فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص: ۱- ۱۴

الگوریتم رقابت استعماری آشوبی متعامد اصلاح شده و بکارگیری آن در بهبود بازشناسی الگو در شبکهٔ عصبی پرسپترون‌های چند لایه

پیمان معلم* مهرداد صادقی حریری** مهدی هاشمی***

* استاد، دانشگاه اصفهان، گروه مهندسی برق

** دانشجوی دکتری تخصصی مهندسی برق کنترل، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

*** مربی، موسسه آموزش عالی پیام گلپایگان، دانشکده مهندسی برق

تاریخ دریافت: ۱۳۹۶/۰۶/۱۹ تاریخ پذیرش:۱۳۹۶/۱۲/۲۰

چکیده

علی‌رغم موفقیت الگوریتم رقابت استعماری (ICA) در حل مسائل بهینه‌سازی، این الگوریتم کماکان از به دام افتادن مکرر در کمینه محلی و سرعت پایین همگرایی رنج می‌برد. در این مقاله، نسخهٔ جدیدی از این الگوریتم، به نام رقابت استعماری آشوبی متعامد اصلاح شده (COICA)، پیشنهاد می‌شود. در سیاست جذب نسخه پیشنهادی، هرمستعمره از طریق تعریف بردار متعامد نوینی، فضای حرکت به سمت استعمارگر را جستجو می‌کند. همچنین احتمال انتخاب امپراطوری‌های قدرتمند، از طریق تابع توزیع بولتزمان تعریف شده و عمل انتخاب از طریق روش چرخ رولت انجام گرفته است. از الگوریتم پیشنهادی برای آموزش شبکه عصبی پرسپترون چند لایه[1] (MLP) جهت طبقه‌بندی مجموعه داده‌های استاندارد، از جمله یونسفر و سونار استفاده شده است. برای ارزیابی عملکرد این الگوریتم و بررسی میزان تعمیم‌پذیری شبکه عصبی آموزش دیده با نسخه پیشنهادی، از روش اعتبارسنجی متقابل K-Fold استفاده شده است. نتایج بدست آمده از شبیه‌سازی‌ها، کاهش خطای آموزش شبکه و همچنین بهبود تعمیم‌پذیری الگوریتم پیشنهادی را تایید می‌کند.

واژه‌های کلیدی: الگوریتم رقابت استعماری آشوبی متعامد، شبکه عصبی پرسپترون چند لایه، طبقه‌بندی داده

۱- مقدمه

روش‌های اکتشافی و فرا اکتشافی در حل مسائل بهینه‌سازی در علوم مختلف به کار می‌روند. این روش‌ها سعی در کشف یک راه حل بدون داشتن درک عمیقی از ساختار مساله دارند. به عبارت دیگر، مساله برای الگوریتم به عنوان یک جعبه سیاه به نظر می‌رسد. این روش‌ها معمولا بصورت تصادفی با استفاده از آمار بدست آمده از نمونه‌هایی از فضای جستجو عمل می‌کنند و یا بر اساس مدلی از برخی پدیده‌های

نویسنده عهده‌دار مکاتبات: پیمان معلم p_moallem@eng.ui.ac.ir

[1] Multilayer Perceptron

طبیعی یا فرآیندهای فیزیکی هستند. این الگوریتم‌ها شامل الگوریتم ژنتیک[۲] (GA) [۱]، شبیه‌سازی تبرید[۳] (SA) [۲]، [۲]، بهینه‌سازی ازدحام ذرات[۴] (PSO) [۳]، بهینه‌سازی جمعیت مورچگان[۵] (ACO) [۴]، الگوریتم تکاملی فرهنگی[۶] (CE) [۵]، تکامل تفاضلی[۷] (DE) [۶]، جستجوی هارمونی[۸] (HS) [۷]، الگوریتم جستجوی گرانشی[۹] (GSA) [۸]، الگوریتم تپه‌نوردی[۱۰] [۹]، الگوریتم سیستم جستجوی ذرات باردار[۱۱] (CSS) [۱۰] و غیره می‌باشد.

الگوریتم رقابت استعماری[۱۲] (ICA) [۱۱] از روش‌های فرااکتشافی بهینه‌سازی است که مبتنی بر پدیده‌های انسانی- اجتماعی عمل کرده و نشان داده شده که در مقایسه با الگوریتم‌های مبتنی بر تکامل پدیده‌های طبیعی، به سرعت بالاتری از همگرایی با متغیرهای مستقل زیاد دست یافته است [۱۲].

الگوریتم رقابت استعماری، یک الگوریتم چند عاملی است که هر عامل، یک کشور به عنوان مستعمره یا استعمارگر می‌باشد. این الگوریتم به فرآیند شکل گیری امپریالیسم، رشد و زوال آن، به عنوان مرحله‌ای از تکامل اجتماعی- سیاسی انسان نگاه می‌کند. کشورها تعدادی امپراطوری، در فضای جستجو را شکل می‌دهند. حرکت مستعمرات به سمت استعمارگر مربوطه و رقابت استعماری بین امپراطوری‌ها اساس و پایهٔ این الگوریتم را تشکیل می‌دهد. در طول این جابجایی‌ها، امپراطوری‌های قدرتمند تقویت یافته و امپراطوری‌های ضعیف تضعیف می‌شوند و به تدریج سقوط می‌کنند. در الگوریتم رقابت استعماری، مستعمرات با شعاع حرکتی تصادفی به سمت استعمارگر حرکت می‌کنند.

در سال‌های اخیر در راستای بهبود عملکرد الگوریتم رقابت استعماری، در حل مسائل بهینه‌سازی، تحقیقات مختلفی صورت گرفته است. کاوه و طلاطاهری [۱۳] در سال ۲۰۱۰ الگوریتم ICA را با افزودن یک بردار متعامد تصادفی بین استعمارگر و مستعمره در مرحلهٔ جذب، بهبود بخشیدند. این بردار بر راستای خط واصل مستعمره- استعمارگر عمود می‌باشد. بنابراین این الگوریتم، رقابت استعماری متعامد[۱۳] (OICA) نام گرفت. در این مقاله برای بهبود الگوریتم پایه، دو گام حرکتی تعریف شده است که عبارتند از: (۱) بکارگیری از مقادیر تصادفی مختلف برای مولفه‌های بردار پاسخ به جای استفاده از یک مقدار؛ (۲) ایجاد انحراف با استفاده از بردار متعامد بر خط واصل مستعمره- استعمارگر به جای استفاده از متغیر θ. در ادامه، در سال ۲۰۱۰ الگوریتم رقابت استعماری آشوبی[۱۴] (CICA) توسط بهرامی و همکارانش پیشنهاد شده است [۱۴] که موفق به بهبود عملکرد الگوریتم ICA شده‌اند. در این روش از نگاشت‌های آشوبی برای بروز رسانی زاویهٔ حرکتی مستعمرات به سمت موقعیت استعمارگر در راستای افزایش قابلیت گریز از دام اپتیمم محلی استفاده شده است. همچنین الگوریتم رقابت استعماری برای یادگیری شبکهٔ عصبی به کار برده شده است [۱۵].

در سال ۲۰۱۰ طی مقاله‌ای عبدچیری و همکارانش [۱۶] الگوریتم رقابت استعماری تطبیقی[۱۵] (AICA) را مطرح کردند. در این الگوریتم پیشنهادی، به منظور جستجوی موثر، سیاست جذب الگوریتم جهت بروز رسانی زاویهٔ حرکتی مستعمره به سمت موقعیت استعارگر به صورت دینامیکی تغییر یافته است. در این روش، مدلی احتمالی به کار رفته است که با بکارگیری اطلاعات موقعیت مستعمرات، اقدام به برقراری تعادل بین توانایی جستجو و بهره‌برداری

[2] Genetic Algorithm
[3] Simulated Annealing
[4] Particle Swarm Optimization
[5] Ant Colony Optimization
[6] Cultural Evolutionary Algorithm
[7] Differential Evolution
[8] Harmony Search
[9] Gravitational Search Algorithm
[10] Hill Climbing
[11] Charged System Search
[12] Imperialist Competitive Algorithm

[13] Orthogonal Imperialist Competitive Algorithm
[14] Chaotic Imperialist Competitive Algorithm
[15] Adaptive ICA

الگوریتم رقابت استعماری کرده است. در سال ۲۰۱۲ کوئلهو، آفونسو و آلوتو [۱۷]، الگوریتم جدیدی مبتنی بر الگوریتم ICA معرفی کرده‌اند. در این مقاله روش اصلاح شدهٔ ICA (MICA[۱۶]) مبتنی بر مفاهیم و اصول جاذبه و دافعه بین مستعمره و استعمارگر آن در طول جستجو برای پاسخ‌های بهتر ارائه شده است.

سلطانی سروستانی، لطفی و رمضانی در سال ۲۰۱۲ [۱۸]، الگوریتم تکاملی بهبود یافته‌ای مبتنی بر الگوریتم رقابت استعماری معرفی کرده‌اند. در الگوریتم ICA، کشورها به دو گروه استعمارگرها و مستعمرات تقسیم شده است. در حالی که در QCA[۱۷] دو نوع دیگر از کشورها که عبارتند از کشورهای مستقل و کشورهای به دنبال استقلال نیز به مجموعه کشورها افزوده شده است. در الگوریتم ICA موقعیت استعمارگرها ثابت است، در حالی که در الگوریتم QCA قادر به حرکت هستند. طلاطاهری و همکارانش در سال ۲۰۱۲ [۱۲] طی مقاله‌ای سرعت همگرایی الگوریتم ICA را با جایگزینی توابع آشوبی به جای توابع تصادفی در گام جذب الگوریتم، بهبود دادند. در این مقاله سه نسخه از الگوریتم CICA ارائه شده است، که در نهایت نسخهٔ سوم از الگوریتم‌های پیشنهادی را که می‌توان به عنوان رقابت استعماری آشوبی متعامد دانست، عملکرد بهتری نسبت به سایر الگوریتم‌ها از خود نشان داده است. در واقع این نسخه ترکیبی از روش متعامد و روش آشوبی می‌باشد. در الگوریتم پیشنهاد شده از چندین نگاشت آشوبی به کار رفته، توابع آشوبی سینوسی و منطقی نتایج بهتری نسبت به بقیه از خود نشان داده‌اند.

از مسائل کاربردی که می‌توان الگوریتم‌های بهینه‌سازی را به چالش کشید، آموزش شبکه‌های عصبی پرسپترون چند لایه است که علاوه بر نحوه رسیدن به پاسخ مطلوب، سرعت همگرایی و نرخ موفقیت اجرا، پارامتر عمومیت پذیری شبکه آموزش دیده در برخورد با داده‌های غیر آموزشی نیز به چالش کشیده می‌شود. از اینرو، بسیاری از الگوریتم‌های فرااکتشافی مدعی، عملکرد خود را در مقایسه با سایرین در محک آموزش شبکه‌های عصبی پرسپترون چند لایه قرار می‌دهند.

در بخش دوم این مقاله، ابتدا به جزییات الگوریتم رقابت استعماری پرداخته می‌شود. سپس در بخش بعد، اصلاحات پیشنهادی برای حل مشکلات این الگوریتم، مطرح شده و بلوک دیاگرام الگوریتم رقابت استعماری پیشنهادی مطرح می‌شود. بخش چهارم، به ارزیابی روش پیشنهادی در آموزش شبکه عصبی پرسپترون چند لایه برای کلاس بندی داده‌های یونسفر و سونار که از داده‌های پیچیده در کلاس بندی است، و مقایسه آن با سایر روش‌های مشابه می‌پردازد. در نهایت مقاله با ارائه نتایج در بخش پنجم به اتمام می‌رسد.

۲- الگوریتم رقابت استعماری

الگوریتم رقابت استعماری پایه، شامل ۶ مرحله است که در ادامه، تشریح می‌شود [۱۱].

۲-۱- تولید امپراطوری‌های اولیه

این الگوریتم مانند سایر الگوریتم‌های تکاملی از یک سری جمعیت اولیه تشکیل شده که کشور نامیده می‌شوند. در یک مساله N_{var} بعدی، یک کشور یک آرایه به طول $1 \times N_{\mathrm{var}}$ است. این آرایه به صورت رابطهٔ (۱) تعریف می‌شود. در واقع هر درایه نقش یک مشخصه از کشور مانند فرهنگ، زبان، ساختار اقتصادی و غیره را بازی می‌کند.

$$\mathrm{country} = [p_1, p_2, \ldots, p_{\mathrm{Nvar}}] \quad (۱)$$

هزینهٔ هر کشور از طریق ارزیابی تابع هزینهٔ f در متغیرهای $(P_1, P_2, P_3, \ldots, P_{N_{var}})$ بدست می‌آید که در رابطهٔ (۲) نشان داده شده است.

$$Cost = f(country) = f(P_1, P_2, P_3, \ldots, P_{N_{var}}) \quad (۲)$$

برای شروع الگوریتم بهینه‌سازی جمعیت اولیه به تعداد N_{pop} تولید می‌شود. به تعداد N_{imp} از قدرتمندترین کشورها به عنوان استعمارگر انتخاب می‌شوند که هر کدام یک امپراطوری را تشکیل می‌دهند. تعداد N_{col} جمعیت باقیمانده به عنوان مستعمره خواهد بود که بر حسب قدرت استعمارگرها بین امپراطوری‌ها توزیع می‌شوند. بنابراین کشورها به دو نوع مستعمره و استعمارگر تقسیم می‌شوند.

[16] Modified ICA
[17] Quad Countries Algorithm

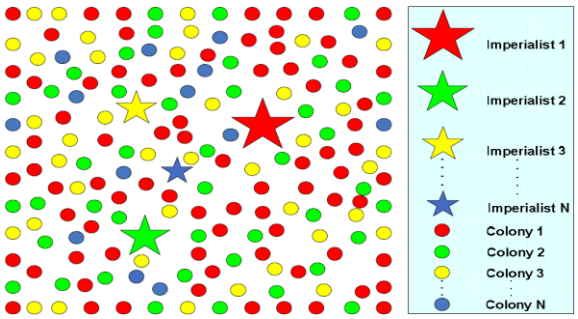
به منظور شکل‌گیری امپراطوری‌های اولیه، مستعمرات بین استعمارگرها بر اساس قدرتشان تقسیم می‌شوند. یعنی تعداد اولیهٔ مستعمرات هر امپراطوری به طور مستقیم با قدرت آن متناسب است. برای توزیع تناسبی مستعمرات در میان استعمارگرها، هزینهٔ نرمالیزه شدهٔ هر استعمارگر به صورت رابطه (۳) تعریف می‌شود:

$$C_n = c_n - \max_i\{c_i\} \quad (۳)$$

متغیر c_n هزینهٔ استعمارگر n ام و C_n هزینهٔ نرمالیزه شدهٔ آن است. با داشتن همهٔ هزینه‌های نرمالیزه شدهٔ کل استعمارگرها، قدرت نرمالیزه شدهٔ هر استعمارگر به صورت رابطه (۴) تعریف می‌شود:

$$p_n = \left| \frac{c_n}{\sum_{i=1}^{N_{imp}} c_i} \right| \quad (۴)$$

متغیر $N.C._n$ تعداد اولیهٔ مستعمرات امپراطوری nام و N_{col} تعداد کل مستعمرات را نشان می‌دهد. برای تقسیم مستعمرات، برای هر استعمارگر $N.C._n$ مستعمره به تصادف انتخاب شده و به آنها داده می‌شود. این مستعمرات به همراه استعمارگر، امپراطوری n ام را تشکیل خواهد داد. در شکل (۱) جمعیت اولیه هر امپراطوری نشان داده شده است. هر ستاره بیانگر یک استعمارگر است که ستاره‌های بزرگتر قدرت بیشتری را دارا می‌باشند. در شکل زیر Imperialist نشان دهندهٔ استعمارگر و Colony بیانگر مستعمرات است.



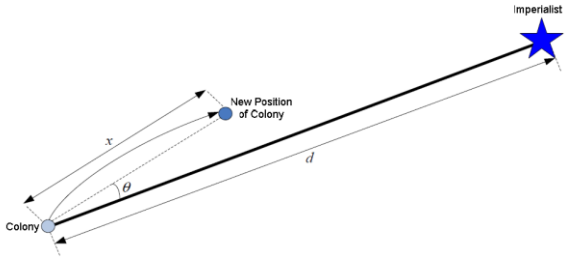
شکل ۱- تولید امپراطوری‌های اولیه؛ استعمارگر قدرتمند با ستارهٔ بزرگتر نشان داده شده است [۱۱]

۲-۲- حرکت مستعمرات یک امپراطوری به سمت استعمارگر

در این الگوریتم کشورهای استعمارگر شروع به توسعهٔ مستعمرات خود می‌کنند. این فرآیند با حرکت تمام مستعمرات به سمت استعمارگر مدل شده است. در راستای این سیاست، کشور مستعمره، به اندازه x واحد در جهت خط واصل مستعمره به استعمارگر، حرکت کرده و به موقعیت جدید، کشانده می‌شود. x عددی تصادفی با توزیع یکنواخت است (و یا هر توزیع مناسب دیگر) که طبق رابطهٔ (۵) می‌باشد. اگر فاصله میان استعمارگر و مستعمره با d نشان داده شود، معمولاً برای d داریم.

$$x \sim U(0, \beta \times d) \quad (۵)$$

که در آن β عددی بزرگتر از یک و نزدیک به ۲ می‌باشد. یک انتخاب مناسب می‌تواند $\beta = 2$ باشد. وجود ضریب $\beta \geq 1$ باعث می‌شود تا کشور مستعمره در حین حرکت به سمت کشور استعمارگر، از جهت‌های مختلف به آن نزدیک شود. همچنین در کنار این حرکت، یک انحراف زاویه‌ای کوچک نیز با توزیع یکنواخت به مسیر حرکت افزوده می‌شود. یک نمای گرافیکی از اعمال سیاست جذب در الگوریتم رقابت استعماری در صفحه دو بعدی در شکل (۲) نشان داده شده است.



شکل ۲- حرکت مستعمرات به سمت استعمارگر مربوطه با زاویه انحراف تصادفی [۱۱]

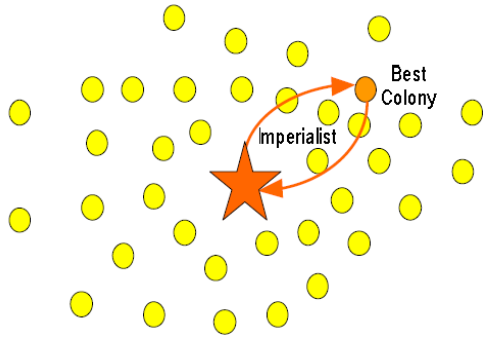
که مقدار زاویهٔ θ توسط رابطهٔ (۶) تعریف می‌شود:

$$\theta \sim U(-\gamma, \gamma) \quad (۶)$$

پارامتر γ در رابطهٔ بالا جهت تنظیم انحراف از مسیر اصلی اعمال می‌شود. در شکل بالا θ یک عدد تصادفی با توزیع یکنواخت است.

۲-۳-جابجایی موقعیت بین استعمارگر و یک مستعمره

اگر مستعمره‌ای در حین حرکت به سمت استعمارگر، مقدار هزینهٔ کمتری نسبت به استعمارگر آن امپراطوری بدست آورد، جای مستعمره و استعمارگر با یکدیگر تعویض خواهد شد. شکل (۳) این فرآیند را به تصویر کشیده است.



