‌های کامپیوتری و نرم‌افزاری سازمان خود دانش کافی دارند و (۲) از قوانین و چارچوب‌های امنیتی لحاظ شده در سازمان آگاهی دارند.

تهدیدهای داده‌های ذخیره‌شده در پایگاه داده یکی از انواع تهدیدهای خودی در سامانه‌های نرم‌افزاری است. این تهدید می‌تواند هنگامی رخ دهد که کاربر با سوءاستفاده از مجوزهای قانونی اقدام به ارسال یک دستور پایگاهی کرده، درحالی‌که دستور صادره شده خارج از دستورهای معمول وی (برپایهٔ اطلاعات فایل ثبت تراکنش‌ها در پایگاه داده) برای انجام وظایف سازمانی است [20]. برای نمونه کاربری که اجازه بازیابی داده‌ها از یک جدول را دارد اقدام به درج داده‌های جدید در آن جدول می‌کند. این در حالی است که بر اساس فایل ثبت تراکنش‌ها درج داده‌ها در فهرست دستورهای ارسالی برای انجام وظایف قانونی نیست. در مثالی دیگر حالتی را فرض کنید که یک کاربر به داده‌های چند جدول دسترسی دارد. این کاربر ممکن است با به‌کارگیری دانشی که کسب کرده اقدام به تهیه گزارشی از ترکیب داده‌های چند جدول نماید که خارج از وظایف سازمانی وی است. بر این اساس تهدیدهای خودی در پایگاه داده را می‌توان به‌صورت زیر دسته‌بندی کرد:

(۱) دسترسی به مقادیر ستون‌های غیرمجاز (خارج از وظایف سازمانی) از یک یا چند جدول.

(۲) دسترسی به داده‌های ترکیبی از اتصال مجاز ستون‌های چند جدول.

(۳) ارسال دستور پایگاهی خارج از وظایف سازمانی برای منابع پایگاهی.

۴- چارچوب کنترل دسترسی پیشنهادی

در این بخش یک چارچوب کنترل دسترسی بر پایه کارایی به‌منظور تعیین سطح دسترسی کاربر به منابع پایگاه داده

[1] Session

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]

جدول، دید[1]، رویه[2]) ارائه خواهد شد. هدف این چارچوب کاهش دسترسی کاربر مهاجم (سوءاستفاده عمدی و یا غیرعمدی) به منابع پایگاه داده بر اساس سطح اهمیت منابع است. در این چارچوب هنگامی کاربر مجوز دسترسی به یک منبع را دارد که میانگین مقدار کارایی وی در بازه‌های زمانی ($Perf_u \in [0,1]$) از سطح اهمیت منبع درخواستی ($ST_i^{Rel} \in [0,1]$) بیشتر باشد.

در این چارچوب پس از محاسبه کارایی کاربر در یک بازه زمانی O مقدار میانگین کارایی با توجه به سابقه وی محاسبه می‌گردد. چنانچه $Perf_u = 0$ باشد، کاربر از حداقل کارایی و هنگامی‌که $Perf_u = 1$ کاربر از بیشینه کارایی برخوردار است و می‌تواند به‌تمامی منابع در محدوده تحت مسئولیت خود دسترسی داشته‌باشد. فرض بر این است که منابع تحت مسئولیت کاربر درقبل توسط کاربر ارشد تعیین‌شده است. مقدار کارایی اولیه کاربر برابر با یک فرض شده‌است. بدین ترتیب کاربر به‌تمامی منابع تحت مسئولیت خود در ابتدا دسترسی دارد.

شکل (۱) ساختار چارچوب پیشنهادی را نشان‌می‌دهد. واحد *محاسبه کارایی* وظیفه تعیین مقدار کارایی کاربر را به عهده دارد. مقدار کارایی کاربر با توجه به سوءاستفاده کاربر از مجوزهای مجاز محاسبه می‌شود. واحد محاسبه *حساسیت جدول* وظیفه محاسبه اهمیت هر جدول را با توجه به ویژگی‌های جدول دارد. هرگاه واحد *تشخیص سوءاستفاده* یک سوءاستفاده از مجوزها را شناسایی کند، آن را به واحد *محاسبه مقدار سوءاستفاده* و واحد محاسبه کارایی اعلام کرده تا مقدار کارایی کاربر به‌روزرسانی شود. مقدار کارایی کاربر به‌تناوب در فواصل زمانی معین و یا هنگام تشخیص سوءاستفاده به‌روزرسانی می‌شود. واحد *درخواست تراکنش*، وظیفه دریافت درخواست کاربر به منابع پایگاه داده را داشته و آن را برای واحد *تصمیم‌گیری تراکنش* ارسال می‌کند. این واحد درخواست موردنظر را با توجه به مقدار کارایی کاربر و سطح دسترسی مورد تقاضا، بررسی و نتیجه را در غالب اجازه و یا عدم اجازه دسترسی به کاربر اعلام می‌کند. واحد *محاسبه حساسیت مجوز* وظیفه تعیین مقدار حساسیت مجوز را با توجه به نوع مجوز دارد. شکل (۲) روند اختصاص و تعیین مجوزهای کاربر را هنگام ورود به سامانه نمایش می‌دهد.

