روشی جدید برای تعیین موجودیت‌های مخرب در محیط‌های ابری

سیده متین چیرگی[1] و نیما جعفری نویمی‌پور[2]

[1] باشگاه پژوهش‌گران جوان و نخبگان، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران
matinchiregi@iaut.ac.ir

[2]گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران
Jafari@iaut.ac.ir

چکیده

رایانش ابری به‌عنوان یکی از فناوری‌های پیشرفته در جوامع امروزی مطرح و یکی از مزیت‌های مهم آن کاهش هزینه‌های زیرساختی است. امروزه رایانش ابری توسط طیف گسترده‌ای از سازمان‌ها مورد استفاده قرار می‌گیرد و به‌سرعت به یک سرویس محاسباتی مهم در اینترنت تبدیل شده است. اعتماد یکی از چالش‌های مهم در حوزهٔ رایانش ابری محسوب می‌شود که نقش مهمی در عملکرد سامانه دارد، اعتماد به‌عنوان یک راه‌حل امنیتی در برابر موجودیت‌های مخرب است. موجودیت‌های مخرب با قراردادن پیام‌های نادرست‌ونظرات غیر واقعی در شبکه، موجب گمراهی موجودیت‌های دیگر می‌شوند که بایستی در شبکه شناسایی و درنهایت حذف شوند. انتظار می‌رود بیش‌تر این موجودیت‌ها در شبکه، مورد شناسایی قرار گیرند. در این مقاله روش‌های متفاوتی برای شناسایی موجودیت‌های مخرب با استفاده سه معیار اندازه‌گیری هم‌بندی درجهٔ وارده، درجهٔ خارجه و اعتبار ارائه شده‌اند که براساس ارزیابی‌های صورت‌گرفته، این روش‌ها قادر به شناسایی ٪۹۲ از موجودیت‌های مخرب هستند.

واژگان کلیدی: رایانش ابری، موجودیت مخرب، محیط‌های ابری، اعتماد و اعتبار.

۱- مقدمه

رایانش ابری به‌سرعت در حال تبدیل‌شدن به یک سرویس مهم در ارزیابی اینترنت است [۱]. رایانش ابری به‌طوراساسی ترکیبی از فناوری‌هایی است که موفق به ساخت و نگهداری سامانه‌های محاسباتی توزیع‌شده، فناوری مجازی‌سازی و شبکه‌های مبتنی بر ذخیره‌سازی داده‌های پراکنده و شبکه‌ها شده است [۲]. همچنین یک نوع رایانش جدید براساس شبکه‌های بزرگ رایانه‌ای است که یک نمونه جدید برای عرضه، مصرف و تحویل خدمت‌های فناوری اطلاعات ارائه می‌کند [۳]. رایانش ابری نسل بعدی از سامانه‌های رایانه‌ای است که معماری شبکه را به ظرفیت مقیاس بزرگ و پویا، با استفاده از روش‌های مجازی‌سازی گسترش می‌دهد [۴]. زیر ساخت‌های ابر چهار نوع از مدل‌های ارائه خدمات از قبیل نرم‌افزار به‌عنوان خدمات[1] [۵, ۶]، سکو به‌عنوان خدمات[2] [۷]، زیرساخت به عنوان خدمات[3] [۸, ۹] و ابرخبره به‌عنوان خدمات[4] [۱۰, ۱۱] را پشتیبانی می‌کنند.

اعتماد به‌عنوان یکی از مهم‌ترین چالش‌های رایانش که امروزه بسیار مورد بحث قرار گرفته است، به‌شمار می‌آید. اگرچه اعتماد در زمینه‌های مختلفی مورد مطالعه قرار گرفته است، اما در تعاریف آن توافق جهانی بین پژوهش‌گران وجود ندارد [۱۲]. به‌عنوان نمونه گرندیسون[5] و سلمون[6] تعریف زیر را از اعتماد ارائه

[1] Software as a Service
[2] Plat form as a Service
[3] Infrastructure as a Service
[4] Expert cloud as a Service
[5] Grandison
[6] Selmon

داده‌اند: "اعتماد راسخ به توانایی یک موجودیت به عمل‌کردن به‌طور مداوم، ایمن و قابل اعتماد در یک زمینه مشخص‌شده گفته می‌شود." یکی از تعاریف دیگر اعتماد به‌صورت زیر بیان می‌شود: "اعتماد به سطح اطمینان در شخصی یا چیزی گفته می‌شود [۱۳, ۱۴]." اما شاید بهترین تعریف برای اعتماد را بتوان تعریف زیر دانست "اعتماد یک احتمال ذهنی است که توسط یک گروه، برای اجرای یک عمل تعریف شده است [۱۲]."

سازوکار اعتماد دارای فاکتورهای کلیدی از قبیل تمامیت[1]، امنیت و دقت[2]، دسترس‌پذیری، قابلیت اطمینان، قابلیت اعتماد، ایمنی، پویایی، محرمانگی[3] و مقیاس‌پذیری است. روش اعتماد منطقه‌ای و جزء روش‌های بهینه‌سازی قدرتمند است [۱۵] و نقش مهمی در تمام محیط‌های تجاری ابر ایفا می‌کند که یک بخش مهم از جنبه‌های تجاری در فناوری ابر است [۱۶].

اعتماد در رایانش ابری تا حد بسیاری می‌تواند از رفتارهای بدخواهانهٔ موجودیت‌ها جلوگیری کند. مخرب‌ها موجودیت‌هایی هستند که نظرات آشکار و غلط می‌دهند و یک وضعیت غیر قابل اطمینان ایجاد می‌کنند؛ به‌طوری که یک انتقاد ناخواسته می‌تواند منجر به یک واکنش نامناسب شود. اگر در یک شبکه، اعتماد وجود نداشته باشد، موجودیت‌های مخرب به‌راحتی می‌توانند اطلاعات غلط وارد شبکه کنند و باعث ایجاد نظرات اشتباه بین موجودیت‌ها شوند؛ بنابراین، در این مقاله موجودیت‌های مخرب را با توجه به میزان اعتمادشان مورد بررسی قرار می‌گیرند.

در این مقاله به مطالعه و بررسی اعتماد، اعتبار و موجودیت‌های مخرب پرداخته شده است. ساختار مقاله به‌صورت زیر دنبال خواهد شد و شامل بخش‌های زیر است. در بخش دوم، مفاهیم، چارچوب‌های متدوال و روش‌های قبلی مرور می‌شوند. در بخش سوم، روش پیشنهادی ارائه خواهد شد که شامل ارزیابی اعتبار و موجودیت‌های مخرب است. همچنین، نتایج آزمایش در بخش چهارم نشان داده شده است و درنهایت مقاله در بخش پنجم با نتیجه‌گیری و کارهای آتی خاتمه می‌یابد.

