فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال پنجم، شماره سه، پاییز ۱۴۰۰

کنترل دسترسی در قراردادهای هوشمند با استفاده از یادگیری ماشین برای اینترنت اشیا

عبدالرضا عندلیب[۱]، افشین رضاخانی[۲]، اکبر مرشد اسکی[۳]، پریسا رحمانی[۴]*

تاریخ دریافت : ۱۴۰۰/۰۷/۱۷ **تاریخ پذیرش: ۱۴۰۰/۱۰/۱۵**

چکیده

کنترل دسترسی در شبکه بلاک‌چین یکی از چالش‌هایی است که با رشد شبکه بلاک‌چین با آن روبه‌رو هستیم. در شبکه بلاک‌چین، مجموعه فعالیت‌های مالی کاربران که نیاز به امضای دیجیتال دارد انجام می‌شود، این اطلاعات در سرور بلاک‌چین ذخیره می‌شود. امضای دیجیتال و تأیید هویت و صحت تراکنش‌ها به‌صورت دستی فرایندی وقت‌گیر بوده و کاربرپسند نیست و از دلایلی است که تکنولوژی بلاک‌چین به طور کامل پذیرفته نمی‌شود. در این مقاله، یک روش نوین بر اساس ترکیب روش‌های خوشه‌بندی و دسته‌بندی پیشنهاد می‌شود، ابتدا برچسب‌گذاری داده‌ها، به کمک روش خوشه‌بندی انجام شده و سپس از داده‌های برچسب‌گذاری شده برای آموزش الگوریتم SVM برای تعیین تراکنش‌های سالم استفاده می‌شود. روش پیشنهادی، یک روش مبتنی بر یادگیری ماشین برای کنترل دسترسی است که امضای خودکار تراکنش‌های بلاک‌چین و شناسایی تراکنش‌های غیرعادی را انجام می‌دهد. به‌منظور ارزیابی روش پیشنهادی، آزمایش و تجزیه‌وتحلیل بر روی داده‌های اتریوم انجام شده است و به کمک الگوریتم خوشه‌بندی K-Means و روش بردار پشتیبان ماشین تراکنش‌های سالم از مشکوک شناسایی می‌شود که این روش توانایی شناسایی بادقت ۸۹ درصد را نشان می‌دهد.

واژگان کلیدی: بلاک‌چین، اتریوم، SVM، K-Means

[۱] دانشجوی دکتری گروه کامپیوتر،واحد بروجرد، دانشگاه آزاد اسلامی، بروجرد، ایران Abdolrezaandalib@gmail.com

[۲*] استادیار، گروه کامپیوتر دانشگاه آیت اله بروجردی Rezakhani@abru.ac.ir

[۳] استادیار، گروه کامپیوتر، دانشکده فنی و مهندسی، دانشگاه ورامین - پیشوا، دانشگاه آزاد اسلامی، ورامین، تهران، ایران Morshed486@gmail.com

[۴] استادیار، گروه کامپیوتر، واحد پردیس، دانشگاه آزاد اسلامی، پردیس، ایران Rahmani@pardisiau.ac.ir

۱. مقدمه

اگر بخواهیم به زبان ساده بلاک‌چین را تعریف کنیم باید بگوییم که زنجیره‌ای از بلوک‌های به‌هم‌وابسته است که مجموعه‌ای از داده‌ها و اطلاعات را با خود به همراه دارد و می‌تواند اطلاعاتی مانند دارایی‌های دیجیتال یک فرد تا اطلاعات قضایی ثبت شده باشند. حال مسئله این است، اطلاعاتی را که این بلوک‌های به‌هم‌وابسته حمل می‌کنند تا چه اندازه قابل‌اطمینان و اعتماد است. مدیریت هویت دیجیتالی در تسهیل تبادلات مبتنی بر بلاک‌چین و اینترنت اشیا به کار می‌رود و این امر سبب می‌شود که معاملات بر بستر بلاک‌چین سریع‌تر و با امنیت بالاتری صورت پذیرد. یکی از اصلی‌ترین چالش‌های تکنولوژی بلاک‌چین، توانایی کاربران برای انتقال پول و اعتبارات به طور مستقیم به یکدیگر درون یک شبکه غیرمتمرکز و توزیع‌شده است که بدون نیاز به شخص ثالث (به‌عنوان‌مثال، مؤسسه مالی) انجام می‌شود و انجام معاملات، مالکیت منابع و پول و اعتبارات را انتقال می‌دهد. هر تراکنشی که در شبکه انجام می‌شود، باید توسط کاربر به‌صورت دیجیتالی امضا و تأیید شود که توسط الگوریتم امضای دیجیتال انجام می‌شود. به‌منظور انتقال صحیح اطلاعات نیاز به رمزگذاری بسته‌های حاوی پیام نمود در این فرایند یک کلید عمومی و یک کلید خصوصی برای استفاده از بستر رمزگذاری نیاز است که کلید عمومی در اختیار همه می‌تواند قرار گیرد ولی کلید خصوصی باید در اختیار دریافت‌کننده پیام باشد.

استفاده از امضاهای دیجیتال به‌عنوان یکی از اصلی‌ترین بلوک‌های سازنده فناوری بلاک‌چین برای تضمین یکپارچگی و عدم انکار تراکنش‌ها ضروری است[۱] [۲]. باتوجه‌به نتایج مقاله [۳] در مورد قابلیت استفاده از امضاهای دیجیتال، هنوز موانع زیادی وجود دارد که کاربران را از پذیرش استفاده از امضاهای دیجیتال در استفاده روزمره شان باز می‌دارد. این موانع مربوط به مدیریت، کنترل و استفاده از کلیدهای رمزنگاری است. در مطالعات بررسی شده، نشان داده می‌شود که چنین وظایف پیچیده‌ای برای کاربران طاقت‌فرسا است و قادر به تشخیص نفوذهای بالقوه در حین درگیر شدن در فرایند امضای دیجیتال نیستند. در مقاله [٤] نشان می‌دهد که امضای دیجیتال با حساب بلاک‌چین آن‌ها (به‌عنوان مثال، کلید عمومی-خصوصی) در ارتباط است. فرایند امضا در نرم‌افزار اختصاصی (دیجیتال یا رمزنگاری) کیف پول دیجیتال انجام می‌شود. با کیف پول دیجیتال، کاربران فرایند امضای دیجیتال را کنترل کرده و تعاملات را در شبکه بلاک‌چین انجام می‌دهند. هر حساب دارای یک آدرس منحصربه‌فرد و یک نسخه متشکل از یک کلید عمومی است که نشان‌دهنده آدرس هویت دیجیتالی یک کاربر در شبکه بلاک‌چین است. انتقال منابع دیجیتال بر روی شبکه ارز دیجیتالی و بلاک‌چین با استفاده از تراکنش‌های امضا شده به‌صورت رمزنگاری شده انجام می‌شود و آدرس‌ها نقش مهمی در تعریف مالک جدید ایفا می‌کنند. ازآنجاکه هر تراکنش با بلاک‌چین باید توسط کاربر به‌صورت دیجیتالی امضا شود، این امر می‌تواند به مشکلات امنیتی منجر شود. بیشتر مسائل پیرامون موضوعات استفاده از امضای دیجیتالی به پیچیدگی فرایند امضای دیجیتال مربوط می‌شوند[۵].