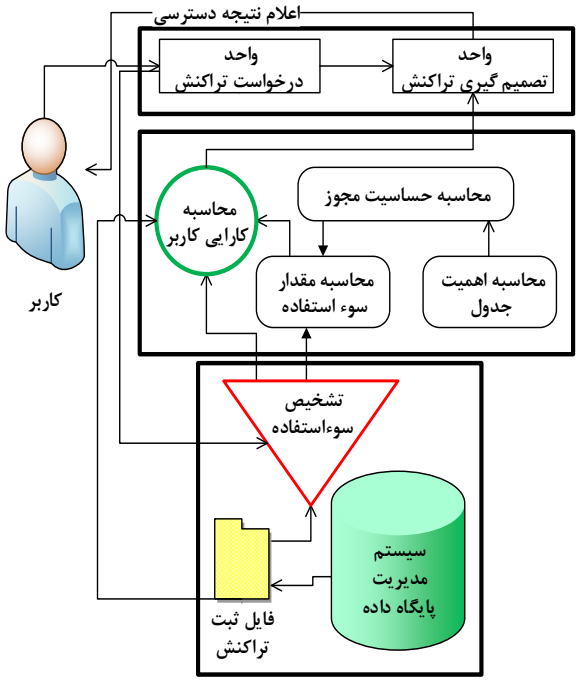
۴-۱- تعیین سطح حساسیت جدول

در این مقاله روشی جدید بر اساس ویژگی‌های جدول (مانند درجه محرمانگی داده‌ها، تعداد شاخص‌های جدول، تعداد ستون‌های هیچ مقدار[3] پذیر، و نرخ پویایی جدول) برای تعیین سطح حساسیت جدول ارائه‌شده است. فرض کنید، مجموعه $\{p_1, p_2, ..., p_k\}$ شامل ویژگی‌های جدول و $w_k^{Tab} \in [0,1]$ مقدار وزن ویژگی p_k و I تعداد جدول‌ها باشد. چنانچه $g_{ik} \in [0,1]$ امتیاز کسب‌شده جدول iام برای ویژگی p_k باشد، سطح حساسیت یک جدول با به‌کارگیری رابطه زیر محاسبه خواهد شد:

$$ST_i^{Abs} = \sum_{k=1}^{K} w_k^{Tab} g_{ik} \qquad (۱) \quad ST^{Max} = \max_{1 \le i \le I} ST_i^{Abs} \qquad (۲)$$

$$ST_i^{Rel} = \frac{ST_i^{Abs}}{ST^{Max}} \qquad (۳)$$

در این رابطه ST_i^{Rel} عبارت است از نسبت حساسیت کسب‌شده جدول iام به حداکثر حساسیت کسب‌شده جدول‌ها در پایگاه داده.



شکل (۱): مدل کلی چارچوب پیشنهادی
(Figure 1): The proposed framework architecture.

۴-۲- تعیین سطح حساسیت مجوز

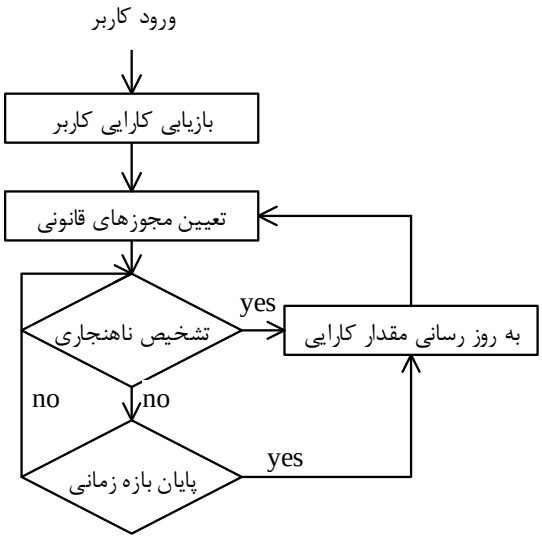
سطح حساسیت هر مجوز متناسب با نوع مجوز (بازیابی رکورد، حذف رکورد، به‌روزرسانی رکورد، ایجاد رکورد جدید) و سطح حساسیت جدولی است که مجوز برای آن تعیین می‌گردد. فرض کنید مجوزها به J نوع تقسیم‌شده باشند. چنانچه $w_j^{Per} \in [0,1]$ وزن مجوز jام باشد سطح حساسیت مجوز jام از جدول iام به‌صورت زیر محاسبه خواهد شد.