[1] Integrity
[2] Security and accuracy
[3] Confidentiality

۲- ادبیات پژوهش

در این بخش، برخی از روش‌های مرتبط در زمینهٔ اعتماد، اعتبار و موجودیت‌های مخرب در رایانش ابری به‌همراه مزایا و معایب آن‌ها بررسی و ارائه می‌شوند.

در سال ۲۰۱۲، روشی به نام اعتبار قطبیدگی[4] معرفی شد که یک سامانهٔ اعتماد و اعتبار براساس انتشار رأی‌های مثبت و منفی از کاربران به‌منظور شناسایی موجودیت‌های مخرب در شبکه‌های اجتماعی ارائه کرد [۱۷]. استفاده از اعتبار قطبیدگی به‌منظور به‌دست‌آوردن دو نمره: مثبت یک، نشان‌دهندهٔ یک کاربر خوب و منفی یک، نشان‌دهندهٔ یک کاربر بد است. اعتبار، اعتبار قطبیدگی توسط آزمایش، رفتار خود را در زیر برخی از حملات بر ضد "تی آر اس[5]" و همچنین با مجموعه داده‌های دنیای واقعی از اخبار اجتماعی سایت Slashdot.org ثابت کرده است. همچنین معرفی یک افزونه به مدل اولیه از اعتبار قطبیدگی برای مجازات آن دسته از کاربرانی که رفتار نادرست (با توجه به شدت این رفتار) نشان می‌دهند. آزمایش‌ها با مجموعه داده‌های "اسلش زوو[6]" نشان می‌دهد که اعتبار قطبیدگی در یک شبکهٔ اجتماعی در دنیای واقعی حتی زمانی که چند لبهٔ جدید به‌منظور انجام مجموعه‌ای از حملات پیچیده، علیه شبکه افزوده می‌شود، قابل اطمینان است. این روش قابلیت اعتماد بالایی دارد؛ اما دسترس‌پذیری و محرمانگی آن کم است.

در [۱۸] یک الگوریتم جدید برای تشخیص و شناسایی حمله موجودیت‌های مخرب در لایهٔ MAC، پیشنهاد شده است. الگوریتم قادر به شناسایی موجودیت‌های مخرب است؛ حتی زمانی که اطلاعات پیشینی درباره فعالیت‌های کانال اصلی و ویژگی اشخاص وجود نداشته باشد. همچنین این الگوریتم بر روش غیرپارامتری آماری استوار و در سناریوهای پیچیده بسیار قوی است. این روش دسترس‌پذیر است؛ اما یکپارچگی و محرمانگی پایینی دارد.

در سال ۲۰۱۳ یک روش برای تشخیص مخرب در محیط ابری با استفاده از استخراج قوانین پی در پی

[4] Polarity Trust
[5] Trust and Reputation Systems (TRS)
[6] Slashdot Zoo

ارائه شد [۱۹]. در این روش یک الگوریتم یادگیری قوانین در یادگیری الگوی رفتاری کاربران به‌منظور ساخت پروفایل‌های کاربر استفاده شده است. نتایج تجربی نشان می‌دهد که این روش می‌تواند کاربران داخلی را که با لباس مبدل وارد سامانه شده‌اند، با مشاهده الگوی رفتاری آنها شناسایی کند.

در سال ۲۰۱۰ یک مدل اعتماد مشترک از طریق دیوارهٔ آتش[1] در رایانش ابری پیشنهاد شد [۲۰]. در این روش، طراحی دقیق از مدل اعتماد، الگوریتم‌های اندازه‌گیری و به‌روزرسانی مقدار اعتماد مورد بررسی قرار گرفت. همچنین این روش دارای مزایای زیر است: سیاست ایمنی مختلفی برای مناطق متفاوت در ابر وجود دارد؛ اندازه‌گیری مقدار اعتماد به‌صورت پویا است و مدل اعتماد به‌خوبی با دیوارهٔ آتش همسان می‌شود و سیاست‌های کنترل محلی دیوارهٔ آتش را نمی‌شکنند. عیب این روش امنیت پایین آن است.

در سال ۲۰۱۱ یک مدل ارزیابی اعتماد توسعه‌پذیر به نام مدل ارزیابی اعتماد توسعه‌پذیر در محیط‌های ابری ETCE [2] پیشنهاد شد [۲۱]. این مدل شامل یک روش ارزیابی جامع انواع فضا[3] برای محاسبه اعتماد است. همچنین این مدل می‌تواند به ایجاد تصمیم درست، حمله به اطلاعات موجودیت‌های مخرب کمک کند. علاوه‌بر این، یک اندازه‌گیری مفید برای بهبود استحکام، تحمل خطا و امنیت در رایانش ابری ارائه می‌دهد. این مدل می‌تواند تأثیر درجهٔ اعتماد را در محیط رایانش ابری محاسبه کند. این روش ایمنی و پویایی را توسعه داده است؛ اما مقیاس‌پذیری کمی دارد.

در سال ۲۰۱۱ یک روش فرمول‌بندی و تکاملی اعتماد که برای ارزیابی عملکرد سامانه‌های ابری مورد استفاده قرار می‌گرفت، ارائه شد [۲۲]. در این روش، نمرهٔ اعتماد برای نیازمندی‌های مختلف، سطح سرویس است. این روش پویا، اما قابلیت اطمینان آن پایین می‌باشد.

در سال ۲۰۱۲ چارچوب جدیدی برای ارزیابی اعتماد پیشنهاد شد [۲۳]. شناسایی چالش‌های مربوط به ایجاد اعتماد در ابر و سپس یک چارچوب پایه که می‌تواند در نشانی‌دهی شناسایی چالش‌های ابر کمک کند. همچنین در مورد روش‌های در حال توسعه برای کمک به کاربران و ارائه‌دهندگان ابر برای ایجاد اعتماد در بهره‌برداری از زیرساخت‌ها توسط ارزیابی مستمر وضعیت عملیاتی متمرکز شده‌اند. چارچوب ارائه‌شده نیاز به پسوند بیشتری به‌عنوان ایجاد اعتماد در ابر دارد. علاوه‌براین آنها راه را برای انتقال قدرت از مدیریت داده‌های نرم‌افزاری کاربران از دست ارائه‌دهندگان ابر به دست کاربران معرفی کرده‌اند. مزیت این چارچوب این است که از دامنه‌های ابر با ویژگی‌های خاص حمایت می‌کند؛ اما این روش معیارهای کافی را برای ایجاد اعتماد در ابر ندارد.

