
بسم الله الرحمن الرحيم

دانشکده : فنی و مهندسی

پایان‌نامه کارشناسی ارشد رشته: مهندسی فناوری اطلاعات

گرایش: تکنولوژی اطلاعات و ارتباطات

عنوان پایان‌نامه:

ارائه روش همبستگی هشدار برای سیستم تشخیص نفوذ با استفاده از سیستم خبره فازی

نام دانشجو:

زهرا اسدی

استاد راهنما:

دکتر علی یزدیان

آبان ۹۳

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه

خانم زهرا اسدی پایان نامه ٦ واحدی خود را **با عنوان همبستگی هشدار برای سیستم تشخیص نفوذ با استفاده از سیستم خبره فازی** در تاریخ ۱۳۹۳/۸/۱۰ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی فناوری اطلاعات - سیستمهای اطلاعاتی پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر علی یزدیان ورجانی	استادیار	
استاد ناظر	دکتر محمدتقی حمیدی بهشتی	دانشیار	
استاد ناظر	دکتر حمید رضا اسکندری	استادیار	
استاد ناظر	دکتر محمد حسام تدین	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر حمید رضا اسکندری	استادیار	

این نسخه به عنوان نسخه نهایی پایان نامه/رساله مورد تایید است.
امضای استاد راهنما

دستورالعمل حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیات علمی، دانشجویان، دانش آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی که با هماهنگی دانشگاه انجام شده است، موارد ذیل را رعایت نمایند:

ماده ۱- حقوق مادی و معنوی پایان نامه‌ها / رساله‌های مصوب دانشگاه متعلق به دانشگاه است و هرگونه بهره‌برداری از آن باید با ذکر نام دانشگاه و رعایت آیین‌نامه‌ها و دستورالعمل‌های مصوب دانشگاه باشد.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و استاد راهنما مسئول مکاتبات مقاله باشد.

تبصره: در مقالاتی که پس از دانش آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

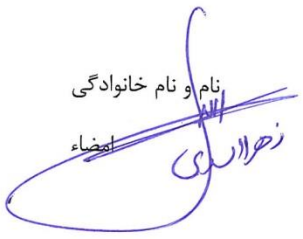
ماده ۳- انتشار کتاب حاصل از نتایج پایان نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آئین نامه های مصوب انجام می‌شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم الاجرا است و هرگونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری می شود.

نام و نام خانوادگی

امضاء



آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان‌نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش‌آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان‌نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان‌نامه کارشناسی ارشد/ رساله دکتری نگارنده در رشته ـــــــــ است که در سال ـــــــــ در دانشکده ـــــــــ دانشگاه تربیت مدرس به راهنمایی سرکار خانم/جناب آقای دکتر ـــــــــ ، مشاوره سرکار خانم/جناب آقای دکتر ـــــــــ و مشاوره سرکار خانم/جناب آقای دکتر ـــــــــ از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب زهرا اسدی دانشجوی رشته ICT مقطع کارشناسی ارشد

تعهد فوق ضمانت اجرایی آن را قبول کرده، به آن ملتزم می‌شوم.

نام و نام خانوادگی: زهرا اسدی

تاریخ و امضا:

من به سر چشمه خورشید نه خود بردم راه ذره‌ای بودم و مهر تو مرا بالا برد

سپاس به پیشگاه حضرت دوست که هر چه داریم از اوست.

با تشکر از زحمات بی دریغ استاد ارجمند، جناب آقای دکتر علی یزدیان که با راهنمایی‌های ارزشمند خود همواره اینجانب را یاری نمودند.

با تشکر از پدر و مادر عزیزم، مهربان فرشتگانی که لحظات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن، عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگی‌ام، مدیون حضور سبز آن‌هاست.

با تشکر از همسر عزیزم، که سایه مهربانی‌اش سایه‌سار زندگی‌ام می‌باشد، و بی او این نوشتار را نه آغازی بود و نه پایانی

تقدیم به فرزند دلبندم آریتا، که با لبخندهای شیرین‌منش، سختی راه را بر من هموار نمود و مشوق و مایه آرامش من گردید.