شکل ۳- تعویض موقعیت مستعمره‌ای با وضعیتی بهتر با استعمارگر [۱۱]

۲-۴- قدرت کل یک امپراطوری

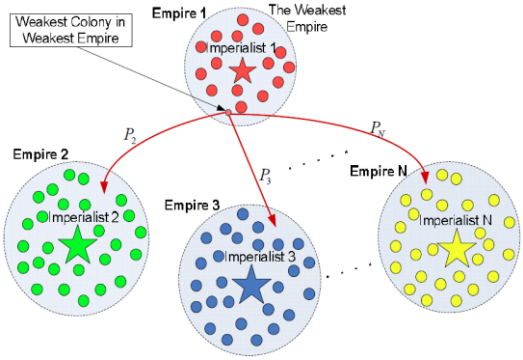
قدرت کل یک امپراطوری اساسا تحت تاثیر قدرت کشور استعمارگر است. البته قدرت مستعمرات نیز اثر خواهد گذاشت، هر چند که در مقابل قدرت کل امپراطوری قابل اغماض است. در نهایت هزینهٔ کل بصورت رابطه (۷) مدل شده است:

$$T.C._n = Cost(imperialist_n) + \xi mean\{Cost(colonies\ of\ empire_n)\} \quad (۷)$$

بطوریکه $T.C._n$ نشان‌دهنده هزینهٔ کل امپراطوری n ام و ξ عدد مثبتی است که کمتر از یک در نظر گرفته می‌شود. افزایش مقدار ξ نقش مستعمرات در تعیین قدرت کل امپراطوری را بیشتر می‌کند.

۲-۵- رقابت استعماری

همهٔ امپراطوری‌ها سعی در تصاحب مستعمرات سایر امپراطوری‌ها دارند. در این رقابت استعماری چندین امپراطوری قدرتمند برای تصاحب مستعمرات ضعیف امپراطوری ضعیف با هم رقابت می‌کنند. طی این فرآیند امپراطوری‌های قدرتمند، قوی‌تر و امپراطوری‌های ضعیف، ضعیف‌تر می‌شوند. شکل (۴) این رقابت را به تصویر می‌کشد.



شکل ۴- رقابت استعماری [۱۱]

برای شروع رقابت، احتمال مالکیت هر امپراطوری بر اساس قدرت کل آن تعیین می‌شود. هزینهٔ کل نرمالیزه شده بصورت رابطهٔ (۸) بیان می‌شود:

$$N.T.C._n = T.C._n - \max_i\{T.C._i\} \quad (۸)$$

که متغیرهای $T.C._n$ و $N.T.C._n$ به ترتیب نشان‌دهنده هزینهٔ کل و هزینهٔ کل نرمالیزه شدهٔ امپراطوری n ام است. با استفاده از هزینهٔ کل نرمالیزه شده، احتمال مالکیت هر امپراطوری از رابطهٔ (۹) بدست می‌آید:

$$P_{p_n} = \left| \frac{N.T.C._n}{\sum_{i=1}^{N_{imp}} N.T.C._i} \right| \quad (۹)$$

برای توزیع مستعمرات ذکر شده در میان استعمارگرها بر اساس احتمال هر یک، بردار P بصورت رابطهٔ (۱۰) تشکیل می‌یابد:

$$P = [p_{p_1}, p_{p_2}, p_{p_3}, \dots, p_{p_{N_{imp}}}] \quad (۱۰)$$

سپس برداری با ابعاد برابر با بردار P تولید خواهیم کرد که مولفه‌های آن اعداد تصادفی با توزیع یکنواخت باشد که در رابطه (۱۱) نشان داده شده است:

$$R = [r_1, r_2, r_3, \dots, r_{N_{imp}}]$$
$$r_1, r_2, r_3, \dots, r_{N_{imp}} \sim U(0,1) \quad (۱۱)$$

بردار D از طریق کسر بردار R از بردار P بصورت رابطه (۱۲) بدست می‌آید:

$$D = P - R = \left[D_1, D_2, D_3, \dots, D_{N_{imp}}\right] = [p_{p_1} - r_1, p_{p_2} - r_2, p_{p_3} - r_3, \dots, p_{p_{N_{imp}}} - r_{N_{imp}}] \quad (۱۲)$$

با رجوع به بردار D مستعمرات مذکور به امپراطوری‌ای که اندیس مربوطهٔ آن در بردار D بیشینه است، تحویل داده می‌شود.

۲-۶- سقوط امپراطوری‌های ضعیف

زمانی که یک امپراطوری تمام مستعمرات خود را به سایر امپراطوری‌ها واگذار کند و هیچ مستعره‌ای نداشته باشد، سقوط می‌کند که این عمل با حذف آن امپراطوری مدل می‌شود. البته در نهایت استعمارگر آن امپراطوری نیز به عنوان یک مستعمره به امپراطوری قدرتمندی ملحق می‌شود.

۳- اصلاحات پیشنهادی در الگوریتم رقابت استعماری

علی رغم تحقیقات موفقی که در زمینهٔ توسعه و بهبود الگوریتم رقابت استعماری انجام شده است، همچنان برخی از مسائل چالش برانگیز در آن وجود دارد، که از آن جمله می‌توان به (۱) افتادن در دام بهینه محلی، (۲) سرعت کم همگرایی در برخی از مسائل، (۳) پیچیدگی محاسباتی بسیار بالا برای توابعی با متغیرهای مستقل زیاد، (۴) عدم تضمین رسیدن به پاسخ مطلوب اشاره کرد که در این مقاله سه پیشنهاد برای بهبود عملکرد الگوریتم رقابت استعماری پیشنهاد شده است.

برای مقابله با چالش‌های بالا، الگوریتم رقابت استعماری آشوبی متعامد اصلاح شده پیشنهاد شده است. در این الگوریتم در دو گام بسیار حیاتی الگوریتم ICA یعنی سیاست جذب و رقابت استعماری، تغییراتی اعمال شده است. در ابتدا از یک تابع توزیع احتمال جدیدی برای امپراطوری‌ها استفاده خواهد شد. سپس از روش نمونه برداری چرخ رولت برای عملیات انتخاب استفاده کرده‌ایم. همچنین روش جدیدی جایگزین روش بردار متعامد پیشنهاد خواهیم کرد. در نهایت روش اعتبارسنجی متقابل $K-Fold$ را برای بررسی تعمیم پذیری الگوریتم پیشنهادی به کار برده‌ایم. در ادامه به تغییرات اعمال شده به تفصیل خواهیم پرداخت.

۳-۱- تعریف تابع توزیع بولتزمان

یکی از اساسی‌ترین ایراداتی که می‌توان بر الگوریتم ICA پایه گرفت، نوع نمونه‌برداری در انتخاب امپراطوری قدرتمند برای تصاحب ضعیف‌ترین مستعمره از ضعیف‌ترین امپراطوری است. اگرچه شاید روش به کار رفته یک روش کاملاً سرراست و ساده‌ای باشد، اما از نظر مفاهیم یکنواخت نیست، یعنی الزاما کسی که قوی‌ترین است انتخاب نمی‌شود و همچنین رفتار این روش شدیداً غیرخطی است.

در گام رقابت استعماری الگوریتم ICA، بایستی یکی از امپراطوری‌های قدرتمند جهت جذب مستعمرهٔ ضعیف در ضعیف‌ترین امپراطوری، انتخاب شود. بنابراین برای انجام چنین کاری، قدرت هر امپراطوری توسط تابع توزیع احتمال بولتزمان تعریف می‌شود. از رابطهٔ (۱۳) برای محاسبهٔ احتمال انتخاب امپراطوری‌ها استفاده شده است:

$$P_n = e^{\left(-\alpha \times TotalCost_n / \max(TotalCost)\right)} \quad (۱۳)$$

متغیر P_n احتمال انتخاب امپراطوری n ام، و $TotalCost_n$ مقدار هزینهٔ کل مربوط به امپراطوری n ام است و عبارت $\max(TotalCost)$ بیشترین مقدار تابع هزینهٔ کل بین تمام امپراطوری‌ها را شامل می‌شود. مقدار α پارامتر فشار انتخاب نامیده می‌شود. هر چه α بزرگتر انتخاب شود، احتمال انتخاب امپراطوری‌های قدرتمند بیشتر و احتمال انتخاب امپراطوری‌های ضعیف، کمتر خواهد شد. با اعمال این فاکتور، به آسانی می‌توان بر سرعت همگرایی تاثیر گذاشت. البته در کل باید بین فرآیند بهره‌برداری و جستجو تعادلی برقرار ساخت.

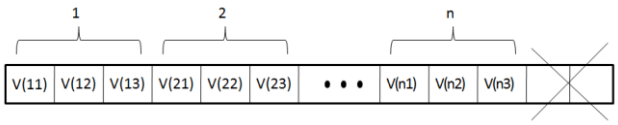
۳-۲- روش پیشنهادی جایگزین بردار متعامد در رقابت استعماری متعامد

در مقالهٔ کاوه و طلاطاهری [۱۹] نسخه‌های مختلفی از الگوریتم ICA مطرح کرده و عملکرد آنها را با یکدیگر مورد بررسی قرار داده‌اند. یکی از روش‌های بهبود قابلیت جستجو، افزودن بردار متعامد به راستای حرکتی مستعمره به سمت استعمارگر می‌باشد که این بردار با V_2 در رابطهٔ (۱۴) نشان داده شده است [۱۲].

$$\{x\}_{new} = \{x\}_{old} + \beta \times d \times \{cm\} \otimes \{V_1\} + cm \times \tan(\theta) \times d \times \{V_2\}$$
$$\{V_1\} \cdot \{V_2\} = 0, \quad \|\{V_2\}\| = 1 \quad (۱۴)$$

یکی دیگر از مشکلاتی که هنگام بالا بودن تعداد متغیرهای مستقل تابع (متغیرهای تصمیم) مطرح است، ایجاد بردار متعامد در گام الگوریتم رقابت استعماری متعامد می‌باشد. در واقع تولید چنین بردار تصادفی متعامد در ابعاد بالا کار بسیار دشواری است. ما در این مقاله روشی جایگزینی برای روش بالا ارائه خواهیم کرد که شبه کد آن در ادامه به صورت زیر می‌باشد. روش پیشنهادی سرعت تولید بردار متعامد را تسریع بخشیده و فضای جستجوی الگوریتم را هدف‌دار می‌سازد.

گام اول: تقسیم بردار به بردارهای سه درایه‌ای که در شکل (۵) به تصویر کشیده شده است. همان طور که در شکل نشان داده شده است درایه‌های اضافی را در گام اول حذف می‌کنیم.



شکل ۵- تقسیم بردار اصلی V به زیر بردارهای سه درایه‌ای

که بردارهای V_1 و V_2 و ... به صورت روابط (۱۵) تعریف می‌شوند:

$$V_1 = [V(11)\ V(12)\ V(13)]$$
$$V_2 = [V(21)\ V(22)\ V(23)]$$
$$V_i = [V(i1)\ V(i2)\ V(i3)] \qquad i = 1,2,\dots,n \quad (۱۵)$$

گام دوم: ضرب بردار تفکیک شده در بردار تصادفی جهت تولید بردار متعامد کوچک می‌باشد، که عمل ضرب خارجی بین دو بردار مطابق رابطه (۱۶) انجام می‌گیرد.

$$U \times V = (u_1 i + u_2 j + u_3 k) \times (v_1 i + v_2 j + v3k = u2v3 - u3v2i + u3v1 - u1v3j + u1v2 - u2v1k \quad (۱۶)$$

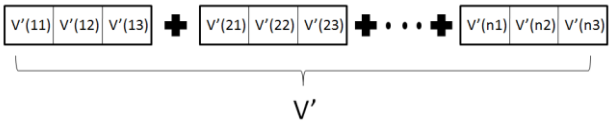
با استفاده از ضرب برداری بالا بردار متعامد V' بر بردار V و بردار تصادفی W بدست می‌آید که طبق روابط (۱۷) تعریف می‌شود:

$$W = rand(1,3)$$
$$V_i' = V_i \otimes W = [V(i1)\ V(i2)\ V(i3)] \otimes W \qquad i = 1,2,\dots,n \quad (۱۷)$$

گام سوم: بردار تولیدی V_i' بر بردار V_i و W عمود است که تعامد بین بردارهای V_i' و V_i حائز اهمیت است که به این معنی است که ضرب داخلی دو بردار V_i' و V_i مطابق رابطه (۱۸) برابر با صفر خواهد بود.

$$V_i' \perp V_i, W$$
$$V_i' \cdot V_i = 0 \qquad i = 1,2,\dots,n \quad (۱۸)$$

گام چهارم: با کنار هم قرار دادن بردارهای V_i' بردار نهایی V' را بدست می‌آوریم که این گام در شکل (۶) به تصویر کشیده شده است:

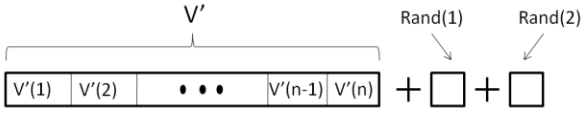


شکل ۶- تشکیل بردار V' از به هم پیوستن ریز بردارهای V_i'

گام پنجم: بردار حاصل از گام قبلی باید بر بردار اصلی اولیه عمود باشد، یعنی باید رابطه‌ی (۱۹) همواره برقرار باشد:

$$V'.V = 0 \quad \Rightarrow \quad V' \perp V \quad (۱۹)$$

گام ششم: در صورتی که تعداد درایه های بردار V' و V با هم برابر نباشند ضرب بالا عملا ممکن نخواهد بود. بنابراین برای این منظور برای برابرسازی تعداد درایه های بردار V' با بردار V به تعداد لازم درایه به انتهای بردار V' اضافه خواهیم کرد. شکل (۷) چگونگی این گام را نشان می‌دهد.



شکل ۷- برابرسازی تعداد درایه‌های بردار V' با تعداد درایه‌های بردار اصلی V

همان طور که در شکل بالا مشاهده می‌شود درایه‌های تصادفی $rand(1)$ و $rand(2)$ به منظور برابرسازی تعداد درایه‌ها به بردار V' اضافه می‌کنیم. در صورتی که تعداد درایه‌های بردار V برابر با $3k+1$ باشد تنها به اضافه کردن $rand(1)$ و در صورتی که برابر با $3k+2$ باشد با اضافه کردن هر دو مقادیر $rand(1)$ و $rand(2)$ تعداد درایه‌های بردار V' را با تعداد درایه‌های بردار V یکسان می‌کنیم.

گام هفتم: در نهایت حاصل ضرب داخلی دو بردار V و V' برابر با مقدار کوچکی خواهد بود و از این رو بردار V' برداری نزدیک به بردار عمود بر V خواهد بود.

۳-الگوریتم رقابت استعماری پیشنهادی در آموزش شبکه عصبی پرسپترون چند لایه

در این مقاله برای بررسی توانایی طبقه‌بندی شبکه عصبی پرسپترون چند لایه که توسط الگوریتم رقابت استعماری آشوبی متعامد اصلاح شده، از دو مجموعه داده با ابعاد مختلف استفاده شده است. مورد اول مجموعه دادهٔ یونسفر با ابعاد متوسط و مورد دوم مجموعه دادهٔ سونار با ابعاد بالا می‌باشد. جدول زیر ویژگی‌های مجموعه داده‌های بکار رفته را به طور جامع به تصویر می‌کشد. در جدول (۱) تعداد داده‌های آموزش و تست با توجه به روش ارزیابی $k-Fold$ بیان شده است.

جدول ۱- مشخصات و ویژگی‌های داده‌های به کار رفته در آموزش شبکه عصبی

تعداد الگو	نوع ابعاد داده	ویژگی مجموعه داده	نوع مجموعه داده	تعداد خروجی	نوع ورودی	تعداد ورودی	نام داده
۳۵۱	با بعد متوسط	چند متغیره	طبقه‌بندی	۱	اعداد صحیح و حقیقی	۳۴	دادهٔ یونسفر
۲۰۸	با بعد بالا	چند متغیره	طبقه‌بندی	۱	اعداد حقیقی	۶۰	دادهٔ سونار

مجموعه دادهٔ یونسفر شامل طبقه‌بندی سیگنال‌های بازگشتی رادار از الکترون‌های آزاد یک یونسفر است. این مجموعه شناسایی نوع خاصی از ساختار در یونوسفر را شامل می‌شود [۲۰]. در این مجموعه داده ۳۴ مشخصه ورودی وجود دارد و تعداد کل الگوها ۳۵۱ عدد می‌باشد. با اعمال این مجموعه داده به شبکه عصبی، ساختار پرسپترون چند لایه ۱-۳-۳۴ خواهد بود. در نتیجه ورودی‌های شبکه عصبی شامل اعداد صحیح و حقیقی است و تعداد وزن‌های کل شبکه که توسط الگوریتم پیشنهادی نیاز به بروز رسانی خواهد داشت، ۱۰۹ وزن است.

مجموعه دادهٔ سونار شامل ۲۰۸ الگو با ۶۰ ویژگی می‌باشد. هدف ما آموزش یک شبکه عصبی پرسپترون ۳ لایه به منظور تشخیص و تفکیک سیگنال‌های سونار منعکس شده از یک استوانهٔ فلزی و سیگنال‌های منعکس شده از تخته سنگی تقریبا استوانه‌ای می‌باشد [۲۱]. ساختار تعیین شده برای لایه‌های شبکه عصبی MLP طبق ۱-۳-۶۰ است. در جدول (۲) ویژگی‌های شبکه MLP آموزش داده شده، نشان داده شده است.

جدول ۲- مشخصات شبکه عصبی به کار رفته در آموزش

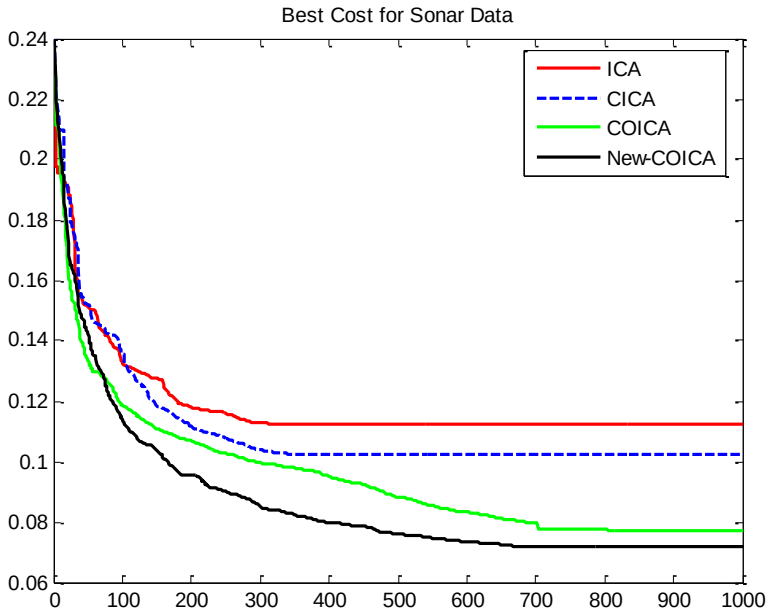
محدودهٔ بروزرسانی	تعداد وزنهای بروزرسانی شده	نوع توابع فعال‌سازی	ساختار لایه-های شبکه	
(-۱,۱)	۱۰۹	تانژانت هایپربولیک سیگموید	۱-۳-۳۴	دادهٔ یونسفر
(-۱,۱)	۱۸۷	تانژانت هایپربولیک سیگموید	۱-۳-۶۰	دادهٔ سونار

۳-۱-مقایسه روش پیشنهادی با سایر نسخه‌های الگوریتم رقابت استعماری

در این قسمت از مقاله، شبکه عصبی MLP را با الگوریتم پیشنهادی به همراه سه نسخهٔ دیگر از الگوریتم رقابت استعماری شامل الگوریتم استاندارد (ICA)، رقابت استعماری آشوبی (CICA) و نسخهٔ اولیهٔ الگوریتم COICA آموزش داده و منحنی خطای میانگین مربعات را در یک شکل بدست آورده‌ایم. در این شبیه‌سازی‌ها تعداد تکرارهای هر الگوریتم در ۱۰۰۰ تکرار محدود شده است. به منظور مقایسهٔ صحیح الگوریتم‌ها با یکدیگر، شرایط اولیه برای شروع الگوریتم‌ها را یکسان فرض می‌کنیم. برای این منظور، جمعیت اولیه‌ای را ایجاد و ذخیره کرده‌ایم. برای آموزش شبکه توسط الگوریتم مربوطه، همان جمعیت اولیهٔ تعیین شده را فراخوانی کرده‌ایم. جدول (۳) پارامترهای مختلف و قابل تنظیم الگوریتم‌های مذکور را نشان می‌دهد.