در ارتباط با فناوری بلاک‌چین، این امر می‌تواند امنیت دارایی‌های دیجیتال متعلق به کاربران را تحت‌تأثیر قرار دهد هر بار که یک کاربر می‌خواهد یک دارایی دیجیتال را انتقال دهد، باید یک تراکنش امضا شده دیجیتالی فراهم شود. در صورت نقل و انتقالات مکرر در یک دوره زمانی طولانی، فرایند امضای دیجیتال را می‌توان به طور سطحی‌تری انجام داد و در نتیجه امنیت دارایی‌های دیجیتال تحت‌تأثیر قرار می‌گیرد. در این وضعیت، هکرها می‌توانند از این رفتار کاربر به‌عنوان یک مزیت استفاده کنند و تلاش کنند تا امضای تراکنش‌هایی را که اثرات نامطلوبی (سرقت حساب) بر منابع دیجیتال آن‌ها دارند را به کاربران پیشنهاد کنند. برای مثال، کاربر یک تراکنش را از طریق یک برنامه کاربردی وب انجام می‌دهد که در آن هدف انتقال مقداری ارز دیجیتال است[٦]. در این فرایند، برنامه واسط، تراکنش را برای فرایند امضای دیجیتال به کاربر ارائه و آماده می‌کند. بعد از امضای دیجیتالی تراکنش، به شبکه بلاک‌چین به طور غیرقابل بازگشتی اجرا می‌شود. یک مشکل که ممکن است رخ دهد این است که برنامه یک تراکنش مخرب با داده‌های مشابه ایجاد کند (به‌عنوان مثال، یک مقدار بالاتر از مقدار اولیه تعیین‌شده توسط کاربر) کاربر ممکن است معامله ساختگی را امضا کند، که بعدا نمی‌تواند لغو شود، در نتیجه منجر به از دست

دادن مبلغی برای کاربر می‌شود. این مقاله یک روش یادگیری ماشین برای تشخیص تراکنش‌های سالم از تراکنش‌های غیرعادی است. در این مقاله باتوجه‌به اطلاعات جمع‌آوری شده از تراکنش‌های ارز دیجیتال اتریوم و مبادلات صورت‌گرفته [۷] [۸] یک سیستم هوشمند آموزش داده می‌شود. سیستم آموزش داده شده به کمک ترکیب الگوریتم خوشه‌بندی K-Means و الگوریتم SVM پیشنهاد شده است. چالش اصلی این پژوهش در کلاس‌بندی داده‌های تراکنش بدون برچسب مجموعه‌ای از تراکنش‌های مالی در بستر اتریوم است که باید بر روی آن دسته‌بندی انجام شود..

ساختار مقاله، به‌صورت زیر است. بخش دوم مقاله، کارهای مرتبط در شناسایی تراکنش‌های غیرعادی در تکنولوژی‌های بلاک‌چین را بررسی می‌کند. بخش سوم وضعیت فعلی امضای معاملات در فناوری‌های بلاک‌چین را نشان می‌دهد. بخش چهارم الگوریتم پیشنهادی امضای خودکار و شخصی معاملات بلاک‌چین را به طور مفصل بررسی می‌نماید و در بخش پنجم نتیجه‌گیری ارائه می‌شود.

۲. پیشینه تحقیق

در این بخش، کارهای مرتبط در زمینه شناسایی تقلب در شبکه بلاک‌چین مورد بررسی قرار می‌گیرد. پم و لی، به مسئله شناسایی کاربران مشکوک و تراکنش‌های آن‌ها بر روی گراف ایجاد شده از شبکه بلاک‌چین، بیت‌کوین پرداخته‌اند. برای تشخیص تراکنش‌های غیرعادی، از روش‌های خوشه‌بندی K-Means، فاصله ماهالانوبیس و یادگیری ماشین بردار پشتیبانی (SVM) استفاده کرده‌اند [۹]، در [۱۰]، نویسندگان همین تحقیق را با استفاده از قوانین فشرده‌سازی درجه توان، همراه با روش‌های یادگیری بدون نظارت عامل خروجی محلی توسعه داده‌اند، که در آن به نتایج مشابهی دست یافته‌اند. در [۱۱]، قابلیت‌های جنگل‌های تصادفی، ماشین‌های بردار پشتیبانی، و روش‌های یادگیری تحت نظارت برای شناسایی حساب‌های متقلبانه در شبکه بلاک‌چین اعمال و مقایسه شده‌اند. در [۱۲] با روش یادگیری بدون نظارت K-Means که قادر به خوشه‌بندی هم‌زمان اشیا برای تشخیص ناهنجاری در شبکه بیت‌کوین است، پیشنهاد شده است. ارزیابی با همان مجموعه‌داده مورداستفاده در [۹] [۱۰] انجام شد. رویکرد پیشنهادی نتایج بهتری با تراکنش‌های شناسایی متقلبانه به دست می‌آورد.

باتوجه‌به مطالعات انجام شده، هیچ راه‌حلی وجود ندارد که هدف آن معرفی روش‌های یادگیری ماشین در فرایند امضای دیجیتال تراکنش‌های بلاک‌چین باهدف فعال‌کردن امضای خودکار دیجیتال تراکنش‌ها باشد. اگرچه کار شناسایی بی قاعدگی‌ها در میان تراکنش‌ها قبلاً انجام شده است، هیچ یک از روش‌های بازنگری شده با الگوهای تراکنش آدرس سازگار نیست، و هیچ بررسی روی رویکرد استفاده از داده‌های کاربر که برچسب‌گذاری شده‌اند صورت نگرفته است نوآوری رویکرد پیشنهادی این است که می‌تواند با هر نشانی که دارای سابقه کافی از تراکنش، صرف‌نظر از الگوهای تراکنش، و تراکنش‌های غیرعادی شناسایی‌شده، استفاده شود.

۱ . جدول مقایسه

اسم نویسنده	عنوان مقاله	سال	مطالعه برای پیش‌بینی	روش شناسی
پم و لی [10]	Anomaly detection in bitcoin network using unsupervised learning methods	2016	Bitcoin	خوشه‌بندی
پم و لی [10]	Anomaly detection in the bitcoin system-a network perspective	2016	Bitcoin	خوشه‌بندی
اوستاپوویچ و زبیکوفسکی [11]	Detecting Fraudulent Accounts on blockchain: A Supervised Approach	2019	Block chain	روش دسته‌بندی
مونامو، ماریواته و توالا [12]	Unsupervised learning for robust bitcoin fraud detection	2016	Bitcoin	خوشه‌بندی kmeans

یکی از جنبه‌های نوآوری در این مقاله ترکیب روش‌های خوشه‌بندی و دسته‌بندی به‌صورت هم‌زمان است.

۳. شبکه بلاک‌چین

در شبکه بلاک‌چین، تراکنش‌ها به شیوه‌ای امن و تغییرناپذیر در بلوک‌ها مهروموم می‌شوند و در یک دفتر به هم متصل می‌شوند[۱۳]. هر بلوک خود شامل چندین تراکنش تأیید شده توسط امضاهای دیجیتال است که به‌عنوان یک حالت در یک دفترکل توزیع‌شده به اشتراک گذاشته می‌شود و بین تمام شرکت کنندگان در شبکه بلاک‌چین ثبت می‌شود و در نتیجه شفافیت و تغییرناپذیری معاملات انجام‌شده در شبکه را فراهم می‌کند[۱٤]. انواع حساب در بستر بلاک‌چین به دو دسته حساب با مالکیت خارجی و حساب مبتنی بر قرارداد هوشمند تقسیم می‌شود.

حساب با مالکیت خارجی یا (Externally Owned Account) EOA ها، حساب‌هایی هستند که متعلق به کاربران بوده و به آن‌ها حساب کاربران (User Account) گفته می‌شود و توسط آن‌ها کنترل می‌شوند. این حساب‌ها دارایی‌های اتر کاربران را در خود نگهداری می‌کنند و از طریق رمزنگاری نامتقارن و کلید خصوصی (Private Key) محافظت می‌شوند. کلید خصوصی (در بلاک‌چین هر رمزارزی) کدی است که دسترسی شما به‌حسابتان را میسر کرده و مانند رمزهای عبور کارت‌های بانکی‌تان عمل می‌کند؛ بدون داشتن کلید خصوصی، امکان دسترسی به‌حساب و استفاده از رمزارزتان را نخواهید داشت. برای انجام هر تراکنشی در بلاک‌چین اتریوم، باید از حساب‌های با مالکیت خارجی استفاده کنید. هر حسابی در بلاک‌چین اتریوم (بلاک‌چین هر رمزارز دیگری) دارای یک آدرس منحصربه‌فرد است که برای انجام تراکنش‌ها و دریافت و انتقال اتر از آن استفاده می‌شود. آدرس حساب در بلاک‌چین رمزارزها، همانند شماره کارت بانکی شماست که برای دریافت پول از سایرین، آن را در اختیار آن‌ها قرار می‌دهید و یا برای انتقال پول به آن‌ها، از آن استفاده می‌کنید.

