نشریـه علمـی
دانش مالی و تحلیل اوراق بهادار
دوره ۱۵ / شماره ۱ (پیاپی ۵۳) / بهار ۱۴۰۱
صفحه ۱۱۱ تا ۱۲۲

# کنترل دسترسی در قراردادهای هوشمند مالی با استفاده از مدیریت هویت دیجیتالی و یادگیری ماشین برای تسهیل تبادلات اینترنت اشیا

علی آبی زاده[۱]
زاداله فتحی✉[۲]
مهرزاد مینویی[۳]

تاریخ دریافت: ۱۴۰۰/۰۶/۱۷ تاریخ پذیرش: ۱۴۰۰/۱۲/۰۷

**چکیده**

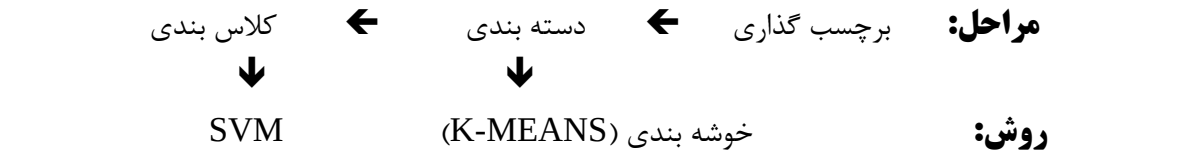
کنترل دسترسی در شبکه بلاکچین یکی از چالش‌هایی است که با رشد شبکه بلاک‌چین با آن روبه‌رو هستیم. در شبکه بلاک‌چین، مجموعه فعالیت‌های مالی کاربران که نیاز به امضای دیجیتال دارد انجام می‌شود، این اطلاعات در سرور بلاک‌چین ذخیره می‌شود. امضای دیجیتال و تایید هویت و صحت تراکنش‌ها به صورت دستی فرآیندی وقت‌گیر بوده و کاربر پسند نیست و از دلایلی است که تکنولوژی بلاکچین به طور کامل پذیرفته نمی‌شود. در این مقاله یک روش نوین براساس ترکیب روش‌های خوشه‌بندی و دسته‌بندی پیشنهاد می‌شود. که 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 به منظور ارزیابی روش پیشنهادی، آزمایش و تجزیه و تحلیل بر روی داده‌های اتریوم انجام شده است و به کمک الگوریتم خوشه‌بندی KMEANS و روش بردار پشتیبان ماشین تراکنش‌های سالم از مشکوک شناسایی می‌شود که این روش توانایی شناسایی با دقت ۸۹ درصد را نشان می‌دهد.

**واژه‌های کلیدی:** بلاکچین؛ اتریوم؛ SVM؛ KMEANS؛ شناسایی تراکنش‌های سالم قراردادهای مالی هوشمند

[۱] دانشجوی دکتری گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. abizadeali70@gmali.com
[۲] استادیارگروه مدیریت مالی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول): z_fathi46@yahoo.com
[۳] استادیارگروه مدیریت مالی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. omm1344@yahoo.com