جدول ۲- پارامترهای قابل تنظیم الگوریتم‌های مورد بررسی

نام پارامتر	ویژگی پارامتر	مقدار انتخاب شده	الگوریتمهای بکار رفته
VarSize	طول بردار اصلی	بسته به نوع مساله	تمام الگوریتم‌ها
VarMin	کران پایین بردار اصلی	-۱	تمام الگوریتم‌ها
VarMax	کران بالا بردار اصلی	+۱	تمام الگوریتم‌ها
MaxIt	ماکزیمم مقدار تکرارها	۱۰۰۰	تمام الگوریتم‌ها
Npop	تعداد جمعیت اولیه	۸۰	تمام الگوریتم‌ها
nEmp	تعداد امپراطوری‌های اولیه	۱۰	تمام الگوریتم‌ها
Ncol	تعداد مستعمرات	۷۰	تمام الگوریتم‌ها
Alpha	فاکتور فشار	۱	تمام الگوریتم‌ها
Beta	ضریب جذب	۲	تمام الگوریتم‌ها
pRevolution	احتمال انقلاب	۰,۱	تمام الگوریتم‌ها
Mu	نرخ انقلاب	۰,۰۵	تمام الگوریتم‌ها
zeta	ضریب میانگین هزینه مستعمرات	۰,۱	تمام الگوریتم‌ها



شکل ۸- مقایسه نتایج نسخه‌های مختلف ICA برای مجموعه دادهٔ سونار

در نمودار شکل (۸) محور عمودی نشان‌دهندهٔ خطای میانگین مربعات[18] آموزش شبکه (MSE) و محور افقی تعداد تکرارها می‌باشد. در شکل بالا می‌توان مشاهده کرد که خطای میانگین مربعات آموزش شبکهٔ عصبی MLP با استفاده از الگوریتم پیشنهادی (New-COICA) نسبت به سایر روش‌ها بیشتر کاهش یافته است. از آنجایی که هدف از آموزش شبکهٔ عصبی، طبقه‌بندی الگوهای جدید می‌باشد، میزان درصد خطای طبقه‌بندی نیز برای هر الگوریتم در جدول (۴) آورده شده است.

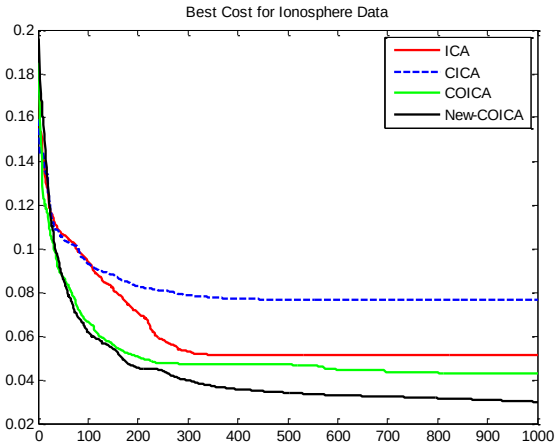
جدول ۳- مقایسه نتایج آماری شبیه‌سازی‌ها برای نسخه‌های مختلف ICA در ۱۰ تکرار برای دادهٔ سونار

	Train MSE	Mean of Classification Error	Std of MSEtr	Std of Error
ICA	0.1125	14.2857	0.0029	4.7619
CICA	0.1038	17.4603	0.0059	5.4986
COICA	0.0803	17.4603	0.0241	2.7493
New-COICA	0.0640	9.5238	0.0088	8.2479

در جدول (۴) پارامتر Train MSE نشان‌دهندهٔ خطای آموزش از طریق روش میانگین مربعات خطا می‌باشد، پارامتر بعدی Mean Classification Error نشان‌دهندهٔ درصد خطای طبقه‌بندی است که در واقع درصد خطای خروجی را نشان می‌دهد. پارامتر Std of MSEtr بیان‌کنندهٔ انحراف معیار خطای آموزش شبکه عصبی مصنوعی است و در نهایت پارامتر Std of Error انحراف استاندارد خطای طبقه‌بندی خروجی را نشان می‌دهد.

در جدول (۴)، پارامترهای انحراف استاندارد خطای آموزش و درصد خطای طبقه‌بندی نیز برای ۱۰ بار تکرار شبیه‌سازی‌ها نشان داده شده است. انحراف استاندارد خطای طبقه‌بندی نسبت به سایر روش‌ها کاهش نیافته است، اما میزان میانگین درصد خطای طبقه‌بندی نسبت به سایر نسخه‌ها کاهش چشم‌گیری یافته است یعنی به مقدار ۹،۵٪ رسیده است و همچنین در خطای آموزش شبکه نیز این برتری از آن الگوریتم پیشنهادی می‌باشد. انحراف معیار درصد خطای طبقه‌بندی نسبت به سایر الگوریتم‌ها با اختلاف اندکی بیشتر است، از این رو الگوریتم پیشنهادی قابلیت اطمینان بر الگوریتم‌ها را بهبود نبخشیده است.

با اعمال شبیه‌سازی‌ها بر روی مجموعه دادهٔ یونسفر نیز نتایج زیر بدست آمده است. شکل (۹) خطای میانگین مربعات برای روش‌های مختلف را به تصویر می‌کشد. در این شکل محور عمودی خطای MSE آموزش شبکه و محور افقی تعداد تکرارها را نشان می‌دهد.



شکل ۹. مقایسه نتایج نسخه‌های مختلف ICA برای مجموعه دادهٔ یونسفر

و نتایج آماری بدست آمده از ۱۰ بار تکرار در شبیه‌سازی‌ها در جدول (۵) نشان داده شده است.

جدول ۴. مقایسه نتایج آماری شبیه‌سازی‌ها در ۱۰ تکرار برای نسخه‌های مختلف ICA در داده یونسفر

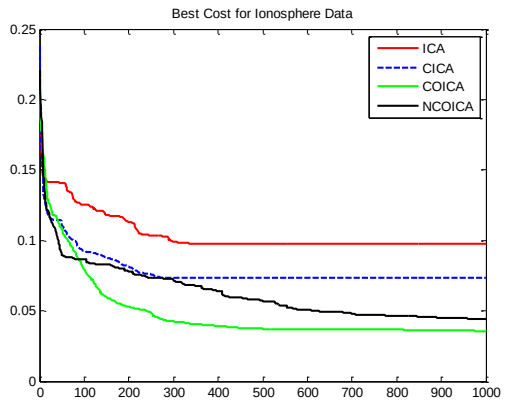
	Train MSE	Mean of Classification Error	Std of MSEtr	Std of Error
ICA	0.1028	15.7143	0.0056	9.7590
CICA	0.0778	17.8571	0.0124	9.4401
COICA	0.0520	12.1429	0.0055	7.1429
New-COICA	0.0491	8.5450	0.0219	3.2991

[18] Mean Square Error

در جدول بالا نیز پارامتر Train MSE نشان دهندهٔ خطای آموزش از طریق روش میانگین مربعات خطا می‌باشد، پارامتر بعدی Mean Classification Error نشان‌دهندهٔ درصد خطای طبقه‌بندی است. پارامتر Std of MSEtr بیان‌کنندهٔ انحراف معیار خطای آموزش شبکه است و پارامتر Std of Error انحراف استاندارد خطای طبقه‌بندی خروجی را نشان می‌دهد.

خطای میانگین مربعات برای آموزش شبکه برای این مجموعه داده نیز با استفاده از الگوریتم پیشنهادی نسبت به سایر نسخه‌ها به مقدار کمتری همگرا شده است و این در حالی است که درصد خطای طبقه‌بندی نیز مقدار ۸٫۵٪ بدست آمده که کمترین مقدار در بین این الگوریتم‌ها می‌باشد. انحراف استاندارد برای درصد خطای طبقه‌بندی در روش پیشنهادی مقدار کمتری نسبت به سایر نسخه‌ها بدست آمده است و این در حالی است که انحراف استاندارد خطای MSE برای الگوریتم پیشنهادی نسبت به سایر الگوریتم‌ها بیشترین مقدار را دارد.

در بعضی از اجراها الگوریتم پیشنهادی نسبت به بعضی از الگوریتم‌ها، در کاهش خطای MSE آموزش توانایی کمتری از خود نشان می‌دهد. شکل (۱۰) نمونه‌ای از این اجرا را نشان می‌دهد. در شکل مذکور محور عمودی بیانگر خطای میانگین مربعات آموزش شبکه و محور افقی بیانگر تعداد تکرارها می‌باشد.

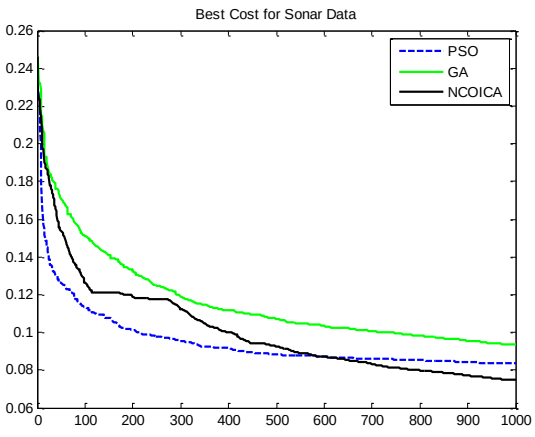


شکل ۱۰- وقوع پدیدهٔ بیش برازش در آموزش شبکه عصبی برای مجموعه دادهٔ یونسفر در نسخهٔ قبلی

با مشاهده شکل (۱۰) انتظار می‌رود که درصد خطای طبقه‌بندی برای الگوریتم COICA سابق نسبت به الگوریتم پیشنهادی مقدار کمتری بدست آید، در حالیکه درصد خطای طبقه‌بندی برای الگوریتم COICA برابر ۲۰٪ و برای الگوریتم پیشنهادی ۵/۷٪ بدست آمده است. می‌توان نتیجه گرفت که شبکه عصبی در حین آموزش توسط الگوریتم COICA دچار پدیدهٔ بیش برازش شده است. می‌توان دید که در اغلب موارد الگوریتم پیشنهادی با وجود خطای آموزش بیشتر، به درصد خطای طبقه‌بندی کمتری دست یافته است. در واقع عمومیت پذیری آموزش توسط الگوریتم پیشنهادی بهبود یافته است.

۳-۲- مقایسهٔ الگوریتم پیشنهادی با سایر الگوریتم‌های تکاملی

در این بخش از مقاله، عملکرد الگوریتم پیشنهادی را نسبت به سایر الگوریتم‌های تکاملی بررسی می‌کنیم. الگوریتم ژنتیک و الگوریتم ازدحام ذرات جزو محبوب‌ترین و پرکاربردترین الگوریتم‌های بهینه‌سازی می‌باشند. به این منظور در ادامه به بررسی نتایج این الگوریتم‌ها با الگوریتم پیشنهادی خواهیم پرداخت. شکل (۱۱) منحنی همگرایی خطای میانگین مربعات آموزش برای الگوریتم‌های GA و PSO با الگوریتم پیشنهادی را برای مجموعه دادهٔ سونار نشان می‌دهد. در این شکل محور عمودی بیانگر خطای MSE آموزش شبکه و محور افقی نشان‌دهنده تعداد تکرارها است.



شکل ۱۱. مقایسه نتایج روش پیشنهادی با سایر الگوریتم‌های تکاملی برای دادهٔ سونار

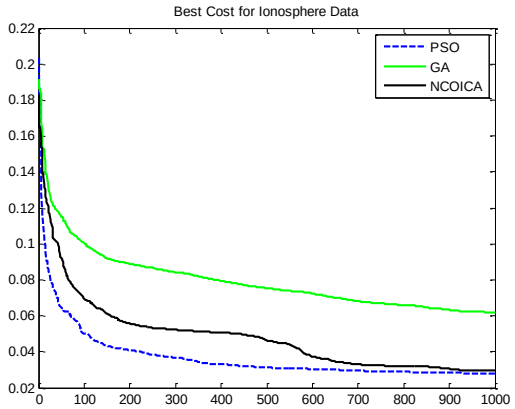
و نتایج آماری برای ۱۰ تکرار برای هر الگوریتم در جدول (۶) نشان داده شده است.

جدول ۵. مقایسه نتایج آماری شبیه‌سازی‌ها در ۱۰ تکرار برای هر الگوریتم در دادهٔ سونار

	Train MSE	Mean Classification Error	Std of MSEtr	Std of Error
GA	0.0926	22.4603	0.0043	10.9971
PSO	0.0774	20.6349	0.0055	5.4986
New-COICA	0.0742	19.0476	0.0053	4.7619

در جدول (۶) نیز پارامتر Train MSE خطای آموزش از طریق روش میانگین مربعات خطا را نشان می‌دهد، پارامتر Mean Classification Error نشان‌دهندهٔ درصد خطای طبقه بندی و پارامتر Std of MSEtr بیان‌کنندهٔ انحراف معیار خطای آموزش شبکه و پارامتر Std of Error انحراف استاندارد خطای طبقه‌بندی خروجی را نشان می‌دهد.

منحنی خطای MSE آموزش برای دادهٔ یونسفر نیز به صورت شکل (۱۲) بدست آمده است. در شکل زیر خطای میانگین مربعات آموزش شبکه توسط محور عمودی نشان داده شده است و محور افقی تعداد تکرارها را نشان می‌دهد.



شکل ۱۲- مقایسه روش پیشنهادی با سایر الگوریتم-های تکاملی برای دادهٔ یونسفر

و نتایج آماری شبیه‌سازی‌ها برای مجموعه دادهٔ یونسفر در ۱۰ تکرار به اختصار در جدول (۷) بدست آمده است.

جدول ۷- مقایسه نتایج آماری شبیه‌سازی‌ها در ۱۰ تکرار برای هر الگوریتم در دادهٔ یونسفر

	Train MSE	Mean Classification Error	Std of MSEtr	Std of Error
GA	0.0628	14.2857	0.0051	10.3016
PSO	0.0303	13.3333	0.0038	3.2991
New-COICA	0.0335	11.4286	0.0036	5.7143

در جدول بالا نیز پارامترهای مطرح شده در جدول از سمت چپ به راست به ترتیب عبارت است از خطای میانگین مربعات خطای آموزش شبکه، درصد خطای طبقه‌بندی شبکهٔ آموزش دیده، انحراف معیار خطای آموزش شبکه و انحراف استاندارد خطای طبقه‌بندی خروجی.

با مشاهدهٔ نتایج بالا مشاهده می‌شود، که خطای میانگین مربعات آموزش با استفاده از الگوریتم PSO نسبت به الگوریتم پیشنهادی به مقدار کمتری کاهش یافته است و این در حالی است که الگوریتم پیشنهادی به درصد خطای طبقه‌بندی بهتری دست یافته است. بهبود درصد خطای طبقه‌بندی را می‌توان به علت توانایی بهتر و بیشتر در جستجو توسط الگوریتم پیشنهادی دانست. این ویژگی باعث کاهش احتمال رخداد پدیدهٔ بیش برازش در روند آموزش شبکه گشته و در نتیجه باعث بهبود قابل توجه طبقه‌بندی داده‌ها توسط شبکه عصبی مصنوعی شده است. انحراف استاندارد خطای آموزش برای الگوریتم پیشنهادی در مقایسه با دو الگوریتم دیگر کاهش یافته است و انحراف استاندارد درصد خطای طبقه‌بندی نسبت به الگوریتم ژنتیک بهبود یافته و با اختلاف اندکی از الگوریتم PSO بیشتر است.

۴- نتیجه‌گیری

در این مقاله با اعمال سه تغییر اصلی در الگوریتم رقابت استعماری آشوبی متعامد سعی در بهبود عملکرد الگوریتم مزبور کرده‌ایم. در الگوریتم پیشنهادی از تابع توزیع بولتزمان جهت تعیین احتمال تصاحب ضعیف‌ترین مستعمره در ضعیف‌ترین امپراطوری استفاده شده است. همچنین جهت انتخاب امپراطوری قدرتمند برای عملیات ذکر شده، از روش انتخاب چرخ رولت استفاده شده است. در نهایت با استفاده از روش جدیدی، تغییراتی در راستای حرکت مستعمره به

سمت استعمارگر مربوطه اعمال کرده‌ایم. اجرای شبیه‌سازی‌ها بر روی دو مجموعه دادهٔ سونار و یونسفر انجام گرفت که شامل دو بخش، یعنی بررسی با سایر نسخه‌های رقابت استعماری و بررسی با سایر الگوریتم‌های تکاملی است. نتایج بدست آمده نشان می‌دهد که الگوریتم پیشنهادی در مقایسه با سایر نسخه‌های رقابت استعماری به خطای میانگین مربعات کمتری در آموزش شبکه رسید و همچنین درصد خطای طبقه‌بندی کمتری نسبت به سایر نسخه‌ها از خود نشان داد. همچنین تعمیم‌پذیری الگوریتم پیشنهادی نسبت به سایر نسخه‌ها بهبود یافت. در مقایسه با سایر الگوریتم‌های تکاملی، الگوریتم پیشنهادی نسبت به الگوریتم ژنتیک به خطای آموزش کمتری همگرا شد و تنها با اختلاف اندکی نسبت به الگوریتم ازدحام ذرات دارای خطای آموزش بیشتری است و این در حالی است که با وجود خطای آموزش بیشتر به درصد خطای طبقه‌بندی بهتری دست یافته است. در کل عمومیت‌پذیری الگوریتم پیشنهادی نسبت به سایر روش‌ها بهبود یافت. انحراف استاندارد درصد خطای طبقه‌بندی و یا خطای آموزش شبکه به طور کلی کاهش محسوسی نیافته است.

منابع

1.M. Melanie, “An Introduction to Genetic Algorithms,” Massachusett's MIT Press, 34(7):pp.1-9, 1999.

2.L. A. Ingber, “Simulated annealing: practice versus theory,” J. Math. Comput. Modell., 18(11):pp. 29–57, 1993.

3.Kennedy, J., Eberhart, R.C.: Particle Swarm Optimization. Proceedings of IEEE, 1942– 1948 (1995)

4.M. Dorigo, V. Maniezzo and A. Colorni, “The ant system: optimization by a colony of cooperating agents,” IEEE Transaction System Man Cybern, B 26(1):pp. 29–41, 1996.

5.B. Franklin and M. Bergerman, “Cultural Algorithms: Concepts and Experiments,” In Proceedings of the IEEE Congress on Evolutionary Computation, 2: pp. 1245–1251, 2000.

6.R. Storn and K. Price, “Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces,” Journal of Global Optimization, 11(4):pp. 341–359, 1997.

7.K. Lee and Z. Geem, “A new structural optimization method based on the harmony search algorithm,” Computers and Structures, 82:781-98, 2004.

8.E. Rashedi, H. Nezamabadi-pour and S. Saryazdi, “A Gravitational Search Algorithm,” Information Science, Special Section on High Order Fuzzy Sets, 179(13): pp. 2232-2248, 2009.

9.Brownlee, J., Clever Algorithms: Nature-Inspired Pro Recipes, LuLu Enterprises Incorporated, (1st Edition), 2011.

10.Kaveh A, Talatahari S. Novel heuristic optimization method: Charged system search, Acta Mechanica, doi: 10.1007/s00707-009-0270-4, 2010.

11.Atashpaz-Gargari, E. and Lucas, C., "Imperialist Competitive Algorithm: An Algorithm for Optimization Inspired by Imperialistic Competition", IEEE Congress on Evolutionary Computation (CEC), pp. 4661-4667, 2007.

12.Talatahari, S. and Farahmand Azar, B. and Sheikholeslami, R. and Gandomi, A.H., "Imperialist competitive algorithm combined with chaos for global optimization", Commun. Nonl. Sci. Numer. Simulat., vol. 17, pp. 1312-1319, 2012.

13.Kaveh, A. and Talataheri, S., "Optimum design of skeletal structures using imperialist competitive algorithm", computers & structures journal, vol. 88(21), pp. 1220-1229, 2010.