در سال ۲۰۱۳، پاول مانوئل[4] یک مدل اعتماد رایانش ابری بر اساس کیفیت سرویس را ارائه کرده است که ارزیابی مقدار اعتماد بر اساس ویژگی‌هایی از قبیل دسترس‌پذیری، قابلیت اعتماد، کارایی چرخش و تمامیت داده‌ها صورت گرفته است. در این روش نشان داده شده است که عملکرد مدل اعتماد "کیفیت سرویس" بهتر از مدل فیفو[5] و مدل‌های مشابه است؛ اما روش ذکر شده پویا نیست [۲۴].

در سال ۲۰۱۴ یک روش ترکیب سرویس اعتماد جهانی براساس محاسبه اعتماد و درنظرگرفتن ارزیابی چندمعیاره کیفیت سرویس ارائه شده است [۲۵]. آن‌ها یک ارزیابی چندمنظوره از کیفت سرویس را با توجه به تأثیرات پویا از عوامل ناپایدار شبکه، ارائه‌دهندگان و مشتریان طراحی کرده‌اند. نتایج تجربی نشان می‌دهد که الگوریتم برای تغییردادن محیط‌های ابری به‌صورت پویا مناسب و همچنین قادر به تضمین کیفیت واقعی ترکیب سرویس است. این روش قابلیت اطمینان و دسترس‌پذیری بالایی دارد و یک روش پویاست؛ اما شایستگی آن کم است.

در سال ۲۰۱۶ یک مدل فازی براساس اعتماد و اعتبار برای تخصیص منابع امن در رایانش ابری ارائه شده بود [۲۶]. آن‌ها مدیریت اعتماد و اعتبار را در روش پیشنهادیشان به‌کار گرفته‌اند. در این روش کاربر به

[1] Firewall-through
[2] Extensible Trust Evaluation model for Cloud computing environments
[3] Space-variant
[4] Paul Manuel
[5] Fifo

بلوک منبعی دسترسی دارد که از طریق مدیر توسعه به کاربر آن بلوک، به‌منظور پرکردن مقادیر معمول از فاکتور اعتماد و اعتبار ارسال می‌شود. روش ذکرشده دارای کنترل‌های امنیتی است؛ اما دسترس‌پذیری و قابلیت اطمینان کمی دارد.

در سال ۲۰۱۶ یک چارچوب انتخابی قابل اعتماد، برای انتخاب سرویس‌های ابر به نام تراس[1] ارائه شد. روش ارزیابی اعتماد از طریق الحاق ارزیابی اعتماد هدفمند با ارزیابی اعتماد ذهنی انجام شده است. از جمله مزایای این روش قابل اطمینان و دسترس‌پذیر است؛ اما مقیاس‌پذیر نیست [۲۷].

در هیچ یک از روش‌های ذکرشده، حذف موجودیت‌های مخرب در محیط‌های ابری با استفاده از روش اعتماد و اعتبار مورد بررسی قرار نگرفته بود؛ لذا روشی ارائه شد که قادر است، موجودیت‌های مخرب را در محیط‌های ابری با استفاده از روش‌های توپولوژیکی شناسایی کند.

۳- روش پیشنهادی

در این بخش ابتدا روشی برای ارزیابی اعتبار براساس پارامترهایی از قبیل دسترسی‌پذیری، قابلیت اطمینان، یک‌پارچگی داده، هویت و شایستگی ارائه و سپس روشی برای شناسایی موجودیت‌های مخرب ارائه شده است.

۳-۱- روش ارزیابی اعتبار

اعتماد و اعتبار یک راه امیدبخشی را برای حل ارزیابی مطمئن در سرویس‌های ابری ارائه می‌دهند. بنابراین، اعتماد و اعتبار نقش مهمی در ارزیابی خدمات ابر ایفا می‌کنند [۲۸]. در این مقاله، ترکیبی از چندین مشخصه شامل دسترسی‌پذیری، قابلیت اطمینان، یکپارچگی داده‌ها، هویت و شایستگی برای ارزیابی اعتبار در نظر گرفته شده است.

- **دسترسی‌پذیری[2]**

دسترسی‌پذیری در رایانش ابری شامل دسترسی مداوم ابر از طریق پروفایل‌های ابر و قابلیت همگام‌سازی اولویت دسترسی ابر است. در دسترس‌پذیری مباحثی با عنوان حریم خصوصی، امنیت و کنترل صادرات مطرح می‌شود. همچنین، در مهندسی نرم‌افزار با متوسط زمان بین خرابی‌ها و تعمیر اندازه‌گیری می‌شود که می‌توان آن را به‌عنوان یک نسبت مستقیم و یا به‌عنوان درصد بیان کرد. دسترس‌پذیری منبع R با استفاده از رابطه (۱) محاسبه می‌شود:

$$AV_R = \frac{A}{N} \qquad (۱)$$

$R_1, R_2, ..., R_M$ منابع ابر هستند، A تعداد کارهایی که در زمان T توسط منابع R پذیرفته شده، N تعداد کارهایی که در زمان T به منابع R ارسال شده است.

- **قابلیت اطمینان[3]**

قابلیت اطمینان در ابر به‌طور معمول به‌عنوان "توانایی‌های ابر برای تحویل یک سرویس که می‌تواند به نحو قابل قبولی مورد اعتماد باشد" تعریف می‌شود [۲۹]. همچنین، به توانایی یک سخت‌افزار یا اجزای نرم‌افزار مربوط به رایانه اشاره دارد که به‌طور مداوم طبق مشخصه‌های خود اجرا می‌شود. قابلیت اطمینان منبع R با استفاده از رابطه (۲) محاسبه می‌شود:

$$RE_R = \frac{C}{A} \qquad (۲)$$

$R_1, R_2, ..., R_M$ منابع ابر هستند، C تعداد کارهایی که در زمان T توسط منابع R با موفقیت کامل شده، A تعداد کارهایی که در زمان T توسط منابع R پذیرفته شده است.