**۱- مقدمه**

در شبکه بلاک‌چین یک مجموعه فعالیت مرتبط با امضای دیجیتال توسط کاربران با هویت دیجیتالی انجام می‌شود، این اطلاعات در محلی در سرور بلاک‌چین ذخیره می‌شود. که این فرآیند وقت‌گیر است و کاربر پسند نیست، و از دلایلی است که تکنولوژی بلاکچین به طور کامل پذیرفته نمی‌شود. در این پژوهش، یک روش مبتنی بر یادگیری ماشین پیشنهاد می‌شود، که امضای خودکار تراکنش‌های بلاک‌چین را انجام می‌دهد و شناسایی تراکنش‌های غیرعادی را نیز انجام می‌دهد.یکی از اصلی‌ترین چالش‌های تکنولوژی بلاک‌چین، توانایی کاربران برای انتقال پول و اعتبارات بطور مستقیم به یکدیگر درون یک شبکه غیرمتمرکز و توزیع‌شده است که بدون نیاز به شخص ثالث (به عنوان مثال، موسسه 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 به صورت دیجیتالی امضا و تایید شود که توسط الگوریتم امضای دیجیتال انجام می‌شود. استفاده از امضاهای دیجیتال به عنوان یکی از اصلی‌ترین بلوک‌های سازنده فن‌آوری بلاک‌چین برای تضمین یکپارچگی و عدم انکار تراکنش‌ها ضروری است [۱-۲]. در مقاله [۴] نشان می‌دهد که امضای دیجیتال مرتبط با بلاک‌چین با حساب بلاک‌چین آن‌ها (به عنوان مثال، کلید عمومی-خصوصی) در ارتباط است. فرآیند امضا در نرم‌افزار اختصاصی (دیجیتال یا رمزنگاری) کیف پول دیجیتال انجام می‌شود. با کیف پول دیجیتال، کاربران فرآیند امضای دیجیتال را کنترل کرده و تعاملات را در شبکه بلاک‌چین انجام می‌دهند. از آنجا که هر تراکنش با بلاک‌چین باید توسط کاربر به صورت دیجیتالی امضا شود، این امر می‌تواند به مشکلات امنیتی منجر شود. بیشتر مسائل پیرامون موضوعات استفاده از امضای دیجیتالی به پیچیدگی فرآیند امضای دیجیتال مربوط می‌شوند. در صورت نقل و انتقالات مکرر در یک دوره زمانی طولانی، فرآیند امضای دیجیتال را می‌توان به طور سطحی‌تری انجام داد و در نتیجه امنیت دارایی‌های دیجیتال تحت‌تاثیر قرار می‌گیرد. در این وضعیت، عامل‌های مخرب می‌توانند از این رفتار کاربر به عنوان یک مزیت استفاده کنند و تلاش کنند تا امضای تراکنش‌هایی را که اثرات نامطلوبی 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 از ارز دیجیتال است. در این فرآیند، برنامه کاربردی وب، تراکنش را برای فرآیند امضای دیجیتال به کاربر ارایه 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 (به عنوان 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 ماشینی فرآیند امضای دیجیتال تراکنش‌های بلاک‌چین است که خودکار و ساده است و شامل یک سیستم تشخیص تراکنش‌های سالم از تراکنش‌های غیرعادی می‌باشد. در این مقاله با توجه به اطلاعات جمع‌آوری شده از تراکنش‌های ارز دیجیتال اتریوم و مبادلات صورت گرفته[1] یک سیستم هوشمند آموزش داده می‌شود. سیستم آموزش داده شده به کمک الگوریتم SVM ساخته شده است. چالش اصلی این پژوهش در کلاس‌بندی داده‌های بدون برچسب مجموعه ای از تراکنش‌های مالی در بستر اتریوم می‌باشد که باید به کمک روش دسته‌بندی انجام شود. برای استفاده از روش‌های دسته‌بندی نیاز است که داده‌های برچسب‌گذاری شود. برای حل این مشکل از الگوریتم‌های خوشه‌بندی برای برچسب گذاری داده استفاده می‌شود و سپس دسته‌بندی به کمک بردار پشیتبان ماشین صورت می‌گیرد. در ابتدا خوشه‌بندی به کمک KMEANS انجام شده و سپس دسته‌بندی به کمک SVM صورت می‌گیرد (شکل۳).




**۲- بحث و بررسی**

چگونه می‌توان مشکل امنیت کنترل دسترسی در اینترنت اشیا در را با استفاده از بلاک چین و قراردادهای هوشمند حل نمود ؟ چگونه می‌توان با استفاده از قراردادهای هوشمند -اسکریپت قرار گرفته روی بلاک چین فرایندهای چند مرحله ای - را به شکل خودکار انجام دهیم ؟

انواع حساب در بستر بلاکچین به دو دسته حساب با مالکیت خارجی و حساب مبتنی بر قرارداد هوشمند تقسیم می‌شود.