چکیده

سیستم‌های تشخیص نفوذ یکی از ابزارهای پرکاربرد در امنیت شبکه‌های کامپیوتری هستند. تعداد زیاد هشدارهایی که توسط سیستم‌های تشخیص نفوذ ایجاد می‌شوند، کاذب و تکراری بودن اکثر این هشدارها و عدم توانایی اپراتورهای امنیتی در تجزیه‌وتحلیل آن‌ها یکی از مشکلات اساسی سیستم‌های تشخیص نفوذ است. یکی از روش‌های مقابله با این مشکلات استفاده از روش‌های همبستگی هشدارهاست که به ما امکان می‌دهد هشدارهای کاذب و تکراری را از بین برده و اطلاعات مفید و سطح بالا را استخراج نماییم. در این پایان‌نامه ضمن بررسی روش‌های موجود برای همبسته سازی هشدارها به معماری‌ای خواهیم پرداخت که روش‌های مبتنی بر سیستم ایمنی مصنوعی را با سیستم خبره فازی ترکیب کرده تا بر اساس اولویت‌ها و دانش اپراتورهای امنیتی عمل نمایش و استدلال را انجام دهد. در ابتدا فرآیند همبسته سازی هشدارها شامل چندین مؤلفه ارائه‌شده است. در مدل پیشنهادی فرآیند نرمال‌سازی و پیش‌پردازش روی تمامی هشدارها اعمال می‌شود. پس از نرمال‌سازی، هشدارها نام و ساختار استانداردی دارند که توسط سیستم همبسته ساز شناخته می‌شود. سیستم‌های تشخیص نفوذ سپس هشدارهای خود را به روی یک سرور مرکزی فرستاده و آن‌ها را در پایگاه داده خود ذخیره می‌کنند. در مرحله بعد هشدارهای تکراری حذف می‌شوند. با استفاده از الگوریتم سیستم ایمنی مصنوعی و همچنین با بهبود تولید ابر هشدارها با استفاده از قوانین فازی هم نرخ تشخیص هشدارهای مربوط به حملات و هم نرخ خطای مثبت کاذب به حد قابل قبولی رسید. درنهایت نتایج استفاده توأم این دو مؤلفه را به دست آورده و باکارهای معتبر دیگر در این زمینه جهت اعتبار سنجی مدل نهایی مقایسه کردیم. مقایسه نشان‌دهنده مطلوبیت بالای میزان خطای مثبت کاذب و نتایج طبقه‌بندی حملات بوده است.

کلمات کلیدی: همبستگی هشدارها، تشخیص نفوذ، سیستم خبره فازی، سیستم ایمنی مصنوعی، مثبت کاذب

فهرست مطالب

عنوان صفحه

فهرست جداول

عنوان صفحه

فهرست شکل ها

عنوان صفحه

فصل اول

کلیات تحقیق

۱-۱- مقدمه

با روند رو به رشد استفاده از شبکه‌های کامپیوتری به‌خصوص اینترنت و مهارت رو به رشد کاربران و مهاجمانِ این شبکه‌ها و وجود نقاط آسیب‌پذیری مختلف در نرم‌افزارها، ایمن‌سازی سیستم‌ها و شبکه‌های کامپیوتری، نسبت به گذشته از اهمیت بیشتری برخوردار شده است. تأمین امنیت در هر سیستم یا شبکه کامپیوتری در واقع به معنای تأمین سه بعد اساسی محرمانگی، جامعیت و دسترس‌پذیری در آن است. (آذرکسب&قیداری, ۱۳۸۷)

سیستم‌های تشخیص نفوذ، بر اساس منبع تأمین‌کننده داده‌های ورودی به دودسته سیستمهای مبتنی بر میزبان و سیستم‌های مبتنی بر شبکه تقسیم می‌گردند. بر اساس روش تحلیل و تشخیص نیز سیستمهای تشخیص نفوذ به دودسته عمده سیستم‌های تشخیص مبتنی بر امضاء و سیستم‌های تشخیص ناهنجاری تقسیم می‌شوند. در سیستم‌های تشخیص مبتنی بر امضاء، تشخیص حمله بر اساس اطلاعات موجود از الگوهای حمله‌های شناخته‌شده صورت می‌پذیرد. درحالی‌که در سیستم‌های