[3] View
[4] Procedure

[2] Null

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]
[DOI: 10.61186/jsdp.19.4.61]

$$SP_{ij} = ST_i^{Rel}.w_j^{Per} \quad (۴)$$



شکل (۲): تعیین مجوزهای کاربر هنگام ورود به سامانه
(Figure 2): Privileg
when logging into system e assignment

۴-۳- تشخیص سوءاستفاده

برای تشخیص سوءاستفاده ضروری است تا رفتار عادی کاربر هنگام به‌کارگیری جداول پایگاه داده تعیین شده و برپایهٔ آن، هرگونه دسترسی غیرعادی به جداول به‌عنوان سوءاستفاده از داده‌ها به چارچوب پیشنهادی اعلام شود. جزئیات نحوه تعیین رفتار عادی کاربر و تشخیص سوءاستفاده، خارج از محدوده این مقاله است. برای این منظور می‌توان از روش‌های پیشنهادی در [21] و [20] استفاده‌کرد.

۴-۴- محاسبه مقدار سوءاستفاده

هرگونه عملیات غیرمجاز در پایگاه داده (که به‌عنوان سوءاستفاده در چارچوب تشخیص داده شده باشد)، شامل مجموعه‌ای از مجوزهای دسترسی است. بر این پایه چنانچه در بازه زمانی O (بازرسی دوره‌ای) مجوز $j \in [1, N]$ ام جدول $i \in [1, M]$ ام مورد سوءاستفاده قرار گرفته باشد، مجموع مقدار سوءاستفاده را می‌توان به‌صورت زیر محاسبه کرد:

$$S_o^{MisUse} = \sum_{i=1}^{M}\sum_{j=1}^{N} SP_{ij} \quad (۵)$$

۴-۵- محاسبه مقدار کارایی

در چارچوب پیشنهادی برای محاسبه مقدار کارایی راهکاری ارائه شده‌است تا (۱) چنانچه به‌علت اشتباه غیرعمدی سوءاستفاده‌ای تشخیص داده شده و درنتیجه از کارایی کاربر کاسته شده‌است، فرصت جبران (افزایش کارایی) به وی داده شود، (۲) علاوه‌بر کارایی جاری به سابقه کارایی کاربر نیز توجه شود.

در این چارچوب کارایی کاربر برپایهٔ توانایی وی در استفاده مجاز از مجوزها و عدم سوءاستفاده از مجوزهای مجاز محاسبه می‌شود. در هر نوبتِ بازرسی از عملکرد کاربر، مجوزهای مجاز استفاده و سوءاستفاده‌شده کاربر مورد بررسی قرار می‌گیرند. فرض بر آن است که بازرسی‌ها در فواصل زمانی منظم و یا در مواقع اضطراری (هنگام تشخیص سوءاستفاده) انجام می‌شوند. فرض کنید در بازرسی O، S_o^{Use} و S_o^{MisUse} به‌ترتیب مقدار استفاده و سوءاستفاده از مجوزها باشند، در اینصورت مقدار کارایی کاربر با به‌کارگیری فرمول زیر محاسبه خواهد شد:

$$\begin{cases} Perf_o = 1 - \dfrac{S_o^{MisUse}}{S_o^{Use}} & ,if \quad S_o^{Use} \neq 0 \\ Perf_o = Perf_{o-1} & ,if \quad S_o^{Use} = 0 \end{cases} \quad (۶)$$

برای محاسبه S_O^{Use}، مشابه رابطه (۵)، چنانچه مجوز $j \in [1, J]$ ام جدول $i \in [1, I]$ ام مورد استفاده مجاز قرار گرفته باشد، به‌صورت زیر اقدام می‌کنیم.

$$S_o^{Use} = \sum_{i=1}^{I}\sum_{j=1}^{J} SP_{ij} \quad (۷)$$

بدین ترتیب چنانچه کاربر در بازه زمانی O هیچ عملی انجام نداده باشد، مقدار کارایی وی بدون تغییر معادل کارایی *O-1* باقی خواهد ماند، و در غیر این‌صورت چنانچه دارای سوءاستفاده نباشد، مقدار کارایی وی به مقدار بیشینه یعنی ۱ و درصورت سوءاستفاده به نسبت مقدار سوءاستفاده از مقدار ۱ کم خواهد شد.