حساب‌های 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 رمز ارزی) کدی است که دسترسی شما به حسابتان را میسر کرده و مانند رمزهای عبور کارت‌های بانکی‌تان عمل می‌کند؛ بدون داشتن کلید خصوصی، امکان دسترسی به حساب و استفاده از رمز ارزتان را نخواهید داشت. برای انجام هر تراکنشی در بلاک چین اتریوم، باید از حساب‌های با مالکیت خارجی استفاده کنید. هر حسابی در بلاک‌چین اتریوم (یا بلاک‌چین هر رمز ارز دیگری)، دارای یک آدرس منحصربفرد است که برای انجام تراکنش‌ها و دریافت و انتقال اتر از آن استفاده می‌شود. آدرس حساب در بلاک‌چین رمز ارزها، 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.

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 منحصر بفرد هستند؛ اما تفاوت آن‌ها در این است که در حساب‌های مبتنی بر قرارداد هوشمند ، چیزی به عنوان 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 به صورت 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 به حساب این قرارداد هوشمند است. برای ارسال ۱۰ اتر به این حساب، کافیست که شما وارد حساب کاربری (یا همان حساب با مالکیت خارجی) خود شده و ۱۰ اتر را به شکل یک تراکنش معمولی، به آدرس حساب قرارداد هوشمند خود ارسال کنید. به محض دریافت این مقدار، این قرارداد به صورت خودکار و غیرقابل توقف، 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 به حساب مبتنی بر قرارداد فرستاده می‌شود، فراتر از انتقال ارزش است. این پیام کد آن حساب را فعال کرده و به این ترتیب، 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 دستورالعمل‌ای است که حالت حساب بر اساس آن تغییر می‌یابد. این دستورالعمل به صورت 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. به طور کلی 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. به محض ثبت شدن این قرارداد در بلاک‌چین، یک آدرس عمومی به آن اختصاص می‌یابد و از این پس، 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 رد و بدل شده میان قراردادهای هوشمند را می‌توان شبیه به تراکنش‌ها درنظر 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 به خودی‌خود کاری انجام نمی‌دهد و برای فعال شدن، 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 به منظور 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 بیت کوین 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؛ درحالی که یک پیام بیت کوینی 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)؛
- و سومین تفاوت اینکه اگر گیرنده پیام در شبکه اتریوم یک حساب مربوط به قرارداد هوشمند باشد، می‌تواند به این پیام پاسخ دهد. این بدان معنیست که پیام‌ها در شبکه اتریوم، می‌توانند در بردارنده مفاهیم توابع نیز باشند.

حساب‌ها را می‌توان از طریق تراکنش‌های انجام‌شده و ارسال‌شده به شبکه بلاک‌چین توسط EOA یا CA تغییر داد، در حالی که گیرنده تراکنش می‌تواند آدرس EOA (یعنی قرارداد هوشمند) یا آدرس CA (یعنی کاربر) باشد [۲- ۱۶]. 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 در صورتی که گیرنده یک EOA است، مورد استفاده قرار گیرد. به منظور 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 به عنوان 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 [۲- ۱۶]. 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 [۱۷-۳]. در این مقاله، خود را محدود به تراکنش‌هایی می‌کنیم که دریافت کنندگان، آن‌ها را به عنوان CA یا EOA تعریف می‌کنند و از طریق برنامه‌های غیرمتمرکز به شبکه بلاکچین پخش می‌شوند [۱۸]. کاربر با یک برنامه کاربردی غیر متمرکز 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 فرآیند 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 (به عنوان مثال، Ether) را از طریق یک برنامه کاربردی غیر متمرکز به یک آدرس CA یا EOA دیگر منتقل کند. با استفاده رمز عبور در کیف پول، کاربر به حساب 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 غیر متمرکز 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 تایید 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 (به عنوان مثال، جعلی نیست) و باعث از دست دادن بالقوه ناخواسته وجوه (به عنوان مثال، ارز دیجیتال) برای کاربر نمی‌شود. کاربر این اختیار را دارد که تراکنش را تایید کند، به عنوان مثال به صورت دیجیتالی تراکنشی را امضا کند که انجام فرآیند رمزنگاری را به گیرنده تایید می‌کند یا معامله‌ای را که انتقال ارز دیجیتال را به گیرنده قطع می‌کند رد کند. 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 [۲۳- ۲۴] مرور شده‌اند. روش‌های تحلیل سری‌های زمانی سنتی تنها با تغییرات داده‌های مشاهده شده سروکار دارند و نه با فرکانس و مقدار ترکیب آن [۲۱] 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. از آنجا که 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 [۲۹]، که با مقدار کمی از داده‌ها کار می‌کنند و زمان کمتری برای ساخت مدل صرف می‌کنند، باید مورد استفاده قرار گیرند.