14.H. Bahrami, K. Faez, M. Abdechiri, “Imperialist Competitive Algorithm using Chaos Theory for Optimization,” UKSim-AMSS 12th International Conference on Computer Modeling and Simulation, 2010.
15.M. Abdechiri, K. Faez and H. Bahrami, “Neural Network Learning based on Chaotic Imperialist Competitive Algorithm,” The 2nd International Workshop on Intelligent System and Applications (ISA2010), 2010.
16.Abdechiri, M. and Faez, K. and Bahrami, H., "Adaptive Imperialist Competitive Algorithm (AICA)", 9th IEEE International Conference on Cognitive Informatics (ICCI), pp. 940-945, 2010.
17.Coelho, L. D. and Afonso, L. and Alotto, P., "A Modified Imperialist Competitive Algorithm for Optimization in Electromagnetics", IEEE Transactions on Magnetics, vol. 48, pp. 579-582, 2012
18.Soltani-Sarvestani, M. A. and Lotfi, S. and Ramezani, F., "Quad Countries Algorithm (QCA)", Lecture Notes in Computer Science, vol. 7198, pp. 119-129, 2012.
19.Kaveh, A. and Talataheri, S., "Imperialist Competitive Algorithm For Engineering Design Problems", Asian Journal Of Civil Engineering, vol. 11, pp. 675-697, 2010.
20.Sigillito, V.G., Wing, S.P., Hutton, L.V., and Baker, K.B. (1989), ‘Classification of Radar Returns from the Ionosphere using Neural Networks’, Johns Hopkins APL Technical Digest, 10, 262–266.
21.Gorman, R.P., and Sejnowski, T.J. (1988), ‘Analysis of Hidden Units in a Layered Network Trained to Classify Sonar Targets’, Neural Networks, 1, 75–89.

فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص:۱۵- ۲۶

مدل‌های چرخشی تطابقی و الگوهای ترافیکی جهت کاهش اتلاف نوری در شبکه‌های روی تراشه‌ی نوری

بهاره اسدی* میدیا رشادی** احمد خادم‌زاده*** مصطفی کرباسی****

* دانشکده مهندسی کامپیوتر و برق، غیاث‌الدین جمشیدکاشانی، دانشگاه غیردولتی، آبیک، ایران
** دانشکده مهندسی کامپیوتر، علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
*** ساختمان همکاری‌های علمی وآموزشی بین‌المللی، مرکز تحقیقات و مخابرات، تهران، ایران
****دانشکده مهندسی کامپیوتر و برق، غیاث‌الدین جمشیدکاشانی، دانشگاه غیردولتی، آبیک، ایران

تاریخ دریافت: ۱۳۹۵/۱/۲۹ تاریخ پذیرش: ۱۸/ ۱۳۹۶/۱

چکیده

تعداد زیادی از هسته‌های پردازشی که در داخل یک تراشه تجمیع شده‌اند سرعت رشد بالایی را دارند، شبکه‌های روی تراشه‌ی نوری یکی از روش‌های ساده برای حل مشکل آدرس‌دهی در بین شبکه‌های درون اتصالی حجیم می‌باشد به همین دلیل در آینده تراشه‌های چند پردازنده‌ای با کارآیی و پهنای باند بالا نیاز خواهد بود. شبکه‌های روی تراشه‌ی نوری به‌عنوان نسل جدیدی از شبکه‌های روی تراشه مطرح شدند که تمامی محدودیت‌های این نوع از شبکه‌ها را رفع کرده و دارای مزایای زیادی از جمله پهنای باند ارتباطی بالا، تاخیر انتقال کم و توان مصرفی پایین می‌باشد. از طرفی شبکه‌های روی تراشه‌ی نوری دارای چالش‌هایی است که یکی از مهمترین آن‌ها مسیریابی داده‌های نوری در بستر لایه‌ی نوری است زیرا نحوه انتخاب مسیر بر روی عامل اتلاف نوری تاثیرگذار است. در این مقاله، الگوریتم‌های مسیریابی عاری از بن‌بست مدل‌های چرخشی تطابقی، سوئیچینگ مداری و الگوهای ترافیکی مختلف برای کاهش اتلاف نوری در لایه‌ی نوری با در نظر گرفتن مسیریاب بدون انسداد ۵ درگاهه و همبندی دو بعدی توری یا مش ارائه خواهد شد. در آخر نتایج بدست آمده از شبیه‌سازی را با روش‌های مشابهی مانند الگوریتم مبتنی بر بعد XY مقایسه کرده و بهبودهای بدست آمده را بررسی می‌نماییم.

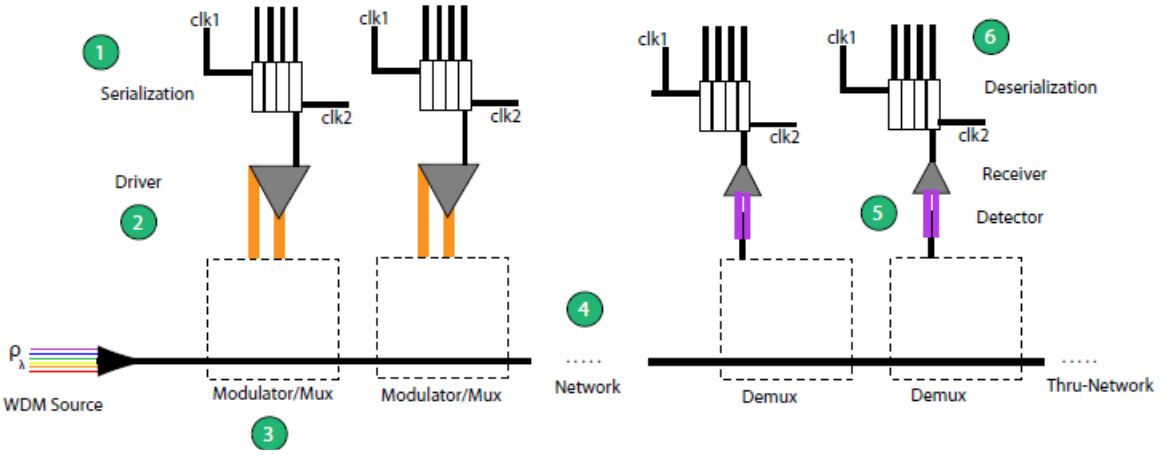
واژه‌های کلیدی : اتلاف نوری، الگوهای ترافیکی، مدل‌های چرخشی، مسیریاب.

۱- مقدمه

شبکه‌های روی تراشه‌ی نوری نقش مهمی را در ساختار شبکه‌های درون اتصالی ایفا می‌کنند. بنابراین، تعداد هسته‌های پردازشی و فرکانس ساعت مربوطه افزایش می‌یابد. پهنای باند ارتباطی بالا در شبکه‌های روی تراشه به معنی واقعی به ارتباط میان هسته‌های پردازشی نیاز دارد. افزایش یافتن پهنای باند ارتباطی، مصرف توان و تاخیر انتقال به‌عنوان یک گلوگاه در شبکه‌های روی تراشه مطرح شد[۱و۵]. در نتیجه شبکه‌های روی تراشه‌ی نوری حاوی پهنای باند بالا، تاخیر انتقالی پایین و توان مصرفی کم پیشنهاد شده است و در مقایسه با قطعات الکتریکی بهینه‌تر شده است[۱۰]. مسیریاب‌های نوری یکی از اجزای کلیدی و

نویسندهٔ عهده‌دار مکاتبات: بهاره اسدی b_asadi@jku.ac.ir

مهم در شبکه‌های روی تراشه‌ی نوری هستند، مخصوصاً زمانیکه کارآیی و توان مصرفی مطرح باشد.



شکل ۱- تکنولوژی تسهیم طول موج[۳۰]

شبکه‌های روی تراشه‌ی نوری مبتنی بر تکنولوژی نور بوده و از اتصالات نوری سیلیکون و مسیریاب‌های که با تکنولوژی CMOS ساخته شده‌اند استفاده می‌کنند [۶و۷]. همچنین، کارآیی این نوع از شبکه‌ها به کمک تکنولوژی تقسیم طول موج افزایش چشمگیری می‌یابد [۸]. علاوه بر این، طول موج‌ها مستقل از فاصله بوده و نرخ انتقال داده نیز متاثر از مصرف توان در طول موج‌ها و سوئیچ‌های نوری نیست بنابراین، مصرف توان در این نوع از شبکه‌ها مطلوب است [۹]. شکل ۱ ساختار تسهیم طول موج را نشان می‌دهد.

۱) داده به سمت لینک ارسالی می‌رسد، که از مدولاسیون نرخ ساعت برای همگام سازی استفاده می‌کند. این فاز نیاز به بافرها و مداراتی دارد که بتواند بین دو پالس ساعت تبدیلات را انجام دهد [۳۰].

۲) مدارات آنالوگ یک‌ها و صفرها را به سمت مدولاتور هدایت می‌کند که شامل برخی تقویت‌کننده‌هاست [۳۰].

۳) مدولاتورها طول موج‌های پیوسته را در یک فرکانس خاص به طول موجی که بتوان اطلاعات دیجیتال را انتقال دهد تبدیل می‌کند [۳۰].

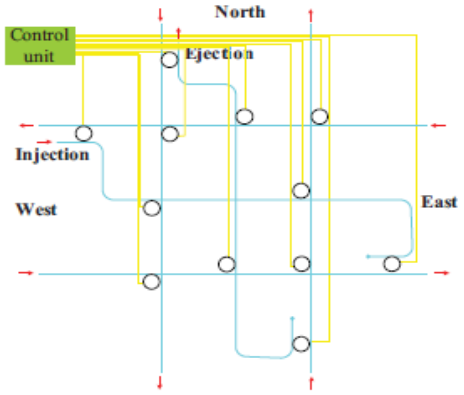
۴) سوئیچ‌های موجود در شبکه یا همان مسیریاب‌ها اطلاعات را با استفاده از یکسری فیلترها یا سوئیچ‌های فعال مسیردهی می‌کنند [۳۰].

۵)هر کدام از طول موج‌ها که از مرحله فیلترینگ خارج شدند به دیدکتور یا شناسایی کننده می‌رسند تا نور جذب شده و به جریان تبدیل شود. دریافت کننده، جریان را تبدیل به ولتاژ کرده و برای ارسال به مرحله‌ی بعد و مدارات دیجیتال تقویت می‌کنند. اگر برخی از طول‌موج‌ها فیلتر یا شناسایی نشوند، به قسمت‌های دیگر شبکه هدایت خواهند شد [۳۰].

۶)داده‌هایی که نگه داشته شده‌اند در این مرحله دوباره در نرخ ساعت دیگری شروع خواهند شد که این فاز بنام ناهمگام سازی معروف است [۳۰].

در این مقاله، از الگوریتم‌های مسیریابی عاری از بن‌بست مدل‌های چرخشی تطابقی، سوئیچینگ مداری و الگوهای ترافیکی مختلف مانند Random، Paratec، Madbench، Bitreverse، Cactus وTornado برای کاهش اتلاف نوری در لایه‌ی نوری با در نظر گرفتن مسیریاب عاری از انسداد با ۵ درگاه بنام Crux و همبندی دو بعدی مش یا توری استفاده کرده‌ایم [۲۹و ۲۸و ۱۲]. مسیریاب Crux از دو اجزای سوئیچینگ مانند موجبرها و ریزحلقه‌های تشدیدگر تشکیل شده است. مسیریاب ذکر شده دارای ۴ تا موجبر و ۱۲ تا ریزحلقه‌ی تشدیدگر می‌باشد و می‌توان در

تمامی الگوریتم هایی که مبتنی بر بعد XY هستند از این مسیریاب استفاده نمود. Crux شامل یکسری سوئیچ‌ها، واحد کنترل، درگاه‌های دو طرفه از جمله شمال، جنوب، شرق، غرب و درگاه‌هایی برای تزریق و دریافت داده‌ی نوری که بنام‌های injection/ejection معروف است می‌باشد. دو درگاه اخیر به هسته پردازشی محلی به کمک واسط نوری/الکتریکال متصل است. Crux از اجزای سوئیچینگ موازی برای کاهش اتلاف نوری استفاده کرده است. بر خلاف سایر سوئیچ‌ها که سیگنال نوری را فقط در یک بعد هدایت می‌کنند، Crux با هدایت داده‌ی نوری در مسیرهایی که نیاز به ریزحلقه‌های تشدیدگر زیادی ندارد (با غیرفعال‌سازی ریزحلقه‌های تشدیدگر اضافی) باعث کاهش اتلاف نوری می‌شود. اغلب زمانیکه سیگنال‌های نوری از درگاه‌های injection/ejection تزریق یا دریافت می‌شوند به هنگام تغییر بعد در آن صورت نیاز به فعال-سازی ریزحلقه‌های تشدیدگر خواهیم داشت. در این مسیریاب حداکثر تعداد تقاطع موج‌برها ۵ تاست. مسیریاب Crux عاری از انسداد و دور باطل است. شکل ۲ ساختار مسیریاب نوری Crux را نشان می‌دهد[۱۲].



شکل ۲- خطوط آبی موج‌برها، دایره‌های توخالی ریزحلقه‌های تشدیدگر، خطوط زردرنگ هم واسط‌ها می‌باشند [۱۲]

ایده ارائه شده می‌تواند گره‌های مبدا و مقصد مختلفی را در نظر گرفته و مسیرهای موجود را با توجه به مقادیر اتلاف نوری بنام‌های بهترین-حالت، متوسط-حالت و بدترین- حالت در نظر بگیرد. سپس داده را از مسیری که کمترین مقدار اتلاف را دارد یعنی همان بهترین-حالت انتقال می‌دهد. با استفاده از الگوریتم‌های مسیریابی عاری از بن‌بست مدل‌های چرخشی تطابقی، سوئچینگ مداری و الگوهای ترافیکی مختلف می‌توان اتلاف نوری کل را در لایه‌ی نوری نیز ارزیابی نمود و کاهش قابل توجهی را در مقدار اتلاف نوری در مقایسه با الگوریتم مسیریابی مبتنی بر بعد XY نشان دهد.

این مقاله بدین صورت سازمان‌دهی شده است: بخش ۲، برخی از روش‌های پیشنهادی رایج که باعث کاهش اتلاف نوری در همبندی دو بعدی مش یا توری می‌شود را بررسی می‌نماییم. در بخش ۳، همبندی مش یا توری و اجزای استفاده شده در شبکه‌های نوری، همچنین ایده پیشنهادی خودمان را نیز توضیح خواهیم داد. بخش ۴، ارزیابی نتایج شبیه‌سازی ایده

پیشنهادی را بحث می‌کنیم. در بخش ۵، نتیجه‌گیری و کارهای آینده ذکر شده است.

۲- پیشینه‌ی تحقیق

زمانیکه شبکه‌های روی تراشه‌ی نوری معرفی و یکسری راهکارهای موثری توسط Shacham و همکارانش ارائه شد[۱۳] در مورد چالش‌های این نوع از شبکه‌ها مخصوصاً مسیریابی و اتلاف نوری بحث‌هایی نیز مطرح گردید. در این بخش، برخی از روش‌های رایج انجام شده را بررسی می‌نماییم.

Xie و همکارانش[۷ و ۱۲] یک مسیریاب عاری از انسداد با ۵ درگاه بنام Crux را پیشنهاد کردند که می‌توان از الگوریتم مسیریابی مبتنی بر بعد XY به همراه همبندی توری یا مش و توری مدور یا توروس استفاده نمود. جدول مسیریابی استفاده شده دارای پیچیدگی کمتری است. هر بسته ابتدا در بعد X هدایت می‌شود تا زمانیکه به گره مقصد در همان ستون برسد. اگر گره مقصد هم ستون با گره مبدا نباشد در نتیجه بسته در بعد Y هم هدایت می‌شود. از این نوع مسیریاب به همراه الگوریتم مسیریابی XY برای کاهش اتلاف نوری استفاده می‌شود.

Gu و همکارانش[۱۴] یک مسیریاب عاری از انسداد با ۵ درگاه بنام Cygnus را معرفی کردند. که قابلیت‌هایی مانند کارآیی بالا، توان پایین را دارا بود و به کمک الگوریتم

مسیریابی مبتنی بر بعد XY می‌توانست داده‌ی نوری را با مقدار اتلاف کم انتقال دهد.

Ye و همکارانش[۱۵] یک مسیریاب ۵ درگاهه‌ی دیگری را به همراه الگوریتم مسیریابی مبتنی بر بعد XY برای همبندی توری و توری مدور بررسی کرده‌اند و نتایج حاصل را با مقدار اتلاف بدست آمده از سایر مسیریاب‌های ۵ درگاه مقایسه نموده‌اند.

Gu و همکارانش[۱۶] یک مسیریاب عاری از انسداد با ۵ درگاه جدیدی بنام OXY را ارائه کرده‌اند که مختص همبندی توری بوده و می‌توانست از الگوریتم مسیریابی مبتنی بر بعد XY برای ارزیابی مقدار اتلاف نوری و مصرف انرژی استفاده کند.

Hatamirad و همکارانش[۱۱] مسیریاب آگاه از اتلاف را طراحی کردند که می‌توانست الگوریتم مسیریابی مبتنی بر بعد را در شبکه‌های روی تراشه‌ی نوری استفاده نماید. این مسیریاب حاوی ۴ درگاه بود. این مسیریاب با کاهش اجزای سوئیچ موازی در ساختار خود سعی در کاهش اتلاف نوری را داشت.

Ji و همکارانش[۱۷] یک مسیریاب نوری با ۵ درگاه را طراحی نمودند و بیشتر به تعداد ریزحلقه‌ها تشدیدگر و حرارت ناشی از آن‌ها دقت کردند. خصوصیات این مسیریاب این بود که خروجی را از دو درگاه بدست می‌آورد تا بدین صورت بتواند در کارآیی تعادل برقرار شود. این مسیریاب از استاندار CMOS استفاده کرد. علاوه بر کاهش تعداد ریزحقله‌های تشدیدگر سعی در کاهش تعداد موج‌برها را نیز داشتند تا بدین صورت بتوانند ساختاری از مسیریاب را ارائه نمایند تا بتواند به کمک الگوریتم مسیریابی مبتنی بر بعد XY مقدار اتلاف نوری را کاهش دهد.

Shacham و همکارانش[۱۸] ساختار ترکیبی از نور و الکترونیک را برای شبکه‌های روی تراشه ارائه نمودند و مسیریاب نوری عاری از انسداد را بهبود دادند تا بتوانند اتلاف نوری را ارزیابی نمایند. همچنین، از الگوریتم مسیریابی مبتنی بر بعد XY برای انتقال داده‌ی نوری بین گره‌های مبدا و مقصد استفاده کردند.

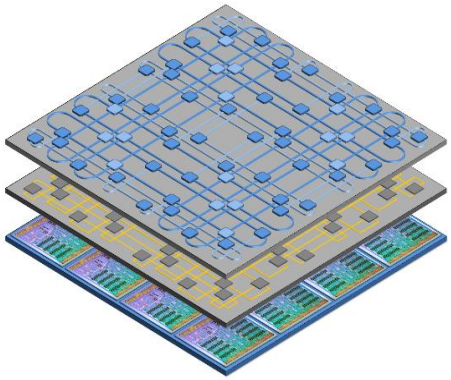
بعداز بررسی و مرور برخی از راهکارهای رایج ارائه شده در مورد مسیریابی و کاهش اتلاف نوری، در بخش ۳ برخی از مفاهیم مهم و اساسی مطرح شده در ایده‌ی پیشنهادیمان را توضیح می‌دهیم.

۳- مفاهیم اساسی و پایه

۳-۱- معماری شبکه‌ی روی تراشه‌ی نوری

یکی از خصوصیات ارتباطات نوری عدم وجود بافر است زیرا طراحی بافری که بتواند نور را در خود نگه دارد غیرممکن است [۱۳]. بنابراین، بر خلاف شبکه‌های روی تراشه که از سوئیچینگ بسته‌ای استفاده می‌کنند، در ارتباطات نوری از سوئیچینگ مداری استفاده خواهیم نمود زیرا در این روش نیازی به استفاده از بافر نیست [۱]. روش‌های مختلفی برای پیاده‌سازی سوئیچینگ مداری در شبکه‌های روی تراشه‌ی نوری ارائه شده است.