به‌منظور درنظرگرفتن سابقه کارایی کاربر می‌توان از رابطه میانگین موزون متحرک نمایی[1] [22] به‌صورت زیر استفاده‌کرد:

$$Perf_u = (1-\beta).Perf_{u-1} + \beta.Perf_o \quad (۸)$$

در این رابطه $Perf_{u-1}$ میانگین وزنی کارایی‌های قبلی کاربر و $\beta \in [0,1]$ ضریب کارایی جاری وی است. چنانچه در این رابطه از دو مقدار متفاوت برای β استفاده شود $(\beta_1 < \beta_2)$، دراین‌صورت امکان جریمه کاربر هنگام مشاهده سوءاستفاده وجود خواهد داشت. بدین ترتیب چنانچه هنگام مشاهده سوءاستفاده از مقدار β_2، و در غیر این صورت از مقدار β_1 استفاده گردد،

[1] Exponentially Weighted Moving Average (EWMA)

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]
[DOI: 10.61186/jsdp.19.4.61]

سرعت کاهش کارایی کاربر بیشتر از افزایش آن خواهد بود.

۴-۶- تصمیم گیری تراکنش

تصمیم‌گیری در مورد اجازه دسترسی کاربر به یک جدول بر اساس مقدار میانگین کارایی وی و سطح حساسیت جدول مورد تقاضا است. چانچه مقدار کارایی کاربر بیشتر از سطح حساسیت جدول باشد، دسترسی مجاز شناخته شده و در غیر این‌صورت از دسترسی کاربر جلوگیری به عمل می‌آید.

تصمیم‌گیری در مورد دسترسی به یک دید و یا اجرای یک رویه برپایهٔ مقدار میانگین کارایی کاربر متقاضی و سطح حساسیت جدول‌های مورد تقاضا بررسی می‌شود. از آنجایی که برای اجرای یک دید و یا رویه ممکن است، نیاز به دسترسی یک یا چند جدول باشد، ضروری است تا کاربر (۱) مجوز دسترسی به‌تمامی جداول مورد تقاضا را از پیش داشته و (۲) میانگین کارایی وی از سطح حساسیت هر یک از جداول مورد نیاز بیشتر باشد.

۵- راستی آزمایی و نتایج شبیه‌سازی

در این بخش به‌منظور آنالیز چارچوب پیشنهادی، دو سناریوی *حمله (سوءاستفاده)* و *جبران سوءاستفاده* از داده‌های پایگاه داده موردبررسی قرار گرفته‌اند. نتایج شبیه‌سازی و مجموعه‌دادهٔ استفاده‌شده برپایهٔ یک سامانهٔ اطلاعات بیمارستانی[1] است. مجموعه‌داده مورد استفاده اطلاعات فایل ثبت تراکنش‌های سامانهٔ مدیریت پایگاه داده MS SQL Server و شامل ۶۰۰۰ رکورد است. در این سامانه فرض بر آن است که دسترسی کاربران به جداول پایگاه داده پیشتر با به‌کارگیری مدل کنترل دسترسی RBAC مشخص شده‌است. بر این اساس موارد زیر درنظر گرفته‌شده‌اند:

- نقش‌های سیستم: پزشک، پرستار
- جداول سیستم:

```
PatientRecord {
        PID (PrimaryKey) (not Null) (Index),
        PName (not Null) (Index),
        PJob (not Null),
        PPhone (not Null) (Index),
        PAddress (not Null),
        PGender (not Null),
        PDescription
}
StaffRecord {
        SID (Primary Key) (not Null),
        SName (not Null) (Index),
        SResidency (not Null)
}
DrugRecord {
        DID (primary Key) (not Null) (Index),
        DName (not Null) (Index),
        DDescription
}
VisitRecord {
        VID (Primary Key) (not Null) (Index),
        DID (Foreign Key) (not Null) (Index),
        PID (Foreign Key) (not Null) (Index),
        DDate (not Null) (Index),
        VTime
}
MedicalRecord {
    MID (Primary Key) (not Null) (Index),
    VID (Foreign Key) (not Null) (Index),
    DID (Foreign Key) (not Null) (Index)
}
```