## روش شناسی

الگوریتم خوشه‌بندی K-means

الگوریتم K-means جز روش‌های افرازی رویکرد خوشه‌بندی می‌باشد. در روش‌های افرازی با فرض داشتن یک پایگاه داده با n شی K افراز از این داده‌های اشیا درست می‌کند. بطوریکه هر افراز یک خوشه را نشان می‌دهدو K<n. پس داده‌های اشیا در K گروه خوشه‌بندی شده و دارای دو شرط زیر می‌باشند:

الف- هر گروه حداقل یک شی دارد.

ب- هرشی تنها به یک گروه تعلق دارد.

در روش افرازی برای K معلوم، یک افراز ابتدایی ایجاد می‌شود. سپس یک روش جابجایی تکراری[1]را به کار برده 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 تا حد امکان متفاوت باشند.

در الگوریتم K-mean که هر خوشه با میانگین یا مرکز آن نمایش داده می‌شود. K را به عنوان ورودی گرفته و مجموعه n شی را به K خوشه افراز می‌کند. بطوریکه 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. این الگوریتم به صورت زیر کار می‌کند.

ورودی: K تعداد خوشه‌ها ویک پایگاه داده شامل n شی

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

**الگوریتم:**

۱) به صورت تصادفی K نقطه دلخواه را به عنوان مراکز خوشه‌های ابتدایی انتخاب کن.( بهتر است K نقطه از n نقطه موجود انتخاب شود.)

۲) هر شی را با توجه به بیشترین شباهت آن به مراکز خوشه‌ها، به خوشه‌ها تخصیص بده.

۳) مراکز خوشه‌ها را به روز کن به این معنی که برای هر خوشه میانگین اشیا آن خوشه را محاسبه کن.

۴) با توجه به 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 رابطه‌ی زیر آمده است:

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

در این رابطه E مجموع مربع خطا برای تمام اشیا پایگاه داده می‌باشد. P نقطه‌ای در فضاست که نماینگر یک شی می‌باشد، و $m_i$ میانگین خوشه $C_i$می‌باشد که نقطه p به آن متعلق است.

**الگوریتم SVM**

دسته‌بندی کاربران متصل به سرور به معنی انتصاب کاربران به دسته‌های از پیش تعیین شده می‌باشد که در ده سال اخیر تمام توجهات را به خود جلب کرده است. این مسئله به خاطر دسترسی کاربران و تعداد زیاد هکرها

[1] Itterative Relocation Techniqe

و نیاز مبرم به سازماندهی آنهاست. در جامعه تحقیقاتی روش اصلی در این زمینه، روش‌های براساس یادگیری ماشین هستند.

یادگیری تحت نظارت، یک روش عمومی در یادگیری ماشین است که یک شخص ناظری وجود دارد که برچسب گذاری برای تمایز دسته‌های مختلف را بر روی کاربران و هکرها اعمال می‌کند. یک مجموعه از مثال‌های یادگیری وجود دارد که به‌ازای هر ورودی، مقدار خروجی و یا تابع مربوطه نیز مشخص است. هدف سیستم یادگیر به دست آوردن 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 به صورت دستی یا به صورت الگوریتمی انجام شود:

- روش دستی: همانند کاری که در کتابخانه انجام می‌شود و کاربران به دسته‌های مختلف تقسیم می‌شوند.
- روش الگوریتمی: رده بندی اصولا در علم کامپیوتر و در مبحث داده کاوی جای می‌گیرد و به صورت یادگیری ماشین انجام می‌شود.

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 هر جایی که نیاز به تشخیص الگو یا دسته‌بندی 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 پایگاه داده، بردارهای پشتیبان را استفاده می‌کند.