به‌عنوان مثال، یکی از روش‌ها برای انتقال داده با استفاده از سیگنال‌های نوری با طول موج‌های مختلف، بدین صورت می‌باشد که ابتدا هر بسته از موج‌برهای مسیر خود برای انتقال استفاده می‌کند. مزیت این روش استفاده از فرکانس‌های مختلف برای انتقال چندین داده بصورت همزمان می‌باشد. از طرفی، از معایب این روش هزینه بالا و اتلاف توان به خاطر وجود منابع لیزری مختلف است [۶ و ۱۹-۲۲]. روش دیگر برای پیاده‌سازی ارتباطات نوری استفاده از مدارات کنترلی الکتریکال می‌باشد. همچنین، از مداراتی بنام تعیین اولویت برای اختصاص درگاه به خود استفاده می‌کنند. معایب این روش نیز افزایش اتلاف توان می‌باشد. ساختار نوری- الکتریکال را بنام ساختار هیبرید یا ترکیبی می‌شناسیم [۶ و ۲۳]. سوئیچینگ مدارای نوری باعث شده است که تراشه شامل سه لایه بنام‌های لایه‌ی پردازشی، لایه‌ی کنترلی الکترونیک و لایه‌ی نوری باشد. لایه‌ی پردازشی گره‌های پردازشی را دارد و به‌عنوان مبدا و چاهک‌هایی برای تمامی ارتباطات رفتار می‌کنند و پایین‌ترین لایه است. بالاترین لایه، لایه‌ی نوری است که ارتباطات نوری با تکنیک تسهیم طول موج را شامل است. تمامی اجزای نوری موجود در لایه‌ی نوری باید قبل ار انتقال داده‌ی نوری پیکربندی شوند بدین منظور از لایه‌ی میانی بنام لایه کنترلی الکترونیک استفاده می‌نماییم. شکل ۳ ساختار مربوط به این سه لایه را نشان می‌دهد[۲۴].



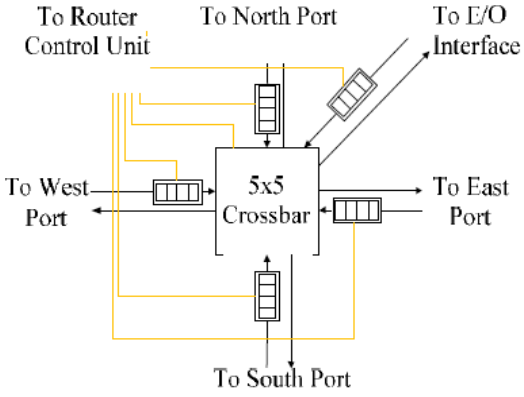
شکل ۳- معماری لایه‌ها [۲۴]

۳-۲- اجزای پایه شبکه‌ی روی تراشه‌ی نوری

شبکه‌ی روی تراشه‌ی نوری شامل برخی اجزا و تجهیزات پایه می‌باشد که در ادامه هر کدام از آن‌ها را بررسی می‌نماییم.

۳-۲-۱- اجزای الکتریکال

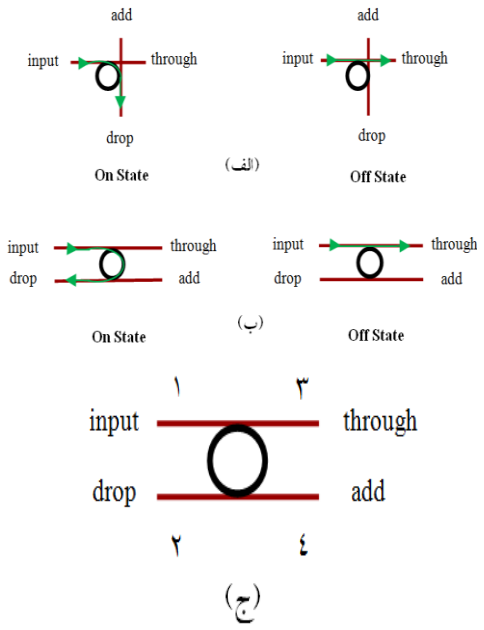
قطعات الکتریکال ترکیبی از ارتباطات سیمی و مسیریاب‌های الکتریکال است. این مسیریاب شامل مداراتی بنام کنترلر و تعیین کننده اولویت می‌باشد. شکل ۴ ساختار این مسیریاب را نشان می‌دهد [۲۵].



شکل ۴- ساختار یک مسیریاب الکتریکال [۲۵]

۳-۲-۲- اجزای نوری

موجبرها داده‌ی نوری را حمل می‌کنند. مدولاتورها تبدیل سیگنال الکتریکال به نور را انجام می‌دهند. دیدکتورها تبدیل مجدد نور به سیگنال‌های الکتریکال را انجام می‌دهند. که این موارد بطور مفصل به همراه شکل در بخش ۱ مقدمه بحث شده است. ریز حلقه‌ی تشدیدگر برای تصمیم‌گیری انتخاب و یا برای تغییر مسیر داده‌ی نوری در موجبرها استفاده می‌شود. همچنین یک ریزحلقه‌ی تشدیدگر می‌تواند با فرکانس‌های مختلفی از طول‌موج‌ها کار کند. یک ریز حلقه‌ی تشدیدگر شامل دو حالت است: روشن و خاموش [۱۱]. اجزای سوئیچینگ موازی و متقاطع از جمله‌ی دو اجزای اساسی در طراحی مسیریاب‌های نوری می‌باشد. اجزای نوری موازی شامل یک ریزحلقه‌ی تشدیدگر و دو تا موجبر است. به عبارتی دیگر موجبرها به موازات ریزحلقه قرار دارند. اجزای نوری متقاطع همانند اجزای قبلی است با این تفاوت که موجبرها عمود به هم و ریز حلقه هستند. در حالت کلی ۴ درگاه بنام‌های input، drop، through و add در این اجزا داریم. زمانیکه ریزحلقه روشن است سیگنال مسیرش را تغییر داده و به سمت درگاه drop می‌رود. وگرنه، به مسیر خود ادامه داده و به درگاه دیگری هدایت می‌شود. در برخی از طراحی‌ها برای این درگاه شماره نیز در نظر می‌گیرند. شکل ۵ الف وب ساختار اجزای متقاطع و موازی، شکل ۵ ج همین ساختار را به همراه شماره نشان می‌دهد [۲۶].



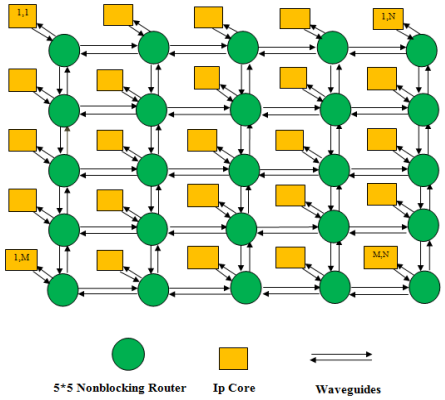
شکل ۵- ساختار اجزای موازی و متقاطع

۳-۳- همبندی و مدل‌های چرخشی تطابقی

۳-۳-۱- همبندی دو بعدی مش یا توری

در این مقاله از همبندی توری دو بعدی به خاطر سادگی ساختارش استفاده می‌کنیم. ساختار این همبندی در شکل

۶ نشان داده شده است. فلش‌های دو سر موج‌برها، مربع‌های نارنجی هسته‌های پردازشی و دایره‌های سبز رنگ مسیریاب‌های عاری از انسداد با ۵ درگاه را نشان می‌دهد. شماره‌گذاری را بصورت ستونی از بالا به پایین با شروع از شماره یک آغاز می‌کنیم.



شکل ۶- همبندی توری دو بعدی

۳-۳-۲- مدل‌های چرخشی تطابقی

در همبندی توری دو بعدی سیگنال می‌تواند در چهار جهت شمال، جنوب، شرق و غرب مسیریاب حرکت نماید. چرخش یعنی تغییر جهت سیگنال. بدین دلیل، ما چهار مدل چرخشی بنام‌های West-first، North-last، Negative-first وOdd-even را بررسی می‌نماییم. در این مدل‌های چرخشی برای اجتناب از بن‌بست یک چرخش را در حالت ساعتگرد و یک چرخش در حالت پادساعتگرد یا در ستون‌های فرد و زوج حذف می‌شود. به همین دلیل تمامی مدل‌های چرخشی عاری از بن‌بست و دور باطل می‌باشند. در ادامه مدل‌های چرخشی را بررسی می‌نماییم.

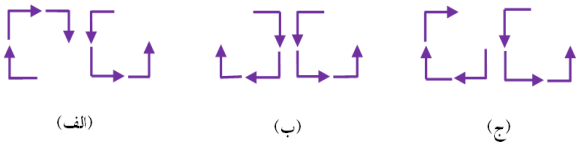
West-first: در حالت ساعتگرد چرخش جنوب به غرب، در حالت پادساعتگرد چرخش شمال به غرب حذف شده است.

North-last: در حالت ساعتگرد چرخش شمال به شرق و در حالت پادساعتگرد چرخش شمال به غرب حذف شده است.

Negative-first: در حالت ساعتگرد چرخش شرق به جنوب و در حالت پادساعتگرد چرخش شمال به غرب حذف شده است.

Odd-even: در ستون‌های زوج چرخش‌های شرق به شمال و شمال به غرب، در ستون‌های فرد چرخش‌های شرق به جنوب و جنوب به غرب حذف شده است.

شکل ۷ الف مدل چرخشی West-first ، ۷ ب مدل چرخشی North-last، ۷ ج مدل چرخشی Negative-first را نشان می‌دهد. به چرخش‌های حذف شده، چرخش‌های ممنوعه نیز گفته می‌شود.



شکل ۷- مدل‌های چرخشی تطابقی

۳-۴- راهکار پیشنهادی ارائه شده

در این مقاله، با استفاده از الگوریتم‌های مسیریابی عاری از بن‌بست مدل‌های چرخشی تطابقی، سوئیچینگ مداری و الگوهای ترافیکی مختلف اتلاف نوری را در مسیرهای مختلف بین گره‌های مبدا و مقصد محاسبه و مناسبترین مسیر را برای انتقال داده‌ی نوری در بستر لایه‌ی نوری انتخاب می‌کنیم همچنین راهکار پیشنهادی از همبندی بدون بن‌بست دو بعدی توری یا مش با سایز M*N و مسیریاب عاری از انسداد با ۵ درگاه Crux [۱۲] نیز استفاده می‌کند. ابتدا سطرها و ستون همبندی را همانطور که در شکل ۶ نشان داده شد، شماره گذاری می‌کنیم. گره‌های مبدا و مقصد می‌توانند در یک سطر و ستون یا سطر و ستون‌های مختلف باشند. با در نظر گرفتن الگوهای ترافیکی مختلف برای شناسایی گره‌های مبدا و مقصد، الگوریتم مسیریابی سه مسیر مختلف را بین این گره‌ها در نظر گرفته سپس مقدار اتلاف نوری را در هر مسیریاب محاسبه کرده و در نهایت برای هر مسیر اتلاف کل را بدست می‌آوریم. الگوریتم‌های مسیریابی عری از بن‌بست مدل‌های چرخشی تطابقی، سوئیچیگ مداری، انواع الگوهای ترافیکی مختلف از جمله Random، Paratec، Madbench، Bitreverse، Cactus و Tornado [۲۸و ۲۹] را در زیر بخش ۳-۳-۲ بررسی نمودیم.

با تعیین گره‌های مبدا و مقصد در لایه‌ی نوری الگوریتم مسیریابی در مسیریاب Crux ۵ درگاهه [۱۲] که

در مسیرهای موجود بین گره‌ها قرار گرفته‌اند اجرا می‌شود. تمام چرخش‌های ساعتگرد و پادساعتگرد موجود در هر چهار نوع مدل چرخشی تطابقی در نظر گرفته شده سپس از درگاه‌ها و جهت‌های مجاز به سمت مسیریاب بعدی گام به گام هدایت می‌شود. همزمان با اجرای مدل‌های چرخشی تطابقی، سوئیچینگ مداری نیز برای رزرو مسیریاب‌ها و مسیرها اجرا می‌شود. به‌عبارتی دیگر، الگوریتم مسیریابی عاری از بن‌بست تا زمانی در هر مسیریاب اجرا می‌شود که به گره مقصد مورد نظر برسیم و مسیر موجود بین گره‌های مبدا و مقصد به کمک سوئیچینگ مداری رزرو گردد. بعد از این مرحله، داده‌ی نوری ارسال می‌شود. همانطور که اشاره شد ۳ مسیر مختلف به کمک الگوریتم مسیریابی رزرو می‌شود. به طور کاملتر می‌خواهیم هدف از ارائه این الگوریتم را توضیح دهیم. در واقع ما می‌خواهیم یک مسیر مناسب از بین مسیرهای مختلف را برای انتقال داده‌ی نوری انتخاب نماییم. به همین دلیل عامل اتلاف نوری را در نظر می‌گیریم. یعنی هر مسیری که اتلاف نوری کمتری را در مقایسه با مسیرهای دیگر داشته باشد آن مسیر انتخاب شده و داده‌ی نوری از آن مسیر انتقال می‌یابد. همانطور که قبلاً نیز اشاره شد اجزای نوری مانند اتلاف تقاطع موج‌برها، اتلاف خمش موج‌برها مخصوصاً خمش‌های ۹۰ درجه و ریز حلقه‌های تشدیدگر در هر دو حالت روشن و خاموش از عوامل تأثیرگذار در اتلاف نوری می‌باشند. بعد از رزرو کردن مسیر و آماده‌سازی برای انتقال داده‌ی نوری، باید مقدار اتلاف نوری را در هر مسیریاب تا زمانیکه داده به گره مقصد برسد را محاسبه نماییم. سپس مقادیر بدست آمده را با هم جمع می‌کنیم و نتیجه‌ی بدست آمده را به‌عنوان اتلاف کل آن مسیر در نظر می‌گیریم. همین مراحل را برای مسیرهای ۲ و ۳ نیز تکرار می‌کنیم. سپس اتلاف کل هر سه مسیر را با هم مقایسه کرده و مسیری را که کمترین مقدار اتلاف نوری را داشته باشد برای انتقال داده‌ی نوری در نظر می‌گیریم. با مقایسه سه مقدار بدست آمده برای اتلاف کل کمترین مقدار را به عنوان بهترین-حالت Best-case بیشترین مقدار را به عنوان بدترین-حالت Worst-case و مقداری که بین این دو حالت باشد به‌عنوان متوسط-حالت Average-case معرفی می‌کنیم. در هر مدل چرخشی تطابقی و الگوهای ترافیکی مختلف، ۱۶ حالت مختلف را تست می‌نماییم که می‌توانیم در برخی حالت‌ها گره‌های مبدا یا مقصد را در یک سطر و ستون در نظر بگیریم. در شبیه‌سازی ۱۲ حالت با گره‌های مبدا و مقصد در سطر و ستون‌های مختلف و ۴ حالت با گره‌های مبدا و مقصد در سطر و ستون‌های یکسان در نظر می‌گیریم. دقت شود زمانیکه گره‌های مبدا و مقصد در سطر و ستون‌های یکسان هستند مقادیر هر سه حالت Best-case، Worst-case و Average-case با هم مساوی خواهند شد. در نهایت نتایج بدست آمده برای اتلاف نوری با استفاده از الگوریتم مسیریابی ارائه شده را با الگوریتم مسیریابی مبتنی بر بعد XY مقایسه خواهیم نمود تا درصد بهبود در مقدار اتلاف نوری در شبکه‌ی روی تراشه‌ی نوری را نشان دهیم. بدین منظور، بعداز محاسبه‌ی مقدار اتلاف در هر سه مسیر و تعیین بهترین، متوسط و بدترین حالت، مجموع تمام شانزده تا بهترین-حالت و ۱۶ تا بدترین-حالت را محاسبه می‌کنیم. در آخر، تفاضل بین بهترین و بدترین را بدست می‌آوریم و به‌عنوان درصد اتلاف نوری در نظر می‌گیریم.

۴-نتایج شبیه‌سازی

در این بخش، برای بدست آوردن کمترین مقدار اتلاف نوری بین گره‌های مبدا و مقصد شبیه‌سازی انجام شده است.

۴-۱- پیکربندی و محیط شبیه‌سازی

در این مقاله ما از شبیه‌سازهای CLAP [۲۶] و متلب برای ارزیابی اتلاف نوری در شبکه‌های روی تراشه‌ی نوری استفاده می‌کنیم. در این راستا، مقادیر اولیه برخی از متغیرها و اجزای فیزیکی باید تنظیم و مقدار دهی شود. شبیه‌سازی را برای سناریو و سایزهای مختلف شبکه ارزیابی کردیم. اجزای اساسی و پیکربندی مورد نیاز برای شبیه‌سازی در جداول ۱و ۲و ۳و ۴ نشان داده شده است.

جدول ۱- پیکربندی شبیه‌سازی

مقادیر	علایم	متغیرها
۰٫۱۵ dB	L_{WC}	اتلاف چرخش موج‌بر
۰٫۰۰۵ dB/90°	L_{WB}	اتلاف خمش موج‌بر
۰٫۵ dB	L_{DRon}	اتلاف ریزحلقه‌ی تشدیدگر در حالت روشن
۰٫۰۰۵ dB	L_{PRoff}	اتلاف ریزحلقه‌ی تشدیدگر در حالت خاموش

جدول ۲- متغیرهای مربوط به اتلاف نوری[۲۷]

مقادیر	متغیرهای شبیه‌سازی
۱۰۲٤ بیت	اندازه پیام
۳۲ بیت	حداکثر سایز بسته
۱۰ دسی‌بل بر متر	منبع تولید لیزر

جدول ۳- متغیرهای مربوط به اتلاف نوری

علایم	متغیرها
$L_{(Pi, Pj)}R(x,y)$	اتلاف نوری در مسیریاب (x, y) از درگاه i به درگاه j
$R(x,y)$	مسیریاب (x, y)
$Switching\ (P_i,P_j)$	اتلاف سوئیچ از درگاه i به j
C_S	سایز تراشه (cm^2)
M*N	سایز شبکه

جدول ۴- متغیرهای مربوط به مسیریاب Crux ۵ درگاهه

علایم	متغیرها
P_i	درگاه i
P_j	درگاه j
In	درگاه Injection
Eje	درگاه Ejection
N	درگاه شمال یا North
S	درگاه جنوب یا South
W	درگاه غرب یا West
E	درگاه شرق یا East

۴-۲- ارزیابی اتلاف نوری

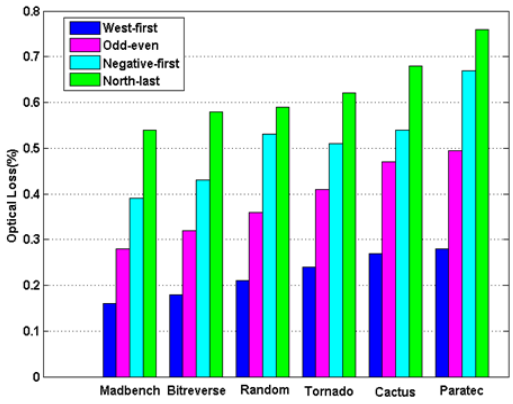
یکی از متغیرهای مهم در شبکه‌های روی تراشه‌ی نوری همان طور که قبلاً نیز اشاره شد عامل اتلاف نوری می‌باشد. بدین منظور با در نظر گرفتن سایزهای مختلف برای همبندی توری دو بعدی مثلاً ۲*۲ تا ۸*۸ می‌توانیم این ارزیابی را انجام دهیم. که در این قسمت برای سایز ۸*۸ شبیه‌سازی را در نظر گرفته‌ایم. شبیه‌سازی را بر اساس فرضیات ذکر شده در جداول ۱ تا ۴ و الگوریتم مسیریابی بحث شده انجام می‌دهیم. بنابراین، رابطه‌ی ۱ را بدست آورده و اتلاف نوری را محاسبه می‌نماییم.

$$L_{(P_i,P_j)}^{R(x,y)} = \sum_{i}^{j} Switching(P_i, P_j) \quad (۱)$$

$$Switching(P_i, P_j) = L_{WC} * L_{WB} * L_{DRon} * L_{PRoff}$$

در رابطه‌ی ۱ می‌توانیم با جایگذاری مقادیر متغیرهای موجود مقدار اتلاف نوری را در هر مسیریاب بدست آوریم. بعداز اجرای شبیه سازی، نتایج بدست آمده را در نمودار شکل ۸ و جدول ۵ نشان داده‌ایم. مقدار درصد اتلاف در الگوریتم مبتنی بر بعد XY با همین فرضیات، ۶۴ درصد است [۱۵]. که بعد از شبیه‌سازی و مقایسه مقادیر بدست آمده، درصد اتلاف در راهکارارائه شده بهینه‌تر است. از طرفی، مدل چرخشی تطابقی West-first در الگوهای

ترافیکی مختلف درصد اتلاف نوری کمتری را در مقایسه با مدل‌های چرخشی دیگر دارد.



