

سامانه مدیریت اعتماد مبتنی بر

آنتروپی جهت کاهش رفتارهای بدخواهانه در

سامانه‌های مدیریت اعتماد بر اساس نظریه

اخلاق اطلاعاتی

امیر خشکبارچی* و حمیدرضا شهریاری

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)، تهران، ایران

چکیده

سامانه‌های مدیریت اعتماد در محیط‌های تعاملی، جایی که یک عامل باید در مورد استفاده از یک خدمات تصمیم بگیرد، استفاده می‌شوند. به دلیل فراگیر شدن این سامانه‌ها، موجودیت‌های بدخواه انگیزه مضاعفی برای تأثیرگذاری بر سامانه‌های مدیریت اعتماد و ایجاد خدشه در فرایند تصمیم‌گیری دارند. با وجود روش‌های ارائه‌شده برای کاهش فعالیت‌های مخرب در الگوهای اعتماد قبلی، بسیاری از آنها نتوانستند به طور مؤثر این مشکل را حل کنند. به عنوان مثال، مقابله با تغییر رفتار عامل‌ها یک مشکل رایج برای بسیاری از الگوهای اعتماد است. علاوه بر این، هیچ رویکرد قوی، منعطف و تطبیقی ارائه نشده است و این مشکل همچنان وجود دارد. در این مقاله، رویکرد جدیدی برای جلوگیری از اعمال مخرب و شناسایی ناهنجاری‌ها با استفاده از یک سامانه مدیریت اعتماد مبتنی بر آنتروپی با قابلیت تشخیص ویژگی‌های ذاتی اقدامات عامل‌ها، اعم از اینکه اقدام مخرب باشد یا خیر، ارائه شده است. محاسبه اعتماد بر اساس ساختار آنتروپی، از نظریه اخلاق اطلاعات الهام گرفته شده است. با استفاده از این روش، اقدامات مخربی که سامانه مدیریت اعتماد را مختل می‌کنند، پالایش می‌شوند و در نتیجه، دقت محاسبه اعتماد افزایش می‌یابد. نتایج تجربی حاصل از شبیه‌سازی نشان می‌دهد که عملکرد سامانه پیشنهادی از نظر دقت محاسبه، قابلیت اعتماد خدمات و همچنین، تشخیص رفتار مخرب عامل‌ها قابل قبول است. به طور ویژه، الگوی پیشنهادی از نظر سرعت انطباق با تغییرات محیطی و رفتارهای متغیر عامل‌ها، حدود ده درصد نسبت به الگوهای اعتماد شناخته شده بهبود یافته است.

واژگان کلیدی: اعتماد، نظریه اخلاق اطلاعاتی، آنتروپی، کشف خدمات، محیط مبتنی بر سامانه، مبتنی بر سرویس، مبتنی بر خدمات

Entropy-Based Trust Management System for Mitigating Malicious Behaviors in Trust Management Systems, Considering Information Ethics Theory

Amir Khoshkbarchi* And Hamid Reza Shahriari

^{1, 2} Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran

Abstract

Trust management systems are used in interactive environments, where an agent needs to make a decision about using a service. Due to the preponderance of these systems, malicious entities have strong incentives to influence trust management systems and divert their decisions. In spite of approaches presented in previous trust models to mitigate the malicious activities, many of them could not cope with the problem efficiently. For example, tackling the variable behavior of agents is a common failure point for many trust models. Moreover, no rigid, flexible and adaptive general approach has been presented and the problem somehow remains.

This paper presents a novel approach to prevent malicious actions and identify anomalies using an entropy-based trust management system. The system is capable of recognizing the intrinsic characteristics of actions, determining whether they are malicious or not. To achieve this, the

* Corresponding author

* نویسنده عهده‌دار مکاتبات

سال ۱۴۰۲ شماره ۴ پیاپی ۵۸

• تاریخ ارسال مقاله: ۱۴۰۲/۱/۱۲ • تاریخ پذیرش: ۱۴۰۰/۴/۲۷ • تاریخ انتشار: ۱۴۰۲/۱۲/۲۹ • نوع مطالعه: پژوهشی



information environment is divided into four main parts based on entropy changes. Trust calculation in this system relies on an entropy structure derived from information ethics theory. To enhance the system's resistance and resilience against malicious behavior, it is important to understand the nature of the actions performed by the agents. To accomplish this, we define the patterns of entropy changes for the four parts and use these patterns to identify and refine the nature of actions as good, bad, or insignificant. The simulation-based experimental results indicate that the proposed system shows promising performance in terms of accurately calculating trust and detecting malicious behavior. Specifically, the proposed system exhibits a 10 percent advantage over well-known trust systems with regards to swiftly adapting to environmental changes and diverse agent behaviors. Moreover, the observed experiments have displayed a notable trend in the fluctuation of good, bad, and insignificant actions. The results indicate a consistent increase in the number of good actions and a corresponding decrease in bad actions. Put simply, the method demonstrates improvement over time through repeated system implementations. This improvement can be attributed to the agents' heightened honesty as they gain a better understanding of the nature of their actions. Additionally, the provision of feedback on their behavior plays a pivotal role in reinforcing more accurate decision-making within the system.

Keywords: Trust, Information Ethics Theory, Entropy, Service Discovery, Service-Oriented environment

اجتماعی و اینترنت اشیا استفاده می‌شود. به‌کارگیری سامانه‌های اعتماد باعث افزایش کیفیت ارتباطات و خدمات می‌شود؛ که این امر نیز با ایجاد انگیزه برای رفتار منصفانه و خوب، ارائه خدمات با کیفیت بالا و ممنوعیت رفتار بد و فعالیت‌های مخرب حاصل می‌شود.

اعتماد، ریشه اخلاقی در ذهن انسان و جوامع بشری دارد. لاهنو اعتماد را در بستر فلسفی این‌گونه تعریف می‌کند: «اعتماد عبارت است از کنش و واکنش خطرناک ناشی از روابط شخصی و اخلاقی بین دو موجودیت» [۴] و در برخی مراجع از اعتماد به‌عنوان فعالیت اخلاقی یاد می‌شود [۵]. بنابراین، اعتماد یکی از ابعاد اخلاق است. مطالعات بی‌شماری در مورد رابطه بین مفهوم اعتماد و اخلاق انجام شده‌است [۶]-[۸].

فلوریدی یک سامانه اخلاقی را برای محیط‌های اطلاعاتی بر اساس اصول نظریه اطلاعات توسعه داده‌است [۹]-[۱۱]. جنبه محاسباتی نظریه اخلاق اطلاعاتی را می‌توان مبتنی بر آنتروپی اطلاعات و نظریه اطلاعات شانون دانست. نظریه اخلاق اطلاعات (IE) آنتروپی^۳ اطلاعات را به‌عنوان معیاری برای سنجش اخلاقی بودن/ نبودن اقدامات در یک محیط اطلاعاتی در نظر می‌گیرد؛ بنابراین، بر اساس نظریه اخلاق اطلاعاتی امکان سنجش میزان اخلاقی بودن یک اقدام در محیط اطلاعاتی وجود دارد. با در نظر گرفتن ماهیت اخلاقی اعتماد، تغییرات آنتروپی در حوزه اخلاق اطلاعاتی می‌تواند تخمین خوبی از اعتماد ارائه دهد.

برای محاسبه اعتماد در یک محیط مبتنی بر سامانه به‌عنوان مثالی از فضای اطلاعاتی بررسی شده، دو منبع اطلاعاتی یعنی تجربیات شخصی کاربر و نظرات یا

۱- مقدمه

به‌منظور جلوگیری از خطا و خرابی در محیط‌های مبتنی بر خدمات، نیازمند شناسایی رفتارهای مخرب و فریب‌کارانه هستیم. این امر می‌تواند به‌وسیله سامانه مدیریت اعتماد^۱ انجام شود [۱]. در برخی از سامانه‌ها، چنین خطاهایی مستعد ایجاد شکست‌های بی‌شمار و جدی در تشخیص خدمات مناسب می‌شوند. پویایی و تصادفی بودن از خصوصیات ذاتی محیط‌های مبتنی بر سامانه^۲ است. فراهم‌کنندگان مختلف خدمات که خدمات‌هایی با عملکرد یکسان و کیفیت‌های متفاوت ارائه می‌کنند و همچنین، توصیه‌کنندگان با الگوهای رفتاری متفاوت و پویا برخی از عناصر متداول محیط مبتنی بر سامانه هستند [۲]. با این حال، انصاف و صداقت در چنین محیط‌های غیرقابل پیش‌بینی بسیار نادر است [۳]. به‌عنوان مثال، توصیه‌کنندگان ممکن است توصیه‌های فریبنده‌ای برای رسیدن به اهداف غیرمنصفانه و خصمانه خود ارائه دهند. علاوه بر این، بسیاری از فراهم‌کننده‌های خدمات، عملکردی را که از خدمات پیشنهادی خود دارند، ارائه نمی‌دهند. بنابراین، اقداماتی از این دست موجب تأثیر منفی در فرایند تصمیم‌گیری راجع به قابلیت اعتماد یک خدمات، یا میزان اعتماد یک عامل در محیط مبتنی بر سامانه می‌شود. این امر نیاز به سامانه‌های اعتماد را، که بخشی جدایی‌ناپذیر از برنامه‌های کاربردی و ابزارهای پشتیبانی تصمیم در نظر گرفته می‌شود، توجیه می‌کند. از این برنامه‌های کاربردی برای کاهش خطر در معاملات برخط، شبکه‌های سیار و بی‌سیم، تعاملات اجتماعی در بستر وب، شبکه‌های

¹ Trust Management System (TMS)

² Service-oriented Environment (SoE)

³ Entropy

(بدخواهانه یا غیرمنصفانه) در نظر گرفته می‌شوند. این امر یک مبنای کمی و محاسباتی برای تشخیص منصف بودن عامل‌ها و اقدامات آنها ارائه می‌دهد. بر اساس این رویکرد، همه اقدامات مخرب، از جمله اقداماتی که به صورت فردی یا گروهی انجام می‌شود، آنتروپی را به شیوه‌ای غیرمتعارف افزایش می‌دهد.

برای نشان دادن عملکرد و نتایج روش و مقایسه روش پیشنهادی با سایر روش‌ها، آزمایش‌هایی روی دو سامانه مدیریت اعتماد معروف، eBay و Beta انجام شده است. در نهایت، توانمندی این سامانه‌ها را بر اساس برخی از معیارهای بازدهی و دقت مشخص شده ارزیابی و مقایسه کردیم [۱۴]-[۲۰]. روش پیشنهادی می‌تواند در تمام محیط‌های مبتنی بر سامانه از جمله محیط‌های مربوط به اینترنت اشیا، شبکه‌های حسگر بی‌سیم و شبکه‌های اجتماعی استفاده شود.

در ادامه، متن مقاله به شرح زیر سازمان‌دهی شده است: در بخش (۲)، بررسی مختصری از مرتبط‌ترین الگوها و راهکارها در زمینه سامانه‌های اعتماد مقاوم ارائه شده است. بخش (۳) به تشریح سامانه مدیریت اعتماد پیشنهادی و همچنین، نحوه تشخیص ماهیت اقدامات می‌پردازد. برخی از آزمایش‌های تجربی حاصل از شبیه‌سازی انجام شده برای ارزیابی الگوی پیشنهادی در بخش (۴) ارائه شده است. در نهایت، در بخش (۵)، مقاله با بحث و نتیجه‌گیری پیرامون سامانه پیشنهادی به پایان می‌رسد.

۲- کارهای مرتبط پیشین

یکی از چالش‌های اصلی سامانه‌های مدیریت اعتماد حاضر توانایی مقابله سامانه با تهدیدهای وارد شده به خود سامانه اعتماد است. بارزترین عملی که باعث به اشتباه انداختن یک سامانه اعتماد می‌شود، ارائه نظرات و توصیه‌های اشتباه و با مقاصد بدخواهانه به سامانه است [۴۹]. الگوها و روش‌های مختلفی برای مقابله با این مسئله ارائه شده است؛ ولی دقت و عملکرد آنها با توجه به پیچیدگی رفتارهای انسانی و تغییر الگوی اعمال بدخواهانه کفایت نمی‌کند. علاوه بر این، الگوها و روش‌های ارائه شده پیشین به طور عمد مسئله محور بوده که با تغییر شرایط و عوامل دخیل در مسئله و همچنین، در مواجهه با مسائل جدید توانایی و بازدهی لازم را از دست داده و دچار اختلال در تصمیم‌گیری می‌شوند. هدف سامانه‌های مدیریت اعتماد فراهم‌سازی امکان تصمیم‌گیری در چنین شرایط غیرقطعی و بر اساس اعتماد است. تصمیمات امنیتی سامانه، مانند تشخیص ناهنجاری^۴، ارائه خدمات ایمن^۵

پیشنهادهای عامل‌های توصیه‌کننده حاضر در محیط وجود دارد. شهرت چیزی جز تجمیع نظرات عامل‌ها نیست. هرچه اختلاف بین نظرات کمتر باشد، (نظرات یکسان) میزان شهرت عامل افزایش می‌یابد. هرچه تنوع نظرات افزایش یابد، میزان آنتروپی محیط نیز نافزایش می‌یابد. پس با افزایش تنوع بین نظرات، میزان آنتروپی بیشتر و میزان شهرت کمتر می‌شود؛ و با کاهش شهرت یک عامل، میزان اعتماد به آن نیز کمتر خواهد شد؛ بنابراین، اعتماد و آنتروپی رابطه عکس با یکدیگر دارند [۴۸].