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

**الگوریتم پیشنهادی**

روش‌های یادگیری با نظارت برای تشخیص تراکنش‌های غیر معمول در این مقاله استفاده شده است. چالش اصلی در این مقاله عدم برچسب‌گذاری داده‌های موجود می‌باشد که در آن تراکنش‌های غیر معمول برچسب گذاری 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 KMEANS برای برچسب گذاری استفاده می‌شود و سپس داده‌های برچسب گذاری شده به الگوریتم SVM برای دسته بندی تراکنش‌های می‌پردازد.

۱- استخراج ویژگی به منظور شناسایی حساب

اتریوم متشکل از حساب‌هایی است، که در آن هر حساب آدرس ۲۰ بایتی منحصر به فردی دارد.

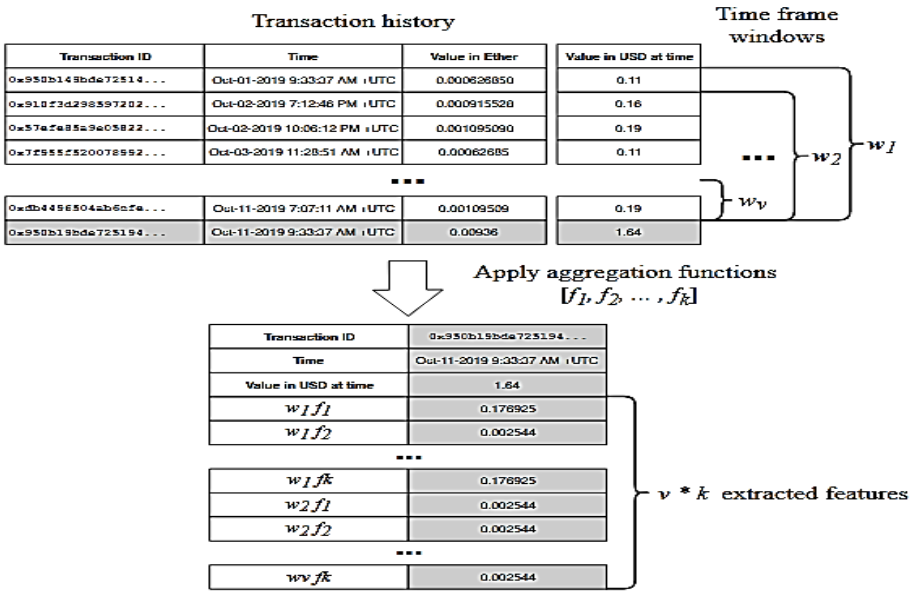
هر معامله اطلاعاتی دارد که شامل موارد زیر است:

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، به صورت w تعریف می‌شود که تعداد اندازه‌گیری‌ها در یک پنجره است.




**شکل ۱: استخراج ویژگی در بستر بلاک‌چین به منظور دسته‌بندی**

در این تحقیق، اندازه پنجره درحال حرکت به عنوان چارچوب زمانی تعریف می‌شود. هر آدرس بلاک‌چین می‌تواند الگوهای مختلفی از معاملات داشته باشد.