شکل ۸: درصد اتلاف نوری با مدل‌های چرخشی و ترافیکی ختلف

در حالت کلی، با توجه به انتخاب مکان قرارگیری گره‌های مبدا و مقصد ممکن است نتایج دیگری بدست آید. مثلاً با انتخاب گره‌ها در لبه‌های همبندی دو بعدی توری یا مش برخی از درگاه‌ها و چرخش‌های ممنوعه حذف می‌شود. چرا که الگوی‌های ترافیکی به گام‌های الگوریتم‌هایشان وابسته هستند که با چه فرآیندی گره‌ها و ارتباطات بین آن‌ها را شناسایی می‌کنند [۲۸ و ۲۹].

۵-نتیجه‌گیری و کارهای آینده

با در نظر گرفتن همبندی توری دوبعدی، الگوریتم‌های مسیریابی عاری از بن‌بست مدل‌های چرخشی تطابقی، سوئیچینگ مداری، الگوهای ترافیکی مختلف و مسیریاب عاری از انسداد Crux با ۵ درگاه[۱۲] راهکاری را در جهت کاهش اتلاف نوری ارائه نمودیم. بر اساس نتایج بدست آمده از شبیه‌سازی در نمودار شکل ۸، جدول ۵ و با مقایسه روش‌هایی که از تغییرات سخت‌افزاری در ساختار مسیریاب‌ها ایجاد کرده بودند مانند کاهش تعداد موجبرها و تعداد ریزحلقه‌های تشدیدگر به همراه الگوریتم مسیریابی مبتنی بر بعد XY، راهکار ارائه شده درصد اتلاف کمتری داشته و به‌عبارت دیگر آگاه از اتلاف است. در این مقاله، ایده مطرح شده مستقل از ساختار مسیریاب بوده و می‌تواند مسیرهای متنوعی را بین گره‌های مبدا و مقصد بدست آورد و مسیر با کمترین مقدار اتلاف را انتخاب و برای انتقال داده‌ی نوری استفاده می‌کند. به‌عنوان کار آینده، الگوریتم پیشنهادی را برای مسیریاب‌های نوری مختلف عاری از انسداد با ۵ درگاه، هچنین الگوهای ترافیکی دیگر تست خواهیم نمود. هدف این ارزیابی، نشان دادن قابلیت مدل‌های چرخشی تطابقی در جهت کاهش اتلاف نوری در شبکه‌های روی تراشه‌ی نوری است.

جدول ۵- مقایسه درصد اتلاف

Optical Loss (%)	Madbench	Bitreverse	Random	Tornado	Cactus	Paratec
West-first	۰,۱۷	۰,۱۸	۰,۲۰	۰,۲۳	۰,۲۷	۰,۲۸
Odd-even	۰,۲۸	۰,۳۲	۰۳۵	۰,۴۱	۰,۴۸	۰,۵۰
Negative-first	۰,۳۹	۰,۴۳	۰,۵۳	۰,۵۱	۰,۵۴	۰,۶۷
North-last	۰,۵۵	۰,۵۷	۰,۵۹	۰,۶۲	۰,۶۷	۰,۷۷

منابع

1.Shacham A, Bergmen K, Carloni LP (2008) Photonic Network-on-Chip for Future Generations of Chip Multiprocessors. IEEE Trans Comput 57: 1246-1260. doi: 10.1109/TC.2008.78

2.Hung MK, Yaoyao Y, Xiaowen W, Wei Z, Weichen L, Jiang X (2010) A Hierarchical Hybrid Optical-Electronic Network-on-Chip. In Proc IEEE Compute SOC Ann Symp 327-332. doi: 10.1109/ISVLSI.2010.17

3.Miller DAB (2009) Device Requirements for Optical Interconnects to Silicon Chips. Proc. IEEE 977:1166-1185. doi: 10.1109/JPROC.2009.2014298

4.Lee BG, Biberman A, Chan J, Bergmen K (2010) High-Performance Modulators and Switches for Silicon Photonic-Network-on-Chip. IEEE J. Sel. Topics Quantum Electron 16: 6-22. doi: 10.1109/JSTQE.2009.2028437

5.Min R, Ji R, Chen Q, Zhang L (2012) A Universal Method for Constructing N-Port Nonblocking Optical Router for Photonic Networks-on-Chip. Journal of Lightwave Technology 30: 3736-3741. doi: 10.1109/JLT.2012.2227945

6.Beausoleil RG, Kuekes PJ, Snider GS, Yuan WS, Williams RS (2008) Nanoelectronic and Nanophotonic Interconnect. Proceeding of the IEEE 96: 230-247. doi: 10.1109/JPROC.2007.911057

7.Xie Y, Nikdast M, Xu J, Wu X, Zhang W, Ye Y, Wang X, Wang Z, Liu W (2012) Formal Worst-Case Analysis of Crosstalk Noise in Mesh-Based Optical Networks-on-Chip. IEEE Transaction on very large Scale integration (VLSI) Systems 21:1823-1836. doi: 10.1109/TVLSI.2012.2220573

8.Chan J, Hendry G, Bergman K, Carloni LP (2011) Physical-Layer Modeling and System-Level Design of Chip-scale Photonic Interconnection Networks. Computer-Aided Design of Integrated Circuits and Systems, IEEE Trans, 30: 337-345. doi: 10.1109/TCAD.2011.2157157

9.Biberman A, Preston K, Hendry G, Sherwood N, Chan J, Levy JS, Lipson M, Bergman K (2011) Photonic Network-on-Chip Architectures Using Multilayer Deposited Silicon Materials for High-Performance Chip Multiprocessor. J. Emerge Techno Compute Syst 7:1-25. doi: 10.1145/1970406.1970409

10.Pan Y, Kumar P, Kim J, Memik G, Zhang Y, Choudhary A (2009) Firefly: Illuminating Future Network-on-Chip with Nanophotonics. Presented at the Proceedings of the 36th Annual International Symposium on Computer Architecture Austin Texas USA 429-440.

11.Hatamirad M, Reza A, Shabani H, Niazmand B, Reshadi M (2012) Loss-Aware Router Design Approach for Dimension-ordered Routing Algorithms in Photonic Networks-on-Chip. IJCSI International Journal of Computer Science Issues 9: 337-345.

12.Xie Y, Nikdast M, Xu J, Zhang W, Li Q, Wu X, Ye Y, Wang X, Liu W (2010) Crosstalk Noise and Bit Error Rate Analysis for Optical Network-on-Chip. DAC'10 Anaheim California USA 657-660.

13.Shacham A, Hendry G, Bergman K, Carloni LP (2007) On the Design of a Photonic Network-on-Chip. In networks-on-chip first International Symposium 53-64.

14.Gu H, Hung KM, Xu J, Zhang W (2009) A Low-power Low-cost Optical Router for Optical Networks-on-Chip in Multiprocessor System-on-Chip. IEEE Computer Society Annual Symposium on VLSI 19-24. doi: 10.1109/ISVLSI.2009.19

15.Ye Y, Wu X, Xu J, Zhang W, Nikdast M, Wang X (2012) Holistic Comparison of Optical Routers for Chip Multiprocessors. Supported by RPC11EG18 and SBI06/07. EG01-4 1-5. doi: 10.1109/ICASID.2012.6325348

16.Gu H, Xu J, Wang Z (2008) A Novel Optical Mesh Network-on-Chip for Gigascale Systems-on-chip. IEEE 1728-1731. doi: 10.1109/APCCAS.2008.4746373

17.Ji R, Yang L, Zhang L, Tian Y, Ding J, Chen H, Lu Y, Zhou P, Zhu W (2011) Five-port Optical Router for Photonic Networks-

on-Chip**.** Optics Express, 19: 20258-202668. doi: 10.1364/OE. 19.020258
18.Shacham A, Lee BG, Chen Q, Carloni LP (2007) Photonic NoC for DMA Communications in Chip Multiprocessors. 15th IEEE Symposium on High-performance Interconnects IEEE Computer Society 29-38. doi: 10.1109/HOTI.2007.9
19.Vantrease D (2008) CORONA: System Implications of Emerging Nanophotonic Technology. In Computer Architecture, ISCA '08. 35th International Symposium, 153-164. doi: 10.1109/ISCA.2008.35
20.Joshi A (2009) Silicon-Photonic CLOS Networks for Global on-Chips Communication. In Networks-on-Chip 3RD ACM/IEEE International Symposium, 124-133. doi: 10.1109/NOCS.2009.5071460
21.Koohi S, Abdollahi M, Hessabi S (2011) All-Optical Wavelength-Routed NoC based on a Novel Hierarchical Topology. In Networks-on-Chips (NoCs) Fifth IEEE/ACM International Symposium 97-104.
22.Sherwood-Droz N, Wang H, Chen L, Lee BG, Biberman A, Bergman K, Lipson M (2008) Optical 4*4 Hitless Silicon Router for Optical Networks-on-Chip (NoCs). Opt. Express 16:15915-15922. doi: 10.1364/OE. 16.015915
23.G (2011) Time-Division-Multiplexed Arbitration in Silicon Nanophotonic Networks-on-Chip for High Performance Chip Multiprocessors. J. Parallel Distrib Compute 71: 641-650. doi:10.1016/j.jpdc.2010.09.009
24.Wu Chan J (2012) Architecture Exploration and Design Methodologies of Photonic Interconnection Networks. Columbia University, Columbia, New York City.
25.Mo KH, Ye Y, Wu X, Zhang W, Liu W, Xu J (2010) A Hierarchical Hybrid Optical-Electronic Network-on-Chip. Presented at the proceedings of the 2010 IEEE Annual Symposium on VLSI.
26.Nikdast M, Xu J (2007) Crosstalk noise and Loss Analysis Platform (CLAP) publishing Hong Kong University of Science and Technology. http://www.ece.ust.hk/~eexu/CLAP.html.
27.Chan J, Hendry G, Biberman A, Bergman K, Carloni LP (2010) Phoenixsim: A simulator for physical-layer analysis of chip-scale photonic interconnection networks. Proceedings of the Conference on Design Automation and Test in Europe 691-696.
28.Singh A (2005) Load-balanced routing in interconnection networks. Submitted to the department of electrical engineering and the committee on graduate studies of Standford University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.
29.Hendry G, Kamil S, Biberman A, Chan J, Lee B. G, Mohiyuddin M, Bergman K, Carloni L. P, Oliker L, Shalf J (2009) Analysis of Photonic Networks for a Chip Multiprocessor Using Scientific Applications. 3rd ACM/IEEE International Symposium 104-113. doi: 10.1109/NOCS.2009.5071458.
30.Hendry G (2011) Architectures and Design Automation for Photonic Networks on Chip. Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate School of Arts and Sciences Columbia University.

فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص: ۲۷- ۴۲

ارائه چارچوبی برای ارتقاء امنیت خانه‌های هوشمند مبتنی بر اینترنت اشیاء با استفاده از معماری مرجع IoT-A

ستار هاشمی* شهروز ستوده**
* دانشیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، ایران
** پژوهشگر، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران
تاریخ دریافت: ۱۳۹۸/۰۹/۲۳ تاریخ پذیرش:۱۳۹۸/۱۱/۰۲

چکیده

امروزه خانه هوشمند به‌عنوان یکی از کاربردهای اصلی و رو به رشد اینترنت اشیاء محسوب می‌شود که راحتی، امنیت، کاهش مصرف انرژی و هزینه‌های زندگی را به همراه دارد. در کنار مزایا و محاسنی که این فنّاوری به ارمغان آورده است مسئله امنیت و حریم خصوصی به یکی از نگرانی‌های عمده تبدیل‌شده است که نیاز به توجه جدی دارد. معماری مرجع IoT-A باهدف بررسی پروتکل‌ها و منابع موجود، حصول اطمینان از سازگاری اشیاء و پروتکل‌های ارتباطی و همچنین ارائه راه‌کاری جامع برای کاربردهای مختلف اینترنت اشیا پایه‌گذاری شده است. این مقاله باهدف قرار دادن چالش امنیت در اینترنت اشیا و خانه‌های هوشمند، با استفاده از معماری مرجع IoT-A سعی در ارائه یک چارچوب کلی جهت بهبود امنیت در کلیه سطوح طراحی، اجرا و استفاده از تجهیزات و پروتکل‌ها دارد. در این مقاله از اصطلاح چارچوب امنیتی برای شناسایی مجموعه فناوری‌ها، سازوکارها، نرم‌افزارها و مؤلفه‌های موردنیاز برای تأمین مجموعه‌ای از نیازهای امنیتی استفاده‌شده است. این مقاله پس از بررسی و نگاشت آسیب‌پذیری‌ها و تهدیدات در مدل کاربردی معماری، یک چارچوب امنیتی بهبودیافته نسبت به چارچوب استاندارد معماری مرجع ارائه می‌کند. بر اساس ارزیابی نظری انجام‌شده، چارچوب جدید که با اضافه شدن دو مؤلفه مدیریت تهدیدات و آسیب‌پذیری‌ها و مدیریت زمینه و انجام برخی تغییرات در مؤلفه صدور مجوز شکل‌گرفته، الزامات امنیتی خانه‌ی هوشمند را تا حد قابل قبولی برآورده کرده و به میزان مناسبی درجه امنیت و حفظ حریم خصوصی خانه هوشمند مبتنی بر معماری اینترنت اشیاء IoT-A را ارتقاء می‌بخشد.

واژه‌های کلیدی: تابع ابیراهی فاز، خطای خروج از مرکز تصویر، چندجمله‌ای زرنیک، چندجمله‌ای چبیشف، آنالیز چندطیفی.

۱- مقدمه

اینترنت اشیاء، به امکان برقراری ارتباط تمام اشیاء با یکدیگر و با انسان‌ها، به همراه شناسایی و کشف آن‌ها تحت یک شبکه یکپارچه با شناسه مشخص اطلاق شده و امکان برقراری ارتباط هرکسی، در هر زمان و مکان[1] را به هر چیزی در هر زمان و مکان فراهم می‌آورد [۱]. این فن‌آوری شامل اشیاء و فن‌آوری‌های گوناگون مانند حسگرها، ماشین به ماشین، میان‌افزار، داده‌های بزرگ، پردازش ابری، پردازش مه است که در یک شبکه جهانی کار می‌کنند [۲-۱۱]. اینترنت اشیاء یک الگوی تحول‌گرا و در حال تحول است که

[1] Anyone, Anytime, Anywhere

نویسنده عهده‌دار مکاتبات : شهروز ستوده sotoudeh@itrc.ac.ir

در چندین حوزه کاربرد ازجمله خانه‌های هوشمند، محیط هوشمند، مراقبت‌های بهداشتی از راه دور موردتوجه قرارگرفته است [۱۲]. این حوزه‌های کاربردی همگی با استفاده از فناوری اینترنت اشیاء می‌توانند انسان‌ها را در جهت بهبود سلامت، کاهش مصرف انرژی و ایمنی یاری رسانند [۱۳]. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، به‌ویژه سیستم‌های هوشمند در منازل، سبب شده است تا امنیت در به‌کارگیری این فناوری به‌طور ویژه موردتوجه قرار گیرد و معماری‌ها و سکّوهای متعددی برای آن ارائه شود. به‌علاوه، حجم زیادی از ارتباط بین دستگاه‌ها به‌صورت ماشین به ماشین بوده و این بدان معنی است که بر روی این ارتباط کنترل چندانی نخواهیم داشت [۱۴]. همچنین به دلیل وجود بحث مالکیت اشیاء و همین‌طور حفظ حریم خصوصی افراد، توجه به نکات امنیتی مرتبط با شناسایی و کشف، دسترس‌پذیری، کنترل دسترسی، حریم خصوصی و اعتماد نیز در مبحث اشیاء هوشمند از اهمیت بیشتری برخوردار خواهد بود [۱۵]. سوءاستفاده از فناوری اینترنت اشیاء در خانه هوشمند، امکان به خطر انداختن جان انسان‌ها را در پی خواهد داشت؛ بنابراین، امنیت یک مبحث کلیدی در برابر اجرایی شدن این فناوری است که مستلزم تحقیقات گسترده است. تضمین ایمنی زندگی انسان‌ها، جلوگیری از زنجیره حوادث نامطلوب، در دسترس بودن اشیاء، رمزنگاری و فناوری‌های حفاظت، محرمانگی و یکپارچگی اطلاعات، انکارناپذیری، سازگاری اطلاعات و سطوح امنیتی آن‌ها در سیستم‌های مختلف، احراز هویت اشیاء و اشخاص با استفاده از چند عامل مانند رمز عبور، مکان و بیومتریک، مدل‌های مختلف برای اعتماد و احراز هویت غیر مرکزی ازجمله این نیازها است [۱۶]. بااین‌وجود، با افزایش توسعه در برخی از دستگاه‌های خانگی متصل به اینترنت، ریسک‌های امنیتی و حریم خصوصی به‌طور هم‌زمان در حال افزایش است [۱۷]. پنج مشخصه کلی شامل خودکارسازی، چندمنظوره بودن، انطباق، تعامل، بهره‌وری می‌بایست در یک‌خانه هوشمند فراهم گردد [۱۷]. با توجه به اینکه امکان اتصال به اینترنت جهت ارائه خدمات بهتر و هوشمندانه‌تر خانه‌های هوشمند امروزه بسیار موردتوجه است و فنّاوری‌های به‌کاررفته در این خانه‌ها ممکن است در کنار مزایای زیادی که ارائه می‌کنند دارای چالش‌ها و مشکلات امنیتی نیز باشند که البته این امر دور از ذهن نیست [۱۸]. موضوع امنیت در یک‌خانه هوشمند از مسائل کلیدی است که قبل از انتخاب سکّوی مناسب جهت پیاده‌سازی آن مطرح می‌گردد و اساساً ارائه یک سکّوی ناامن می‌تواند بستر مناسبی را برای وقوع حملاتی از قبیل شنود، استراق سمع، مردی در میان و حمله بازپخش ایجاد کند [۱۹]؛ بنابراین یکی از مهم‌ترین چالش‌ها در به‌کارگیری این فناوری، پذیرش معماری است که دارای راه‌حل‌های امنیتی مناسبی بوده و نه‌تنها مسائل مربوط به ارتباط و عملکرد سیستم‌ها را پوشش دهد، بلکه قادر به تأمین امنیت کاربران نیز باشد. این مقاله به ارائه‌ی یک چارچوب مناسب برای ارتقاء امنیت، حفظ حریم خصوصی و ایجاد اعتماد کاربران در خانه‌های هوشمند می‌پردازد.

این مقاله در ۴ بخش ارائه‌شده است. بخش ۲ به بررسی مبانی نظری پژوهش در حوزه اینترنت اشیاء، خانه هوشمند، امنیت، معماری‌ها و موضوعات امنیتی مرتبط با پژوهش می‌پردازد. در بخش ۳ روش پژوهش در قالب ارائه و بررسی راهکار پیشنهادی مقاله موردبحث قرار می‌گیرد و درنهایت بخش ۴ به تحلیل راهکارهای پیشنهادی و بررسی نتایج اختصاص‌یافته است.

۲- مبانی نظری پژوهش

این بخش به ارائه مبانی نظری پژوهش در مورد چالش‌ها و تهدیدات امنیتی خانه هوشمند مبتنی بر اینترنت اشیاء خواهد پرداخت.