- **یک‌پارچگی داده‌ها[4]**

یک‌پارچگی داده‌ها به‌عنوان دقت و درستی داده‌های ذخیره‌شده در ابر به کار می‌رود. همچنین موضوع کلیدی است که نیاز به توجه ویژه‌ای در ابرهای امنیتی دارد [۳۰-۳۲]. یک‌پارچگی داده‌ها اصطلاح گسترده‌ای است که شامل: امنیت، حفظ حریم خصوصی و صحت داده‌ها است [۸]. امنیت شامل ایمنی داده‌ها و دقت شامل صحت داده‌ها است [۳۳]. ازدست‌دادن داده‌ها ممکن است به‌علت ضعف پنهانی شبکه و

[1] Truss
[2] Availability
[3] Reliability
[4] Data Integrity

ازدست‌دادن صحت ممکن است، به‌علت ازکارافتادن زیر ساخت‌های محاسباتی منسوخ‌شده رخ دهد [۳۳]. یک‌پارچگی داده منبع R با استفاده از رابطه (۳) محاسبه می‌شود:

$$DI_R = \frac{A}{N} \quad (۳)$$

منابع ابر هستند، A تعداد کارهایی که در زمان T توسط منابع R پذیرفته شده است، N تعداد کارهایی که در زمان T به منابع R ارسال شده است.

- **هویت**[1]

هویت در رایانش ابری یک ناحیه‌ای است که نیاز به توجه زیادی در ابر دارد. سطح امنیت شامل سطوح امنیتی طبقه‌بندی‌شدهٔ سطح مجوز[2]، سطح امنیت[3]، سطح حفاظت[4] و سطح ترمیم[5] است. سطح مجوز برای اطمینان حاصل‌کردن مدیر از این‌که به‌طور اصولی مجاز به دسترسی به منابع است یا نه. سطح امنیت فراهم‌کنندهٔ خدماتی است که از داده‌های رمزگذاری‌شده در ابر حفاظت و سطح حفاظت از یک سری اطلاعات مربوط به کاربر مثل شماره تلفن حفاظت می‌کند و سطح ترمیم اشاره به بازیابی اطلاعات درصورت هر گونه خرابی یا ازدست‌دادن اطلاعات در ابر دارد. هویت منبع R با استفاده از رابطه (۴) محاسبه می‌شود:

$$ID_R = W1_{ID} \times AL + W2_{ID} \times EL + W3_{ID} \times SL + W4_{ID} \times RL \quad (۴)$$

AL نشان‌دهنده سطح مجوز، EL نشان‌دهنده سطح حفاظت، SL نشان‌دهنده سطح امنیت و RL نشان‌دهنده سطح‌ترمیم است.

به شرطی که $W1_{ID} + W2_{ID} + W3_{ID} + W4_{ID} = 1$ باشد و همچنین $R1, R_2, \ldots, R_M$ منابع ابر هستند.

- **شایستگی**[6]

شایستگی توصیف یک مجموعه سریع در حال رشد از فناوری و تجارت توانایی‌های ابر و خدمات قابل حصول ابر است. قابلیت فعلی از منابع ابر، عملکرد اجرای نرم‌افزار و فایل‌ها یا انتقال داده را تحت تأثیر قرار می‌دهد، شامل پارامترهای محاسباتی مانند سرعت پردازنده (P)، سرعت حافظه (M) و پارامترهای شبکه مانند پهنای باند و زمان تأخیر است.

$R_1, R_2, \ldots, R_M$ منابع ابر هستند. شایستگی منبع R با استفاده از رابطه (۵) محاسبه می‌شود:

$$CA_R = \frac{Bandwidth \times \left(P + M + \frac{1}{Latency}\right)}{Bandwidth \times \left(P_{Max} + M_{Max} + \frac{1}{Latency_{Min}}\right)} \quad (۵)$$

- **اعتبارسنجی**[7]

در جامعهٔ رایانش ابری، محاسبهٔ اعتبار با استفاده از بازخورد مشتریان ابر به‌طور گسترده‌ای برای رسیدگی به موضوع اعتماد در رایانش ابری به تصویب رسیده است. ساختن یک طرح اعتبار هدف‌دار و قابل اعتماد در ترویج توسعه رایانش ابری بسیار مهم است. اعتبار منبع R با استفاده از رابطه (۶) به دست می‌آید:

$$RE_R = W1 \times \frac{A}{N} + W2 \times \frac{C}{A} + W3 \times \frac{D}{C} + W4 \times ID_R + W5 \times CA_R \quad (۶)$$

به شرط آن که $W1+W2+W3+W4+W5=1$ باشد. همچنین $W1$، $W2$، $W3$، $W4$ و $W5$ فاکتورهای وزن هستند، N تعداد کارهایی که به‌صورت سراسری در زمان T به منابع R ارسال شده، A تعداد کارهایی که به‌صورت سراسری در زمان T توسط منابع R پذیرفته شده، C تعداد کارهایی که به‌صورت سراسری در زمان T توسط منابع R با موفقیت کامل شده، D تعداد کارهایی که به‌صورت سراسری در زمان T توسط منابع R حفاظت شده، ID_R هویت منبع R و CA_R به‌عنوان شایستگی منبع R تعریف شده است.

۳-۲- موجودیت‌های مخرب[8]

موجودیت‌های مخرب، اشخاص یا منابعی هستند که پیام‌های تحریک‌آمیز ارسال و دوستان و غریبه‌ها را تحریک به دعوا می‌کنند. آن‌ها مردم را با تأکید بر بیماری یا با ازدست‌دادن یک دوست اذیت می‌کنند. مردم به هویت آنها یا نگاه‌هایشان نامطمئن هستند. مخرب‌ها به هر کجایی که موجودیت‌های برخط واکنش نشان می‌دهند، متمایل می‌شوند؛ مثل وبلاگ‌ها، شبکه‌های اجتماعی، بازی‌های چندنفره، بحث و تبادل نظر، سایت‌های سرگرمی، سامانه‌های توزیع‌شدهٔ رایانش

[1] Identity
[2] Authorization level
[3] Security level
[4] Security level
[5] Protection level
[5] Reparation level
[6] Capability
[7] Reputation
[8] Troll entities

ابری و مواردی از این قبیل. در این بخش ترکیبی از سه اندازه‌گیری هم‌بند درجه وارده، درجه خارجه و اعتبار برای شناسایی یک گروه از موجودیت‌های مخرب ارائه شده است. نمره برای هر موجودیت مخرب با استفاده از رابطهٔ (۷) به دست می‌آید:

$$Tl_{1R} = \frac{1}{RE_R}\left((1-\alpha) \times input\_degree^{-} + \left(\alpha \times output\_degree^{ic^{-}}\right)\right) \quad (۷)$$

به شرط آن‌که $\alpha \in (0, 0.1, 0.2,\ldots, 0.9, 1)$ باشد. RE_R نشان‌دهنده اعتبار، $input\text{-}degree^{-}$ نشان‌دهنده رأی‌های منفی که منبع R از موجودیت‌های دیگر گرفته است و $output\text{-}degree^{ic^{-}}$ نشان‌دهنده رأی‌های منفی غلطی می‌باشد که منبع R به موجودیت‌های دیگر داده است.