همان‌طور که می‌دانیم، محاسبه اعتماد در محیط مبتنی بر سامانه بر اساس توصیه‌ها و نظرات ارائه شده از سوی عامل‌ها و کاربران حاضر در محیط و تحلیل‌های ذهنی کاربر متقاضی خدمات صورت می‌پذیرد. در واقع یکی از دو مؤلفه محاسبه اعتماد، بر پایه نظرات عامل‌های توصیه‌کننده است. شهرت چیزی جز توافق جمعی نظرات بین کاربران در رابطه با یک مورد هدف نیست و پر واضح است که گوناگونی و عدم توافق بین نظرات که یکی از مصادیق آنتروپی است، در محاسبه اعتماد تأثیر مستقیم دارد [۴۳].

روش‌ها و الگوهای مختلفی برای توسعه سامانه‌های اعتماد برای محیط مبتنی بر سامانه پیشنهاد شده است که کاربران را برای کشف خدمات‌های بهتر راهنمایی می‌کنند. بسیاری از رویکردها، روش‌ها و سامانه‌های ارائه شده، در خصوص راه‌حل‌های موردی و مسئله محور و برای مشکلاتی که به طور متداول وجود دارند، توسعه یافته‌اند. این رویکردها اغلب تمایل دارند که محیط را بر اساس مجموعه محدودی از مؤلفه‌ها الگو کنند که بهترین تناسب را با مشکلات و مسائل خاص آنها دارند. این امر منجر به نادیده گرفتن شمار زیادی از ویژگی‌های چنین محیط‌های پیچیده‌ای می‌شود و دقت محاسبه میزان قابلیت اعتماد خدمات‌ها، عامل‌ها و موجودیت‌های هوشمند محیط را کاهش می‌دهد [۱۲]، [۱۳].

در مقاله حاضر، با استفاده از نظریه اخلاق اطلاعاتی، یک سامانه مدیریت اعتماد ارائه کرده و اقدامات عامل‌ها در یک محیط مبتنی بر سامانه را بررسی می‌کنیم، در واقع، یک سامانه اعتماد محاسباتی مبتنی بر آنتروپی با در نظر گرفتن ماهیت اقدامات صورت گرفته توسط عامل‌ها و نتیجه تغییرات آنتروپی را که در پی انجام اقدامات در محیط ایجاد می‌شود، توسعه می‌دهیم.

اقدامات عامل‌ها بر اساس تغییرات آنتروپی مربوط به آنها دسته‌بندی می‌شوند. اقداماتی که باعث افزایش آنتروپی در سامانه اعتماد می‌شود، به عنوان اقدامات بد

⁴ Anomaly Detection



احراز هویت^۶ و مدیریت دسترسی^۷ از قابلیت اعتماد محاسبه شده بهره می‌برند [۲۱]. با این حال، ممکن است از خود این سامانه‌ها به عنوان یک هدف به وسیله عوامل مخرب استفاده شود [۲۲]. استحکام سامانه مدیریت اعتماد در محیط‌های متخصص (باتوجه به تأثیرات عوامل مخرب) توجه زیادی را در ادبیات حوزه امنیت نرم به خود جلب کرده است. برای توصیف الگوهای اعتماد قوی، به بررسی حملات در سامانه‌های اعتماد و انواع آن‌ها می‌پردازیم.

در سامانه‌های مدیریت اعتماد، مهاجمان بازیگرانی متخصص هستند که به وسیله اهداف خودخواهانه یا بدخواهانه هدایت می‌شوند. حملات مهاجمان خودخواه برای برآورده کردن منافع شخصی صورت می‌گیرد، در حالی که هدف مهاجمان مخرب تضعیف اعتماد دیگران و ایجاد خدشه در عملکرد سامانه اعتماد است. به طور کلی، می‌توان اعمال بدخواهانه را در سه بخش کلی دسته‌بندی کرد و در هر بخش حملات شناخته شده‌ای وجود دارد که به تفکیک تشریح می‌شود:

I. توصیه‌های غیرمنصفانه

عامل‌های بدخواه با مقاصد خراب کارانه توصیه‌های نادرستی در مورد رفتار عوامل حاضر در محیط در اختیار دیگران قرار می‌دهند. این نوع حملات می‌توانند به صورت انفرادی و توسط یک شخص، یا جهت اعمال تأثیرات گسترده‌تر در قالب تبانی بین عوامل بدخواه انجام شود. حملاتی چون بدگویی^۸، خودبالابری^۹ و نظرات تصادفی در این دسته طبقه‌بندی می‌شوند.

II. حملات مربوط به مدیریت شناسه‌ها

این نوع حملات به نحوه احراز هویت موجودیت‌ها در جامعه و چگونگی مدیریت شناسه‌ها مرتبط بوده و عامل‌ها قابلیت‌هایی نظیر امکان تعریف چندین هویت در سامانه، می‌توانند رفتارهایی بدخواهانه از خود نشان دهند. حملاتی چون حمله شخص میانی^{۱۰}، حمله سایبیل^{۱۱} و حملات مربوط به تازه‌واردان^{۱۲} در این دسته طبقه‌بندی می‌شوند.

III. رفتارهای ناهماهنگ

رفتار برخی عامل‌ها ممکن است همواره و در شرایط و موقعیت‌های گوناگون ثابت نبوده و به صورت از پیش تعیین شده و به قصد تخریب در سامانه، در مواردی رفتار متناقض از خود نشان دهند و به این ترتیب، سامانه را برای واکنش در برابر رفتار خود دچار سردرگمی کنند. حملاتی چون رفتار متناقض با موجودیت‌های مختلف^{۱۳}، حمله روشن-خاموش^{۱۴} و جعل شهرت از نمونه‌های شناخته شده این دسته از حملات محسوب می‌شوند.

بیش از یک دهه است که تجزیه و تحلیل و ارزیابی عملکرد سامانه‌های مدیریت اعتماد در محیط‌های متخصص یکی از حوزه‌های پژوهشی داغ محسوب می‌شود. هافمن و همکاران در [31]، روش‌های دفاعی برای مقابله با حملات را در سامانه‌های مدیریت شهرت ارزیابی کردند. آنها از معیارهای مقاومت خاصی به منظور مقایسه بیست و چهار نمونه، از سامانه‌های مدیریت اعتماد معروف بهره برده‌اند.

جوسانگ و همکاران در [16] و همچنین، واولیس و همکاران در [32] و مارمول در [33]، در مورد عوامل مخرب و بدخواه، پژوهش‌های گسترده‌ای انجام داده و منتشر کرده‌اند و در آن‌ها نگرانی‌های امنیتی و موانعی که سامانه‌های مدیریت اعتماد با آن روبه‌رو هستند، بررسی شده است. نوریان و همکاران [34] معیارهای مقایسه‌ای را برای ارزیابی امنیتی سامانه‌های مدیریت اعتماد ارائه کردند. به تازگی، براگا و همکاران [35] حدود چهل مطالعه معاصر را در مورد اعتماد محاسباتی و سامانه‌های شهرت مقایسه کردند. این مطالعه بر اساس ویژگی‌های مشابه، مجموعه‌ای از معیارها را برای مقایسه سامانه‌های مدیریت اعتماد ارائه کرده، سپس مقالات را با استفاده از معیارهای تعیین شده ارزیابی کردند.

مطالعات دیگر، همانند مواردی که در بالا توضیح داده شد، تلاش کردند تا نظریات سامانه‌های مدیریت اعتماد همچون گنجاندن تهدیدات امنیتی جهت مقایسه این سامانه‌ها را با استفاده از مجموعه‌ای از معیارهای امنیتی توضیح داده و دسته‌بندی کنند. این مطالعات به طور عمده، مبتنی بر تجزیه و تحلیل تصادفی، موردی یا شهودی هستند و روشی مبتنی بر الگو یا الگویی در این حوزه از مطالعات ارائه نشده است.

مطالعات حاوی تجزیه و تحلیل مبتنی بر الگو در گروه متفاوتی قرار می‌گیرند. الگوهای پیشنهادی این دسته به طور عموم، یا برای سامانه‌های مدیریت اعتماد خاص یا جهت مقابله با حملات خاص ارائه شده‌اند. به عنوان مثال، حمله روشن-خاموش در شبکه‌های حسگر

⁵ Secure Service Provision

⁶ Authentication

⁷ Access Control

⁸ Bad-mouthing

⁹ Self-Promoting

¹⁰ Man in the middle

¹¹ Sybil

¹² Newcomer

¹³ Conflicting Behavior Attack

¹⁴ One-off Attack

اعتماد مبتنی بر آنتروپی به‌طور بالقوه می‌تواند هر موجودیت و مفهوم مهمی را در محاسبات تخمین اعتماد خود پوشش دهد. در بخش بعدی یک الگوی اعتماد مبتنی بر آنتروپی را توضیح خواهیم داد.

تمامی روش‌های مختل و گمراه‌کردن سامانه‌های اعتماد، اعم از عمدی یا سهوی، به‌طور جزئی یا کلی باعث ایجاد ناهنجاری در فضای اطلاعاتی موردبررسی (برای مثال محیط مبتنی بر سامانه) می‌شوند. تشخیص ناهنجاری‌ها و جلوگیری از تکرار آنها می‌تواند از رفتارهای مخرب جلوگیری کند و قابلیت اعتماد سامانه را افزایش دهد. ناهنجاری‌های ایجادشده در فضای اطلاعاتی موجب ازدست‌رفتن اطلاعات در مورد ساختار و عملکرد سامانه اعتماد می‌شود که در نتیجه این فقدان اطلاعاتی، آنتروپی محیط افزایش می‌یابد. در نتیجه، با رعایت اصول اخلاق اطلاعاتی، جلوگیری از ایجاد آنتروپی و کاهش آن، می‌توان از ایجاد و افزایش ناهنجاری‌های محیطی که اغلب با مقاصد بدخواهانه همراه هستند، جلوگیری کرد. در این مقاله بر اساس تغییرات آنتروپی به شناسایی ماهیت اقدامات عامل‌ها می‌پردازیم، به عبارت دیگر، با شناسایی اقدامات انجام‌شده به‌وسیله عامل‌ها می‌توان از بروز رفتارهای مخرب جلوگیری کرد. در ادامه به تشریح و الگو-سازی روش پیشنهادی می‌پردازیم.

۳- ساختار آنتروپی در سامانه مدیریت اعتماد بر اساس شناسایی اقدامات

ساختار آنتروپی در سامانه‌های مدیریت اعتماد مبتنی بر شناسایی اقدامات^{۱۸} (ESTAR)، یک سامانه مدیریت اعتماد برای کاهش رفتارهای مخرب بر اساس تغییرات آنتروپی و شناسایی اقدامات بوده و در اساس، مبتنی بر نظریه اخلاق اطلاعاتی و الگوسازی ساختار آنتروپی است. نظریه اخلاق اطلاعاتی فلوریدی [۹]-[۱۱] آنتروپی اطلاعات را به‌عنوان معیاری برای اخلاقی/بی‌اخلاق بودن رفتار عامل‌ها در محیط‌های اطلاعاتی در نظر می‌گیرد. بنابراین، می‌تواند مبنای خوبی برای رویکرد محاسباتی اعتماد به‌عنوان یک مفهوم در اصل، اخلاقی باشد. در [۹] و [۱۱]، افزایش آنتروپی به‌عنوان شاخصی از رفتار غیراخلاقی در نظر گرفته شده‌است. بر این اساس، ما در این مقاله یک الگوی ارزیابی اعتماد مبتنی بر محاسبات آنتروپی مرتبط با رفتارهای عامل‌ها، یعنی نظرات و توصیه‌ها، پیشنهاد می‌کنیم. شکل (۱) روابط بین مفاهیم

بی‌سیم مورد توجه شی و همکاران [۲۰]، چن و همکاران [۳۶] و پرون و همکاران [۳۷] بوده‌است. پژوهش‌های دیگری همچون وانگ و همکاران [۳۸]، [۳۹] برای بررسی حملات تبانی در سامانه‌های مدیریت اعتماد، ارائه شده‌است. الگوهای پیشنهادی بسیار پیچیده‌تر از آن است که برای سایر حملات یا سامانه‌های مدیریت اعتماد قابل‌استفاده باشد.