۳-۱. کلید عمومی و خصوصی

برای رمزگذاری از دو کلید استفاده می‌شود که اگر از کلید برای رمزگذاری استفاده شود، کلید دیگر می‌بایست برای رمزگشایی به کار گرفته شود. الگوریتم‌هایی که برای تولید این زوج کلیدها استفاده می‌شوند، این موضوع را تضمین می‌کنند که درصورتی‌که یکی از کلیدها که کلید عمومی نامیده می‌شود، منتشر گردد. کلید دیگر، یعنی کلید خصوصی را نمی‌توان به‌سادگی کشف نمود.

بلاک‌چین یک سیستم همتا به همتا است که امکان دسترسی به آن برای همگان وجود دارد. هرکسی می‌تواند با منابع محاسباتی خود (ابزارهای رایانه‌ای) به آن متصل شود و یا اطلاعات تراکنش‌های جدید را به سیستم ارسال کند. بااین‌حال دسترسی همگان به اموال اختصاص‌داده‌شده به‌حساب‌هایی که توسط بلاک‌چین مدیریت می‌شود، مطلوب نیست. ویژگی بارز ملک خصوصی، انحصار آن است. حق انتقال مالکیت به‌حساب دیگر تنها محدود به مالک حساب است که مالکیت را واگذار کند. ازاین‌رو، چالش بلاک‌چین، محافظت از دارایی‌های اختصاص‌داده‌شده به‌حساب‌ها بدون محدودکردن معماری باز سیستم توزیع شده است.

رمزنگاری کلید خصوصی – عمومی. کلیدهای عمومی برای شناسایی حساب‌هایی استفاده می‌شوند که توسط آن هرکسی می‌تواند مالکیتی را انتقال دهد، درحالی‌که دسترسی به آن حساب‌ها تنها به کسانی محدود شده است که کلید خصوصی مربوط را دارند.

۳-۲. رمزنگاری

بلاک‌چین علاوه بر توابع هش، از یک فناوری پایه دیگر به نام رمزنگاری نامتقارن نیز به‌صورت گسترده استفاده می‌کند. رمزنگاری نامتقارن، اساس ایجاد هویت کاربران در بلاک‌چین و محافظت از اموال آن‌ها است. درک رمزنگاری تا حدی پیچیده و سخت است. ایدهٔ اصلی رمزنگاری محافظت از اطلاعات در برابر دسترسی افراد غیرمجاز است.

۳-۳. امضای دیجیتال

این بخش به مفهوم امضای دیجیتال اختصاص‌داده‌شده که از رویکرد خصوصی به عمومی رمزنگاری نامتقارن استفاده می‌کند. ازآنجاکه لازم است بلاک‌چین اطمینان حاصل کند تنها مالکان قانونی قادر به انتقال دارایی‌ها به سایر حساب‌ها هستند، مفهوم مجوز دسترسی وارد صحنه می‌شود ازاین‌رو توضیح داده می‌شود که چگونه در بلاک‌چین از رمزنگاری نامتقارن برای مجوز دادن به تراکنش‌ها استفاده می‌کند.

تضمین اینکه تنها دارنده یک حساب می‌تواند دارایی‌های مرتبط با حساب خود را به‌حساب‌های دیگر انتقال دهد بسیار مهم است. هرگونه تلاشی جهت دسترسی به یک حساب و دارایی‌های مرتبط با آن توسط هر شخصی غیر از مالک قانونی حساب، باید به‌عنوان غیرمجاز شناسایی و رد شود. در واقع چالش بلاک‌چین این است که درحالی‌که باز بودن خود را حفظ می‌کند، انتقال مالکیت را صرفاً به صاحب قانونی حساب محدود کند.

ایدهٔ اصلی بلاک‌چین، استفاده از یک معیار امنیتی دیجیتال مانند امضای دیجیتال است که معادل امضاهای دست‌نویس است.

از سوی دیگر، حساب‌های مبتنی بر قرارداد هوشمند حساب‌هایی هستند که کد قرارداد هوشمند، در آن‌ها قرار می‌گیرد. این حساب‌ها نیز مانند حساب‌های با مالکیت خارجی، دارای یک آدرس منحصربه‌فرد هستند؛ اما تفاوت آن‌ها در این است که در حساب‌های مبتنی بر قرارداد هوشمند، چیزی به‌عنوان کلید خصوصی وجود ندارد و حساب توسط کد قرارداد هوشمند محافظت می‌شود. برای درک بهتر چگونگی کارکرد حساب مبتنی بر قرارداد هوشمند، به مثال زیر توجه کنید: فرض کنید که شما قرارداد هوشمندی را طراحی کرده‌اید که قرار است در صورت دریافت ۱۰ اتر، این اترها را به‌صورت هم‌زمان و مساوی در بین ۵ نفر تقسیم کند. شما این شرایط را در قرارداد هوشمند خود کدنویسی کرده‌اید و پنج آدرسی که قرار است اترها به آن‌ها ارسال شوند را نیز از قبل مشخص نموده‌اید. حال تنها چیزی که باقی می‌ماند، ارسال ۱۰ اتر به‌حساب این قرارداد هوشمند است. برای ارسال ۱۰ اتر به این حساب، کافی است که شما وارد حساب کاربری (همان حساب با مالکیت خارجی) خود شده و ۱۰ اتر را به شکل یک تراکنش معمولی، به آدرس حساب قرارداد هوشمند خود ارسال کنید. به‌محض دریافت این مقدار، این قرارداد به‌صورت خودکار و غیرقابل‌توقف، به هر یک از پنج آدرس از پیش تعیین شده مقدار ۲ اتر را ارسال خواهد کرد. این مثال یکی از موارد استفاده ساده اما بسیار کاربردی و محوری قرارداد هوشمند است؛ بنابراین می‌توان این‌گونه جمع‌بندی کرد که یک حساب مالکیت خارجی می‌تواند با استفاده از کلید خصوصی‌اش یک تراکنش انجام دهد، آن را امضا کند و از این طریق، پیامی را به یک حساب مالکیت خارجی یا حساب مبتنی بر قرارداد دیگر ارسال کند. پیام قابل انتقال بین دو حساب با مالکیت خارجی، یک نوع «انتقال ارزش» ساده است. اما پیامی که از یک حساب مالکیت خارجی به‌حساب مبتنی بر قرارداد فرستاده می‌شود، فراتر از انتقال ارزش است. این پیام کد آن حساب را فعال کرده و به‌این‌ترتیب، حساب مبتنی بر قرارداد می‌تواند اقدامات مختلفی نظیر انتقال توکن‌ها، نوشتن چیزی روی فضای ذخیره‌سازی داخلی، ایجاد توکن‌های جدید، انجام یک سری محاسبات و ایجاد قراردادهای جدید را انجام دهد. تراکنش در واقع دستورالعملی است که حالت حساب بر اساس آن تغییر می‌یابد. این دستورالعمل به‌صورت رمزنگاری شده امضا شده و توسط یک حساب با مالکیت خارجی ایجاد و به بلاک‌چین اعلام می‌شود. هر بلاک مجموعه‌ای از تراکنش‌ها و در واقع مانند دستورالعملی است که به شبکه اطلاع می‌دهد حالت جهانی (global state) بعدی به چه صورت باشد. به‌طورکلی تراکنش‌ها در شبکه اتریوم سه نوع هستند:

۱. از یک حساب با مالکیت خارجی (EOA) به یک حساب با مالکیت خارجی (EOA)
۲. از یک حساب با مالکیت خارجی (EOA) به یک حساب قرارداد هوشمند (CA)
۳. از یک حساب با مالکیت خارجی به یک حساب صفر (Zero)

هر سه نوع تراکنش در شبکه اتریوم، توسط یک حساب با مالکیت خارجی (انسان) آغاز می‌شوند. به تعبیر دیگری می‌توان گفت تراکنش‌های اتریوم همچون پلی هستند که اطلاعات دنیای خارجی را به حالت داخلی شبکه اتریوم متصل می‌کنند.

۱. تراکنش‌های نوع اول میان دو انسان صورت می‌گیرد؛
۲. تراکنش‌های نوع دوم میان انسان و یک قرارداد هوشمند؛
۳. تراکنش نوع سوم توسط یک انسان (حساب با مالکیت خارجی) فرستاده شده و گیرنده‌ای ندارد.