۲-۱- خانه هوشمند مبتنی بر اینترنت اشیاء[۲]

امروزه خانه‌ها با استفاده از فناوری‌های هوشمند به‌صورت خودکار درآمده و توانایی برطرف ساختن نیازهای ساکنین ازجمله راحتی، امنیت و حفظ حریم خصوصی را داشته و نسبت به نیازهای انسان مدرن و محیط زندگی او حساس و پاسخگوست[۲۰, ۲۱]. کاربرد اصلی خودکارسازی در محیط یک‌خانه هوشمند، کنترل نور، حرارت و تهویه هوا،

[2] Internet of things based smart home

مانیتورینگ، ایجاد امنیت و محافظت، پزشکی از راه دور، کنترل مصرف انرژی، کنترل عوامل محیطی بوده و دسترسی به اطلاعات موردنیاز نیز از کاربردهای دیگر آن است. ورود خانه هوشمند به بحث اینترنت اشیاء به معنی سپردن امر ذخیره‌سازی، پردازش و تحلیل داده‌ها به امکانات عرضه‌شده در فضای مجازی است که موجب ایجاد چالش‌های امنیتی جدیدی شده است [۲۲-۲۵].

۲-۲- امنیت[3]، چالش‌ها[4] و تهدیدات[5]

امنیت و حریم خصوصی از مهم‌ترین چالش‌ها برای استفاده از اینترنت اشیاء در خانه‌های هوشمند است و معماری مناسب امنیتی باید چرخه حیات و قابلیت‌های اینترنت اشیاء را در این حوزه تحت پوشش قرار دهد [۲۶, ۲۷]. تحقیقات متعددی به‌منظور افزایش امنیت در اینترنت اشیاء صورت انجام‌شده است؛ اما مواردی همچون مکانیسم‌های مناسب جهت رمزنگاری، پروتکل‌های شبکه، مدیریت داده و شناسه‌ها، حریم خصوصی کاربران و معماری‌های قابل‌اعتماد هنوز قابل‌بحث می‌باشند [۲۸-۳۰]. طبق تحقیقات انجام‌شده در مورد امنیت خانه هوشمند، حریم خصوصی، اعتماد، امنیت و ارتباطات از عمده چالش‌های تأثیرگذار بر خانه هوشمند هستند [۲۵]. این موارد در جدول ۱ قابل‌مشاهده است.

جدول ۱- چالش‌های اینترنت اشیاء در حوزه خانه هوشمند

عنوان چالش	مراجع	توضیح
حریم خصوصی	[۲۵, ۳۱-۳۴]	حفظ حریم خصوصی و مسائل وابسته مانند امنیت اطلاعات و افشای اطلاعات و داده‌ها
ارتباطات	[۲۵, ۳۳, ۳۵, ۳۶]	استحکام، پایداری امنیت و پروتکل‌های زیاد ارتباطی و ناهمگونی این ارتباطات
ایمنی	[۳۱, ۳۵, ۳۷]	ایمنی فیزیکی اشیاء، دسترسی فیزیکی و قابلیت خود ایمنی
شبکه و امنیت	[۲۵, ۳۱, ۳۳]	شبکه به‌واسطه ارتباطات و گستردگی و تنوع ارتباطات نیز از نگرانی‌ها است
امنیت	[۳۱, ۳۲, ۳۴]	حفظ امنیت به‌صورت مستقل از چالش‌های اینترنت اشیاء است
اعتماد	[۲۵, ۳۳, ۳۵]	مکانیسم‌های اعتماد
محرمانگی و رمزنگاری	[۲۵, ۳۱, ۳۳]	حفظ محرمانگی و راهکارهای وابسته مانند رمزنگاری و محدودیت‌های اشیاء چالش‌هایی را ایجاد نموده است
امنیت اطلاعات	[۳۱, ۳۳]	افزایش حجم اطلاعات، تعداد اشیاء و ناهمگونی‌ها، حفظ امینت اطلاعات را در برابر اینترنت اشیاء قرار داده است
نام‌گذاری و مدیریت هویت	[۳۱, ۳۶]	احراز هویت‌ها، شناسایی و اشیاء و استاندارد گذاری در این زمینه از نگرانی‌های اینترنت اشیاء است.
تعداد زیاد اشیاء	[۳۳, ۳۵, ۳۶]	تعدد اشیاء و ارتباطات گوناگون و داده‌های زیاد تولیدشده و پردازش و کنترل حجم اطلاعات و ارتباطات نیز جز چالش‌ها است
مصرف انرژی	[۳۱, ۳۴, ۳۵]	توسعه اینترنت اشیاء موجب افزایش مصرف انرژی برق و بالا رفتن هزینه و تأثیر بر روی محیط خواهد شد که ارائه راهکارهای کنترل مصرف انرژی نیز از چالش‌های اینترنت اشیاء است
داده بزرگ و ابر	[۲۵, ۳۳, ۳۸]	افزایش حجم داده‌های تولیدشده و راهکارهای انتقال آن و ایجاد داده‌های بزرگ، نگرانی‌های در جمع‌آوری، نگهداری و کنترل پردازش این نوع داده‌ها را ایجاد کرده است
قابلیت کار دستگاه‌ها و اشیاء با یکدیگر	[۲۵, ۳۳, ۳۶]	جهت برقراری ارتباطات و حداکثر بهره‌وری از اینترنت اشیاء با توجه به گسترش تعداد و ناهمگونی اشیاء قابلیت کار با اشیاء متنوع را تحت تأثیر قرار داده است
ذخیره‌سازی	[۳۱, ۳۲]	افزایش حجم داده نگرانی ذخیره‌سازی در حجم داده‌های تولیدشده را در برداشته
ناهمگونی اشیاء	[۳۱, ۳۳, ۳۵]	افزایش تعداد ناهمگونی‌ها و نیاز به برقراری ارتباطات و انواع مختلف داده ایجادشده و مدیریت و پردازش آن‌ها

[3] Security
[4] Challenge
[5] Threat

آسیب‌پذیری‌های[۶] موجود در اینترنت اشیاء و خانه هوشمند موجب بروز تهدیدات متنوعی می‌شوند. برخی از این تهدیدات بر اساس پژوهش‌های انجام‌شده در جدول ۲ معرفی‌شده است.

جدول ۲ -معرفی تهدیدات

ردیف	عنوان تهدید	مراجع
۱	دست‌کاری ترافیک[۷]	[۳۹-۴۳]
۲	جعل هویت	[۴۰, ۴۱, ۴۳, ۴۴]
۳	استراق سمع	[۳۹, ۴۱-۴۵]
۴	بلاک کانال[۸] و جمینگ[۹]	[۴۰, ۴۲, ۴۳, ۴۵]
۵	تحلیل ترافیک[۱۰]	[۳۹-۴۳]
۶	ممانعت از سرویس	[۳۹, ۴۱, ۴۳-۴۶]
۷	باج افزارها[۱۱]	[۴۳]
۸	برنامه‌های تقلبی کنترل گوشی	[۳۹, ۴۳]
۹	فردی در میان[۱۲]	[۳۹, ۴۳, ۴۵]
۱۰	جعل	[۳۹, ۴۳]
۱۱	حمله اکتشافی[۱۳]	[۴۳, ۴۷]
۱۲	کدک‌های مخرب[۱۴]	[۳۹, ۴۳, ۴۴]
۱۳	حمله بازتاب[۱۵]	[۳۹, ۴۰, ۴۳]
۱۴	تکه‌تکه سازی[۱۶]	[۳۹, ۴۳, ۴۴, ۴۷]
۱۵	حمله تکثیر[۱۷]	[۳۹, ۴۳]

۳-روش پژوهش

در قسمت قبل به معرفی چالش‌ها، آسیب‌پذیری‌ها و تهدیدات امنیتی اینترنت اشیاء در حوزه کاربردی خانه هوشمند پرداخته شد. در ادامه به معرفی معماری‌های مرجع پرداخته می‌شود و ضمن انجام مقایسه بین قابلیت‌های آن‌ها، معماری مناسب برای ادامه کار پیشنهاد می‌شود. نگاشت آسیب‌پذیری‌ها و تهدیدات امنیتی بر اجزاء معماری انتخاب شده انجام شده و مجموعه نیازها جهت ارتقاء امنیت معماری در حوزه کاربردی خانه هوشمند مشخص می‌شود. با تغییر و تکمیل چارچوب امنیتی معماری انتخاب‌شده، راهکاری برای ارتقاء امنیت خانه هوشمند ارائه خواهد شد (شکل ۱).

شکل ۱- روش تحقیق

۳-۱- پیشنهاد معماری مناسب

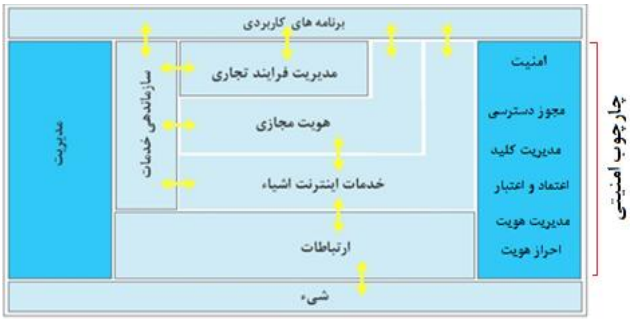
مراکز تحقیقاتی مختلف اقدام به ارائه راهکارهای جامعی با عنوان معماری‌های مرجع برای حل چالش‌های موجود درزمینهء اینترنت اشیاء نموده‌اند. معماری Wso2 باهدف فراهم نمودن خدمات ابری، معماری مرجع Korean باهدف ورود این فناوری به عرصه صنعت و معماری مرجع Chinese برای استانداردسازی این حوزه در کشور چین ارائه‌شده است [۴۸, ۴۹].

معماری مرجع IoT-A، باهدف بررسی پروتکل‌ها و منابع موجود، حصول اطمینان از سازگاری اشیاء و پروتکل‌های ارتباطی و همچنین ارائه راه‌کاری جامع برای کاربردهای مختلف اینترنت اشیا در اتحادیه اروپا پایه‌گذاری شد. این معماری شامل چند زیر مدل است که برای پیشبرد اهداف

[6] Vulnerability
[7] Tampering
[8] Block Channel
[9] Jamming
[10] Traffic Analyzing
[11] RansomWare
[12] Man in the middle
[13] Reconnaissance
[14] Malicious Codec
[15] Replay
[16] Fragmentation
[17] Replication

مقاله از مدل کاربردی[18] آن استفاده می‌شود. مدل کاربردی یک چارچوب انتزاعی برای درک گروه‌های کاربردی اصلی و روابط آن‌ها در محیط IoT-A است. این چارچوب معنای مشترکی را جهت استفاده در توسعه دیدگاه‌های کاربردی سازگار با IoT-A تعریف می‌کند [۵۰].

مدل کاربردی معماری مرجعIoT-A شامل هفت قابلیت عمودی و دو گروه عملکرد افقی مدیریت و امنیت است. چارچوب امنیت در مدل کاربردی از ۵ مؤلفه تشکیل‌شده است؛ که برای ارتقاء سطح امنیت در معماری، نیاز به بهینه‌سازی دارد. در شکل ۲ اجزاء تشکیل‌دهنده مدل کاربردی نمایش داده‌شده است [۵۰].



شکل ۲- مدل کاربردی و مؤلفه‌های چارچوب امنیتی معماری IoT-A [۵۰]

به منظور پیشنهاد معماری مناسب، با توجه به بررسی و مقایسه رویکرد معماری‌های معرفی‌شده، می‌توان دریافت که مدل و معماری ارائه‌شده توسط IoT-A با توجه به هدف، تنوع مستندات، گستردگی گروه تحقیق و گستره جغرافیایی آن یعنی اتحادیه اروپا، از جامعیت بیشتری نسبت به سه معماری دیگر برخوردار است. همچنین با توجه به نتایج حاصله از تحقیقات قبل که در جدول ۳ قابل‌مشاهده است، می‌توان دریافت که معماری IoT-A در مقایسه با معماری‌های دیگر دو مورد نیازهای کاربردی موضوع مقاله را هم‌زمان برآورده می‌کند [۵۱]؛ بنابراین به دلیل جامعیت معماری IoT-A و همچنین ارضای برخی الزامات کاربردی موردپژوهش، در ادامه از این معماری جهت ادامه روند پژوهش استفاده می‌شود.

جدول ۳- الزامات کاربردی معماری‌های مرجع [۵۱]

معماری			*IoT-A ARM*	*WSO2*	*Korean ARM*	*Chinese ARM*
نیاز کاربردی	الزامات پشتیبانی از برنامه‌ها	سرویس‌های قابل‌اعتماد و امن متصل به بدن انسان	√	-	-	√
	الزامات حفاظت امنیت و محرمانگی	ممیزی امنیتی	√	√	-	-

[18] Functional Model

۳-۲- نگاشت آسیب‌پذیری‌ها و تهدیدات در معماری مرجع IoT-A

این زیر بخش باهدف شناسایی نقاط ضعف امنیتی مؤلفه‌های مدل کاربردی معماری IoT-A، به نگاشت حملات، تهدیدات و آسیب‌پذیری‌ها بر روی هریک از مؤلفه‌ها پرداخته و نتایج را در جدول ۴ خلاصه می‌کند (جدول ۳).

جدول ۴- نگاشت آسیب‌پذیری‌ها و تهدیدات بر اجزای معماری IoT-A

نام مؤلفه	آسیب‌پذیری	تهدیدات و حملات
ارتباطات و زیرساخت	امنیت ارتباطات	استراق سمع / مسیریابی غلط/تحلیل ترافیک / دست‌کاری ترافیک/جعل هویت/ فردی در میان/ ارسال پیام منتخب/ حمله درج/حمله ack
	امنیت رمزنگاری	
هویت‌های مجازی	امنیت در ذخیره‌سازی	دست‌کاری داده/ تهدید حریم خصوصی / رمزگشایی و استخراج اطلاعات
	امنیت در رمزنگاری	
خدمات	امنیت خدمات بر روی شیء	کُدِک‌های[1] مخرب/ ابزار Xmpp
	امنیت دستگاه‌های پایانی	
	امنیت در رمزنگاری	
سازمان‌دهی خدمات	امنیت خدمات شبکه	DOS / دست‌کاری ترافیک / اغتشاش در مسیر/ تهدید حریم خصوصی
	امنیت ارتباطات	
مدیریت فرایندها	امنیت ارتباطات	دست‌کاری دستگاه/ جایگزینی میان‌افزار/ حمله اکتشافی
	محدودیت نرم‌افزار	
	امنیت خدمات ابری	
	امنیت شرکت ابری	
امنیت	امنیت نرم‌افزار و میان‌افزار	رمزگشایی و استخراج اطلاعات/ جعل هویت / فردی در میان
مدیریت	امنیت نرم‌افزار و میان‌افزار	تحریف ساعت Jamming/GTS بلاک کانال
	امنیت خدمات شبکه	/برنامه تقلبی کنترل از راه دور/ ارسال پیام منتخب /DOS
	ناهمگونی دستگاه‌ها	
	امنیت ارتباطات	
	محدودیت قابلیت توسعه	

۳-۳- نیازهای امنیتی خانه هوشمند

پس از بررسی تهدیدات و آسیب‌پذیری‌ها و نگاشت آن‌ها در مؤلفه‌های معماری، شناخت نیازها جهت بهبود وضعیت امنیت الزامی است. در همین راستا مطالعه و بررسی جهت شناخت نیازهای امنیتی به انجام رسید که نتیجه آن در جدول ۵ قابل‌مشاهده است. به‌کارگیری یا قالب مؤلفه امنیت معماری مرجع است.

بهبود عملکرد مکانیسم‌های امنیتی در هر یک از این مؤلفه‌ها موجب ارتقاء امنیت در حوزه کاربرد خانه هوشمند خواهد شد؛ بنابراین هدف اصلی این مقاله ارائه راهکارهایی جهت تأمین نیازهای امنیتی ذکرشده در قالب مؤلفه امنیت معماری مرجع است.

جدول ۵- نیازهای امنیتی خانه هوشمند

عنوان نیازمندی	مراجع
احراز هویت	[۳۱]
مدیریت هویت	[۴۱]
حریم خصوصی	[۳۱, ۴۱]
دسترس‌پذیری	[۳۱] [۴۱]
مقاوم بودن	[۳۱, ۴۱, ۴۲]
حفاظت اطلاعات	[۳۱]
کنترل دسترسی	[۳۱]
تفویض اختیار	[۳۱]
اعتماد	[۴۱]

۳-۴- راهکار پیشنهادی برای ارتقاء امنیت

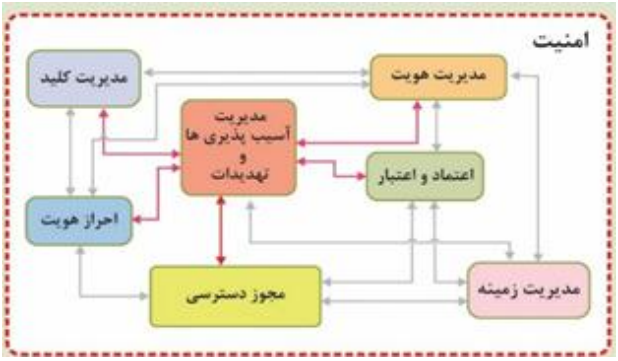
مدل کاربردی معماری مرجع IoT-A، مجموعه‌ای از مؤلفه‌ها را با درجه مشخصی از انتزاع به‌عنوان یک چارچوب امنیتی ارائه می‌کند. مدل مذکور به توسعه‌دهندگان این امکان را می‌دهد تا با توجه به حوزه کاربرد، رویکردهای متنوعی را در پیاده‌سازی داشته باشند. لذا در این مقاله، با توجه به الزامات امنیتی ذکرشده، مدل انتزاعی فوق به شکلی تکمیل می‌شود که درجه امنیت در حوزه کاربردی خانه هوشمند ارتقاء یابد. جهت نیل به این هدف، مؤلفه مدیریت زمینه[19] به‌منظور جمع‌آوری، به‌روزرسانی و مدیریت صحیح اطلاعات مربوط به اشیاء موجود و ارائه اطلاعات صحیح و تازه به سایر مؤلفه‌های امنیتی موجود اضافه‌شده است. همچنین مؤلفه مدیریت آسیب‌پذیری‌ها و تهدیدات[20] جهت پایش حداکثری، کشف و مقابله با تهدیدات و آسیب‌پذیری‌ها به ۵ مؤلفه چارچوب امنیتی معماری اضافه‌شده است. مؤلفه صدور مجوز به نحوی تغییر پیداکرده تا دسترسی به منابع اطلاعاتی خانه هوشمند با رعایت هر چه بیشتر حریم خصوصی و حفظ امنیت ساکنین انجام شود. این تغییر باعث نظارت بیشتر در جهت امن‌تر شدن نحوه دسترسی سایر حوزه‌های کاربردی ازجمله حوزه سلامت از راه دور به خانه هوشمند خواهد شد. مؤلفه‌های چارچوب پیشنهادی با مؤلفه‌های چارچوب استاندارد IoT-A در جدول ۶ مقایسه شده است.

جدول ۶- مقایسه مؤلفه‌های چارچوب پیشنهادی با مؤلفه‌های چارچوب معماری IoT-A

مؤلفه‌های معماری	مؤلفه‌های پیشنهادی
احراز هویت	احراز هویت
مدیریت هویت	مدیریت هویت
مجوز دسترسی	مجوز دسترسی توزیع‌شده**
تبادل و مدیریت کلید	تبادل و مدیریت کلید
اعتماد و اعتبار	اعتماد و اعتبار
-	مدیریت آسیب‌پذیری‌ها و تهدیدات**
-	مدیریت زمینه**

۳-۵- تشریح راهکار پیشنهادی

این بخش به تشریح مؤلفه‌های چارچوب پیشنهادی می‌پردازد که در شکل ۳ نمایش داده‌شده است. همان‌طور که در جدول ۵ مشاهده شد دو مؤلفه مدیریت آسیب‌پذیری‌ها و تهدیدات و مدیریت زمینه به چارچوب مرجع اضافه‌شده و تغییراتی در نحوه صدور مجوز دسترسی داده‌شده است که در ادامه توضیح داده می‌شود.