در پژوهشی دیگر، چو و همکاران [۴۰] از شبکه‌های پتری و الگوی هزینه/پاداش برای بررسی رفتار بدخواهانه عامل‌ها در محیط استفاده کردند. هر دو الگو با هدف خاصی طراحی شده‌اند، ولی با سامانه‌های مدیریت اعتماد مختلف یا حملات اعتماد سازگار نیستند.

آلدینی و همکاران [۴۱] به‌ترتیب از فرآیندهای تصمیم‌گیری مارکوف^{۱۵} و مکانیزم هزینه/پاداش برای توصیف سامانه‌های مدیریت اعتماد و سناریوهای تعامل با عامل هوشمند استفاده کردند. اگرچه این روش‌های الگوسازی مناسب و مفید هستند، ولی هر دو الگو فاقد رسمیت لازم برای پشتیبانی از طیف گسترده‌ای از سامانه‌های مدیریت اعتماد و نحوه برخورد با سوءاستفاده‌های احتمالی‌اند. پژوهشی دیگر در این زمینه، الگوسازی اعتماد مبتنی بر منطق مولر و همکاران [۴۲] است. پژوهش‌گران این مطالعه معتقدند که اعتماد یک مفهوم بولی است. با توجه به این که این الگوسازی از ماهیت احتمالی و چندعاملی بودن اعتماد پیروی نمی‌کند، تنها برای تعداد کمی از سامانه‌های مدیریت اعتماد قابل‌استفاده است.

باتوجه به نظریه اخلاق اطلاعاتی [9]، [10]، [43]، بسیاری از الگوهای اعتماد موجود در دسته اخلاق خرد^{۱۶} قرار می‌گیرند؛ یعنی الگوهای اخلاقی که برآوردها و محاسبات خود را بر اساس مجموعه محدودی از مفاهیم اخلاقی می‌سازند. این الگوها برخی از شاخص‌های معین از محیط را در نظر گرفته و با ارائه تفسیرهای رسمی محکم از رفتار «خوب» و «بد» عامل‌ها در محیط در مورد آن شاخص‌ها، مبنای محاسباتی خود را ایجاد می‌کنند و بسیاری از شاخص‌ها و ویژگی‌های اطلاعاتی دیگر را نادیده می‌گیرند.

همان‌طور که نظریه اخلاق اطلاعاتی بیان می‌کند، یک نگرش اخلاقی کلان^{۱۷} از محیط‌های اطلاعاتی می‌تواند دید جامع‌تری از محیط ارائه دهد. نظریه اخلاق اطلاعاتی مفهوم آنتروپی اطلاعاتی را به‌عنوان یک مؤلفه محاسباتی معرفی می‌کند که می‌تواند هر مفهوم مشخصه محیطی را در شرایط اخلاقی قابل محاسبه کند. بنابراین، یک الگوی

¹⁵ Markov Decision Processes (MDP)

¹⁶ Micro-ethics

¹⁷ Macro-ethics

¹⁸ Entropy Structure in TMS based on Actions Recognition (ESTAR)



اصلی و روش‌شناسی رویکرد ارائه‌شده را نشان می‌دهد. همچنین، این رویکرد راه را برای استفاده از محاسبات عمیق و توسعه‌یافته برای آنتروپی در نظریه اطلاعات شانون هموار می‌کند.

شرح مفصلی از محاسبات اعتماد در این الگو، پیشتر در [۴۴] منتشر شده‌است که هدف آن شناسایی خدمات قابل اعتماد در یک محیط مبتنی بر سامانه است. در اینجا به بررسی مختصری از محاسبات اعتماد مبتنی بر آنتروپی می‌پردازیم و سپس آنها را برای تشخیص ماهیت اخلاقی اقدامات عامل‌ها در محیط به کار می‌بریم. برای توسعه سامانه، چهار دسته از عناصر آنتروپی در یک محیط مبتنی بر سامانه مشخص کردیم. سپس، یک روش محاسبه آنتروپی خاص برای هر یک از این دسته‌ها بر اساس محاسبه آنتروپی ارائه‌شده در نظریه اطلاعات شانون ارائه کردیم. سامانه اعتماد این چهار مقدار آنتروپی را برای تعیین آنتروپی کلی، و بنابراین، محاسبه میزان اعتماد یک خدمات ویژه برای بهینه‌سازی انتخاب خدمات، ادغام می‌کند.

محاسبات بر روی یک ساختار ریاضی ایجادشده از حالت‌های آنتروپی محیط انجام می‌شود. اقدامات مختلف عامل‌ها در محیط بیان‌گر انتقال بین این حالات آنتروپی در ساختار است. در این بخش، نخست، این ساختار آنتروپی ویژه را به اختصار معرفی می‌کنیم؛ سپس، عناصر آنتروپی در محیط را به همراه محاسبات مربوط نشان می‌دهیم. برای انتخاب خدمات/خدمات‌ها، تمام عناصر آنتروپی (دسته‌های آنتروپی) را جهت محاسبه اعتماد کلی عامل‌ها و خدمات موجود در محیط، ادغام می‌کنیم. سپس، این محاسبات را برای ایجاد یک سامانه ارزیابی اعتماد برای تشخیص وضعیت اخلاقی و قابل‌اعتمادبودن اقدامات انجام می‌دهیم.

۱-۳- ساختار آنتروپی

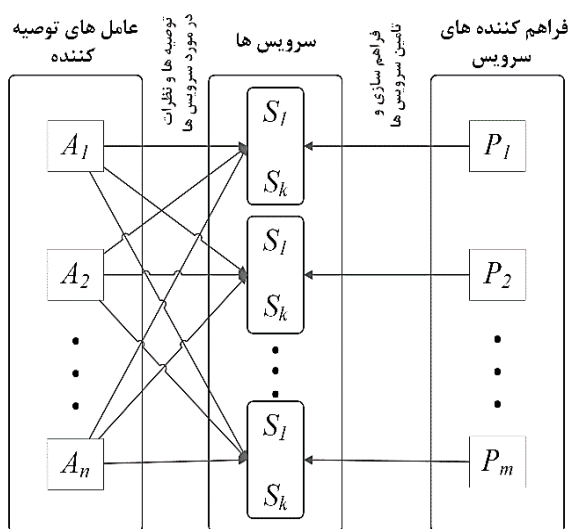
نخست، به‌طور خلاصه به تبیین ساختار آنتروپی موردنیاز برای محاسبه اعتماد که در [۴۴] به‌طور کامل شرح دادیم، می‌پردازیم.

تعریف ۱: ساختار آنتروپی به صورت (X, \leq, \square) تعریف می‌شود که در آن X مجموعه حالت‌های ممکن یک محیط معین را نشان می‌دهد، علامت \leq نشان‌دهنده یک رابطه پیش‌ترتیب^{۱۹} بین حالات مختلف محیط است و \square نشان‌دهنده رابطه هم‌ارزی^{۲۰} بین آنهاست.

تعریف ۲: حالتی از محیط به‌صورت هفت‌تایی تعریف می‌شود (رابطه ۱) و در آن $A = \{a_1, a_2, \dots, a_n\}$ که

شامل مجموعه عامل‌های توصیه‌کننده، مجموعه $P = \{p_1, p_2, \dots, p_m\}$ فراهم‌کنندگان خدمات، $S = \{s_1, s_2, \dots, s_k\}$ مجموعه خدمات، و u کاربری که می‌خواهد از برخی خدمات استفاده کند (کاربر جویای خدمات). سامانه مدیریت اعتماد پیشنهادی برای کمک به کاربر جویای خدمات جهت یافتن خدمات/خدمات‌های مناسب توسعه داده شده‌است.

مجموعه‌ای از توصیه‌های تولیدشده به‌وسیله عامل‌های توصیه‌کننده، Sat_u مجموعه‌ای از نرخ رضایت کاربر بر اساس تجربیات خود از خدمات/خدمات‌ها، و در نهایت، H آنتروپی کل محیط است. بنابراین، فضای حالت به‌صورت زیر تعریف می‌شود:

$$X = \{ \langle A, P, S, u, Rec, Sat_u, H \rangle_y / y \in \square \} \quad (1)$$


(شکل ۲-۲). ساختار جمع‌آوری توصیه‌ها در انبار داده کشف و به‌کارگیری خدمات

(Figure-2). The structure of collecting recommendations in the service discovery and consumption repository

Rec مجموعه‌ای از توصیه‌های تولیدشده به‌وسیله عامل‌ها در محیط که به‌صورت زیر در رابطه (۲) قابل تعریف است:

$$Rec_{a_i} = \{ (r_{i,j,l}, p_j, s_l) \mid p_j \in P, s_l \in S, i \in \{1, \dots, n\}, j \in \{1, \dots, m\}, l \in \{1, \dots, k\} \} \quad (2)$$

به این ترتیب، Rec_{a_i} توصیه‌های عامل a_i در مورد خدمات s_l ارائه‌شده به‌وسیله فراهم‌کننده خدمات p_j است، و مقدار $r_{i,j,l}$ ۱ یا ۰ است که نشان‌دهنده اعتماد یا بی‌اعتمادی عامل a_i به خدمات s_l ارائه‌شده به‌وسیله فراهم‌کننده p_j است. شکل (۲)، ساختار توصیه‌های یک عامل را در طول زمان فعالیت او در محیط نشان می‌دهد.

تعریف ۳: توالی توصیه‌های عامل‌ها به‌صورتی که در رابطه (۳) نمایش داده‌شده، قابل تعریف است:

¹⁹ Pre-order

²⁰ Equivalence

$$O_{a_1} = \langle (r_{1,1,1}, p_1, s_1), \dots, (r_{1,1,k}, p_1, s_k), \dots, (r_{1,m,1}, p_m, s_1), \dots, (r_{1,m,k}, p_m, s_k) \rangle$$

$$O_{a_2} = \langle (r_{2,1,1}, p_1, s_1), \dots, (r_{2,1,k}, p_1, s_k), \dots, (r_{2,m,1}, p_m, s_1), \dots, (r_{2,m,k}, p_m, s_k) \rangle$$

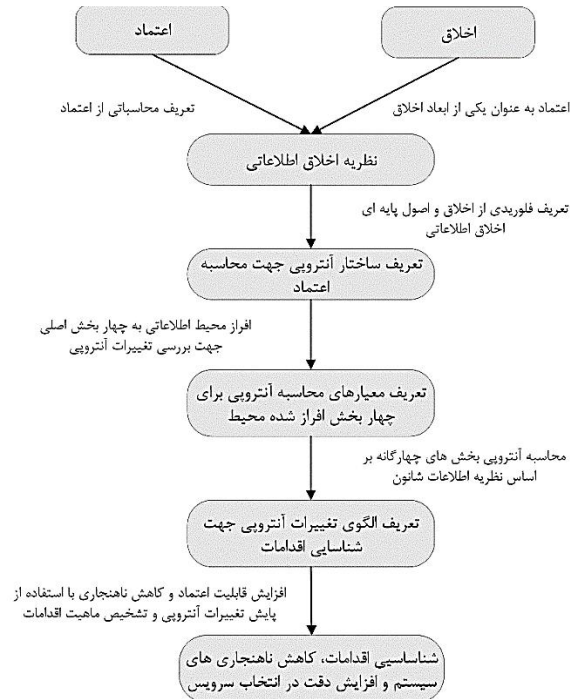
$$O_{a_3} = \langle (r_{3,1,1}, p_1, s_1), \dots, (r_{3,1,k}, p_1, s_k), \dots, (r_{3,m,1}, p_m, s_1), \dots, (r_{3,m,k}, p_m, s_k) \rangle$$

.

.

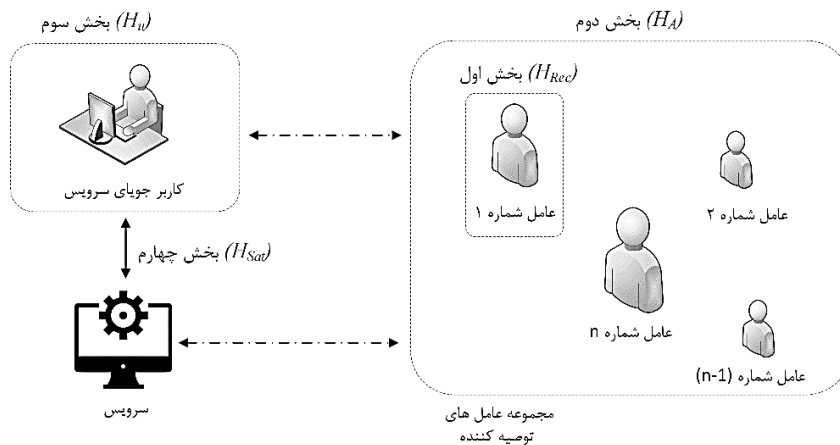
.

$$O_{a_n} = \langle (r_{n,1,1}, p_1, s_1), \dots, (r_{n,1,k}, p_1, s_k), \dots, (r_{n,m,1}, p_m, s_1), \dots, (r_{n,m,k}, p_m, s_k) \rangle$$



(شکل-۱). روش شناسی روش پیشنهادی

(Figure-1). Methodology of the proposed method



(شکل-۳). موقعیت و مبدأ هر یک از بخش ها و عناصر آنترپوی و موجودیت های حاضر در محیط

(Figure-3). The position and origin of each of the parts and elements of entropy and the entities in the environment

x' اگر سطح آنتروپی x از x' پایین تر باشد، خواهیم داشت: $Level(x) \leq Level(x')$.