تشخیص ناهنجاری ابتدا نمایه‌هایی از رفتارهای نرمال و هنجار (سیستم، شبکه و یا کاربران آن) تولید و سپس رفتارهای ناهنجار و مهاجمانه با تخطی و انحراف از این نمایه‌های نرمال تشخیص داده می‌شوند. (آذرکسب&قیداری, ۱۳۸۷)

۱-۲-بیان مسئله

تشخیص نفوذ[1] روند نظارت بر حوادث رخ‌داده در یک سیستم کامپیوتری یا شبکه و تجزیه‌وتحلیل آن‌ها برای نشانه‌هایی از حوادث احتمالی منجر به نقض یا تهدید سیاست‌های امنیتی کامپیوتر است. مطالعه رفتار حمله ، کار چالش‌برانگیزی است. زیرا مهاجمین[2] معمولاً رفتار خود را تغییر می‌دهند تا قابل‌شناسایی نباشند. ازآنجایی‌که آسیب‌پذیری‌ها، مرتباً در حال کشف و شناسایی هستند، حملات نیز از استراتژی‌های حمله جدید، استفاده می‌کنند. یکی از روش‌های مطالعه استراتژی‌های حمله، استخراج آن‌ها از طریق هشدارهایی است که توسط سیستم‌های تشخیص نفوذ تولید می‌شوند.(Zhu&Ghorbani, 2006b)

همه تکنیک‌های کشف نفوذ، نقاط قوت و ضعفی دارند. به‌عنوان‌مثال، کشف نفوذ مبتنی بر امضا، دارای نرخ مثبت کاذب[3] پایین‌تری است، اما برای کشف حملات شناخته‌شده، مورداستفاده قرار می‌گیرد. کشف مبتنی بر ناهنجاری، می‌تواند حملات جدید را کشف کند، اما از نرخ بالای مثبت کاذب رنج می‌برد. علاوه بر این، تعریف رفتار نرمال یک سیستم نیز کار سختی است. سیستم‌های تشخیص نفوذ نمی‌توانند حملات چندمرحله‌ای را تشخیص دهند. برای مقابله با این مشکلات سیستم همبستگی هشدار[4] پیشنهادشده است. همبستگی هشدار فرایندی است که شامل چندین مؤلفه است و هدف این مؤلفه‌ها، آنالیز علائم هشدار و ارائه یک دید سطح بالا در مورد وضعیت امنیتی شبکه تحت نظارت است. (Zhu&Ghorbani, 2006b)

---

1 Intrusion Detection
2 Attacker
3 False Positive
4 Alert Correlation System

این بخش ، شامل تجزیه‌وتحلیل هشدارهای ایجادشده توسط سیستم‌های کشف نفوذ و ابزارهای امنیتی دیگر، جهت کشف طرح‌های حمله، شناسایی هشدارهای کاذب و موارد دیگر است و به ما امکان می‌دهد تا هشدارهای تکراری و کاذب را از بین ببریم و آن‌ها را مطابق با اولویت‌ها و میزان خطرآفرینی فعالیت‌های شناسایی‌شده، اولویت‌بندی نماییم. (Tabia et al., 2011a)

یکی از کاربردهای مهم همبستگی هشدار، شناسایی استراتژی‌ها یا طرح‌های نفوذهای مختلف و درک هدف حملات است. اگر بتوانیم گام بعدی یا هدف نهایی یک مهاجم را بامطالعه الگوی رفتار نفوذگرانه شناسایی کنیم، درنتیجه می‌توانیم از افزایش حمله جلوگیری نموده و آسیب وارده به سیستم را به حداقل برسانیم.(Zhu&Ghorbani, 2006b)

روش‌های همبستگی هشدار، یا باعث کاهش تعداد هشدارهای صادرشده از طریق حذف هشدارهای تکراری و بی‌ربط می‌شوند و یا باعث کشف حملات چندمرحله‌ای می‌گردند(Tabia et al., ۲۰۱۱a)