علاوه بر این چند حالت دیگر برای محاسبه نمرهٔ موجودیت‌های مخرب در نظر گرفته شده است. Tl_{2R} و Tl_{3R} به‌ترتیب توسط روابط (۸) و (۹) محاسبه می‌شوند:

$$Tl_{2R} = \frac{1}{RE_R}\left((1-\alpha) \times input\_degree^{-} + \left(\alpha \times output\_degree^{c^{-}}\right)\right) \quad (۸)$$

به شرط آن‌که $\alpha \in (0, 0.1, 0.2,\ldots, 0.9, 1)$ باشد. RE_R نشان‌دهندهٔ اعتبار، $input\text{-}degree^{-}$ نشان‌دهنده رأی‌های منفی که منبع R از موجودیت‌های دیگر گرفته و $output\text{-}degree^{c^{-}}$ نشان‌دهنده رأی‌های منفی غلطی می‌باشد که منبع R به موجودیت‌های دیگر داده است.

$$Tl_{3R} = \frac{1}{RE_R}\left((1-\alpha) \times input\_degree^{-} + \left(\alpha \times output\_degree^{-}\right)\right) \quad (۹)$$

به شرط آن‌که $\alpha \in (0, 0.1, 0.2,\ldots, 0.9, 1)$ باشد. RE_R نشان‌دهندهٔ اعتبار، $input\text{-}degree^{-}$ نشان‌دهنده رأی‌های منفی که منبع R از موجودیت‌های دیگر گرفته و $output\text{-}degree^{-}$ نشان‌دهنده رأی‌های منفی می‌باشد که منبع R به موجودیت‌های دیگر داده است.

۴- نتایج آزمایش

در این مقاله برای شبیه‌سازی و صحت‌سنجی روش پیشنهادی از نرم‌افزار متلب[1] بهره برده شده است. به‌منظور آزمایش عملکرد روش ارائه شده، از یک روش ارزیابی استاندارد در رایانش ابری استفاده شده است. در این بخش جزئیات آزمایش بر روی مجموعه داده‌های واقعی برای ارزیابی عملکرد ارائه‌شده انجام شده است. این روش بر روی یک سری مجموعه داده‌ها برای ارزیابی اعتبار اعمال شده است. همچنین این بخش به تعیین موجودیت‌های مخرب می‌پردازد.

داده‌های شبیه‌سازی‌شده از مجموعه داده‌های ابرخبره برداشته شده که در www.dataset12.expertcloud.ir قابل دسترسی است. ابر خبره یک گروه جدید از سامانه رایانش ابری است که کاربران را قادر به درخواست مهارت، دانش و تخصص از مردم بدون هیچ‌گونه اطلاعاتی دربارهٔ محل سکونتشان می‌سازد و این کار با استفاده از زیرساخت‌های اینترنت و مفاهیم رایانش ابری انجام می‌شود. یکی از خدمات مهم در ابرخبره، جستجوی مردم قابل اعتماد به‌منظور بهره‌مندی از دانش و مهارت‌هایشان است [۱۰]. در ابر خبره، ۲۰۰۰ منبع با ویژگی‌های مختلف از قبیل تعداد کارهای پذیرفته‌شده A، تعداد کارهای ارسال‌شده N، تعداد کارهای با موفقیت کامل‌شده C، تعداد کارهای حفاظت‌شده D، سطح مجوز AL، سطح حفاظت EL، سطح امنیت SL، سطح‌ترمیم RL، سرعت پردازنده P و سرعت حافظه M وجود دارد. همچنین پهنای باند، زمان تأخیر، نظرات منفی که موجودیت گرفته است $input\text{-}degree^{-}$، نظرات مثبتی که موجودیت گرفته $input\text{-}degree^{+}$، نظرات صحیحی که کاربر گرفته است $input\text{-}degree^{c}$، نظرات منفی که کاربر داده است $output\text{-}degree^{-}$، نظرات مثبتی که کاربر داده است $output\text{-}degree^{+}$، نظرات صحیحی که کاربر داده است $output\text{-}degree^{c}$، نظرات صحیح منفی می‌باشد که کاربر داده است $output\text{-}degree^{c^{-}}$، نظرات نادرستی است که کاربر داده است $output\text{-}degree^{ic}$ و نظرات نادرست منفی که کاربر داده است $output\text{-}degree^{ic^{-}}$، همچنین در این مجموعه داده‌ها ۳۸ موجودیت مخرب وجود دارد. مقدار مجموعه داده‌ها به‌طور خلاصه در جدول (۱) نشان داده شده است.

[1] www.mathworks.com

(جدول ۱): مقادیر مجموعه داده‌ها برای ۲۰۰۰ منبع از ۱ تا ۲۰۰۰(www.dataset12.expetcloud.ir)

R	1	2	3	...	1000	...	2000
A	12	15	13	. . .	15	. . .	12
N	18	21	24	. . .	25	. . .	23
C	6	12	7	. . .	8	. . .	6
D	0	0	2	. . .	3	. . .	0
AL	0.886	0.777	0.112	. . .	0.309	. . .	0.740
EL	0.096	0.864	0.132	. . .	0.245	. . .	0.750
SL	0.053	0.648	0.182	. . .	0.346	. . .	0.855
RL	0.099	0.716	0.269	. . .	0.305	. . .	0.753
P	20	43	2	. . .	12	. . .	79
M	40	40	21	. . .	16	. . .	69
$Bandwidth$	28	60	59	. . .	71	. . .	60
$Latency$	21	73	32	. . .	39	. . .	38
$input\_degree^{c^-}$	28	94	80	. . .	25	. . .	19
$input\_degree^{ic^-}$	3	83	2	. . .	42	. . .	44
$input\_degree^{c^+}$	66	67	51	. . .	93	. . .	69
$input\_degree^{ic^+}$	68	30	15	. . .	29	. . .	57
$output\_degree^{c^-}$	98	32	58	. . .	47	. . .	5
$output\_degree^{ic^-}$	26	95	40	. . .	24	. . .	8
$output\_degree^{c^+}$	51	55	74	. . .	39	. . .	78
$output\_degree^{ic^+}$	7	57	96	. . .	98	. . .	62

۴-۲- ارزیابی اعتبار

در این بخش، چندین مقدار با وزن‌های متفاوت برای اعتبار به دست آمده است. روش ارائه‌شده با سه حالت مختلف مورد ارزیابی قرار گرفته است.