اگر دو حالت، سطح آنتروپی یکسانی داشته باشند، می‌توانیم توابع سطح را به این صورت در نظر بگیریم: $Level(x) \square Level(x')$. اکنون برای هر یک از چهار بخش معرفی شده در بالا یک تابع سطح تعریف می‌کنیم. محاسبه آنتروپی کل برای محیط مبتنی بر سامانه، بر اساس تجمیع آنتروپی چهار بخش، قابل محاسبه خواهد بود.

۲-۳- عناصر آنتروپی در یک محیط مبتنی بر سامانه

باتوجه به [۴۴]، الگوی پیشنهادی شامل چهار عنصر آنتروپی اصلی در کل آنتروپی یک محیط مبتنی بر سامانه است. روش محاسبه هر یک از عناصر در ادامه ارائه شده است.

۱-۲-۳- آنتروپی نظرات عامل‌ها در طول زمان

نخستین عنصر آنتروپی معرفی شده با تغییراتی در توصیه‌های یک عامل خاص در طول زمان همراه است. معادله (۶) این آنتروپی را برای توصیه‌های ارائه شده به وسیله یک عامل خاص در یک خدمات خاص محاسبه می‌کند.

$$H_{Rec}^{a_i, s_l} = - \sum_{y=1}^{t_c-1} (\alpha^{(t_c-t_y)} \times d_{Rec}(\tau_{t_c}, \tau_{t_y}) \times \log(d_{Rec}(\tau_{t_c}, \tau_{t_y}))) \quad (6)$$

در این معادله، t_c زمان انجام محاسبات را نشان می‌دهد، t_y نشان‌دهنده زمان‌هایی است که توصیه‌ها ارائه می‌شوند و α به‌عنوان ضریب محوشدن (فراموشی)^{۲۱} عددی بین ۰ تا ۱ است. این عامل تأثیر توصیه‌های جدید در محاسبه آنتروپی را نسبت به توصیه‌های قبلی افزایش می‌دهد.

برای محاسبه آنتروپی، توصیه‌های یک عامل برای همه خدمات در طول زمان، داریم:

$$H_{Rec}^{a_i} = \sum_{l=1}^k H_{Rec}^{a_i, s_l} \quad (7)$$

در معادله (۷)، $H_{Rec}^{a_i}$ آنتروپی توصیه‌های یک عامل برای همه خدمات‌ها را در طول زمان نشان می‌دهد.

Sat_u مجموعه‌ای از میزان رضایت کاربر بر اساس تجربیات خود از خدمات/ خدمات‌هاست که به‌صورت زیر قابل تعریف است:

$$Sat_u = \{(c_{j,l}, p_j, s_l) \mid p_j \in P, s_l \in S, j \in \{1, \dots, m\}, l \in \{1, \dots, k\}\} \quad (4)$$

در رابطه (۴)، $c_{j,l}$ یک عدد حقیقی بین ۰ و ۱ است که تجربه رضایت کاربر از خدمات l' ام ارائه شده توسط فراهم‌کننده j' ام را نشان می‌دهد.

H آنتروپی کل محیط مورد بررسی است که به‌عنوان مجموعه چهار عنصری از مقادیر آنتروپی بخش‌های مختلف سامانه تعریف می‌شود و به‌صورت زیر قابل تعریف است:

$$H = \{H_{Rec}, H_A, H_u, H_{Sat}\} \quad (5)$$

در رابطه (۵)، چهار بخش آنتروپی به شرح زیر داریم:

I. H_{Rec} ، بیان‌گر آنتروپی توصیه‌های عامل‌ها در طول زمان است.

II. H_A ، بیان‌گر آنتروپی بین نظرات عامل‌های مختلف است.

III. H_u ، بیان‌گر آنتروپی بین توصیه‌های عامل‌ها و تجربه کاربر جویای خدمات است.

IV. H_{Sat} ، بیان‌گر آنتروپی بین خدمات فراهم‌شده و میزان رضایت کاربر جویای خدمات است.

شکل (۳) موقعیت و مبدأ هر عنصر آنتروپی را در موجودیت‌های محیطی نشان می‌دهد. برای ارزیابی آنتروپی هر عنصر، باید ویژگی‌های بخش‌های آنتروپی، عوامل درگیر در هر بخش و برهم‌کنش‌های آنها را در نظر بگیریم.

تعریف ۴: ساختار سامانه اعتماد یک سه‌گانه (X, T, λ) متشکل از فضای حالت (X) ، تابع انتقال حالت (T) و تابع سطح آنتروپی (λ) است، که در آن، تابع انتقال حالت نگاشتی از فضای حالت به خودش است $(T: X \rightarrow X)$ ، و تابع سطح آنتروپی نگاشتی از فضای حالت به مجموعه اعداد حقیقی است $(\lambda: X \rightarrow \square)$. یک تغییر حالت می‌تواند با یک توصیه یا یک تجربه آغاز شود.

سطوح آنتروپی، تابع انتقال حالت و تابع سطح برای محاسبه آنتروپی بر اساس ساختار سامانه اعتماد قابل تعریف هستند. همان‌طور که در تعریف (۱) و تعریف (۴) توضیح داده‌شد، ما به یک تابع سطح نیاز داریم تا حالت‌ها را بر اساس روابط پیش‌ترتیب (\leq) و هم ارزی (\square) مقایسه کنیم. این تابع یک مقدار عددی برای این مقایسه ارائه می‌دهد. برای هر جفت از حالت‌های X و

²¹ Fading Factor

$$H_{Sat} = -(Sat_u \times \log Sat_u - (1 - Sat_u) \times \log(1 - Sat_u)) \quad (11)$$

$$H_u = -\sum_{i=1}^n (J_d(Sat_u, O_{a_i}) \times \log(J_d(Sat_u, O_{a_i}))) \quad (10)$$

۳-۲-۴- رضایت کاربر جویای خدمات دریافت شده و میزان رضایت کاربر جویای خدمات

یک کاربر جویای خدمات یک خدمات خاص را بر اساس نیازهای خود درخواست می‌کند. این درخواست ممکن است به وسیله خدمات مختلف پاسخ داده شود.

در اینجا، مسئله اصلی رضایت کاربر جویای خدمات از خدمات دریافتی است. به عبارت بهتر، تفاوت کمتر بین انتظارات کاربر و ویژگی‌های خدمات دریافتی نشان‌دهنده انتخابی درست است.

این عنصر آنتروپی باتوجه به نسبت رضایت کاربر از یک خدمات خاص (Sat_u) و نسبت نارضایتی مربوط ($1 - Sat_u$) قابل محاسبه است:

در رابطه (۱۱)، H_{Sat} آنتروپی بین خدمات استفاده شده و رضایت کاربر است. این مقادیر رضایت/نارضایتی توسط کاربر بر اساس رضایت وی از خدمات تعیین می‌شود.

۳-۳- تجمیع آنتروپی و اعتماد خدمات

تجمیع مقادیر آنتروپی‌های جزئی (آنتروپی بخش‌ها) که در بالا معرفی شد، آنتروپی کل سامانه مرتبط با یک انتقال (تغییر حالت در اثر یک اقدام به وسیله عامل‌ها یا کاربر جویای خدمات) خاص را به دست می‌دهد. این تجمیع به صورت مجموع وزن دار آنتروپی‌های جزئی محاسبه می‌شود. هر عنصر از معادله کل آنتروپی نشان‌دهنده مقدار آنتروپی محاسبه شده برای یکی از بخش‌های محیط است:

$$H = \bar{w}_{Rec} \times H_{Rec} + \bar{w}_a \times H_A + \bar{w}_u \times H_u + \bar{w}_{Sat} \times H_{Sat} \quad (12)$$

وزن‌های موجود در معادله (۱۲) باید اهمیت مقادیر آنتروپی متناظر خود را نشان دهند؛ یعنی تأثیر نسبی هر عنصر آنتروپی در کل آنتروپی سامانه مشخص می‌شود. برای به دست آوردن قابل اطمینان‌ترین تخمین آنتروپی، مقادیر وزن متناسب با مقدار اطلاعات حمایت‌کننده محیطی^{۲۳} (مقدار اطلاعات حاصل از نظرات و سطح رضایت کاربر در بخش‌های چهارگانه) در نظر گرفته می‌شود:

در نهایت، از معادله زیر برای محاسبه آنتروپی توصیه‌ها برای همه عامل‌ها در طول زمان استفاده می‌شود.

$$H_{Rec} = \sum_{i=1}^n H_{Rec}^{a_i} \quad (8)$$

۳-۲-۲- آنتروپی بین نظرات عامل‌های مختلف

آنتروپی بین نظرات عامل‌های مختلف در محیط تأثیر زیادی در آنتروپی کل دارد. تعریف (۳) شکل کلی توصیه‌های مرتبط با این عنصر آنتروپی را نشان می‌دهد. آنتروپی توصیه‌های عامل‌های مختلف باتوجه به تفاوت بین توالی نظرات عامل‌ها محاسبه می‌شود. از فاصله ژاکارد^{۲۲} به عنوان معیار مقایسه و تفاوت نظرات و توصیه‌های عامل‌ها استفاده می‌کنیم. این فاصله به عنوان احتمال توصیه منطقی برای محاسبه آنتروپی در نظر گرفته می‌شود. مجموع تمام این مقایسه‌های جفتی، مقدار کل آنتروپی مرتبط با این تفاوت‌ها را نشان می‌دهد:

$$H_A = -\sum_{i=1}^n \sum_{j \in \{1, \dots, n\}, j \neq i} (J_d(O_{a_i}, O_{a_j}) \times \log(J_d(O_{a_i}, O_{a_j}))) \quad (9)$$

در این معادله، H_A آنتروپی کل بین نظرات عامل‌ها به عنوان شاخصی از تفاوت تمام توصیه‌های عامل‌ها در محیط است. توصیه‌های مشابه که به وسیله عامل‌های مختلف ایجاد می‌شوند، دلالت بر آنتروپی پایین‌تر در این بخش دارد.

۳-۲-۳- آنتروپی توصیه‌های عامل‌ها و تجربه کاربر جویای خدمات

کاربر جویای خدمات، تجربیات خود را از خدمات مختلف پیگیری می‌کند و سپس این تجربیات را برای تصمیمات آینده در مورد استفاده از آن‌ها محاسبه می‌کند. تجربه شخصی کاربر منبع بسیار مهمی از تخمین اعتماد در مورد خدمات است. آنتروپی بین تجربیات کاربر و توصیه‌های سایر عامل‌ها، تخمین کمی خوبی از اعتماد به عامل‌ها را به دست می‌دهد.

مانند عنصر آنتروپی قبلی، آنتروپی بین تجربه شخصی کاربر و توصیه‌های سایر عامل‌ها نیز با فاصله ژاکارد از تجربه و توصیه‌ها محاسبه می‌شود: که در آن $J_d(Sat_u, O_{a_i})$ فاصله ژاکارد از تجربه کاربر (Sat_u) و توالی توصیه‌های عامل a_i (O_{a_i}) است.

²³ Environmental Supporting Information

²² Jaccard Distance



نمایش، از x به جای استفاده از $\langle A, P, S, u, Rec', Sat_u, H \rangle$ بهره می‌بریم و به صورت $T(x_i) = x'_i$ نمایش می‌دهیم.

II. در فضای حالت، فقط سطح رضایت کاربر جوپای خدمات دخیل باشد و توصیه‌ها وجود نداشته‌باشد. برای بیان آسان، از y به جای استفاده از $\langle A, P, S, u, Rec, Sat'_u, H \rangle$ بهره می‌بریم و به صورت $T(y_i) = y'_i$ نمایش می‌دهیم.

III. در فضای حالت، هم توصیه‌ها و نظرات عامل‌ها و هم سطح رضایت کاربر جوپای خدمات دخیل باشد. برای بیان آسان، از z به جای استفاده از $\langle A, P, S, u, Rec', Sat'_u, H \rangle$ بهره می‌بریم و به صورت $T(z_i) = z'_i$ نمایش می‌دهیم.