### خوشه بندی تراکنش‌ها:

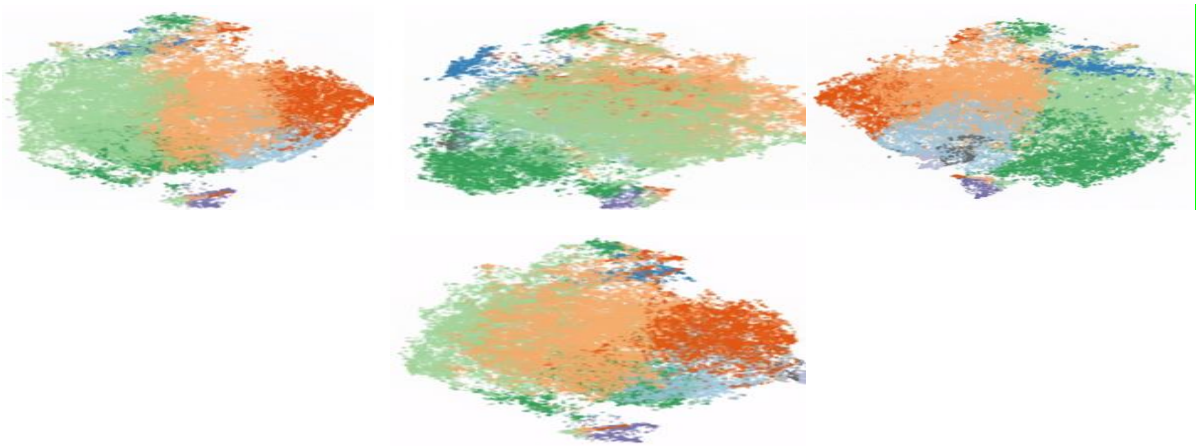
آدرس‌های اتریوم یکی از ویژگی‌های متفاوت فناوری بلاک چین نسبت به تکنولوژی‌های مشابه و امکان فعالیت ناشناس بر روی آن است. با این حال کاربران از آدرس‌هایی استفاده می‌کنند که شناسه‌هایی منحصر به فرد و غیرقابل تغییر هستند. در این مقاله با استفاده از خوشه‌بندی (Clustering) آدرس‌های اتریوم و تحلیل رفتار کاربران براساس فعالیت آن‌ها، امکان دسته‌بندی و شناسایی تراکنش‌ها مورد بررسی قرار می‌گیرد. آدرس‌های اتریوم کاربران ممکن است ناشناس باشند، اما آدرس آن‌ها دارای شناسه‌های منحصر به فردی هستند که اثری قابل‌مشاهده برای عموم را از خود بر روی بلاک چین به جا می‌گذارند. الگوریتم خوشه بندی براساس 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 رمز ارز، یک استخراج‌کننده و یا یک کیف پول ICO تعلق دارد. در شکل ۲ خوشه بندی بر روی پایگاه داده با استفاده از SQL [۳۴] و مدل آن با زبان پایتون انجام شده است. در این خوشه بندی مشخص می‌شود که یک آدرس به یک صرافی رمز ارز، یک استخراج کننده و یا یک کیف پول و یا تراکنش‌های ناسالم قرار دارد. خوشه‌بندی به روش KMEANS و در ۵ خوشه انجام شده است.

نمایشی سه بعدی از نتایج نهایی خوشه‌بندی آدرس‌های معلوم سمت چپ هستند. ما می‌توانیم درباره رفتار کاربر با استفاده از خوشه مربوط به آن نتیجه‌گیری کنیم. تراکنش‌های سالم از غیر معمول در نتایج خوشه بندی قابل تفکیک است که می‌تواند بر چسب ایجاد شده برای مرحله بعد به کار گرفته شود. ناحیه مشکی رنگ ناحیه تراکنش‌های غیرنرمال می‌باشد.

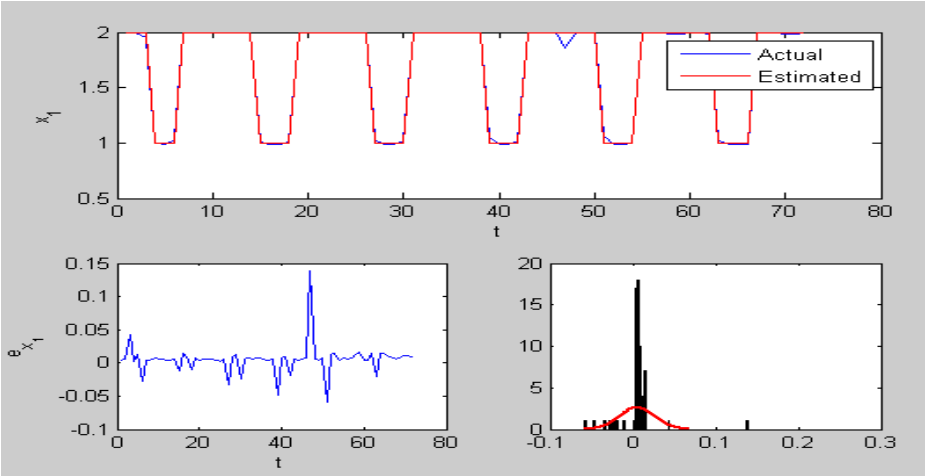
### دسته بندی تراکنش‌ها

در این مقاله هدف ارائه راهکار برای ترکیب روش خوشه‌بندی با الگوریتم دسته‌بندی می‌باشد. خوشه بندی به کمک الگوریتم kmeans انجام می‌شود و داده‌های برچسب‌گذاری می‌شود. به کمک داده‌های برچسب گذاری می‌توان تراکنش معمول از غیرمعمول را برچسب‌گذاری