آروموسو همبستگی هشدار را این‌گونه تعریف می‌کند : "به معنای واقعی کلمه همبستگی نفوذ تعریف‌شده است که تفسیر، ترکیب و تجزیه‌وتحلیل اطلاعات از تمام منابع در دسترس درباره فعالیت سیستم مقصد به‌منظور تشخیص نفوذ و پاسخ اشاره‌شده است".(Kabiri&Ghorbani, 2007)

حملات انکار سرویس یک سلاح برای اخاذی و خرابکاری است که موجب خساراتی در حد میلیون‌ها دلار به سایت‌های تجاری و دولتی شده‌اند. ترکیبی از نیروی حمله و ابزار حمله به‌عنوان سناریوی حمله[1] تعریف می‌شود. روش‌های جاری مقابله با حملات انکار سرویس[2] در پیشگیری از حملات، تشخیص و پاسخ متمرکزشده است. پیشگیری از حملات انکار سرویس شامل تکنیک‌هایی است که یکپارچگی میزبان‌ها را حفظ می‌کند و تکنیک‌هایی برای تشخیص و میزان محدودیت فعالیت

1 Attack Scenario
2 Denial of Service

شبکه غیرطبیعی است. تشخیص حمله به‌طورمعمول بر اساس تکنیک‌هایی مانند تطبیق امضاء[1] یا تشخیص ناهنجاری[2] است. پاسخ به حملات انکار سرویس به‌طورمعمول شامل فیلترکردن بسته‌های حمله است.(Hussain et al., 2006)

تکنیک‌های هوش مصنوعی، محاسبات نرم و سیستم خبره فازی، روش‌های نوینی هستند که می‌توان در همبستگی بین علائم هشدار سیستم‌های تشخیص نفوذ از آن‌ها استفاده کرد. تکنیک‌های هوش مصنوعی ضریب اطمینان سیستم را بالا می‌برد و این توانایی را به سیستم می‌دهد که در مقابل رشد تقاضاها پاسخگو باشد.(Özyer et al., 2007)

۱-۲-۱- اهمیت و ضرورت انجام تحقیق

یکی از مهم‌ترین چالش‌های پیش روی سیستم‌های تشخیص نفوذ تعداد زیاد هشدارهای تولیدشده است. مدیر سیستم با این هشدارها تحت‌الشعاع قرار خواهد گرفت هنگامی‌که او نمی‌تواند این هشدارها را استفاده و مدیریت کند. بهترین راه‌حل شناخته‌شده این است که هشدارهای سطح پایین، به یک حمله سطح بالاتر همبسته شوند و سپس یک هشدار سطح بالا از آن‌ها تولید شود. (Bateni et al., 2013)

۱-۲-۲- اهداف تحقیق

با توجه به مشکلات مطرح‌شده در بالا، هدف این تحقیق طراحی روشی جهت بالا بردن کیفیت اطلاعات هشدارها و ارائه گزارش‌های کامل مدیریتی به کارشناسان و مدیران امنیت شبکه می‌باشد تا از این طریق بتوان هشدارهای تکراری را تجمیع و همبسته نمود و با بررسی روابط بین حوادث و هشدارها، الگوها و یا استراتژی‌های حمله را استخراج کرد.