[1] Hospital Information System (HIS)

جدول (۱) مقادیر درنظرگرفته شده برای تعیین درجه محرمانگی داده‌های هر جدول، جدول (۲) وزن در نظر گرفته شده برای مجوزهای پایگاهی (w_j^{Per})، و جدول (۳) ویژگی‌های درنظرگرفته‌شده جهت ارزش‌گذاری درجه حساسیت جداول را نشان می‌دهد. در جدول (۴) نحوه محاسبه درجه حساسیت جدول‌های شبیه‌سازی‌شده با به‌کارگیری ویژگی‌های جدول (۳) و روابطه (۱) تا (۳) نشان داده شده‌است.

فرض‌هایی که در انجام سناریوها در نظر گرفته‌شده عبارت‌اند از: (۱) فاصله زمانی بازرسی‌ها یک‌هفته در نظر گرفته‌شده است. (۲) مقدار پارامتر در نظر گرفته‌شده عبارت است از: $\beta = 0.125$.

جدول(۱): درجه محرمانگی داده ها در جدول
(Table 2): The confidentiality level of data

محرمانگی	سری (HH)	خیلی محرمانه (H)	محرمانه (L)	عادی (LL)
مقدار	۱	۰/۷۵	۰/۵	۰/۲۵

جدول (۲): وزن مجوزهای پایگاهی
(Table 3): The weighting coefficient for database commands

عنوان	Select	Update	Delete	Insert
w_j^{Per}	۰/۷۵	۰/۷۵	۱	۱

جدول (۳): ویژگی‌های ارزش‌گذاری جهت تعیین درجه حساسیت جدول
(Table 3): Weighting criteria to determine the sensitivity level of table

p_k	w_k^{Tab}	توضیحات	معیار وزن دهی	g_{ik}
p_1	۰/۷۵	نرخ پویایی	=<روزانه	۱
			<روزانه	۰/۵
p_2	۱	محرمانگی داده‌ها	خیلی زیاد(HH)	۱
			زیاد(H)	۰/۷۵
			کم(L)	۰/۵
			خیلی کم(LL)	۰/۲۵
p_3	۰/۵	تعداد ستون‌های هیچ مقدار پذیر	همه ستون‌ها	۱
			در غیر این صورت	۰/۵
p_4	۰/۷۵	تعداد شاخص‌های	همه ستون‌ها	۱

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]
[DOI: 10.61186/jsdp.19.4.61]

		جستجو	درغیراینصورت	۰/۵

۵-۱- سناریوی حمله (سوءاستفاده)

به‌منظور آنکه نشان دهیم در سوءاستفاده‌هایی که توسط کاربران داخلی انجام‌می‌شود، چارچوب پیشنهادی چگونه قادر به شناسایی سوءاستفاده و کاهش دسترسی کاربر به جدول‌ها است، این سناریو موردمطالعه قرار گرفته است. از آنجایی که شبیه‌سازی انجام‌شده فاقد سامانهٔ تشخیص سوءاستفاده (در مقاله‌های دیگر به آن پرداخته شده‌است) است، مجموعه‌دادهٔ درنظرگرفته‌شده به‌نحوی تنظیم شده است که سوءاستفاده به آسانی شناسایی شود. در این سناریو کاربر پس‌ازآنکه مقدار کارایی اولیه‌اش به میزان حداکثر فرض شده‌است $Perf_u = 1$، اقدام به یک سوءاستفاده می‌کند. جدول (۵) سطح حساسیت هر یک از مجوزهای پایگاه داده را با توجه به مقادیر جداول (۲) و (۴) و رابطه (۴) نشان‌می‌دهد. با توجه به فایل مجموعه داده که منطبق با داده‌های واقعی از یک سامانهٔ بیمارستانی است، تعداد دفعات دسترسی انواع کاربران به جداول پایگاه داده مورد بررسی قرار گرفته است. همچنین به‌منظور آنکه نتایج شبیه‌سازی به داده‌های واقعی نزدیک‌تر باشد در این سناریو فرض می‌شود که رفتار عادی کاربر با نقش پرستار برپایهٔ، پنج نوبت ارسال دستور مجاز Insert در جدول MedicalRecord بوده است. گفتنی است که در داده‌های واقعی هیچ‌گونه داده‌ای در رابطه با حمله کاربر به پایگاه داده وجود ندارد؛ لذا در سناریوی شبیه‌سازی تنها رفتار عادی کاربر می‌تواند منطبق با داده واقعی در نظر گرفته شود. بر این اساس جدول (۶) محاسبات مربوط به حالتی را نشان‌می‌دهد که کاربر پرستار به‌منظور سوءاستفاده در نخستین اقدام دستور بازیابی زیر را صادر می‌کند:

```
Select   Pname, Sname, Vdate
From     MedicalRecord mr, VisitRecord vr,
         StaffRecord sr, PatientRecord pr,

DrugRecord dr
Where    mr.VID=vr.VID and vr.SID=sr.SID and
         vr.PID=pr.PID and mr.DID=dr.DID
```