نمود. خروجی الگوریتم خوشه بندی می‌تواند برای الگوریتم‌های دسته بندی به کار گرفته شود. در این مقاله از الگوریتم دسته بندی SVM (بردار پشتبان ماشین) به منظور کلاس بندی و طبقه بندی استفاده شده است. مساله خوشه بندی به مساله کلاس بندی 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 می‌باشد وخروجی نوع تراکنش(سالم یا نا سالم بودن) می‌باشد که از الگوریتم خوشه‌بندی بدست آمده نتایج مدل‌سازی با svm و خطای مدل‌سازی به صورت زیر بدست آمده است. تخمین بین دو کلاس تراکنش‌های سالم و غیر نرمال در شکل ۴ نشان داده شده 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 زیر بخش‌های شکل نشان داده شده است. پیش بینی نمونه‌های آدرس‌های سالم از ناسالم در ۷۵ نمونه تست انجام گرفت. پیش‌بینی هر نمونه و مقایسه با مقدار اصلی در شکل۴ بالا و خطای پیش‌بینی در شکل ۴ پایین چپ و هیستوگرام خطا در شکل ۴ پایین راست نمایش داده شده است. نمودار هیستوگرام خطا نشان می‌دهد که خطای تشخیص دسته بندی به صورت گوسی بوده و تابع چگالی احتمال آن نرمال می‌باشد.



شکل۲: نمایشی سه‌بعدی از فضای آدرس های اتریوم




شکل۴: خطای پیش بینی و مدل سازی توزیع خطا با استفاده از svm

نتایج با svm مورد مقایسه قرار گرفته است و نتایج نشان می دهد که روش پیشنهادی دقت بالاتری نسبت به svm از خود نشان می‌دهد. به کمک ترکیب الگوریتم KMEANS و SVM امکان کلاس بندی تراکنش‌ها در BIG DATA فراهم گردید و دقت ۸۹ درصد پیش بینی درست در نمونه‌ها کارایی روش پیشنهادی را نشان می‌دهد. دقت پیش‌بینی درصد تشخیص درست کلاس بندی را نسبت به کل داده ها نشان می دهد.

## ۳ - 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 شبیه سازی الگوریتم پیشنهادی، مجموعه‌ای از داده‌های تست در نظر گرفته شده و سپس بر روی کاربر (سالم، هکر) متصل به سرور دسته‌بندی صورت گرفته است و آنگاه با توجه به ویژگی‌های هر کاربر می‌توان SVM را به کار برد. در روش ارائه‌شده از کاربرد نوآورانه هوش مصنوعی در حوزه تکنولوژی بلاک‌چین، به ویژه روش‌های یادگیری ماشین استفاده شده است که برای خودکار کردن فرآیند امضای قرارداد و همچنین تامین 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. باتوجه به کاربرد تعریف‌شده در این مقاله، این روش می‌تواند برای بهبود قابلیت استفاده برنامه‌های کاربردی غیر متمرکز استفاده شود. علاوه بر این، استفاده از این روش در محیط‌هایی که به اجرای مداوم معاملات بلاک-چین و فعالیت‌های تبادل منظم نیاز دارند، می‌تواند از کلاهبرداری و یا دیگر فعالیت‌های بدخواهانه‌ای که ممکن است منجر به از دست رفتن وجوه ذخیره‌شده در کیف پول شود جلوگیری نماید.