---

1 Signature matching

2 Anomaly detection

۱-۲-۳- وجه تمایز پژوهش با سایر پژوهش‌ها

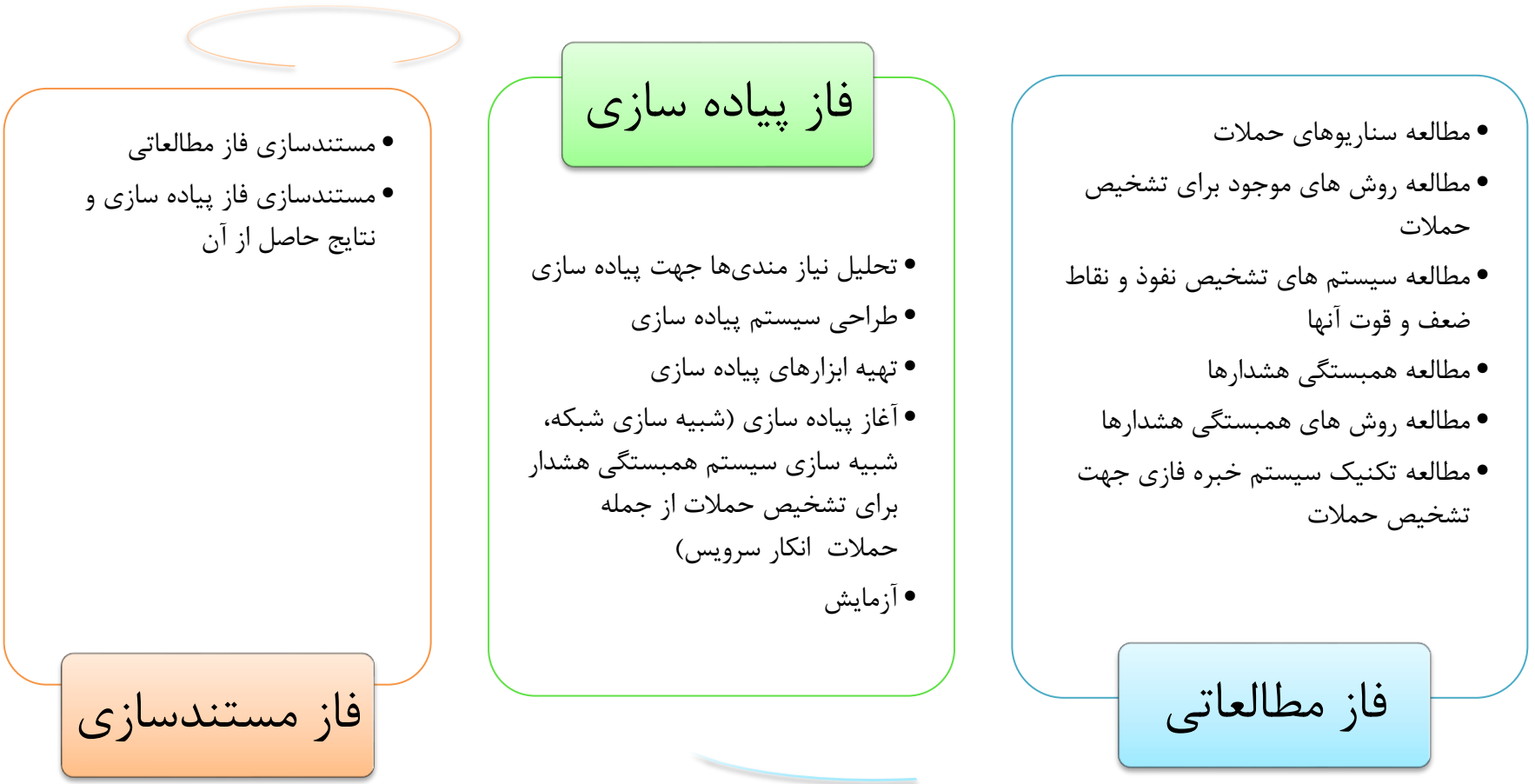
با توجه به بررسی‌های انجام‌شده و مشکلات موجود در سیستم‌های تشخیص نفوذ، همبستگی هشدارها و ترکیب روش‌های مختلف در طراحی سیستم‌های تشخیص نفوذ کمک مؤثری در مدیریت زمان و بهبود کارایی سیستم‌های تشخیص نفوذ دارد. لذا در این تحقیق روشی بر اساس سیستم خبره فازی برای یادگیری درجه همبستگی بین هشدارها در تشخیص و استخراج سناریوی حمله ارائه می‌شود. در این روش سیستم پیشنهادی سعی در پیدا کردن همبستگی هشدارهای جدید با هشدارهای قبلی بر اساس قواعد فازی می‌نماید. در صورت عدم همبستگی قاعده جدیدی ارائه می‌گردد.