همان‌طور که گفته شد، هر عملی در فضای اطلاعاتی یا باعث افزایش آنترویی یا کاهش آن می‌شود، یا تغییر قابل توجهی در آنترویی ایجاد نمی‌کند. برای پی‌گیری تغییرات آنترویی، باید رویدادهای مهم تغییر آنترویی را در نظر بگیریم. شناسایی و کاهش این رویدادها باعث افزایش قابلیت اعتماد سامانه و جلوگیری از رفتارهای مخرب در آن می‌شود.

۱-۴-۳- شناسایی اقدامات برای بخش نخست

تابع انتقال حالت برای بخش نخست سامانه فقط از توصیه‌ها تشکیل شده است ($T(x_i) = x'_i$).

تعریف ۵: اقدام خوب برای بخش نخست: هنگامی که یک توصیه به وسیله یک عامل ارائه می‌شود و در نتیجه، آنترویی توصیه‌های عامل در طول زمان کاهش می‌یابد، اقدام، خوب یا عادی در نظر گرفته می‌شود:

$$\forall x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \Rightarrow H_{Rec}^{a_i}(x') \leq H_{Rec}^{a_i}(x) \quad (16)$$

تعریف ۶: اقدام بد برای بخش نخست: زمانی که یک توصیه جدید (عمدی یا غیرعمدی) با توصیه‌های قبلی در مورد همان خدمات تغییر فاحشی داشته‌باشد، یک اقدام مشکوک به اقدام بد محسوب می‌شود. چنین توصیه‌هایی باعث افزایش آنترویی و به‌عنوان اقدام مخرب تلقی می‌شود:

$$\exists x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \wedge H_{Rec}^{a_i}(x) \leq H_{Rec}^{a_i}(x') \quad (17)$$

$$\begin{aligned} w_{Rec} &= |O_a| \\ w_a &= |O_a| \\ w_u &= |O_a| + |Sat| \\ w_{Sat} &= |Sat| \end{aligned} \quad (13)$$

برای به‌دست‌آوردن یک مقدار معقول برای آنترویی، وزن‌ها عادی/طبیعی می‌شوند تا وزن کل آنترویی‌ها برابر با یک باشد:

$$\bar{w}_{Rec} + \bar{w}_a + \bar{w}_u + \bar{w}_{Sat} = 1 \quad (14)$$

پس از محاسبه آنترویی کل مرتبط با یک خدمات خاص، کاربر اعتماد خود را به خدمات مورد نظر در رابطه با این مقدار آنترویی به صورت زیر محاسبه می‌کند:

$$Trustworthiness_{service_i} = \frac{1}{H} \quad (15)$$

معادله (۱۵) ارزش اعتماد را به نسبت معکوس با کل آنترویی محیط مرتبط تعریف می‌کند. یک آستانه تصمیم برای ترسیم ارزش اعتماد به تصمیم در مورد استفاده یا عدم‌استفاده از خدمات استفاده می‌شود. به‌عنوان مثال، با آستانه تصمیم‌گیری ۰.۵، در صورتی که مقدار اعتماد محاسبه‌شده بالاتر از ۰.۵ باشد، کاربر از خدمات استفاده می‌کند.

۴-۳- شناسایی اقدامات مبتنی بر الگوی

تغییرات آنترویی

عناصر آنترویی تحت تأثیر هر اقدام جدیدی که می‌تواند در قالب توصیه‌ها و نظراتی باشد که به وسیله عامل‌ها ارائه می‌شود، قرار گیرند. همچنین، اقدامات کاربر جوپای خدمات، از جمله استفاده از خدمات و ارائه نرخ رضایت نیز از جمله اقداماتی است که محیط را تحت تأثیر قرار داده و باید ارزیابی و بررسی شود. این تأثیر باعث افزایش یا کاهش سطح آنترویی می‌شود و ممکن است در برخی موارد اثر قابل ملاحظه‌ای نداشته‌باشد.

همان‌طور که در تعریف (۴) بیان شد، فضای حالت تحت تأثیر تابع انتقال به صورت مداوم دچار تغییر می‌شود و شاخص‌های A, P, S, u, H عوض می‌شوند. اما به‌منظور سهولت در نمایش، برای Rec و Sat سه حالت را در نظر می‌گیریم:

I. در فضای حالت، فقط توصیه‌ها و نظرات عامل‌ها دخیل باشد و سطح رضایت کاربر جوپای خدمات وجود نداشته‌باشد. برای بیان آسان و سهولت در

تعریف ۱۱: اقدام خوب برای بخش سوم: تشابه توصیه‌ها و تجربیات خود کاربر می‌تواند آنتروپی را در این بخش کاهش دهد. بنابراین، اقدام به‌عنوان خوب طبقه‌بندی می‌شود:

$$\begin{aligned} \forall z, z' : X \bullet \{a_i\}_{i \in \mathbb{I}} \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \wedge u \text{ Experience } Sat'_u(c_{j,l}, p, s) \\ \Rightarrow H_u(z') \leq H_u(z) \end{aligned} \quad (22)$$

تعریف ۱۲: اقدام بد برای بخش سوم: تفاوت محسوس بین توصیه‌های عامل‌ها و تجربه خود کاربر نشان‌دهنده افزایش آنتروپی است و اقدامات عامل‌ها را به‌عنوان بد/مخرب طبقه‌بندی می‌کند:

$$\begin{aligned} \exists z, z' : X \bullet \{a_i\}_{i \in \mathbb{I}} \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \wedge u \text{ Experience } Sat'_u(c_{j,l}, p, s) \\ \wedge H_u(z) \leq H_u(z') \end{aligned} \quad (23)$$

تعریف ۱۳: اقدام غیرمهم برای بخش سوم: اگر تفاوت بین توصیه‌های عامل‌ها و تجربه کاربر ناچیز و غیرمحسوس باشد، عمل غیرمهم/خوش‌خیم تلقی می‌شود:

$$\begin{aligned} \forall z, z' : X \bullet \{a_i\}_{i \in \mathbb{I}} \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \wedge u \text{ Experience } Sat'_u(c_{j,l}, p, s) \\ \Rightarrow H_u(z) \square H_u(z') \end{aligned} \quad (24)$$

۳-۴-۴ - شناسایی اقدامات برای بخش چهارم
در بخش چهارم، تابع انتقال حالت، تابع تجربه ($T(y_i) = y'_i$) و نشان‌دهنده تغییرات تجربه کاربر از یک خدمات ویژه در طول زمان است. بدیهی است که تجربه پس از استفاده از یک خدمات ایجاد می‌شود. بنابراین، تنها با محاسبات اعتماد آینده (در بخش‌های ۳ و ۴) مفهوم می‌یابد.

تعریف ۱۴: اقدام خوب برای بخش چهارم: شباهت بین کیفیت خدمات دریافتی و تجربه شخصی کاربر می‌تواند آنتروپی این بخش را کاهش دهد. به عبارت دیگر، اگر تجربه کاربر از استفاده از خدمات قابل قبول یا مثبت باشد، انتخاب خدمات درست است و این انتخاب در زمره اقدام خوب طبقه‌بندی می‌شود:

تعریف ۷: اقدام غیرمهم برای بخش نخست: تغییر آنتروپی کم یا غیرمحسوس پس از رخداد، اقدامات کاملاً طبیعی است. بر اساس میزان انحراف آنتروپی و با در نظر گرفتن آستانه‌ای برای این انحرافات، سامانه اقداماتی با تأثیر کم بر سطوح آنتروپی را به‌عنوان غیرمهم/خوش‌خیم در نظر می‌گیرد:

$$\begin{aligned} \forall x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \Rightarrow H_{Rec}^{a_i}(x) \square H_{Rec}^{a_i}(x') \end{aligned} \quad (18)$$

۲-۴-۳ - شناسایی اقدامات برای بخش دوم
برای بخش دوم، تابع انتقال حالت فقط از توصیه‌های عامل تشکیل شده است ($T(x_i) = x'_i$).

تعریف ۸: اقدام خوب برای بخش دوم: طبق رابطه (۱۹)، زمانی که توصیه‌ها به نسبت یکسان هستند، آنتروپی توصیه‌ها کاهش می‌یابد. به عبارت دیگر، توافق بین عوامل در مورد کیفیت خدمات/خدمات‌ها باعث کاهش آنتروپی می‌شود:

$$\begin{aligned} \forall x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \Rightarrow H_A(x') \leq H_A(x) \end{aligned} \quad (19)$$

تعریف ۹: اقدام بد برای بخش دوم: طبق رابطه (۲۰)، زمانی که تنوع توصیه‌های عامل‌ها مختلف در مورد یک خدمات زیاد باشد، اقدام بد تلقی می‌شود. به عبارت دیگر، اختلاف نظرهای چشم‌گیر در مورد کیفیت خدمات/خدمات‌ها بین عامل‌ها، آنتروپی توصیه‌های عامل را افزایش می‌دهد:

$$\begin{aligned} \exists x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \wedge H_A(x) \leq H_A(x') \end{aligned} \quad (20)$$

تعریف ۱۰: اقدام غیرمهم برای بخش دوم: رابطه (۲۱) وضعیتی را نشان می‌دهد که تغییرات آنتروپی ناچیز است. در این حالت اقدام غیرمهم تلقی می‌شود:

$$\begin{aligned} \forall x, x' : X \bullet a_i \text{ Recommend } Rec'_i(r_{i,j,l}, p_j, s_l) \\ \Rightarrow H_A(x) \square H_A(x') \end{aligned} \quad (21)$$

۳-۴-۳ - شناسایی اقدامات برای بخش سوم
در این بخش، تابع انتقال حالت می‌تواند درباره توصیه‌های عامل یا تجربیات کاربر باشد ($T(z_i) = z'_i$).



سایر عامل‌ها را با الگوهای تولید آنتروپی قبلی تخمین می‌زند و این تخمین‌ها را در برآوردهای کیفیت خدمات/ خدمات‌ها در نظر می‌گیرد. به‌طور ویژه، سامانه مدیریت اعتماد پیشنهادی برای محاسبه این تخمین‌ها و همچنین، حذف توصیه‌های ارائه‌شده توسط عامل‌های بدخواه استفاده می‌شود. پالایش توصیه‌ها با لحاظ کردن الگوی تغییرات آنتروپی قابل قبول و حدود آستانه‌ای در نظر گرفته‌شده انجام می‌پذیرد.

به‌عنوان بهبود دیگری برای محیط، کاربر به عامل‌های توصیه‌کننده اعلام می‌کند که آیا توصیه خاصی از آن عامل را استفاده کرده است یا خیر. در نتیجه، عامل‌ها ممکن است در توصیه‌های غیرصادقانه خود تجدیدنظر کنند. نمودار توالی^{۲۴} در شکل (۴)، سیر طبیعی رویدادهای مرتبط با انتخاب خدمات در محیط مبتنی بر سامانه را نشان می‌دهد. باید در نظر داشت که در هر مقطع زمانی، هر عامل می‌تواند ارزیابی خود را از یک خدمات خاص در مخزن خدمات^{۲۵} به‌عنوان یک توصیه ثبت کند (مرحله ۱). هر بار که کاربر می‌خواهد از یک خدمات استفاده کند، از مخزن برای توصیه‌های موجود برای آن خدمات پرس و جو می‌کند (مرحله ۲)، و در ادامه مجموعه نظرات راجع به آن خدمات را دریافت می‌کند (مراحل ۲.۱). سپس، کاربر سامانه محاسبه اعتماد را فراخوانی می‌کند تا کیفیت خدمات‌ها را بر اساس توصیه‌های دریافتی تخمین بزند (مرحله ۳). امکان تشخیص رفتار عامل‌ها بر اساس نظرات در این مرحله فراهم می‌شود و واحد تشخیص اقدامات بر اساس تغییرات آنتروپی این امکان را فراهم می‌کند (مرحله ۴). تخمین حاصل تعیین می‌کند آیا از این خدمات استفاده شود یا خیر. بنابراین، درخواست برای تحویل خدمات به انبار داده خدمات و سپس به فراهم‌کننده خدمات ارسال شده (مرحله ۵) و تحویل کاربر داده می‌شود (مرحله ۵.۱). پس از استفاده از هر خدمات، کاربر یک بازخورد و تصدیق تجربه خود از خدمات را ثبت می‌کند. سپس، هر عاملی که در مورد خدمات استفاده‌شده توصیه‌ای داده‌است، اعلانی دریافت می‌کند که چگونه توصیه‌اش در تصمیم کاربر نقش داشته‌است.

$$\forall y, y' : X \bullet u \text{ Experience Sat}'_u(c_{j,l}, p, s) \\ \Rightarrow H_{Sat}(y') \leq H_{Sat}(y) \quad (25)$$

تعریف ۱۵: اقدام بد برای بخش چهارم: اگر تجربه کاربر از استفاده خدمات غیرقابل قبول یا منفی باشد، انتخاب خدمات اشتباه است و به‌عنوان یک اقدام بد شناخته می‌شود، و داریم:

$$\exists y, y' : X \bullet u \text{ Experience Sat}'_u(c_{j,l}, p, s) \\ \wedge H_{Sat}(y) \leq H_{Sat}(y') \quad (26)$$

تعریف ۱۶: اقدام غیرمهم برای بخش چهارم: اگر تجربه کاربر از استفاده خدمات به‌طور کامل مثبت یا منفی نباشد، انتخاب خدمات یک اقدام غیرمهم است و غیرمهم/خوش‌خیم شناخته می‌شود:

$$\forall y, y' : X \bullet u \text{ Experience Sat}'_u(c_{j,l}, p, s) \\ \Rightarrow H_{Sat}(y) \square H_{Sat}(y') \quad (27)$$

برای تصمیم‌گیری در مورد انتخاب خدمات/خدمات‌ها، توصیه‌های ارائه‌شده و اعتبار توصیه‌کنندگان نیز در نظر گرفته می‌شود. فیلتر کردن اقدامات بد و دادن بازخورد منفی به توصیه‌کنندگان (عامل‌ها)، عملکرد سامانه مدیریت اعتماد را بهبود می‌بخشد.