در آزمایش نخست، وزن‌های اعتبار $W1$=0.1، $W2$=0.2، $W3$=0.3، $W4$=0.1 و $W5$=0.3 همچنین وزن‌های هویت $W1_{ID}$=0.4، $W2_{ID}$=0.1، $W3_{ID}$=0.3 و $W4_{ID}$=0.2 در نظر گرفته شده است. مقدار هویت و شایستگی با استفاده از روابط (۴) و (۵) به‌دست می‌آید. در آزمایش دوم، وزن‌های اعتبار به‌ترتیب $W1$=0.2، $W2$=0.2، $W3$=0.2، $W4$=0.2 و $W5$=0.2 و همچنین وزن‌های هویت $W1_{ID}$=0.2، $W2_{ID}$=0.2، $W3_{ID}$=0.3 و $W4_{ID}$=0.3 در نظر گرفته شده است. در آزمایش سوم، وزن‌های اعتبار $W1$=0.1، $W2$=0.2، $W3$=0.1، W4=0.2 و W5=0.4 و وزن‌های هویت به‌ترتیب $W1_{ID}$=0.1، $W2_{ID}$=0.1، $W3_{ID}$=0.4 و $W4_{ID}$=0.4 در نظر گرفته شده است. نتایج ارزیابی اعتبار برای سه حالت بالا در جدول (۲) و شکل (۱) نشان داده شده است.

همان‌طور که در شکل (۱) مشاهده شد در حالت نخست و سوم نتایج به‌دست‌آمده به‌طورتقریبی مشابه هستند؛ اما حالت دوم مقدار اعتبار بالاتری نسبت به بقیه دارد.

۴-۳- ارزیابی مخرب‌ها

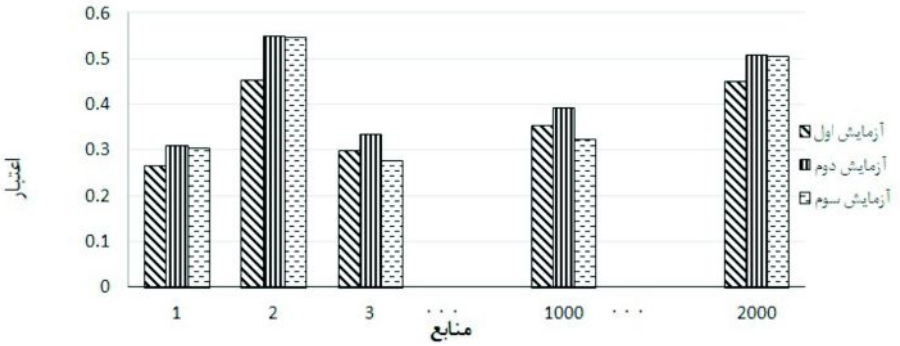
در این بخش، مجموعهٔ سوم آزمایش برای نشان‌دادن عملکرد روش‌های پیشنهادشده برای شناسایی موجودیت‌های مخرب ارائه شده است. همان‌طورکه در بخش قبلی نشان داده شد، سه روش برای شناسایی موجودیت‌های مخرب وجود دارد. هر یک از آن‌ها با سه مقدار مختلف آستانه اعتبار مورد ارزیابی قرار داده شد. این آزمایش برای دوهزار کاربر در محیط رایانش ابری انجام شده است. برای هر روش وزن‌ها و آلفاهای مختلف مورد بررسی قرار گرفته است.

مقادیر وزن‌های اعتبار $W1$=0.1، $W2$=0.2، $W3$=0.3، $W4$=0.1 و $W5$=0.3 و مقادیر وزن‌های هویت

برای محاسبه اعتبار $W1_{ID}$=0.3، $W2_{ID}$=0.2، $W3_{ID}$=0.3 و $W4_{ID}$=0.1 در نظر گرفته شده است. همچنین با سه مقدار مختلف، آستانه اعتبار شامل مقادیر ۰.۲۵، ۰.۳ و ۰.۳۵ با λ_{tl}>400 برای هر یک از آنها مورد ارزیابی قرار داده شد. مقدار آلفا برای هر معیار به‌صورت ذهنی α=0.2 در نظر گرفته شده است. نتایج به‌دست‌آمده در جدول ۳ و شکل ۲ نشان داده شده است.

(جدول ۲): ارزیابی اعتبار

شماره منبع	آزمایش اول	آزمایش دوم	آزمایش سوم
R	W1=0.1, W2=0.2, W3=0.3, W4=0.1, W5=0.3,$W1_{ID}$=0.4,$W2_{ID}$=0.1,$W3_{ID}$=0.3 ,$W4_{ID}$=0.2	W1=0.2, W2=0.2, W3=0.2, W4=0.2, W5=0.2,$W1_{ID}$=0.2,$W2_{ID}$=0.2,$W3_{ID}$=0.3, $W4_{ID}$=0.3	W1=0.1, W2=0.2, W3=0.1,W4=0.2, W5=0.4,$W1_{ID}$ =0.1,$W2_{ID}$=0.1,$W3_{ID}$=0.4, $W4_{ID}$=0.4
1	0.2650	0.3098	0.3034
2	0.4538	0.5497	0.5470
3	0.2986	0.3330	0.2773
. . .	. . .	. . .	. . .
1000	0.3523	0.3909	0.3232
. . .	. . .	. . .	. . .
2000	0.4510	0.5078	0.5053