## مراجع


1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://bitcoin.org/bitcoin.pdf (accessed on 10 November 2019).
2. Buterin, V. A next-generation smart contract and decentralized application platform.White Pap.2014,3, 37
3. Eskandari, S.; Clark, J.; Barrera, D.; Stobert, E. A first look at the usability of bitcoin key management.arXiv2018, arXiv: 1802. 04351.
4. Sheng, S.; Broderick, L.; Koranda, C.A.; Hyland, J.J. Why Johnny Still Can't Encrypt: Evaluating the Usabilityof Email Encryption Software. Available online: https://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf (accessed on 25 December 2019).
5. Gaw, S.; Felten, E.W.; Fernandez-Kelly, P. Secrecy, flagging, and paranoia: Adoption criteria in encryptedemail. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montréal, QC,Canada, 22–27 April 2006; pp. 591–600.
6. Schultz, E. E.; Proctor, R. W.; Lien, M. C.; Salvendy, G. Usability and security an appraisal of usability issues ininformation security methods.Comput. Secur.2001,20, 620–634. [CrossRef]
7. Garfinkel, S. L.; Margrave, D.; Schiller, J.I.; Nordlander, E.; Miller, R.C. How to make secure email easier touse. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, OR,USA, 2–7 April 2005; pp. 701–710.
8. Ruoti, S.; Seamons, K. Johnny's Journey Toward Usable Secure Email.IEEE Secur. Priv.2019,17, 72–76.[CrossRef]
9. Pham, T.; Lee, S. Anomaly detection in bitcoin network using unsupervised learning methods. arXiv2016, arXiv: 1611. 03941.
10. Pham, T.; Lee, S. Anomaly detection in the bitcoin system-a network perspective. arXiv2016, arXiv: 1611. 03942.

11. Ostapowicz, M.; Zbikowski, K. Detecting Fraudulent Accounts on Block chain: A Supervised Approach.arXiv2019, arXiv: 1908. 07886.
12. Monamo, P.; Marivate, V.; Twala, B. Unsupervised learning for robust Bitcoin fraud detection. In Proceedingsof the 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa, 17–18 August 2016;pp. 129–134.
13. Shen, M.Developer Report H1 2019; Technical report; Electric Capital: Palo Alto, CA, USA, 2019. Availableonline: https://www.electriccapital.com/developer_ report_H1_2019_pdf (accessed on 10 November 2019).
14. Turkanovi´c, M.; Hölbl, M.; Koši˘c, K.; Heri˘cko, M.; Kamišali´c, A. EduCTX: A blockchain-based highereducation credit platform.IEEE Access2018,6, 5112–5127. [CrossRef]
15. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture,consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigDataCongress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564
16. Wood, G. Ethereum: A secure decentralised generalised transaction ledger.Ethereum Proj. Yellow Pap.2014, 151, 1–32.
17. Moubarak, J.; Filiol, E.; Chamoun, M. On blockchain security and relevant attacks. In Proceedings of the2018 IEEE Middle East and North

**Journal of Financial Knowledge of Securities Analysis**

Vol. 15 / No. 53, Spring 2022

Abstract

# Access control in smart contracts using digital identity management and machine learning to facilitate IoT exchanges

**Ali abizade**[1]
**Zadale fathi***[2]
**Mehr**[1]**zad minoii**[3]

**Abstract**

Access control in the blockchain network is one of the challenges we face with the growth of the blockchain network. In the blockchain network, the set of financial activities of users that require a digital signature is performed, this information is stored in the blockchain server. Manually signing digitally and verifying the authenticity of transactions is a time consuming and user-friendly process and is one of the reasons why blockchain technology is not fully accepted. In this paper, a new method is proposed based on a combination of clustering and classification methods. First, the data is labeled using the clustering method and then the labeled data is used to teach the SVM algorithm to determine healthy transactions. The proposed method is a machine learning method for access control that automatically blocks blockchain transactions and detects abnormal transactions. In order to evaluate the proposed method, atrium data have been tested and analyzed. And with the help of KMEANS clustering algorithm and machine vector support method, healthy transactions are detected from suspects, which shows the ability to identify with 89% accuracy.

**Keywords:** blockchain; Atrium; SVM; KMEANS; Identify healthy transactions of smart financial contracts

[1] PhD Student, Department of Industrial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran. abizadeali70@gmail.com

[2*] Assistant Professor, Department of Financial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran. (Corresponding Author): z_fathi46@yahoo.com

[3] Assistant Professor of Financial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran. omm1344@yahoo.com