این نوع تراکنش‌ها حاوی کد قرارداد هوشمند هستند و در صورت تأیید، قرارداد هوشمند را روی بلاک‌چین ایجاد می‌کنند. به‌محض ثبت شدن این قرارداد در بلاک‌چین، یک آدرس عمومی به آن اختصاص می‌یابد و سپس قرارداد آماده فعال‌سازی و استفاده توسط تراکنش‌های دیگر خواهد بود. همچنین قراردادهایی که در بلاک‌چین اتریوم موجود هستند نیز می‌توانند از طریق پیام‌ها (تراکنش‌های داخلی) با سایر قراردادها صحبت و تعامل داشته باشند. پیام‌های ردوبدل شده میان قراردادهای هوشمند را می‌توان شبیه به تراکنش‌ها در نظر گرفت؛ با این تفاوت که این تراکنش‌ها توسط اکانت‌های با مالکیت خارجی ایجاد نمی‌شوند بلکه توسط خود قراردادهای هوشمند ایجاد می‌شوند. توجه داشته باشید که قرارداد هوشمند هیچگاه به‌خودی‌خود کاری انجام نمی‌دهد و برای فعال‌شدن، نیازمند ارسال یک تراکنش فعال‌سازی به آدرس این قرارداد هستیم. نتیجه این تعامل، پس از ماین شدن تراکنش در بلاک‌چین ثبت می‌شود. نکته جالب اینجاست که هر تراکنشی که قرارداد هوشمندی را فعال کرده یا از آن استفاده کند، توسط همه نودهای اتریوم اجرا می‌شود. در نتیجه به‌منظور ماین کردن یک تراکنش در یک بلاک، باید محاسبات مربوط به قرارداد استفاده شده در این تراکنش نیز توسط همه نودها اجرا شود. بلاک‌چین اتریوم یک شبکه مبتنی بر پیام است. طبق متن وایت پیپر اتریوم، «پیام‌ها» در شبکه اتریوم، به نحوی شبیه به «تراکنش‌ها» در شبکه بیت‌کوین هستند، اما ۳ تفاوت اساسی وجود دارد:

- ✓ اول اینکه یک پیام در شبکه اتریوم، هم می‌تواند توسط یک موجودیت خارجی و هم توسط قراردادها ایجاد شود؛ درحالی‌که یک پیام بیت‌کوینی فقط توسط یک موجودیت خارجی ایجاد می‌شود.
- ✓ دوم اینکه پیام‌ها در شبکه اتریوم، صراحتاً می‌توانند حاوی داده‌ها و اطلاعات باشند (که در بیت‌کوین این‌گونه نیست)؛
- ✓ سومین تفاوت اینکه اگر گیرنده پیام در شبکه اتریوم یک حساب مربوط به قرارداد هوشمند باشد، می‌تواند به این پیام پاسخ دهد. این بدان معنی است که پیام‌ها در شبکه اتریوم، می‌توانند دربردارنده مفاهیم توابع نیز باشند.

حساب‌ها را می‌توان از طریق تراکنش‌های انجام‌شده و ارسال‌شده به شبکه بلاک‌چین توسط EOA یا CA تغییر داد، درحالی‌که گیرنده تراکنش می‌تواند آدرس EOA (یعنی قرارداد هوشمند) یا آدرس CA (یعنی کاربر) باشد [۱۵]. علاوه بر گیرنده ذکر شده، تراکنش‌های اتریوم نیز شامل امضای دیجیتالی است که فرستنده تراکنش، مقدار رمز را برای تراکنش مشخص می‌کند. مواردی که از فرستنده به گیرنده منتقل خواهند شد و یک حوزه اطلاعاتی اختیاری که می‌تواند درصورتی‌که گیرنده یک EOA است، مورداستفاده قرار گیرد. به‌منظور جلوگیری از حملات سرویس در شبکه بلاک‌چین، برای هر تراکنش باید حدی را تعریف کند که مشخص کند چند مرحله محاسباتی برای انجام تراکنش مجاز است. هر چه معامله از نظر محاسباتی گران‌تر باشد یا مقدار داده‌های ذخیره‌شده در یک حالت به‌عنوان بخشی از معامله بیشتر شود، به نوبه خود مراحل مورد نیاز برای انجام موفقیت‌آمیز یک معامله را افزایش می‌دهد. علاوه بر این، تراکنش نیز باید شامل مقداری باشد که نشان‌دهنده هزینه باشد، که فرستنده مایل به پرداخت آن در هر مرحله محاسباتی است [۱۵]. کاربران تراکنش‌ها را با استفاده از نرم‌افزار اختصاصی یا کیف پول امضا و منتشر می‌کنند. انواع زیادی کیف پول مانند کیف پول کاغذی، کیف پول همراه، کیف پول آنلاین، کیف پول سخت‌افزاری و یک کیف رومیزی وجود دارد. ویژگی مشترک هر نوع کیف پول این است که همه آن‌ها کلید خصوصی کاربر

را اداره می‌کنند، که برای انجام اقدامات (یعنی معاملات) در برنامه‌های کاربردی غیرمتمرکز مورد نیاز است [۱۶]. در این مقاله، خود را محدود به تراکنش‌هایی می‌کنیم که دریافت کنندگان، آن‌ها را به‌عنوان CA یا EOA تعریف می‌کنند و از طریق برنامه‌های غیرمتمرکز به شبکه بلاک‌چین پخش می‌شوند [۱۷]. کاربر با یک برنامه کاربردی غیرمتمرکز تعامل می‌کند و امضای دیجیتال تراکنش‌ها را با کیف پول دسکتاپ انجام می‌دهد، که کلید خصوصی یک کاربر را بر روی دستگاه محلی کاربر، رمزنگاری شده با رمز عبور نگه می‌دارد. برای توصیف فرایند فعلی تعامل کاربر با یک برنامه کاربردی غیرمتمرکز و در نتیجه، با یک شبکه بلاک‌چین، سناریوی مورد کاربرد زیر را تعریف می‌کنیم: یک کاربر با کیف پول دسکتاپ می‌خواهد مقداری از ارز دیجیتال (به‌عنوان مثال، Ether) را از طریق یک برنامه کاربردی غیرمتمرکز به یک آدرس CA یا EOA دیگر منتقل کند. با استفاده رمز عبور در کیف پول، کاربر به‌حساب بلاک‌چین خود (یعنی کلید خصوصی) و برقراری ارتباط با شبکه بسته (مانند شبکه اصلی عمومی) دسترسی پیدا می‌کند. او با یک کیف پول باز و ارتباط برقرار شده با شبکه بلاک‌چین، توانایی استفاده از برنامه‌های کاربردی غیرمتمرکز را به دست می‌آورد. سپس کاربر یک رابط کاربری غیرمتمرکز را در یک مرورگر باز می‌کند که شامل شکلی است که در آن کاربر نیاز به پر کردن مقدار ارز دیجیتال برای انتقال و آدرس گیرنده دارد. پس از تکمیل فرم، کاربر چنین تراکنشی را با کلیک روی دکمه تأیید می‌کند. برنامه غیرمتمرکز تراکنشی را آماده می‌کند که برای بازبینی دستی و امضای دیجیتالی به کاربر فرستاده می‌شود. در این مرحله، یک بازبینی دستی از سوی کاربر مورد نیاز است. بازبینی دستی برای کاربران ضروری است که تصمیم بگیرند آیا تراکنش پیشنهاد شده توسط برنامه کاربردی غیرمتمرکز معتبر است (به‌عنوان مثال، جعلی نیست) و باعث از دست دادن بالقوه ناخواسته وجوه (به‌عنوان مثال، ارز دیجیتال) برای کاربر نمی‌شود [۱۸] [۱۹] . کاربر این اختیار را دارد که تراکنش را تأیید کند، به‌عنوان مثال به‌صورت دیجیتالی تراکنشی را امضا کند که انجام فرایند رمزنگاری را به گیرنده تأیید می‌کند یا معامله‌ای را که انتقال ارز دیجیتال را به گیرنده قطع می‌کند رد کند [۲۰] [۲۱] .