همان‌طور که در جدول (۶) مشاهده می‌شود، در این مرحله مقدار کارایی کاربر به مقدار ۰/۹۳۵ کاهش می‌یابد و درنتیجه از دسترسی کاربر به جدول MedicalRecord جلوگیری به‌عمل می‌آید. چنانچه در حمله‌ای دیگر کاربر با نقش پرستار اقدام به اجرای دستور زیر کند:

```
Select   Pname, Sname
From     PatientRecord pr, StaffRecord sr,
         VisitRecord vr
Where    vr.PID=pr.PID and vr.SID=sr.SID and
         vr.Vdate="dd/dd/dd"
```

در این‌صورت مطابق محاسبات جدول (۶) مقدار کارایی وی به مقدار ۰/۷۵ کاهش می‌یابد و درنتیجه از دسترسی کاربر به جدول VisitRecord جلوگیری به عمل می‌آید.

جدول(۴): درجه حساسیت جدول ها

(Table 4): The sensitivity level of tables

عنوان	جدول ها				
	Patient Record	*Staff Record*	*Drug Record*	*Visit Record*	*Medical Record*
p_1	۰/۷۵	۰/۳۷	۰/۳۷	۰/۷۵	۰/۷۵
p_2	۰/۷۵	۰/۲۵	۰/۲۵	۱	۱
p_3	۰/۲۵	۰/۵	۰/۲۵	۰/۲۵	۰/۵
p_4	۰/۳۷	۰/۳۷	۰/۳۷	۰/۳۷	۰/۷۵
جمع حساسیت	۲/۱۵	۱/۵۵	۱/۳	۲/٤	۳
حساسیت نسبی	**۰/۷۲**	**۰/۵۲**	**۰/۴۳**	**۰/۸**	**۱**

جدول (۵): سطح حساسیت هر یک از مجوزهای پایگاهی بر روی جدول ها

(Table 5): The sensitivity level for database commands

عنوان	جدول ها				
	Patient Record	***Staff Record***	***Drug Record***	***Visit Record***	***Medical Record***
Insert	۰/۷۲	۰/۵۲	۰/٤۳	۰/۸	۱
Delete	۰/۷۲	۰/۵۲	۰/٤۳	۰/۸	۱
Update	۰/٥٤	۰/۳۹	۰/۳۲	۰/٦	۰/۷٥
Select	۰/٥٤	۰/۳۹	۰/۳۲	۰/٦	۰/۷٥

جدول ۶: سناریوی حمله، کاهش مقدار کارایی در بازرسی های مختلف

(Table 6): Attack scenario, Reduce of operator performance in two inspections

بازرسی (۱) – اولین سوءاستفاده					
عنوان	*Patient Record*	*Staff Record*	*Drug Record*	*Visit Record*	*Medical Record*
S_o^{MisUse}	۰/۵۴	۰/۳۹	۰/۳۲	۰/۶	۰/۷۵
$Perf_o$	**۰/۴۸**				
$Perf_u$	**۰/۹۳۵**				

بازرسی (۲)- دومین سوءاستفاده					
عنوان	*Patient Record*	*Staff Record*	*Drug Record*	*Visit Record*	*Medical Record*
S_o^{MisUse}	۰/۵۴	۰/۳۹	۰	۰/۶	۰
$Perf_o$	**-۰/۵۳**				
$Perf_u$	**۰/۷۵**				

۵-۲- سناریوی جبران حمله

در این سناریو فرض بر آن است که کاربری که درقبل به‌علت یک اشتباه غیرعمدی و کاهش مقدار کارایی، از

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]