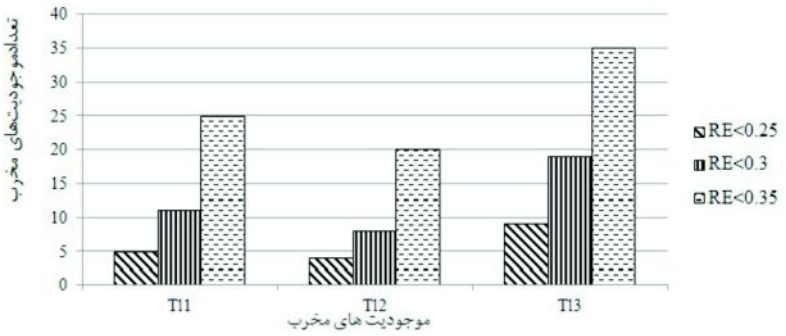
(شکل ۱): مقدار اعتبار برای منابع

همان‌طورکه در شکل (۲) ملاحظه شد، مجموعه متفاوتی از آستانه‌ها تعداد متفاوتی از موجودیت‌های مخرب را فراهم می‌کند. نتایج نشان می‌دهد اگر آستانهٔ اعتبار افزایش پیدا کند، تعداد موجودیت بیش‌تری را به‌عنوان موجودیت مخرب شناسایی می‌کند. همچنین اگر λ_{tl} افزایش یابد، موجودیت مخرب کمتری شناسایی می‌شود. اندازه‌گیری هم‌بند با α=0 منجر به حداکثر تعداد موجودیت‌های مخرب و α=1 منجر به حداقل تعداد موجودیت‌های مخرب می‌شود. بدین معنا که با افزایش α موجودیت‌های مخرب کمتری شناسایی می‌شوند. درصد موجودیت‌های مخرب برای هر کدام از روابط Tl با آستانه‌های مختلف به‌صورت نمودار در شکل (۳) نشان داده شده است.

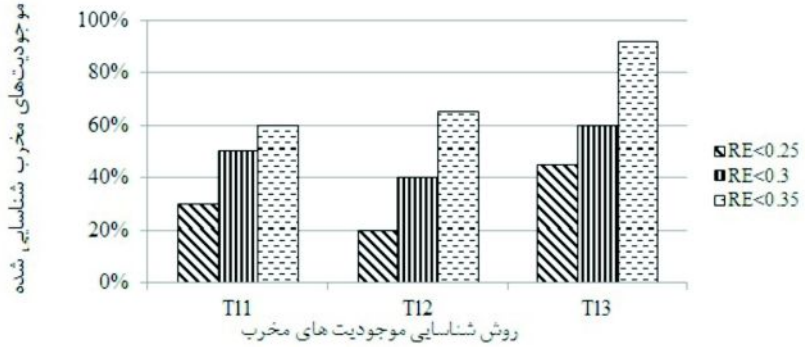
به‌عنوان مثال Tl_3 با RE<0.2 حدود ٪۴۵ موجودیت‌های مخرب را شناسایی یا Tl_1 با RE<0.35 حدود ٪۶۰ موجودیت‌های مخرب را شناسایی می‌کند. بنابراین Tl_3 با RE<0.35 می‌تواند بیش‌ترین تعداد موجودیت‌های مخرب را شناسایی کند.

(جدول ۳): نتایج ارزیابی شناسایی موجودیت‌های مخرب

وزن‌ها	روابط	RE<0.25 tl >400	RE<0.3 tl >400	RE<0.35 tl >400
$W1_{ID}$=0.3, $W2_{ID}$=0.2, $W3_{ID}$=0.4, $W4_{ID}$=0.1, W1=0.1, W2=0.2, W3=0.3, W4=0.1, W5=0.3	$Tl_{1^{R_K}}$	5	11	25
	$Tl_{2^{R_K}}$	4	8	20
	$Tl_{3^{R_K}}$	9	19	35



(شکل ۲): مقایسه موجودیت‌های مخرب



(شکل ۳): درصد تشخیص موجودیت‌های مخرب با استفاده از روش‌های مختلف.

۵- نتیجه‌گیری و کارهای آتی

در این مقاله چند روش جدید برای تعیین موجودیت‌های مخرب پیشنهاد شد. همچنین روش‌های اعتبار برای محیط رایانش ابری مورد تجزیه و تحلیل قرار گرفت. مقدار اعتبار براساس ویژگی‌هایی مانند دسترس‌پذیری، قابلیت اطمینان، یک‌پارچگی داده، هویت و شایستگی محاسبه شد. در این مقاله موجودیت‌های مخرب با استفاده از سه اندازه‌گیری هم‌بند که عبارتند از اندازه‌گیری درجهٔ وارده، اندازه‌گیری درجهٔ خارجه و اعتبار مورد بررسی قرار گرفته است. برخلاف روش‌های دیگر، در روش ارائه‌شده نظرات صحیح منفی، نظرات غیر صحیح منفی، نظرات صحیح مثبت و نظرات غیر صحیح مثبت در نظر گرفته شده است. آزمایش بر روی مجموعه داده‌ها نشان می‌دهد که روش ارائه‌شده، عملکرد بهتری

نسبت به روش‌های دیگر دارد. همچنین ملاحظه شد که تعداد موجودیت‌های مخرب، ارتباط مستقیمی با اعتماد و اعتبار دارند. اگر آستانهٔ اعتبار افزایش یابد، تعداد موجودیت‌های مخرب بیشتری شناسایی می‌شوند. آنچه که در آینده می‌توان انجام داد، برنامه‌ریزی برای بررسی تأثیر الگوریتم‌های تکاملی در ارزیابی اعتماد و اعتبار خواهد بود. روش‌های دیگری را می‌توان برای محاسبهٔ موجودیت‌های مخرب در نظر گرفت. همچنین عملیات انجام‌شده در این مقاله را می‌توان در شبکه‌های اجتماعی نیز پیاده‌سازی کرد.

۶- فهرست منابع

[1] S. S. Manvi and G. K. Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," *Journal of Network and Computer Applications,* vol. 41, pp. 424-440, 2014.

[2] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," presented at the 2011 World Congress on Information and Communication Technologies, 2011.

[3] P. Venkata Krishna, "Honey bee behavior inspired load balancing of tasks in cloud computing environments," *Applied Soft Computing,* vol. 13, pp. 2292-2303, 2013.

[4] M. Saad, M. Izuan, K. Abd Jalil, and M. Manaf, "Achieving trust in cloud computing using secure data provenance," in *Open Systems (ICOS), 2014 IEEE Conference on*, 2014, pp. 84-88.

[5] A. Gani, G. M. Nayeem, M. Shiraz, M. Sookhak, M. Whaiduzzaman, and S. Khan, "A review on interworking and mobility Techniques for seamless connectivity In Mobile Cloud Computing," *Journal of Network and Computer Applications,* vol. 43, pp. 84-102, 2014.

[6] J. Espadas, A. Molina, G. Jiménez, M. Molina, R. Ramírez, and D. Concha, "A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures," *Future Generation Computer Systems,* vol. 29, pp. ۲۸۶-۷۳, ۲۰۱۳.