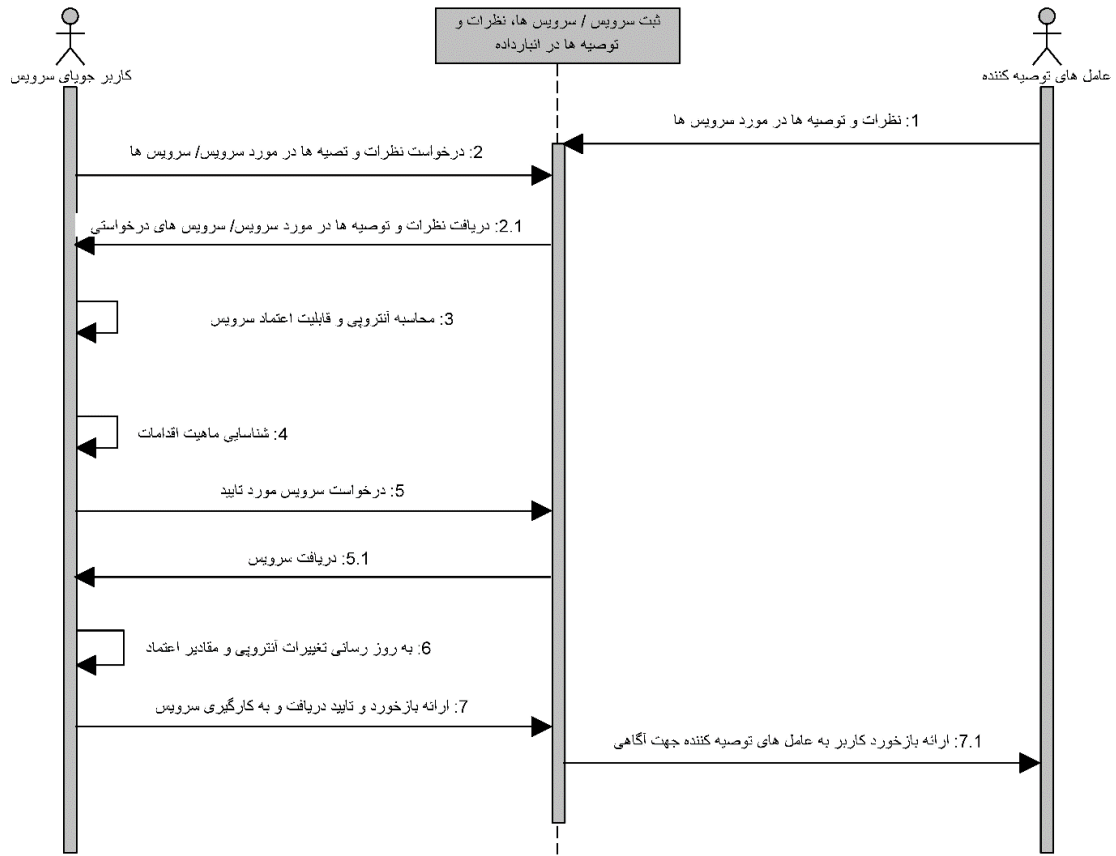
۵-۴-۳- بحث و خلاصه

سامانه مدیریت و ارزیابی اعتماد پیشنهادی در این مقاله ریشه در اندیشه‌هایی از نظریه اخلاق اطلاعاتی دارد [۴۵]، [۴۶] که در آن اقدامات افزایش‌دهنده افزایش آنتروپی در یک محیط اطلاعاتی به‌عنوان اقدامات بد یا بدخواهانه تلقی می‌شوند. بنابراین، میزان آنتروپی ایجادشده به‌وسیله یک اقدام را می‌توان به‌عنوان معیاری برای غیراخلاقی بودن آن در نظر گرفت. رفتارهای فریبنده عامل‌ها در یک محیط مبتنی بر سامانه به‌طور معمول مخرب در نظر گرفته می‌شوند و باید شناسایی و حذف شوند. این، انگیزه اصلی برای توسعه یک سامانه اعتماد مبتنی بر محاسبات آنتروپی است.

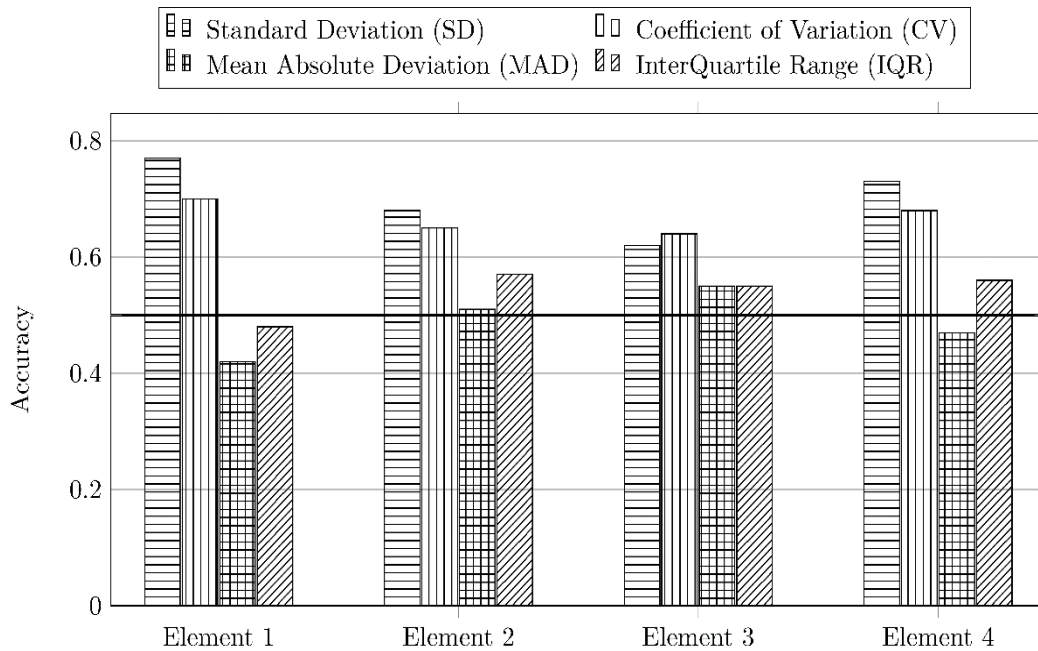
الگوی پیشنهادی تلاش می‌کند اقدامات مخرب عامل‌ها را از طریق الگوی تغییرات آنتروپی مرتبط با رفتار آنها شناسایی کند. به‌منظور افزایش دقت در محاسبات آنتروپی، الگوی تغییرات آنتروپی به چهار دسته مجزا تقسیم و از محاسبات خاص برای هر دسته استفاده شد. پس از هر تصمیم انتخاب خدمات، کاربر قابلیت اعتماد

²⁴ Sequence Diagram

²⁵ Service Repository



(شکل-۴). نمودار توالی برای ESTAR
(Figure-4).ESTAR sequence diagram



(شکل-۵). مقایسه میانگین دقت ESTAR بر اساس معیارهای پراکندگی مختلف
(Figure-5).Comparison of the average accuracy of ESTAR based on dispersion measures

ESTAR برای تعیین وضعیت اخلاقی اقدامات به حد آستانه انحراف آنتروپی نیاز دارد. برای تعیین حد آستانه، چهار معیار پراکندگی را در نظر گرفته‌ایم: انحراف معیار^{۲۶}، ضریب تغییرات^{۲۷}، میانگین انحراف مطلق^{۲۸} و محدوده^{۲۹} بین چارکی^{۲۹}. با در نظر گرفتن مقادیر دقت متناظر برای اندازه‌های مختلف محیط، معیار انحراف استاندارد برای تعیین آستانه انحراف آنتروپی انتخاب می‌شود. شکل (۵) میانگین دقت به دست آمده به وسیله هر اندازه‌گیری را برای چهار اندازه مختلف محیط در ده تکرار مقایسه می‌کند.

۴- ارزیابی

به منظور ارزیابی عملکرد ESTAR، تعدادی آزمایش را در یک محیط مبتنی بر سامانه شبیه‌سازی شده انجام داده‌ایم. در این قسمت به توضیح دقیق این آزمایش‌ها می‌پردازیم.

۴-۱- تنظیمات شبیه‌سازی

محیط، متشکل از مجموعه‌ای از خدمات‌ها، فراهم‌کنندگان خدمات، عامل‌های توصیه‌کننده و یک کاربر جوئی خدمات است. در شروع هر تکرار شبیه‌سازی، هر فراهم‌کننده خدمات تعدادی خدمات با انواع و کیفیت‌های مختلف تولید می‌کند و آنها را در مخزن داده خدمات‌ها و نظرات^{۳۰} ثبت می‌کند. سپس، برخی از عامل‌های مصرف‌کننده خدمات‌ها، از جمله کاربر جوئی خدمات، خدمات/خدمات‌ها را مصرف کرده و توصیه‌های خود را در مورد آنها در همان مخزن ثبت می‌کند. عامل‌ها با یک نسبت صداقت که رفتار توصیه آنها را شکل می‌دهد، مقداردهی اولیه می‌شوند. انتظار می‌رود عامل‌ها با نسبت صداقت کمتر تمایل به انجام اقدامات فریبکارانه و بدخواهانه بیشتری داشته‌باشند، یا به عبارت دیگر، آنتروپی بیشتری ایجاد کنند.

کاربر جوئی خدمات به یک واحد پردازش‌گر اعتماد^{۳۱} مجهز شده است که محاسبات آنتروپی ESTAR را اجرا می‌کند. هر بار که کاربر نیاز به کشف و به‌کارگیری یک خدمات دارد، پردازش‌گر اعتماد مخزن را برای تمام داده‌های موردنیاز برای محاسبات آنتروپی در سامانه جستجو می‌کند که مجموعه‌ای از همه توصیه‌های بیان‌شده به‌وسیله سایر عامل‌ها در مورد آن خدمات ویژه

است. سپس، آنتروپی را در محیط مرتبط با خدمات مشخص‌شده محاسبه می‌کند و از نتایج این محاسبات برای تصمیم‌گیری در مورد مصرف خدمات استفاده می‌کند. کاربر با حذف تأثیر توصیه‌های ارائه‌شده در مورد کیفیت خدمات‌ها توسط عامل‌های غیرمنصف یا بدخواه، دقت انتخاب و برآورد خود را بهبود می‌بخشد.

آزمایش‌های شبیه‌سازی بر روی سخت‌افزاری با ۱۲ گیگابایت حافظه و پردازنده دوهسته‌ای Intel i7-2640M که با فرکانس ۲.۸۰ گیگاهرتز تحت سیستم عامل ویندوز ۱۰ اجرا می‌شود، انجام شد. عوامل و معیارهای هر آزمایش با مجموعه ویژه‌ای از عوامل و معیارهای محیطی، مانند تعداد خدمات‌ها، فراهم‌کنندگان خدمات و عامل‌های توصیه‌کننده، و همچنین، مقدار متوسط صداقت عامل‌ها بین ۰ و ۱ تعریف می‌شود. مقدار صداقت ۰ به این معنی است که عامل همیشه یک توصیه بدخواهانه ارائه می‌دهد و مقدار ۱ بر عکس آن دلالت دارد. مقادیر صداقت به‌طور یک‌نواخت بین عامل‌ها توزیع می‌شود.