اگر کاربر بخواهد یک تراکنش را امضا کند، این تراکنش به یک برنامه کاربردی غیرمتمرکز فرستاده می‌شود و به شبکه بلاک‌چین پخش می‌شود. تحقیقات زیادی در مورد بی‌قاعدگی‌های تشخیص در داده‌های سری زمانی انجام‌شده که به طور مفصل در [۲۲] [۲۳] مرور شده‌اند. روش‌های تحلیل سری‌های زمانی سنتی تنها با تغییرات داده‌های مشاهده شده سروکار دارند و نه با فرکانس و مقدار ترکیب آن [۲۰] همچنین رویکرد دیگر در تحلیل یک سری، استفاده از شبکه‌های عصبی به طور خاص، شبکه‌های عصبی مصنوعی تکرار شونده (RNN)، با استفاده از معماری حافظه کوتاه‌مدت بلند و انواع آن است. اشکال در چنین رویکردهای RNN این است که آموزش مدل به داده‌های زیادی نیاز دارد، که در نتیجه زمان زیادی می‌برد. ازآنجاکه داده‌های تراکنشی یک آدرس محدود هستند، امکان محدودی برای ساخت سیستم تشخیص ناهنجاری با استفاده از RNN برای سری‌های زمانی وجود دارد. از این‌رو، روش‌های سنتی تشخیص ناهنجاری [۲۴]، که با مقدار کمی از داده‌ها کار می‌کنند و زمان کمتری برای ساخت مدل صرف می‌کنند، باید مورداستفاده قرار گیرند.

٤. هوش مصنوعی

اصطلاح هوش مصنوعی جهت توصیف ماشینی استفاده می‌کنند که عملکردهای «شناختی» را از روی ذهن انسان‌ها همچون یادگیری و حل مسئله تقلید می‌کنند. در این مقاله با استفاده از الگوریتم‌های یادگیری ماشین زیر به حل مسئله می‌پردازیم:

٤-١. الگوریتم خوشه‌بندی K-Means

الگوریتم K-Means جز روش‌های افرازی رویکرد خوشه‌بندی است. در روش‌های افرازی با فرض داشتن یک پایگاه‌داده با n شی K افراز از این داده‌های اشیا درست می‌کند. طور یکه هر افراز یک خوشه را نشان می‌دهد و K<n. پس داده‌های اشیا در K گروه خوشه‌بندی شده و دارای دو شرط زیر هستند:

الف- هر گروه حداقل یک شی دارد.

ب- هر شی تنها به یک گروه تعلق دارد.

در روش افرازی برای **K** معلوم، یک افراز ابتدایی ایجاد می‌شود. سپس یک روش جابه‌جایی تکراری ۵ را به کاربردی که تلاش به بهبود افراز بندی دارد. به این صورت که اشیا را از یک گروه به دیگر گروه‌ها می‌برد. یک معیار عمومی برای یک افرازبندی خوب این است که اشیا در یک خوشه به هم نزدیک یا به یکدیگر وابسته باشند و در مقابل اشیا در خوشه‌های مختلف از یکدیگر دور یا تاحدامکان متفاوت باشند.

در الگوریتم K-Means که هر خوشه با میانگین یا مرکز آن نمایش داده می‌شود. K را به‌عنوان ورودی گرفته و مجموعه **n** شی را به K خوشه افراز می‌کند. طور یکه سطح شباهت داخلی خوشه‌ها بالا بوده و سطح شباهت اشیا بیرون خوشه‌ها پایین باشد. شباهت هر خوشه نسبت به متوسط اشیا آن خوشه سنجیده شده که این متوسط مرکز خوشه نیز نامیده می‌شود و الگوریتم به‌صورت زیر کار می‌کند:

ورودی: **K** تعداد خوشه‌ها ویک پایگاه‌داده شامل **n** شی

خروجی: یک مجموعه از **K** خوشه که معیار مربع خطا را حداقل کند.

الگوریتم:

۱) به‌صورت تصادفی **K** نقطه دلخواه را به‌عنوان مراکز خوشه‌های ابتدایی انتخاب کن (بهتر است **K** نقطه از **n** نقطه موجود انتخاب شود)
۲) هر شی را باتوجه به بیشترین شباهت آن به مراکز خوشه‌ها، به خوشه‌ها تخصیص بده
۳) مراکز خوشه‌ها را به‌روز کن به این معنی که برای هر خوشه میانگین اشیا آن خوشه را محاسبه کن
٤) باتوجه‌به مراکز جدید خوشه‌ها به قدم دوم برگرد تا هنگامی که هیچ تغییری در خوشه‌ها رخ ندهد.

در عمل این الگوریتم یک روش هیوریستیکی برای کاهش معیار مربع خطاست که در رابطهٔ زیر آمده است:

$$E = \sum\sum|p - m_i|^2$$

دراین‌رابطه E مجموع مربع خطا برای تمام اشیا پایگاه‌داده است. P نقطه‌ای در فضاست که نمایانگر یک شی است، و mi میانگین خوشه **Ci** است که نقطه p به آن متعلق است.

۲-٤. الگوریتم SVM

دسته‌بندی کاربران متصل به سرور به معنی انتصاب کاربران به دسته‌های از پیش تعیین شده است که در ده سال اخیر تمام توجهات را به خود جلب کرده است. این مسئله به‌خاطر دسترسی کاربران و تعداد زیاد هکرها و نیاز مبرم به سازماندهی آنهاست. در جامعه تحقیقاتی روش اصلی در این زمینه، روش-های بر اساس یادگیری ماشین هستند.

یادگیری تحت نظارت، یک روش عمومی در یادگیری ماشین است که یک شخص ناظری وجود دارد که برچسب‌گذاری برای تمایز دسته‌های مختلف را بر روی کاربران و هکرها اعمال می-کند. یک مجموعه از مثال‌های یادگیری وجود دارد که به‌ازای هر ورودی، مقدار خروجی و یا تابع مربوطه نیز مشخص است. هدف سیستم یادگیر به‌دست‌آوردن فرضیه‌ای است که تابع و یا رابطه بین ورودی و خروجی را حدس بزند.

رده‌بندی کاربران و هکرها یک مسئله مهم در علوم مرتبط با شبکه، امنیت و علوم کامپیوتر است. این کار ممکن است به‌صورت دستی یا به‌صورت الگوریتمی انجام شود:

- ✓ روش دستی: همانند کاری که در کتابخانه انجام می-شود و کاربران به دسته‌های مختلف تقسیم می‌شوند.
- ✓ روش الگوریتمی: رده‌بندی اصولاً در علم کامپیوتر و در مبحث داده‌کاوی جای می‌گیرد و به‌صورت یادگیری ماشین انجام می‌شود.

بر اساس موضوع و یا بر اساس یک ویژگی خاص(مانند تعداد رجوع به سایت ممکن است کاربران و هکرها دسته‌بندی شوند.

[5] Itterative Relocation Techniqe

در دسته‌بندی موضوعی ابتدا برای یادگیری کاربران و هکرهای با موضوع معین به‌عنوان نمونه به ماشین داده می‌شود و ماشین باتوجه‌به کلمات داخل هر سند به یادگیری می‌پردازد و با درنظرگرفتن احتمال وجود کلمات به پیش‌بینی موضوعی سندهای دیگر می‌پردازد. هدف این دسته الگوریتم‌ها تشخیص و متمایزکردن الگوهای پیچیده در داده‌هاست (از طریق کلاسترینگ، دسته‌بندی، رنکینگ، پاک‌سازی و غیره).

مبنای کاری SVM دسته‌بندی خطی داده‌ها است و در تقسیم خطی داده‌ها سعی می‌کنیم خطی را انتخاب کنیم که حاشیه اطمینان بیشتری داشته باشد

الگوریتم SVM، در هرجایی که نیاز به تشخیص الگو یا دسته-بندی در کلاس‌های خاص باشد می‌توان استفاده کرد. آموزش نسبتاً ساده‌ای دارد و برای داده‌های با ابعاد بالا تقریباً خوب جواب می‌دهد. زمان اجرای آن نسبت به سایر طبقه‌بندی‌ها از جمله Decision Tree، C4.5، Naïve Bayesian و ... کمتر است. زیرا در مرحله Training از داده‌های پایگاه‌داده، بردارهای پشتیبان را استفاده می‌کند.