[7] J. Anselmi, D. Ardagna, and M. Passacantando, "Generalized Nash equilibria for SaaS/PaaS Clouds," *European Journal of Operational Research,* vol. 236, pp. 326-339, 2014.

[8] P. Manuel, "A trust model of cloud computing based on Quality of Service," *Annals of Operations Research,* pp. 1-12, 2013.

[9] A. Gajbhiye and K. M. P. Shrivastva, "Cloud computing: Need, enabling technology, architecture, advantages and challenges," in *Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-*, 2014, pp. 1-7.

[10] N. Jafari Navimipour, A. M. Rahmani, A. H. Navin, and M. Hosseinzadeh, "Expert Cloud: A Cloud-based framework to share the knowledge and skills of human resources," *Computers in Human Behavior,* vol. 46, pp. 57-74, 2015.

[11] N. J. Navimipour, "A formal approach for the specification and verification of a Trustworthy Human Resource Discovery mechanism in the Expert Cloud," *Expert Systems with Applications,* vol. 42, pp. 6112-6131, 2015.

[12] F .Z. Filali and B. Yagoubi, "Global Trust: A Trust Model for Cloud Service Selection," *Computing,* vol. 3, p. 19, 2015.

[13] R. K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang*, et al.*, "TrustCloud: A framework for accountability and trust in cloud computing," in *Services (SERVICES), 2011 IEEE World Congress on*, 2011, pp. 584-588.

[14] B. Duckett, "Concise Oxford English Dictionary," *Reference Reviews,* vol. 19, pp. 33-33, 2005.

[15] W. Sun and Y.-x. Yuan, "A conic trust-region method for nonlinearly constrained optimization," *Annals of Operations Research,* vol. 103, pp. 175-191, 2001.

[16] T. H. Noor and Q. Z. Sheng, "Trust as a service: a framework for trust management in cloud environments," in *Web Information System Engineering–WISE 2011*, ed: Springer, 2011, pp. 314-321.

[17] F. J. Ortega, J. A. Troyano, F. L. Cruz, C. G. Vallejo, and F. Enríquez, "Propagation of trust and distrust for the detection of trolls in a social network," *Computer Networks,* vol. 56, pp. 2884-2895, 2012.

[18] F. Adelantado and C. Verikoukis, "Detection of malicious users in cognitive radio ad hoc networks: A non-parametric statistical approach," *Ad Hoc Networks,* vol. 11, pp. 2367-2380, 2013.

[19] L. Nkosi, P. Tarwireyi, and M. O. Adigun, "Detecting a malicious insider in the cloud environment using sequential rule mining," in *Adaptive Science and Technology*

(ICAST), 2013 International Conference on, 2013, pp. 1-10.

[20] Z. Yang, L. Qiao, C. Liu, C. Yang, and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," in *Computer Supported Cooperative Work in Design (CSCWD), 2010 14th International Conference on*, 2010, pp. 329-334.

[21] Q. Guo, D. Sun, G. Chang, L. Sun, and X. Wang, "Modeling and evaluation of trust in cloud computing environments," in *Advanced Computer Control (ICACC), 2011 3rd International Conference on*, 2011, pp. 112-116.

[22] M. Firdhous, O. Ghazali, and S. Hassan, "A trust computing mechanism for cloud computing," in *Kaleidoscope 2011: The Fully Networked Human-?Innovations for Future Networks and Services (K-2011), Proceedings of ITU*, 2011, pp. 1-7.

[23] I. M. Abbadi and M. Alawneh, "A framework for establishing trust in the Cloud," *Computers & Electrical Engineering,* 2012.

[24] P. Manuel, "A trust model of cloud computing based on Quality of Service," *Annals of Operations Research,* vol. 233, pp. 281-292, 2015.

[25] W. Lu, X. Hu, S. Wang, and X. Li, "A Multi-Criteria QoS-aware Trust Service Composition Algorithm in Cloud Computing Environments," *International Journal of Grid & Distributed Computing,* vol. 7, 2014.

[26] K. Chandran, V. Shanmugasudaram, and K. Subramani, "Designing a Fuzzy-Logic Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing," *International Arab Journal of Information Technology (IAJIT),* vol. 13, 2016.

[27] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems,* 2016.

[28] S. Wang, J. Wei, L. Sun, Q. Sun, and F. Yang, "Reputation Measurement of Cloud Services Based on Unstable Feedback Ratings," in *Parallel and Distributed Systems (ICPADS), 2013 International Conference on*, 2013, pp. 474-479.

[29] A. Chilwan, "Dependability Differentiation in Cloud Services," 2011.

[30] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security and Privacy,* vol. 8, pp. 24-31, 2010.

[31] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Engineering,* vol. 15, pp. 2852-2856, 2011.

[32] M. Firdhous, O. Ghazali, and S. Hassan, "Trust management in cloud computing: a critical review," *arXiv preprint arXiv:1211.3979,* 2012.

[33] S. Pearson, "Privacy ,security and trust in cloud computing," in *Privacy and Security for Cloud Computing*, ed: Springer, 2013, pp. 3-42.

سیده متین چیرگی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر (نرم‌افزار) به‌ترتیب در سال ۱۳۹۰ در موسسه غیرانتفاعی احرار رشت و ۱۳۹۳ در دانشگاه آزاد اسلامی واحد تبریز به پایان رساند. زمینهٔ پژوهشی مورد علاقهٔ وی رایانش ابری است. از وی مقاله‌هایی در مجلات بین‌المللی در حوزه یادشده به چاپ رسیده است.

نیما جعفری نویمی‌پور تحصیلات خود را در مقاطع کارشناسی مهندسی کامپیوتر (نرم‌افزار) در سال ۱۳۸۴در دانشگاه آزاد اسلامی واحد تبریز و کارشناسی ارشد مهندسی کامپیوتر (معماری کامپیوتر) در سال ۱۳۸۶ در دانشگاه آزاد اسلامی واحد تبریز به پایان رساند و سپس مدرک دکترای خود را در سال ۱۳۹۳ در رشته مهندسی کامپیوتر (معماری کامپیوتر) از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران اخذ کرد. ایشان هم‌اکنون استادیار گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تبریز است. ایشان تاکنون بیشتر از پنجاه مقاله در مجلات و کنفرانس‌های بین‌المللی به چاپ رسانده است. همچنین زمینه پژوهشی ایشان رایانش ابری، شبکه‌های اجتماعی، نرم‌افزارهای تحمل‌پذیر خطا، هوش محاسباتی، محاسبات تکاملی و شبکه بر روی تراشه است.