۴-۲- معیارهای عملکرد

چهار معیار اصلی برای نشان‌دادن عملکرد سامانه استفاده می‌شود:

- I. دقت^{۳۲} توصیه خدمات، که نسبت تعداد خدمات توصیه‌شده به همه پیشنهادهاست.
 - II. مقابله با تغییرات محیطی و انحرافات رفتاری، یعنی زمانی که تعداد عامل‌ها یا فراهم‌کنندگان خدمات در طول زمان تغییر می‌کند یا یک عامل غیرمنصف رفتار بدخواهانه خود را در میان توصیه‌های صادقانه تصادفی پنهان می‌کند.
 - III. سرعت الگو در تشخیص اقدامات، که تعداد تکرارهایی است که در آن خطای تشخیص الگو کمتر از یک حد آستانه ویژه قرار می‌گیرد که در این مقاله آن را روی ۰.۳ قرار داده‌ایم.
- هر قطعه در نمودارها نشان‌دهنده مقدار متوسط شناسایی‌شده از ده اجرای شبیه‌سازی مجزا برای تنظیمات مشخص‌شده است. هر اجرای شبیه‌سازی با مرحله‌ای از توصیه‌های خدمات به‌وسیله عامل‌های توصیه‌گر آغاز می‌شود که شامل صد بار تکرار مصرف خدمات توسط کاربر و ارائه توصیه به‌وسیله عامل‌های توصیه‌کننده است. خلاصه‌ای از آزمایش‌های انجام‌شده در تعدادی نمودار نشان داده شده است. به‌عنوان پایه مقایسه، ما از دو الگوی محبوب استفاده می‌کنیم:

³² Accuracy

²⁶ Standard Deviation

²⁷ Coefficient of Variation

²⁸ Mean Absolute Deviation

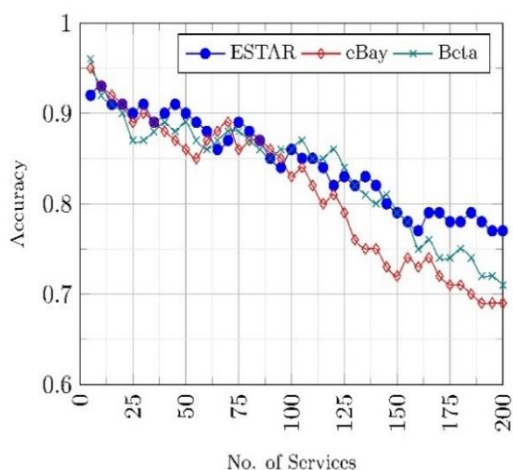
²⁹ Interquartile Range

³⁰ Service and Recommendation Repository

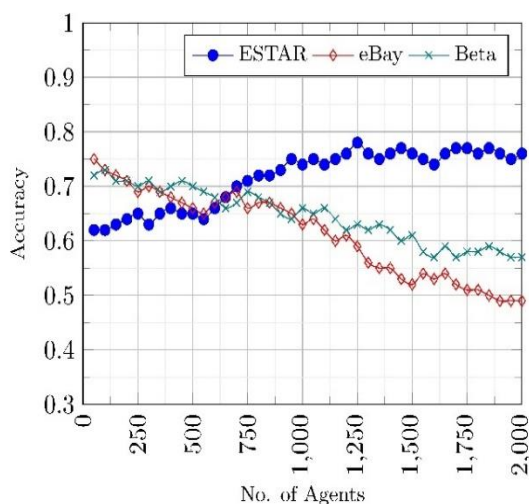
³¹ Trust Processor Module

در نظر گرفتن محاسبات آنتروپی می‌دهد، درحالی که تعداد خدمات‌های بیشتر مستلزم توصیه‌های کمتر در هر خدمات و در نتیجه، اطلاعات کمتری برای تخمین مقادیر آنتروپی است. با این حال، آزمایش‌های اندازه محیط را به صورت ادغام شده برای تعدادی عامل و خدمات انجام می‌دهیم.

نمودار شکل (۶)، مقایسه‌ای از دقت ESTAR با دقت eBay و Beta برای تعداد خدمات‌ها مختلف را نشان می‌دهد. همان‌طور که در نمودار مشاهده می‌شود، میزان کاهش دقت ESTAR کمی بهتر از دو روش دیگر است و در نهایت سریع‌تر همگرا می‌شود.



(شکل-۶). نمودار تغییرات دقت با توجه به تغییرات تعداد خدمات‌ها (Figure-6). The diagram of changes in accuracy according to changes in the number of services



(شکل-۷). نمودار تغییرات دقت با توجه به تغییرات تعداد عامل‌ها

(Figure-7). The diagram of changes in accuracy according to changes in the number of agents

سامانه مدیریت اعتماد eBay³³ eBay یک پایگاه خرید و فروش برخط است که بیشتر به خاطر حراج‌ها و خرید و فروش مصرف‌کننده به مصرف‌کننده شناخته شده است. همچنین، برای بازرگانان برخط استفاده از آن به عنوان کانال فروش بسیار محبوب است. سامانه مدیریت اعتماد eBay در بسیاری از پژوهش‌های مورد مطالعه قرار گرفته است [۱۴]-[۱۷]، [۴۷]. سامانه مدیریت اعتماد eBay امتیازات اعتماد را بر اساس نرخ بازخورد کاربر محاسبه می‌کند. در واقع پس از یک تعامل، خریدار (مشتری) امتیاز مثبت، منفی یا صفر را برای فروشنده (ارائه‌دهنده خدمات) اعمال می‌کند. نرخ که در سامانه مدیریت اعتماد eBay ذخیره می‌شود، برای محاسبه امتیازات اعتماد آینده فراهم‌کنندگان خدمات از طریق مجموع همه نرخ‌های اختصاص داده شده به آن استفاده می‌شود. در سامانه مدیریت اعتماد eBay، نرخ‌های اختصاص داده شده $Q = \{-1, 0, 1\}$ است.

سامانه مدیریت اعتماد بتا³⁴: الگوی بتا یکی دیگر از سامانه‌های مدیریت اعتماد معروف است که موضوع بسیاری از مطالعات [۱۴]، [۱۸]، [۱۹] بوده است. برای تخمین امتیازات اعتماد، این الگو از تابع چگالی احتمال بتا و نرخ‌های پیشتر اختصاص داده شده استفاده می‌کند. تابع چگالی بتا توزیع احتمال رویدادهای دودویی را پیش-بینی می‌کند. در واقع، در سامانه مدیریت اعتماد بتا، اگر r و s به ترتیب تعداد تعاملات رضایت‌بخش و نامطلوب انجام شده به وسیله یک عامل باشد، امتیاز اعتماد به صورت $(r+1)/(s+r+2)$ محاسبه می‌شود. علاوه بر این رابطه، الگوی بتا از یک عامل فراموشی λ برای به کمینه رساندن تأثیر بازخوردهای قدیمی به دلیل ناهنجاری راه‌اندازی استفاده می‌کند.

۳-۴- نتایج

دقت، بصری‌ترین معیار عملکرد است و به طور صرف نسبتی از مشاهدات پیش‌بینی شده درست به کل مشاهدات است. عملکرد ESTAR برای تغییرات در اندازه محیط و تغییرات در میانگین صداقت عامل‌ها محاسبه می‌شود. در ارزیابی عملکرد الگو برای اندازه محیط، متوجه شدیم که تغییرات نسبی رفتار سامانه برای تعداد عامل‌ها با تعداد خدمات متفاوت است؛ زیرا عامل‌های بیشتر، توصیه‌های بیشتری را در مورد خدمات‌ها ایجاد می‌کنند که اطلاعات بیشتری را برای سامانه اعتماد جهت

³³ eBay TMS

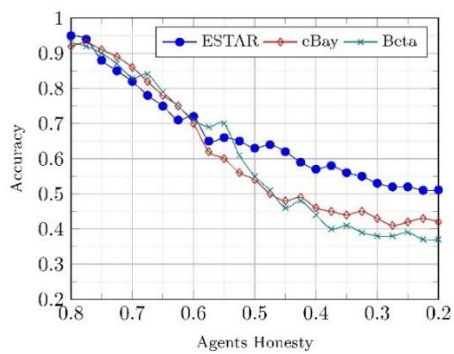
³⁴ Beta TMS



نمودار شکل (۹)، اثر نخستین عنصر آنتروپی را بر میانگین تعداد اقدامات خوب، بد و غیرمهم در طول زمان نشان می‌دهد. برای تولید مقادیر در این نمودار، وزن سه عنصر دیگر را در مقدار کل آنتروپی صفر قرار داده‌ایم. همان‌طور که در نمودار نشان داده شده‌است، این عنصر آنتروپی می‌تواند رفتار کلی عامل‌ها را در طول زمان کمی بهبود بخشد.

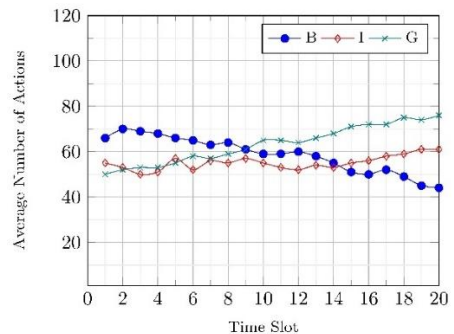
همان‌طور که در شکل (۱۰) نشان داده شده‌است، عنصر دوم آنتروپی تعداد یکسانی از اقدامات را برای هر دسته در تکرارهای اولیه تشخیص می‌دهد و توصیه‌های بد را بسیار شبیه عنصر اول کاهش می‌دهد و اقدامات خوب و غیرمهم را با شیب جزئی بهبود می‌بخشد.

شکل (۱۱) تعداد یکسانی از اقدامات را برای هر دسته شناسایی می‌کند و در طول زمان کمی آنها را بهبود می‌بخشد. به همین ترتیب، شکل (۱۲) نشان می‌دهد که عنصر آنتروپی چهارم به‌طور کلی اقدامات بی‌اهمیت‌تر را تشخیص می‌دهد و هر سه دسته از اقدامات را در طول زمان بهبود می‌بخشد.



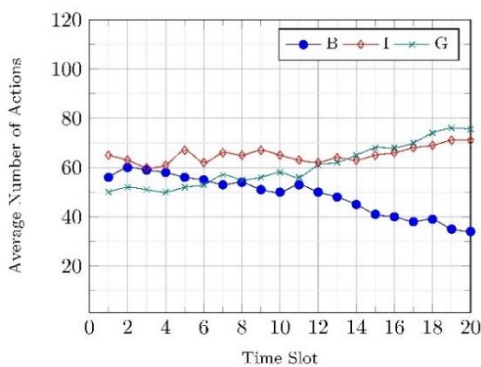
(شکل-۸). نمودار تغییرات دقت باتوجه‌به تغییر میزان صداقت عامل‌ها

(Figure-8). The diagram of changes in accuracy, according to changes in the agents honesty



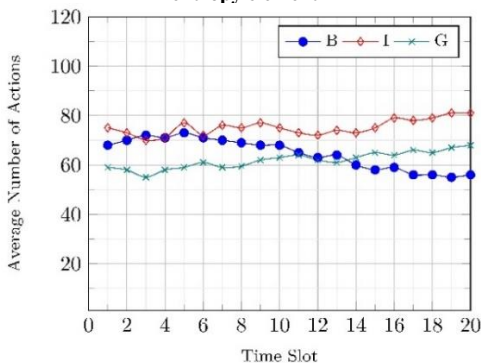
(شکل-۹). روند تغییرات در تعداد متوسط اعمال بد (B)، ناچیز (I) و خوب (G) برای اولین عنصر آنتروپی

(Figure-9). Trend of changes in the average number of bad (B), insignificant (I) and good (G) actions for the first entropy element



(شکل-۱۰). روند تغییرات در تعداد متوسط اعمال بد (B)، ناچیز (I) و خوب (G) برای دومین عنصر آنتروپی

(Figure-10). Trend of changes in the average number of bad (B), insignificant (I) and good (G) actions for the second entropy element



(شکل-۱۱). روند تغییرات در تعداد متوسط اعمال بد (B)، ناچیز (I) و خوب (G) برای سومین عنصر آنتروپی

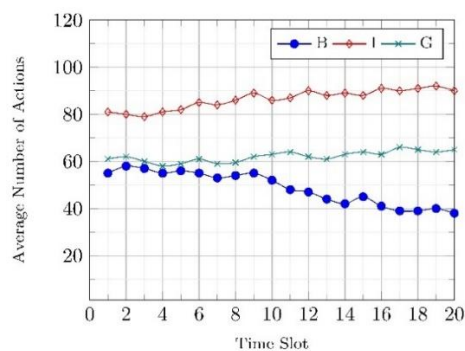
(Figure-11). Trend of changes in the average number of bad (B), insignificant (I) and good (G) actions for the third entropy element

نمودار شکل (۷)، دقت ESTAR را برای تعداد عامل‌های مختلف با eBay و Beta مقایسه می‌کند. همان‌طور که در شکل نشان داده شده‌است، دقت الگو حدود ده درصد بهبود می‌یابد درحالی‌که دقت دو الگوی دیگر برای عامل‌های بیشتر در محیط کاهش می‌یابد.