امروزه دسته‌بندی مهم‌ترین مسئلهٔ یادگیری با ناظر، در بسیاری از حوزه‌ها و بخصوص تحلیل داده‌های آماری و بازیابی اطلاعات موردتوجه بسیاری قرار گرفته است

۵. الگوریتم پیشنهادی

در این بخش، روش پیشنهادی را برای امضای دیجیتالی خودکار در معاملات شخصی بلاک‌چین ارائه می‌دهیم و نشان خواهیم داد که چگونه روش پیشنهادی برای بازبینی خودکار و امضای دیجیتال تراکنش‌های پیشنهاد می‌شود. تاریخچه تراکنش یک آدرس به شکل داده‌های سری زمانی است که در آن داده‌ها به‌صورت متوالی در طول جدول زمانی ذخیره می‌شوند. تشخیص تراکنش‌های غیرمعمول از معمول در این مقاله بررسی می‌شود. روش‌های یادگیری با نظارت برای تشخیص تراکنش‌های غیرمعمول در این مقاله استفاده شده است. چالش اصلی در این مقاله عدم برچسب‌گذاری داده‌های موجود است که در آن تراکنش‌های غیرمعمول برچسب‌گذاری نشده است بدین منظور در این مقاله یک روش ترکیبی از الگوریتم‌های یادگیری با نظارت و بدون نظارت استفاده شده است که در آن الگوریتم K-Means برای برچسب‌گذاری استفاده می‌شود همان‌طور که در شکل ۲ نشان‌داده‌شده است به کمک خوشه‌بندی می‌تواند داده‌های مربوط به تراکنش‌های مالی را برچسب‌گذاری نمود.

و سپس داده‌های برچسب‌گذاری شده به الگوریتم SVM برای دسته‌بندی تراکنش‌های می‌پردازد.

۵-۱. استخراج ویژگی به‌منظور شناسایی حساب

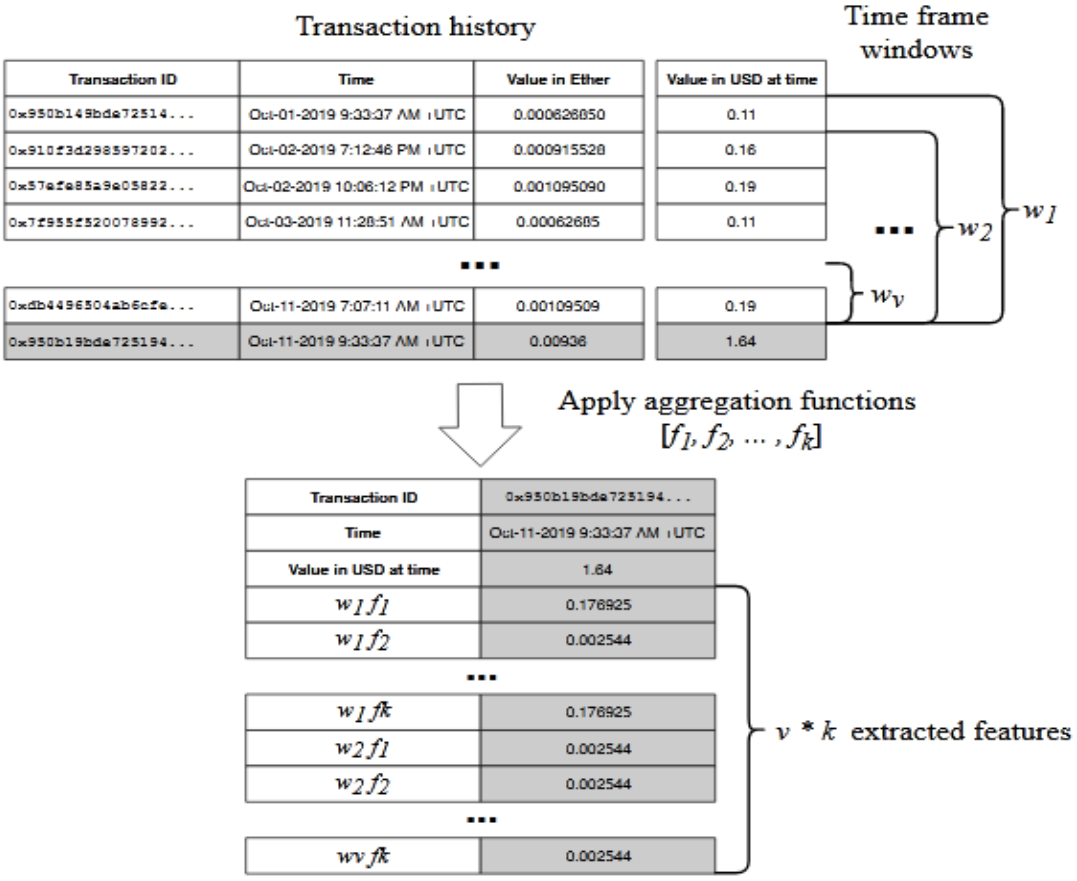
اتریوم متشکل از حساب‌هایی است که در آن هر حساب آدرس ۲۰ بایتی منحصربه‌فردی دارد. هر معامله اطلاعاتی دارد که شامل موارد زیر است:

۱- برچسب زمانی تراکنش
۲- ارزش تراکنش در مقدار دلار آمریکا متناظر آن در زمان تراکنش

هر آدرس دارای فهرستی از تاریخ تراکنش‌ها و سایر پارامترهای مرتبط است که از داده‌های زیر برای شناسایی آن استفاده می‌شود:

- ✓ هش معامله
- ✓ شماره بلوک
- ✓ مهر زمان (یونیکس)
- ✓ تاریخ و زمان (m / dd / yyyy)
- ✓ از (آدرس Ethereum)
- ✓ به (آدرس Ethereum)
- ✓ مقدار خروجی (ETH)
- ✓ هزینه معامله (ETH)
- ✓ هزینه معامله (دلار آمریکا)
- ✓ قیمت تاریخی (دلار آمریکا)

برای تحلیل سری‌های زمانی از روش پنجره غلتان استفاده می‌شود که کمک می‌کند ویژگی‌های جدیدی از آن استخراج شود. استخراج ویژگی پنجره غلتان برای سری‌های زمانی یک روش است که در آن داده‌های سری زمانی به ترتیب از اولین داده‌ها تحلیل می‌شوند، اندازه پنجره، به‌صورت **w** تعریف می‌شود که تعداد اندازه‌گیری‌ها در یک پنجره است.



شکل ۱. استخراج ویژگی در بستر بلاک‌چین به‌منظور دسته‌بندی

در این مقاله، اندازه پنجره در حال حرکت به‌عنوان چارچوب زمانی تعریف می‌شود. هر آدرس بلاک‌چین می‌تواند الگوهای مختلفی از معاملات داشته باشد.