دسترسی وی کاسته شده، هم‌اکنون در پی جبران و افزایش کارایی و درنتیجه رسیدن به مجوزهای قانونی قبل از اشتباه است. این سناریو نشان‌می‌دهد که چنانچه کاربر با استفاده مجاز از مجوزها سعی در جبران سوءاستفاده‌های پیشین کند، چارچوب پیشنهادی قادر است تا مقدار کارایی و در نتیجه تعداد جدول‌های تحت کنترل او را در محدوده نقش تعیین شده برای وی افزایش دهد. این سناریو هنگامی اتفاق می‌افتد که سوءاستفاده از داده‌ها به‌طور غیرعمدی اتفاق افتاده و کاربر در اسرع وقت اقدام مقتضی برای افزایش کارایی و دسترسی‌های مجاز را انجام دهد. بر این اساس سناریو به‌نحوی تنظیم شده‌است که دستورهای کاربر تنها در حوزه دسترسی‌های مجاز اختصاص داده‌شده به وی بوده و لذا مقدار کارایی وی در بازرسی انجام‌شده افزایش یافته‌است. جدول (۷) تغییر مقدار کارایی کاربر در دو بازرسی مختلف را نشان‌می‌دهد. در این سناریو فرض شده که به‌علت یک سوءاستفاده غیرعمدی مقدار کارایی کاربر پیشتر به مقدار ۰/۷۵ کاهش پیدا کرده است. جدول (۷) نشان‌می‌دهد که در پایان بازرسی نخست مقدار سوءاستفاده کاربر صفر بوده و درنتیجه مقدار کارایی وی به ۰/۷۸ افزایش‌یافته است. در این مرحله با توجه به مقدار حساسیت جدول‌ها همچنان محدوده دسترسی کاربر بدون تغییر باقی می‌ماند. در ادامه و در بازرسی دوم مقدار کارایی به مقدار ۰/۸ افزایش می‌یابد. بدین ترتیب در پایان بازرسی دوم اجازه دسترسی به جدول VisitRecord برای کاربر فراهم می‌شود.

جدول ۷: سناریوی جبران حمله، افزایش مقدار کارایی کاربر
(Table 7): Control scenario, Increase of operator performance in two inspections

بازرسی (۱)					
عنوان	*Patient Record*	*Staff Record*	*Drug Record*	*Visit Record*	*Medical Record*
S_o^{MisUse}	۰	۰	۰	۰	۰
$Perf_o$	۱				
$Perf_u$	۰/۷۸				

بازرسی (۲)					
عنوان	*Patient Record*	*Staff Record*	*Drug Record*	*Visit Record*	*Medical Record*
S_o^{MisUse}	۰	۰	۰	۰	۰
$Perf_o$	۱				
$Perf_u$	۰/۸				

۶- نتیجه‌گیری و کارهای آینده

در این مقاله یک چارچوب کنترل دسترسی بر پایه کارایی برای کاهش تهدیدهای کاربر خودی در یک سامانه بر پایه پایگاه داده ارائه شده‌است. مقدار کارایی کاربر با توجه به کارایی وی در استفاده مجاز از مجوزها تعیین می‌شود. در این چارچوب، دسترسی کاربر به جدول‌ها با توجه به مقدار کارایی وی و سطح حساسیت جدول‌ها تعیین می‌شود؛ لذا چنانچه یک تهدید علیه داده‌های یکی از جدول‌ها صورت گیرد، از دسترسی کاربر به جدول‌های دیگر (متناسب با سطح حساسیت جدول‌ها) جلوگیری به عمل خواهد آمد.

به‌منظور ارزیابی روش پیشنهادی از مجموعه داده‌های واقعی در یک سامانهٔ بیمارستانی، شامل ۶۰۰۰ رکورد استفاده شده‌است. نتایج شبیه‌سازی بر روی این داده‌ها نشان‌می‌دهد که روش پیشنهادی قادر است، تا در صورت مشاهده رفتارهایی که منجر به سوءاستفاده از منابع پایگاه داده‌می‌شود، از حقوق دسترسی کاربر به‌نحوی بکاهد که منجر به سوء استفاده‌های بیشتر وی نشود. در مقابل کاربر می‌تواند با رفتارهای منطبق با حقوق دسترسی اعطایی منجر به افزایش کارایی و درنتیجه بازیابی حقوق از دست رفته‌اش شود.

با توجه به آنکه مدل ارزیابی‌شده فاقد سامانه تشخیص سوءاستفاده است، به‌عنوان کارهای آینده ارائه یک روش برای شناسایی و مدل سازی رفتار کاربر با پایگاه داده در حالت عادی و تشخیص رفتارهای منجر به سوء به‌کارگیری پایگاه داده مورد توجه قرار گرفته است.