شکل (۸)، دقت سه سامانه مدیریت اعتماد را برای مقادیر مختلف صداقت عامل‌ها بین ۰.۲ و ۰.۸ مقایسه می‌کند. همان‌طور که در شکل نشان داده شده‌است، دقت هر سه سامانه برای مقادیر صادق کمتر بدتر می‌شود، با این حال، دقت ESTAR با شیب معقول‌تر کاهش می‌یابد. به عبارت دیگر، سازگاری ESTAR بیشتر از دو سامانه دیگر است.

ما همچنین، میانگین تعداد اقدامات خوب، بد و غیرمهم عامل‌ها را در طول زمان شبیه‌سازی اندازه‌گیری کرده‌ایم. همان‌طور که در بخش ۳-۴-۵ فرض شده‌است، انتخاب خدمات/خدمات‌ها و ایجاد تأیید توسط کاربر انجام می‌شود، عامل‌ها باید رفتار خود را اصلاح کنند و توصیه‌های صادقانه‌تری ارائه کنند. این آزمایش‌ها بیش از بیست تکرار برای محیطی از دویست خدمات و دوهزار عامل انجام شده‌است.

- [1] Z. Su *et al.*, "Reliable and resilient trust management in distributed service provision networks," *dl.acm.org*, vol. 9, no. 3, Jun. 2015, doi: 10.1145/2754934.
- [2] D. Chen, F. Lai, and Z. Lin, "A trust model for online peer-to-peer lending: a lender's perspective," *Information Technology and Management*, vol. 15, no. 4, pp. 239–254, Dec. 2014, doi: 10.1007/S10799-014-0187-Z.
- [3] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems*, vol. 74, pp. 302–312, Sep. 2017, doi: 10.1016/J.FUTURE.2016.01.009.
- [4] B. Lahno, "Trust. The Tacit Demand," *Ethical Theory and Moral Practice*, vol. 2, no. 4. Springer, pp. 433–435, 1999.
- [5] M. Ryan, "In AI We Trust: Ethics, Artificial Intelligence, and Reliability," *Sci Eng Ethics*, vol. 26, no. 5, pp. 2749–2767, Oct. 2020, doi: 10.1007/S11948-020-00228-Y/TABLES/1.
- [6] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Computing Surveys (CSUR)*, vol. 48, 2015.
- [7] D. M. Messick and R. M. Kramer, "Trust as a form of shallow morality.," 2001.
- [8] Y. Yamamoto, "A morality based on trust: Some reflections on Japanese morality," *Philos East West*, vol. 40, no. 4, pp. 451–469, 1990.
- [9] L. Floridi, "Information ethics, its nature and scope," *ACM SIGCAS Computers and Society*, vol. 36, no. 3, 2006.
- [10] L. Floridi, *The ethics of information*. 2013. Accessed: Jun. 21, 2022. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=_XHcAAAAQBAJ&oi=fnd&pg=PP1&dq=The+ethics+of+information&ots=fZkH8VOxSZ&sig=QhCILoi1OTYVgBnRvifDNM5lwhY
- [11] L. Floridi and J. W. Sanders, "Entropy as evil in information ethics," *Etica & Politica, Special Issue on Computer Ethics*, vol. 1, no. 2, 1999.
- [12] D. De Siqueira Braga, M. Niemann, B. Hellingrath, and F. B. De Lima Neto, "Survey on computational trust and reputation models," *ACM Comput Surv*, vol. 51, no. 5, Aug. 2018, doi: 10.1145/3236008.
- [13] J. Wang *et al.*, "A survey on trust evaluation based on machine learning," *dl.acm.org*, vol. 53, no. 5, Sep. 2020, doi: 10.1145/3408292.
- [14] A. J. Bidgoly and B. T. Ladani, "Modeling and quantitative verification of trust systems against malicious attackers," *Comput J*, vol. 59, no. 7, pp. 1005–1027, 2016.
- [15] F. Dini and G. Spagnolo, "Buying reputation on eBay: Do recent changes help?," *International Journal of Electronic Business*, vol. 7, no. 6, pp. 581–598, 2009.
- [16] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in *Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009)*, Saint Malo, France, 2009, vol. 5, no. 9.



(شکل-۱۲). روند تغییرات در تعداد متوسط اعمال بد (B)،

ناچیز (I) و خوب (G) برای چهارمین عنصر آنتروپی

(Figure-12). Trend of changes in the average number of bad (B), insignificant (I) and good (G) actions for the fourth entropy element

۵- بحث و نتیجه‌گیری

در این مقاله، سامانه مدیریت اعتمادی به نام ESTAR را برای تشخیص رفتارهای مخرب در محیط‌های مبتنی بر سامانه بر اساس مفهوم تغییرات آنتروپی از نظریه اخلاق اطلاعاتی پیشنهاد کردیم. سامانه پیشنهادی ترکیبی از چهار عنصر آنتروپی متمایز در یک محیط، مبتنی بر سامانه قابل تعریف است. سپس، بر اساس الگوی تغییرات آنتروپی تعریف شده برای هر بخش، اقدامات انجام شده توسط عامل‌ها را از نظر اخلاقی به سه دسته خوب، بد و غیرمهم تقسیم کردیم.

شبیه‌سازی‌های تجربی برای محیط‌های مبتنی بر سامانه با اندازه‌ها و ویژگی‌های مختلف نشان می‌دهد که ESTAR از نظر تخمین قابل اعتماد بودن عامل‌ها و توصیه‌ها در محیط و همچنین، برآورد کیفیت خدمات/ خدمات‌های ناشناخته بر اساس توصیه‌های عامل‌ها، کارآمد است. علاوه بر این، ESTAR بسیار منعطف بوده و می‌تواند به سرعت با تغییرات محیطی سازگار شود.

استفاده طولانی‌مدت از سامانه مدیریت اعتماد در یک محیط مبتنی بر سامانه به تدریج رفتار اخلاقی عامل‌های هوشمند را در محیط بهبود می‌بخشد. این امر در اساس، با بیشتر سامانه‌های رایجی که تمایل به حذف عامل‌های تخریب‌کننده از محیط دارند، متفاوت است.

امکان تعریف بخش‌ها و عناصر دیگری از آنتروپی در محیط و روش‌های متفاوتی برای ترکیب مقادیر آنتروپی‌ها ممکن است منجر به محاسبات اعتماد به نسبت متفاوتی شود. آزمایش چنین جزئیات مختلف گامی در آینده جهت توسعه سامانه مدیریت اعتماد پیشنهادی است.

- WSNs,” *IEEE Access*, vol. 6, pp. 4725–4741, 2017.
- [31] K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, pp. 1–31, 2009.
- [32] S. Vavilis, M. Petković, and N. Zannone, “A reference model for reputation systems,” *Decis Support Syst*, vol. 61, pp. 147–154, 2014.
- [33] F. G. Mármol and G. M. Pérez, “Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems,” *Comput Stand Interfaces*, vol. 32, no. 4, pp. 185–196, 2010.
- [34] Z. Noorian and M. Ulieru, “The state of the art in trust and reputation systems: a framework for comparison,” *Journal of theoretical and applied electronic commerce research*, vol. 5, no. 2, pp. 97–117, 2010.
- [35] D. D. S. Braga, M. Niemann, B. Hellingrath, and F. B. D. L. Neto, “Survey on computational trust and reputation models,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 2018.
- [36] S. Chen, Y. Zhang, P. Liu, and J. Feng, “Coping with traitor attacks in reputation models for wireless sensor networks,” in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1–6.
- [37] L. F. Perrone and S. C. Nelson, “A study of on-off attack models for wireless ad hoc networks,” in *2006 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks*, 2006, pp. 1–10.
- [38] D. Wang, T. Muller, J. Zhang, and Y. Liu, “Quantifying robustness of trust systems against collusive unfair rating attacks using information theory,” in *24th International Joint Conference on Artificial Intelligence*, 2015.
- [39] D. Wang, T. Muller, A. A. Irissappane, J. Zhang, and Y. Liu, “Using Information Theory to Improve the Robustness of Trust Systems,” in *AAMAS*, 2015, pp. 791–799.
- [40] J.-H. Cho, A. Swami, and R. Chen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1001–1012, 2012.
- [41] A. Aldini, “Formal approach to design and automatic verification of cooperation-based networks,” *IARIA Int J Adv Internet Technol*, vol. 6, no. 1, p. 2, 2013.
- [42] T. Muller, “Semantics of trust,” in *International Workshop on Formal Aspects in Security and Trust*, 2010.
- [43] A. Herbon, and D. Tsadikovich. “An efficient entropy-based stopping rule for mitigating risk factors in supply nets.” *International Journal of Production Economics*, 2023.
- [44] A. Khoshkbarchi and H. R. Shahriari, “Improving Agents Trust in Service-Oriented Environment Based on Entropy Structure and Information Ethics Principles,” *Int J Hum Comput Interact*, 2022.
- [17] R. Kerr and R. Cohen, “Smart cheaters do prosper: defeating trust and reputation systems,” in *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, 2009, pp. 993–1000.
- [18] K. Arshad and K. Moessner, “Robust collaborative spectrum sensing based on beta reputation system,” in *2011 Future Network & Mobile Summit*, 2011, pp. 1–8.
- [19] M. Momani, K. Aboura, and S. Challa, “RBATMWSN: recursive Bayesian approach to trust management in wireless sensor networks,” in *2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information*, 2007, pp. 347–352.
- [20] P. Shi and H. Chen, “RASN: Resist on-off attack for wireless sensor networks,” in *Proceedings of the 2012 international conference on computer application and system modeling*, 2012, pp. 690–693.
- [21] D. Wang, T. Muller, Y. Liu, and J. Zhang, “Towards robust and effective trust management for security: A survey,” in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014.
- [22] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, “A survey on trust and reputation models for Web services: Single, composite, and communities,” *Decis Support Syst*, vol. 74, pp. 121–134, 2015.
- [23] N. Kandhoul, S. K. Dhurandher, and I. Woungang, “T_CAFE: a trust based security approach for opportunistic IoT,” *IET Communications*, vol. 13, no. 20, 2019.
- [24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer networks*, vol. 76, pp. 146–164, 2015.
- [25] X. Wang, L. Liu, and J. Su, “RLM: A general model for trust representation and aggregation,” *IEEE Trans Serv Comput*, vol. 5, no. 1, pp. 131–143, 2010.
- [26] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, “MARINE: Man-in-the-middle attack resistant trust model in connected vehicles,” *IEEE Internet Things J*, vol. 7, no. 4, pp. 3310–3322, 2020.
- [27] A. Vasudeva and M. Sood, “Survey on sybil attack defense mechanisms in wireless ad hoc networks,” *Journal of Network and Computer Applications*, vol. 120, pp. 78–118, 2018.
- [28] Y. Ruan and A. Durresi, “A survey of trust management systems for online social communities—trust modeling, trust inference and attacks,” *Knowl Based Syst*, vol. 106, 2016.
- [29] B. Khosravifar, J. Bentahar, M. Gomrokchi, and R. Alam, “CRM: An efficient trust and reputation model for agent computing,” *Knowl Based Syst*, vol. 30, pp. 1–16, 2012.
- [30] B. Sun and D. Li, “A comprehensive trust-aware routing protocol with multi-attributes for

- [45] L. Floridi, *The ethics of information*. 2013. Accessed: Jun. 15, 2022.
- [46] Floridi, L., & Sanders, J. W. (1999). "Entropy as evil" - Google Scholar.
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Floridi%2C+L.%2C+%26+Sanders%2C+J.+W.+%281999%29.+Entropy+as+evil+in+information+ethics.+Etica+%26+Politica%2C+Special+Issue+on+Computer+Ethics%2C+1%282%29.&btnG= (accessed Jun. 15, 2022).
- [47] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," in *The Economics of the Internet and E-commerce*, Emerald Group Publishing Limited, 2002.
- [48] K. RahimiZadeh, and P. Kabiri. "Trust-based routing method using a mobility-based clustering approach in mobile ad hoc networks." *Security and Communication Networks* 7, no. 11, 2014.
- [49] A. Khoshkbarchi, and H.R. Shahriari. "Coping with unfair ratings in reputation systems based on learning approach." *Enterprise Information Systems* 11, no. 10 (2017): 1481-1499.



امیر خشکبارچی در حال حاضر دانشجوی دکترای مهندسی فناوری اطلاعات دانشگاه صنعتی امیرکبیر است. علائق پژوهشی ایشان شامل سامانه‌های مدیریت اعتماد، امنیت و هوش مصنوعی است.

نشانی رایانامه ایشان عبارت است از:

a.khoshkbarchi@aut.ac.ir



حمیدرضا شهرياري استادیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی امیرکبیر است. وی دانش‌آموخته مقطع دکترای مهندسی کامپیوتر از دانشگاه صنعتی شریف است. زمینه‌های پژوهشی موردعلاقه ایشان شامل امنیت اطلاعات و شبکه، سامانه‌های مدیریت اعتماد و امنیت تجارت الکترونیک است.

نشانی رایانامه ایشان عبارت است از:

shahriari@aut.ac.ir