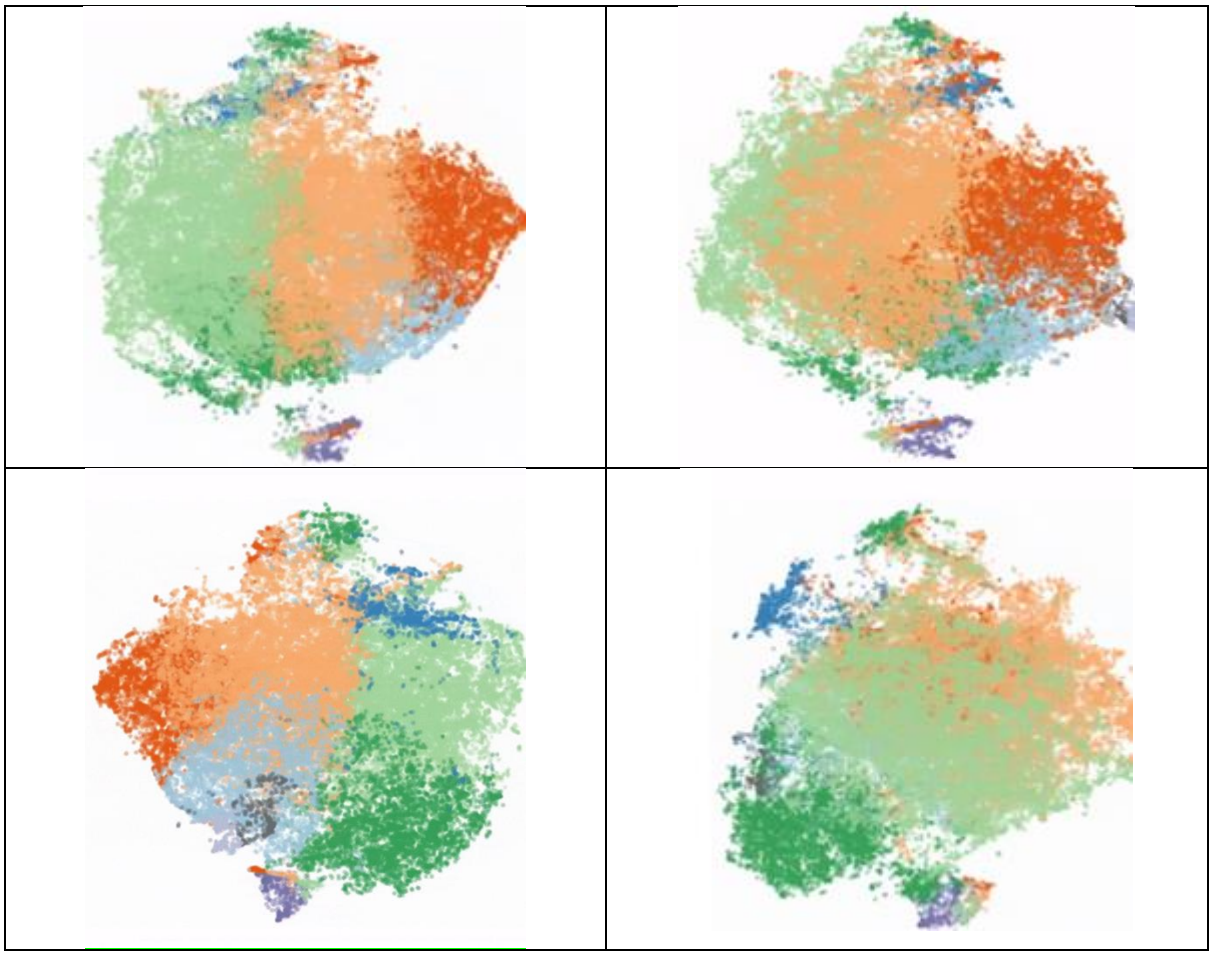
۲-۵. خوشه‌بندی تراکنش‌ها

آدرس‌های اتریوم یکی از ویژگی‌های متفاوت فناوری بلاک‌چین نسبت به تکنولوژی‌های مشابه و امکان فعالیت ناشناس بر روی آن است. بااین‌حال کاربران از آدرس‌هایی استفاده می‌کنند که شناسه‌هایی منحصربه‌فرد و غیرقابل‌تغییر هستند. در این مقاله با استفاده از خوشه‌بندی آدرس‌های اتریوم و تحلیل رفتار کاربران بر اساس فعالیت آن‌ها، امکان دسته‌بندی و شناسایی تراکنش‌ها مورد بررسی قرار می‌گیرد. آدرس‌های اتریوم کاربران ممکن است ناشناس باشند، اما آدرس آن‌ها دارای شناسه‌های منحصربه‌فردی هستند که اثری قابل‌مشاهده برای عموم را از خود بر روی بلاک‌چین به جا می‌گذارند. الگوریتم خوشه‌بندی بر اساس میزان فعالیت تراکنش ایجاد شده است که کاربران اتریوم را به زیرگروه‌های رفتاری متمایزی تقسیم‌بندی می‌کند. این الگوریتم می‌تواند پیش‌بینی کند که آیا یک آدرس به یک صرافی رمزارز، یک استخراج‌کننده و یا یک کیف پول ICO تعلق دارد. بسیاری از

افراد اعتقاد دارند که رمزارزها امکان ناشناسی دیجیتال را مهیا می‌کنند و این اعتقاد تا حدودی صحیح است. بااین‌حال، اتریوم به طور گسترده‌تری استفاده می‌شود و انعطاف‌پذیری زیاد آن منجر به شکل‌گیری یک مجموعه‌داده عمومی غنی از رفتار تراکنشی کاربران شده است. آدرس‌های شناخته‌شده‌ای که به صرافی‌ها، استخراج‌کننده‌ها و ICO ها تعلق دارند، به طور کیفی نشان می‌دهند که نتایج خوشه‌بندی دقیق هستند.

در شکل ۲ خوشه‌بندی در پایگاه‌داده با استفاده از SQL [25] و با زبان پایتون مدل شده است.

در این خوشه‌بندی مشخص می‌شود که یک آدرس به یک صرافی رمزارز، یک استخراج‌کننده و یا یک کیف پول و یا تراکنش‌های ناسالم قرار دارد. خوشه‌بندی به روش **K-Means** و در ۵ خوشه انجام شده است.



شکل ۲. نمایشی سه‌بعدی از فضای آدرس‌های اتریوم

نمایشی سه‌بعدی از نتایج خوشه‌بندی آدرس‌های معلوم سمت چپ هستند. رفتار کاربر با استفاده از خوشه مربوط به آن نتیجه‌گیری می‌شود، تراکنش‌های سالم از غیرمعمول در نتایج خوشه‌بندی قابل تفکیک است که می‌تواند برچسب ایجاد شده در مرحله بعد به کار گرفته شود. ناحیه مشکی رنگ ناحیه تراکنش‌های غیرنرمال است.

۳-۵. دسته‌بندی تراکنش‌ها

در این مقاله هدف ارائه راهکار برای ترکیب روش خوشه‌بندی با الگوریتم دسته‌بندی است. خوشه‌بندی به کمک الگوریتم K-Means انجام می‌شود و داده‌ها برچسب‌گذاری می‌شوند. به کمک داده‌های برچسب‌گذاری می‌توان تراکنش معمول از غیرمعمول را برچسب‌گذاری نمود. خروجی الگوریتم

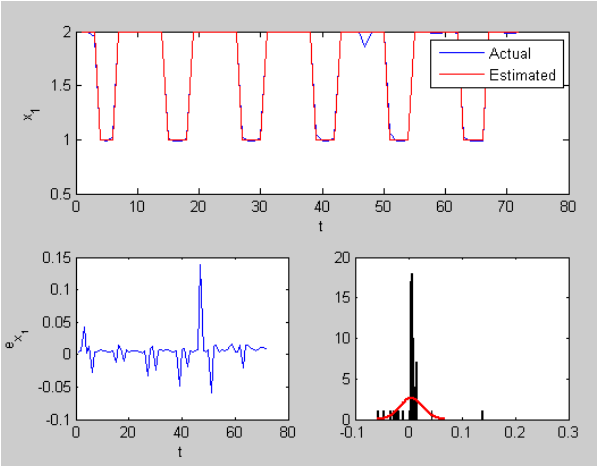
خوشه‌بندی می‌تواند برای الگوریتم‌های دسته‌بندی به کار گرفته شود. در این مقاله از الگوریتم دسته‌بندی SVM (بردار پشتیبان ماشین) به‌منظور کلاس‌بندی و طبقه‌بندی استفاده شده است. مسئله خوشه‌بندی به مسئله کلاس‌بندی تبدیل می‌شود که در آن ورودی‌ها هش معامله، شماره بلوک، مهر زمان، تاریخ و زمان، آدرس ارسال Ethereum، آدرس دریافت Ethereum، مقدار خروجی (ETH)، هزینه معامله(ETH)، هزینه معامله، قیمت است و خروجی نوع تراکنش (سالم یا ناسالم بودن) است که از الگوریتم خوشه‌بندی به‌دست‌آمده است.