۷- مراجع 7- Refrence

[1] S. Dhal and V. Bhuwan, "Cryptanalysis and improvement of a cloud based login and authentication protocol, " in *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, 2018: IEEE, pp. 1-6.

[2] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior rule-based insider threat detection for smart grid, " *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 190-205, 2016.

[3] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45-56, 2018.

[4] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment, " *IEEE Systems Journal*, vol. 11, no. 2, pp. 503-512, 2017.

[5] I. Agrafiotis, P. A. Legg, M. Goldsmith, and S. Creese, "Towards a User and Role-based Sequential Behavioural Analysis Tool for Insider Threat Detection, " *J. Internet Serv. Inf. Secur.*, vol. 4, no. 4, pp. 127-137, 2014.

[6] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into Insiders: A

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]

Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures, " *arXiv preprint arXiv:1805.01612*, 2018.

[7] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1397-1417, 2018.

[8] Q. Lv, Y. Wang, L. Wang, and D. Wang, "Towards a User and Role-Based Behavior Analysis Method for Insider Threat Detection, " in *2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, 2018: IEEE, pp. 6-10.

[9] P. Chattopadhyay, L. Wang, and Y.-P. Tan, "Scenario-Based Insider Threat Detection From Cyber Activities," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 660-675, 2018.

[10] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "A dynamic approach to detect anomalous queries on relational databases, " in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 2015: ACM, pp. 245-252.

[11] A. Almehmadi and K. El-Khatib, "On the possibility of insider threat prevention using intent-based access control (IBAC), " *IEEE Systems Journal*, vol. 11, no. 2, pp. 373-384, 2017.

[12] L. Argento, A. Margheri, F. Paci, V. Sassone, and N. Zannone, "Towards adaptive access control," 2018.

[13] F. Ghofrani and M. Amini, "Privacy Preserving Dynamic Access Control Model with Access Delegation for eHealth, " *Signal and Data Processing*, vol. 17, no. 3, pp. 109-140, 2020.

[14] P. Mahmoudi Nasr and A. Yazdian Varjani, "An Access Management System to Mitigate Operational Threats in SCADA System, " *Signal and Data Processing*, vol. 14, no. 4, pp. 3-18, 2018.

[15] M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, "A trust-based access control model for pervasive computing applications, " in *IFIP Annual Conference on Data and Applications Security and Privacy*, 2009: Springer, pp. 307-314.

[16] N. Baracaldo and J. Joshi, "An adaptive risk management and access control framework to mitigate insider threats, " *Computers & Security*, vol. 39, pp. 237-254, 2013.

[17] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models, " *Computer*, vol. 29, no. 2, pp. 38-47, 1996.

[18] M. Collins, "Common sense guide to mitigating insider threats, " CERT Division, Technical Note, 2016.

[19] P. Mahmoudi-Nasr, A. Yazdian Varjani, "An Access Management System to Mitigate Operational Threats in SCADA System, " *JSDP* 2018; 14 (4) :3-18.

[۱۹] محمودی نصر پیام، یزدیان ورجانی علی. یک سامانه مدیریت دسترسی برای کاهش تهدیدهای عملیاتی در سامانه اسکادا. پردازش علائم و داده‌ها ۱۳۹۶; ۱۴ (۴):۱۸-۳

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

[21] E. Bertino, E. Terzi, A. Kamra, and A. Vakali, "Intrusion detection in RBAC-administered databases, " in *Computer security applications conference, 21st annual*, 2005: IEEE, pp. 10 pp.-182.

[22] D. C. Montgomery, *Introduction to statistical quality control*. John Wiley & Sons (New York), 2009.

پیام محمودی نصر تحصیلات خود را در مقاطع کارشناسی و کارشناسی‌ارشد مهندسی کامپیوتر به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۵ از دانشگاه صنعتی امیرکبیر و در مقطع دکترای مهندسی قدرت در سال ۱۳۹۵ از دانشگاه تربیت مدرس به پایان رسانده و هم‌اکنون استادیار دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه مازندران است. زمینه‌های پژوهشی مورد علاقه ایشان عبارتند از:

امنیت شبکه‌های صنعتی و کامپیوتری، امنیت داده‌ها و شبکه‌های کامپیوتری.

نشانه رایانامه ایشان عبارت است از:

P.mahmoudi@umz.ac.ir

[Downloaded from jsdp.rcisp.ac.ir on 2025-08-21]

[DOI: 10.61186/jsdp.19.4.61]