۱-۳-سؤالات و فرضیات پژوهش

- چه رفتارهایی به‌عنوان حمله شناخته می‌شوند؟
- راه‌های پیشگیری، تشخیص و پاسخ در برابر حملات چیست؟
- هوش مصنوعی شامل سیستم خبره فازی چگونه به تشخیص حملات کمک می‌کند؟
- همبستگی هشدارها به چه روش‌هایی قابل پیاده‌سازی است ؟

۱-۳-۱- بخش بندی تحقیق

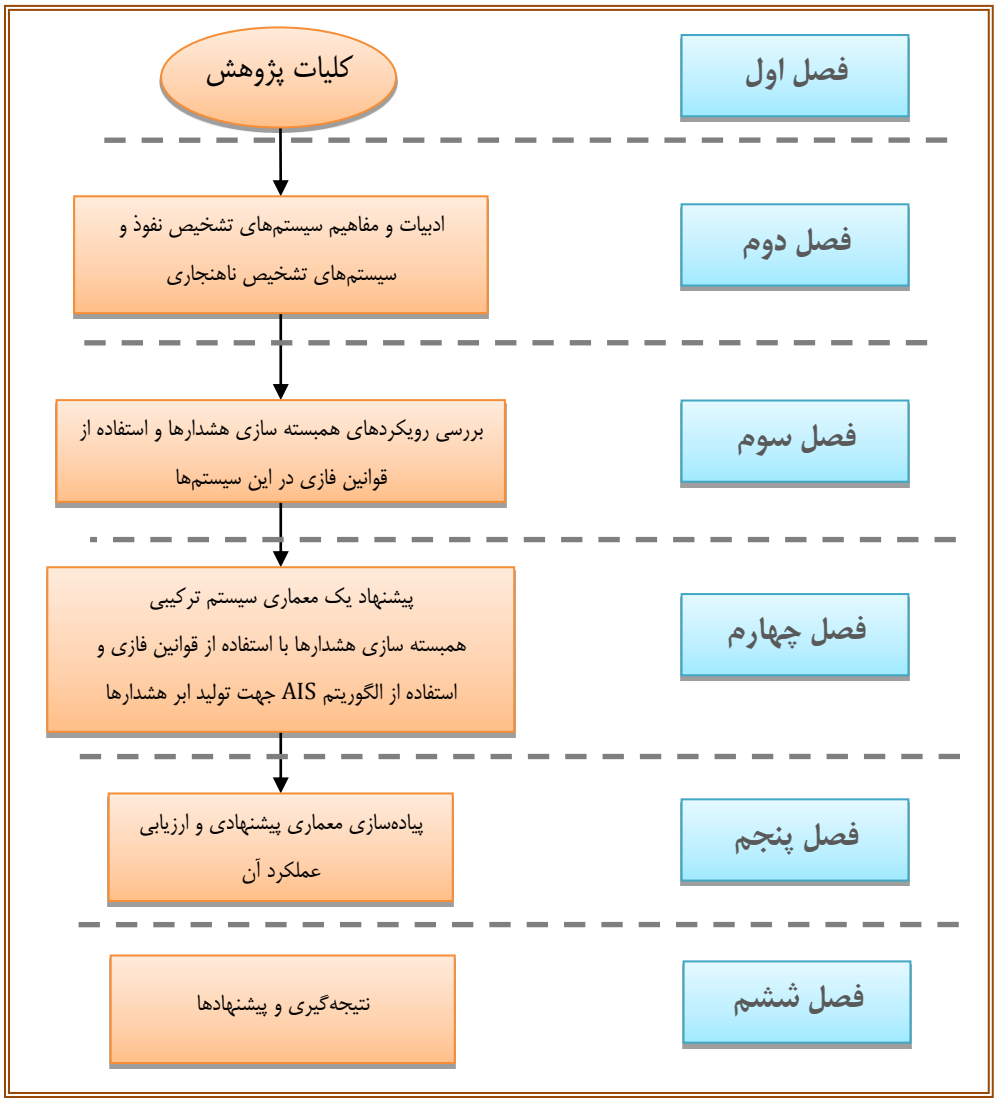
انجام تحقیق از ۳ فاز مطالعاتی، پیاده‌سازی و مستندسازی تشکیل خواهد شد. که در شکل ۱-۱ اقدامات هر فاز مشاهده می‌شود.



شکل ۱-۱ فازهای انجام تحقیق

۱-۳-۲- ساختار پژوهش

ساختار کلی پژوهش به‌صورت کلی در شکل ۱-۲ بیان‌شده است.



شکل ۱-۲ ساختار پژوهش