شکل ۳. روند کلی روش پیشنهادی

٦. ارزیابی و نتایج

در این بخش بر روی ارز دیجیتال اتریوم، به‌عنوان ارز دیجیتالی با بیش‌ترین تعداد توسعه دهندگان فعال و محققانی که بر روی این ارز علاقه‌مند هستند تمرکز خواهیم کرد و همچنین در بخش شبیه‌سازی شبکه اتریوم را مورداستفاده قرار خواهیم داد. باتوجه‌به اینکه داده‌های پایگاه‌داده [25] حجم بالایی از داده‌ها را دارا هستند از ویژگی‌هایی استفاده می‌شود که در دسته‌بندی نقش مؤثری دارند و از داده‌هایی که در دسته‌بندی تأثیرگذار نیستند چشم‌پوشی شده است.

نتایج مدل‌سازی با SVM و خطای مدل‌سازی به‌صورت زیر به‌دست‌آمده است. تخمین بین دو کلاس تراکنش‌های سالم و غیرنرمال در شکل ٤ نشان‌داده‌شده است که داده‌های تست به SVM داده شده است و باید دو کلاس را از یکدیگر تفکیک نماید. همچنین خطای تخمین و توزیع خطای تخمین در زیربخش‌های شکل نشان‌داده‌شده است. پیش‌بینی نمونه‌های آدرس‌های سالم از ناسالم در ۷۵ نمونه تست انجام گرفت. پیش‌بینی هر نمونه و مقایسه با مقدار اصلی در شکل ٤ بالا و خطای پیش‌بینی در شکل ٤ پایین چپ و هیستوگرام خطا در شکل ٤ پایین راست نمایش‌داده‌شده است. نمودار هیستوگرام خطا نشان می‌دهد که خطای تشخیص دسته‌بندی به‌صورت گوسی بوده و تابع چگالی احتمال آن نرمال است.



شکل ٤. خطا پیش‌بینی و مدل‌سازی توزیع خطا با استفاده از SVM

نتایج روش پیشنهادی در این مقاله که با استفاده از ترکیب الگوریتم K-Means و SVM است با روش SVM مورد مقایسه قرار گرفته است و نتایج نشان می‌دهد که روش پیشنهادی دقت بالاتری نسبت به SVM از خود نشان می‌دهد. امکان کلاس‌بندی تراکنش‌ها در BIG DATA فراهم گردید و دقت ۸۹ درصد پیش‌بینی درست در نمونه‌ها کارایی روش پیشنهادی را نشان می‌دهد. دقت پیش‌بینی درصد تشخیص درست کلاس‌بندی را نسبت به کل داده‌ها نشان می‌دهد.

۷. نتیجه‌گیری

در این مقاله، روشی برای کنترل دسترسی با استفاده از امضای شخصی و خودکار معاملات بلاک‌چین برای تسهیل تبادلات اینترنت اشیا معرفی کردیم. برای شبیه‌سازی الگوریتم پیشنهادی، مجموعه‌ای از داده‌های تست در نظر گرفته شده و سپس بر روی کاربر (سالم، هکر) متصل به سرور دسته‌بندی صورت‌گرفته است و آنگاه باتوجه‌به ویژگی‌های هر کاربر می‌توان SVM را به کاربرد.

در روش ارائه‌شده از کاربرد نوآورانه هوش مصنوعی در حوزه تکنولوژی بلاک‌چین، به‌ویژه روش‌های یادگیری ماشین استفاده شده است که برای خودکار کردن فرایند امضای قرارداد و همچنین تأمین امنیت کاربر در برابر تقلب امضای دیجیتال کاربرد دارد. روش پیشنهادی در نرم‌افزار قرار دارد که بر روی تکنولوژی بلاک‌چین و با کیف دستی کاربر مبتنی بر بلاک‌چین عمل می‌کند. علاوه بر این، سیستم تشخیص ناهنجاری که هسته روش امضای خودکار است، داده‌ها (یعنی مدل تشخیص ناهنجاری) را بر روی دستگاه کاربر اجرا و ذخیره می‌کند. باتوجه‌به کاربرد تعریف‌شده در این مقاله، این روش می‌تواند برای بهبود قابلیت استفاده برنامه‌های کاربردی غیرمتمرکز استفاده شود. علاوه بر این، استفاده از این روش در محیط‌هایی که به اجرای مداوم معاملات بلاک‌چین و فعالیت‌های تبادل منظم نیاز دارند، می‌تواند از کلاهبرداری و یا دیگر فعالیت‌های بدخواهانه‌ای که ممکن است منجر به ازدست‌رفتن وجوه ذخیره‌شده در کیف پول شود جلوگیری نماید.

۸. مراجع (Reference)

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review,* p. 21260, 2008.

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper,* vol. 3, no. 37, 2014.

[3] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," *arXiv preprint arXiv:1802.04351,* 2018.

[4] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why johnny still can't encrypt: evaluating the usability of email encryption software," in *Symposium On Usable Privacy and Security*, 2006, pp. 3-4: ACM.

[5] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2006, pp. 591-600.

[6] E. E. Schultz, R. W. Proctor, M.-C. Lien, and G. Salvendy, "Usability and security an appraisal of usability issues in information security methods," *Computers & Security,* vol. 20, no. 7, pp. 620-634, 2001.

[7] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller, "How to make secure email easier to use," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2005, pp. 701-710.

[8] S. Ruoti and K. Seamons, "Johnny's journey toward usable secure email," *IEEE Security & Privacy,* vol. 17, no. 6, pp. 72-76, 2019.

[9] T. Pham and S. Lee, "Anomaly detection in bitcoin network using unsupervised learning methods," *arXiv preprint arXiv:1611.03941,* 2016.

[10] T. Pham and S. Lee, "Anomaly detection in the bitcoin system-a network perspective," *arXiv preprint arXiv:1611.03942,* 2016.

[11] M. Ostapowicz and K. Żbikowski, "Detecting fraudulent accounts on blockchain: a supervised approach," in *International Conference on Web Information Systems Engineering*, 2020, pp. 18-31: Springer.

[12] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust Bitcoin fraud detection," in *2016 Information Security for South Africa (ISSA)*, 2016, pp. 129-134: IEEE.

[13] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE access,* vol. 6, pp. 5112-5127, 2018.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017, pp. 557-564: IEEE.

[15] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper,* vol. 151, no. 2014, pp. 1-32, 2014.

[16] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *2018 IEEE Middle East and North Africa*

Communications Conference (MENACOMM), 2018, pp. 1-6: IEEE.

[17] X. Liu, K. Muhammad, J. Lloret, Y.-W. Chen, and S.-M. Yuan, "Elastic and cost-effective data carrier architecture for smart contract in blockchain," *Future Generation Computer Systems,* vol. 100, pp. 590-599, 2019.

[18] X. Jin, S. Sarkar, K. Mukherjee, and A. Ray, "Suboptimal partitioning of time-series data for anomaly detection," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, 2009, pp. 1020-1025: IEEE.

[19] P. K. Chan and M. V. Mahoney, "Modeling multiple time series for anomaly detection," in *Fifth IEEE International Conference on Data Mining (ICDM'05)*, 2005, p. 8 pp.: IEEE.

[20] M. Teng, "Anomaly detection on time series," in *2010 IEEE International Conference on Progress in Informatics and Computing*, 2010, vol. 1, pp. 603-608: IEEE.

[21] J. Ma and S. Perkins, "Time-series novelty detection using one-class support vector machines," in *Proceedings of the International Joint Conference on Neural Networks, 2003.*, 2003, vol. 3, pp. 1741-1745: IEEE.

[22] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier detection for temporal data: A survey," *IEEE Transactions on Knowledge and data Engineering,* vol. 26, no. 9, pp. 2250-2267, 2013.

[23] M. Gupta, J. Gao, C. Aggarwal, and J. Han, "Outlier detection for temporal data," *Synthesis Lectures on Data Mining and Knowledge Discovery,* vol. 5, no. 1, pp. 1-129, 2014.

[24] M. A. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, "A review of novelty detection," *Signal processing,* vol. 99, pp. 215-249, 2014.

[25] https://figshare.com/articles/dataset/Dataset_of_transactions_of_10_Ethereum_addresses_controlled_by_a_private_key_each_has_at_least_2000_output_transactions_which_include_a_transfer_of_cryptocurrency_and_all_transactions_are_performed_within_no_longer_than_three_months_period_/11537121