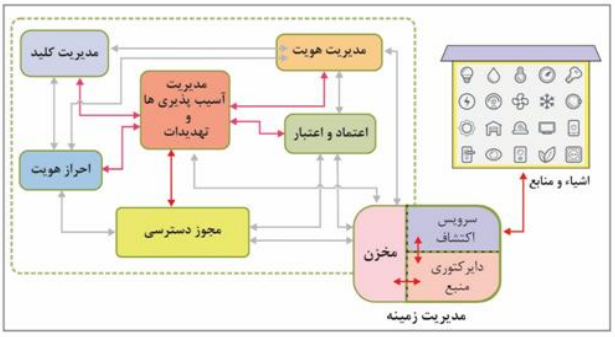
شکل ۳- مؤلفه‌های چارچوب پیشنهادی

۳-۵-۱- مدیریت زمینه

این مؤلفه مسئول شناسایی و حفظ اطلاعاتی است که به‌طور مداوم توسط کاربران و دستگاه‌ها تولید و ردوبدل می‌شود. این اطلاعات شامل خصوصیات اشیاء، خدمات و موجودیت‌های موجود در حوزه کاری است. مکانیسم پیشنهادشده برای شناسایی و ثبت اشیاء هوشمند و خدمات

[19] Context management
[20] Vulnerability & Threat Management

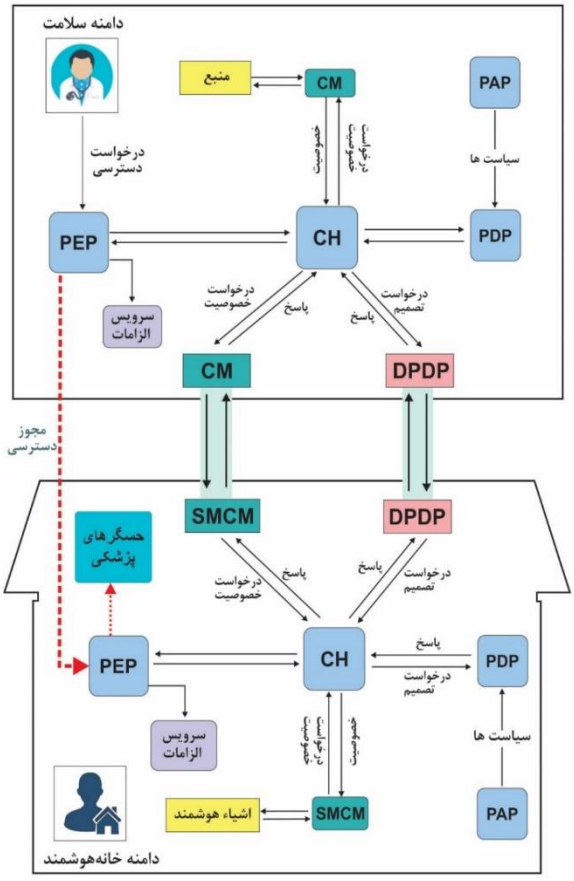
موجود با استفاده از سرویس اکتشاف[۲۱] و مجموعه‌ای از مخزن‌ها[۲۲] در سطح دامنه[۲۳] خواهد بود. اطلاعات پس از اکتشاف در دایرکتوری منبع[۲۴] ثبت و در مخزن ذخیره می‌شود. این سرویس‌ها به‌صورت توزیع‌شده بوده و به مراکز اصلی خود در سرویس‌دهنده اصلی مرتبط خواهند شد و اطلاعات هر دامنه را با توجه به سطح دسترسی و ضرورت به سیستم مرکزی انتقال خواهند داد. این روش امکان ادغام اشیاء هوشمند تحت فنّاوری‌های مختلف و پروتکل‌های گوناگون را میسّر می‌سازد[۵۲]. علاوه بر آن این مؤلفه تأمین‌کننده اطلاعات بروز و تازه برای سایر مؤلفه‌های امنیتی خواهد بود. نحوه ارتباط این مؤلفه با سایر مؤلفه‌ها در شکل ۴ نمایش داده‌شده است.



شکل ۴- مدیریت زمینه و ارتباط آن با سایر مؤلفه‌ها

۲-۳-۵- مجوز دسترسی توزیع‌شده

اجرای سیاست‌های کنترل دسترسی، نیاز به یک مکانیسم تصمیم‌گیری فراگیر و توسعه‌پذیر دارد. این مکانیسم می‌بایست دارای خصوصیاتی همچون قدرت اجرای ارزیابی‌های متنوع، سهولت در مدیریت سیستم‌ها و پشتیبانی از مفهوم الزامات باشد. همچنین قابلیت گسترش و تصمیم‌گیری در مورد کنترل دسترسی به‌صورت مشارکتی در چندین گره و یا اصطلاحاً توزیع‌شده را نیز داشته باشد. با توجه به تعامل خانه هوشمند با سایر حوزه‌های اینترنت اشیاء، روش صدور مجوز توزیع‌شده در چارچوب امنیتی ارائه‌شده، مدنظر قرارگرفته است. ترکیب فرایند احراز هویت و مجوز دسترسی در شکل ۵ قابل‌مشاهده است.



شکل ۵- مکانیسم ارزیابی و صدور مجوز به روش توزیع‌شده بین دو حوزه خانه هوشمند و سلامت

با توجه به شکل، درخواست‌کننده[۲۵]، درخواست دسترسی را به نقطه اجرای سیاست[۲۶] ارسال می‌کند. نقطه اجرای سیاست، درخواست دریافت اطلاعات را به نگه‌دارنده محتوا[۲۷] ارسال می‌کند. با توجه به اینکه حوزه تصمیم‌گیری در حوزه دیگری مانند خانه هوشمند است، نگه‌دارنده محتوا، جهت تکمیل اطلاعات در مورد خصوصیت[۲۸] منبع مورد درخواست،

21 Discovery service
22 Repository
23 Directory
24 Source Directory

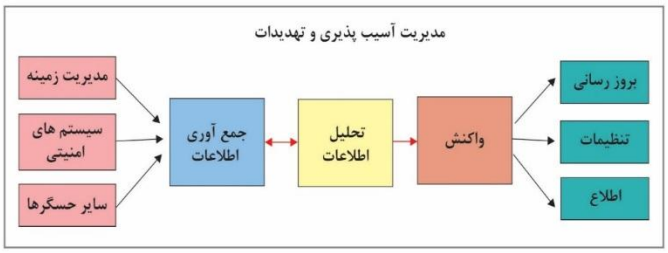
25 Requester
26 Policy Enforcement Point
27 Context Handler
28 Attribute

درخواستی را به مدیریت زمینه[۲۹] ارسال می‌کند. ضمناً جهت اخذ تصمیم مقتضی، پیامی را نیز به نقطه تصمیم‌گیری توزیع‌شده[۳۰] ارسال می‌کند. مدیریت زمینه، از نقطه متقابل خود یعنی مدیریت زمینه خانه هوشمند درخواست اطلاعات می‌نماید. نقطه تصمیم‌گیری توزیع‌شده نیز از نقطه مقابل خود در خانه هوشمند تقاضای ارائه تصمیم می‌نماید. نگه‌دارنده محتوا در خانه هوشمند کلیه درخواست‌ها را دریافت می‌نماید.

نقطه مدیریت سیاست[۳۱]، سیاست‌ها و مجموعه سیاست‌ها[۳۲] را در اختیار نقطه مدیریت تصمیم‌گیری[۳۳] قرار می‌دهد. نقطه تصمیم‌گیری بر اساس سیاست‌های موجود و خصوصیات منبع مورد درخواست، پاسخ نتیجه‌گیری لازم را به نگه‌دارنده محتوا[۳۴] ارسال می‌کند. نگه‌دارنده محتوا تصمیمات را به نقطه تصمیم‌گیری توزیع‌شده ارائه و خصوصیات مورد درخواست را نیز به مدیریت زمینه ارائه می‌کند. نگه‌دارنده محتوا اطلاعات ارسالی از خانه هوشمند را به نقطه اجرای تصمیم ارائه می‌دهد. نقطه اجرای سیاست‌ها[۳۵] الزامات را بررسی و در صورت تائید، مجوز دسترسی به منبع را می‌دهد، در غیر این صورت دسترسی را رد می‌کند.

۳-۳-۵- مدیریت آسیب‌پذیری و تهدیدات

این مؤلفه که به‌نوعی ایفاکننده نقش مرکز عملیات امنیت[۳۶] را برای خانه هوشمند است، جهت پایش، کشف آسیب‌پذیری‌ها و مقابله با تهدیدات با مدیریت متمرکز پیشنهادشده که متشکل از سرویس‌های پایش[۳۷]، جمع‌آوری اطلاعات، تحلیل و پاسخ است [۵۳]. این مؤلفه جهت عملکرد صحیح، نیاز دارد تا با مؤلفه مدیریت زمینه در ارتباط بوده و به جمع‌آوری اطلاعات تازه و قابل‌اطمینان از اشیاء و سرویس‌های موجود در خانه هوشمند بپردازد. پس از تحلیل اطلاعات امنیتی، تشخیص و واکنش مناسب به تهدید احتمالی انجام خواهد شد. هم‌چنین برای رفع آسیب‌پذیری‌های موجود در اشیاء و مقاوم‌سازی[۳۸] آن‌ها بکار می‌رود. به دلیل بالا بودن هزینه طراحی، اجرا و نگهداری این سرویس، استقرار آن در سمت سرویس ابری و ارائه‌کننده خدمات اینترنت اشیاء پیشنهاد می‌شود. نحوه فعالیت آن در شکل ۶ نمایش داده‌شده است.



شکل ۶-مدیریت آسیب‌پذیری و تهدیدات

۳-۶- تحلیل راهکار ارائه‌شده

در این مقاله الزامات و نیازمندی‌های امنیتی خانه هوشمند مبتنی بر اینترنت اشیاء ارائه شد. در مدل کاربردی معماری IoT-A یک چارچوب امنیتی کلی و با درجه مشخصی از انتزاع، جهت برقراری امنیت در نظر گرفته شده است. در این مقاله ضمن انجام تغییرات بر روی این مدل امنیتی، سعی شد تا چارچوبی جهت ارتقاء امنیت در حوزه کاربردی خانه هوشمند به‌عنوان راهکار جدید ارائه شود. این تغییرات شامل اضافه شدن دو مؤلفه مدیریت زمینه و مدیریت آسیب‌پذیری و تهدیدات و به‌کارگیری ارزیابی و صدور مجوز با روش توزیع‌شده و استفاده از مؤلفه جدید مدیریت زمینه بود. هدف از ارائه چارچوب جدید، پوشش حداکثری نیازهای امنیتی قیدشده، برای ارتقاء امنیت در خانه هوشمند بوده است. راهکارهای ارائه‌شده بر اساس نیازهای امنیتی در جدول ۶ نمایش داده شده است. این مقاله به‌صورت نظری و

[29] Context Management (CM)
[30] Distributed decision point (DPDP)
[31] Policy Administration Point (PAP)
[32] Policy sets
[33] Policy Decision Point (PDP)
[34] Context Handler (CH)
[35] Policy Enforcement Point (PEP)
[36] Security operation center
[37] Monitoring
[38] Hardening

از تجمیع راهکارهای موفق تحقیقات قبلی و با درجه‌ای از انتزاع ارائه شده است. لذا جهت ارزیابی مدل نظری ارائه شده از تحلیل و مقایسه استفاده می‌شود.

جدول ۶- نیازهای امنیتی و راهکارهای پیشنهادشده متناظر با آن

عنوان نیاز امنیتی	راهکار پیشنهادی
احراز هویت	مؤلفه احراز هویت توزیع‌شده
مدیریت هویت	مؤلفه مدیریت هویت
حریم خصوصی	مؤلفه مجوز دسترسی / مدیریت هویت/ اعتماد و اعتبار
دسترس‌پذیری	مؤلفه صدور مجوز
مقاوم بودن	مؤلفه مدیریت آسیب‌پذیری و تهدیدات
حفاظت اطلاعات	مؤلفه تبادل و مدیریت کلید/ صدور مجوز توزیع‌شده
کنترل دسترسی	مؤلفه صدور مجوز توزیع‌شده
تفویض اختیار	مؤلفه صدور مجوز توزیع‌شده
اعتماد	مؤلفه اعتماد و اعتبار

در ادامه به تحلیل هر یک از مؤلفه‌های پیشنهادی بر اساس کاربرد و هدف امنیتی آن پرداخته می‌شود. جدول ۷ نمایشگر کاربرد مؤلفه و اهداف امنیتی موردنظر که توسط آن مؤلفه تأمین می‌شود خواهد بود.

جدول ۷- مؤلفه‌های راهکار پیشنهادی به همراه کاربرد و هدف امنیتی آن

مؤلفه پیشنهادی	کاربرد مؤلفه	اهداف امنیتی موردنظر
مدیریت هویت	مدیریت هویت، نام مستعار و خط‌مشی‌های دسترسی مرتبط	حریم خصوصی کاربران حریم خصوصی خدمات
احراز هویت	تائید هویت موجودیت‌ها	تائید هویت مسئولیت‌پذیری
صدور مجوز	کنترل دسترسی بر خدمات	کنترل دسترسی خدمات محرمانگی داده‌ها یکپارچگی داده‌ها حریم خصوصی خدمات دسترس‌پذیری خدمات
	کنترل دسترسی بر زیرساخت	محرمانگی ارتباطات صحت ارتباطات عدم انکار
مدیریت و تبادل کلید	مدیریت و تبادل کلیدهای رمزگذاری	محرمانگی روبه‌جلو و عقب
مدیریت آسیب‌پذیری و تهدیدات	کشف آسیب‌پذیری‌ها و تهدیدات	محرمانگی یکپارچگی اطلاعات صحت اطلاعات حریم خصوصی امنیت ارتباطات
اعتماد و اعتبار	جمع‌آوری امتیاز اعتبار کاربر و محاسبه سطح اعتماد خدمت	اعتبار خدمات اعتماد خدمات حریم خصوصی
مدیریت زمینه	جمع‌آوری اطلاعات مربوط به اشیاء و منابع و خدمات	تازگی و صحت اطلاعات حریم خصوصی دسترس‌پذیری

تغییرات انجام‌شده در چارچوب امنیت معماری به شرح زیر است:

۱-۳-۶- مؤلفه مدیریت زمینه

به‌منظور جمع‌آوری اطلاعات اشیاء، ارتباطات و منابع خانه هوشمند، حفظ حریم خصوصی دسترسی‌پذیری بیشتر به منابع و صحت اطلاعات موردنیاز به چارچوب اضافه‌شده است. این مؤلفه در دو جایگاه، یکی خانه هوشمند و دیگری در خدمات ابری پیاده‌سازی می‌شود. این مؤلفه از چارچوب

امنیتی برای دسترسی به خدمات مبتنی بر اینترنت اشیاء در ساختمان‌های هوشمند الگوبرداری شده است. این مدل توسط یکی از مراکز تحقیقاتی معتبر پیاده‌سازی شده است [۲۵].

۲-۳-۶- مدیریت آسیب‌پذیری و تهدیدات

جهت کشف آسیب‌پذیری‌ها و مقابله متمرکز با تهدیدات، حفظ محرمانگی، صحت و یکپارچگی اطلاعات و بالا بردن امنیت در ارتباطات و حفظ حریم خصوصی افزوده‌شده است. جایگاه این سرویس در خدمات ابری بوده و توسط ارائه‌کننده سرویس مدیریت می‌شود. ازنظر هزینه پیاده‌سازی برای کاربر بار مالی نداشته و بر روی خدمات ارائه‌شده محاسبه خواهد شد. عملکرد این سرویس همانند یک سرویس اطلاعات و مدیریت رخدادهای امنیتی[۳۹] [۳۱] خواهد بود. برای پیاده‌سازی این مؤلفه از مدل‌های معتبر می‌توان کمک گرفت [۲۵].

۳-۳-۶- ارزیابی و صدور مجوز دسترسی توزیع‌شده

به‌منظور کنترل دسترسی مناسب به خدمات و منابع و اشیاء به/از خانه هوشمند با حفظ حریم خصوصی و در نظر گرفتن پایین بودن توان منابع پردازشی تجهیزات خانه هوشمند ارائه گردیده است. به این جهت، پردازش‌های مهم و پیچیده به سرویس‌دهنده مستقر در خانه و یا سرویس ابری محول خواهد شد. ارزیابی و صدور مجوز توزیع‌شده به جهت حفظ محرمانگی اطلاعات ساکنین خانه هوشمند از اهمیت بالایی برخوردار است. به‌این‌ترتیب ارزیابی‌های مربوطه به خود دامنه محول شده و نتایج آن به سرویس ابری اعلام می‌شود. هزینه‌های مربوط به پردازش‌های پیچیده نیز بر عهده ابر سرویس‌دهنده خواهد بود. جایگاه و هدف از پیاده‌سازی هر یک از مؤلفه‌ها در جدول ۸ نمایش داده‌شده است.

جدول ۸ -جایگاه و روش پیاده‌سازی هر یک از مؤلفه‌های چارچوب امنیتی

مؤلفه پیشنهادی	روش پیاده‌سازی	جایگاه پیاده‌سازی	هدف از پیاده‌سازی
مدیریت هویت	توزیع‌شده	سرویس ابری خانه هوشمند	مدیریت متمرکز همه دامنه‌ها حفظ حریم خصوصی- محرمانگی اطلاعات
احراز هویت	توزیع‌شده	سرویس ابری خانه هوشمند	دامنه‌ها –منابع مدیریت متمرکز همه زیاد حفظ حریم خصوصی – محرمانگی اطلاعات
صدور مجوز	توزیع‌شده	سرویس ابری خانه هوشمند	مدیریت متمرکز- منابع زیاد حفظ حریم خصوصی – محرمانگی اطلاعات
مدیریت و تبادل کلید	طبق معماری	سرویس ابری خانه هوشمند	یکپارچگی و محرمانگی ارتباطات و اطلاعات ارتباطات امن بین دامنه کاربرد و ابر
اعتماد و اعتبار	طبق معماری	سرویس ابری خانه هوشمند	اعتماد و اعتبار بین کاربران و خدمات اعتماد و اعتبار بین کاربران و خدمات
مدیریت زمینه	توزیع‌شده	سرویس ابری خانه هوشمند	مدیریت صدور مجوز بین دامنه‌های کاربردی محرمانگی و حفظ حریم خصوصی
مدیریت آسیب‌پذیری و تهدیدات	متمرکز	سرویس ابری	مدیریت متمرکز تهدیدات و آسیب‌پذیری‌ها

[39] Security Information and event management

۳-۷- مقایسه نتایج

در ادامه مدل ارائه‌شده با راهکارهای موجود مقایسه خواهد شد. در ابتدا این مقایسه با مدل کاربردی امنیت معماری پیشنهادی و سپس با چارچوب‌های موجود امنیتی در این حوزه انجام خواهد شد.

۱-۳-۷- مقایسه با چارچوب امنیتی موجود در معماری IoT-A

چارچوب ارائه‌شده در معماری مرجع IoT-A دارای پنج مؤلفه استاندارد برای تأمین امنیت اجزاء معماری است. این مؤلفه‌ها طبق نیازهای استاندارد امنیتی طراحی‌شده و قابل پیاده‌سازی هستند. جدول ۹ مقایسه‌ای بین اهداف امنیتی تأمین‌شده توسط دو چارچوب امنیتی اولیه معماری و چارچوب پیشنهادی ارائه داده است.

جدول ۹ -مقایسه مؤلفه‌های امنیتی چارچوب معماری و پیشنهادی [۲۵, ۳۲]

مؤلفه امنیتی	اهداف امنیتی موردنظر	معماری	پیشنهادی
مدیریت هویت	حریم خصوصی کاربران	✓	✓
	حریم خصوصی خدمات	✓	✓
	مسئولیت‌پذیری	✓	✓
صدور مجوز	کنترل دسترسی خدمات	✓	✓
	محرمانگی داده‌ها	✓	✓
	یکپارچگی داده‌ها	✓	✓
	حریم خصوصی خدمات	✓	✓
	دسترس‌پذیری خدمات	✓	✓
	حریم خصوصی حوزه کاربرد	✓	✓
مدیریت و تبادل کلید	محرمانگی ارتباطات	✓	✓
	صحت ارتباطات	✓	✓
	عدم انکار	✓	✓
	محرمانگی روبه‌جلو و عقب	✓	✓
مدیریت آسیب‌پذیری و تهدیدات	مقاوم‌سازی	-	✓
	محرمانگی	-	✓
	یکپارچگی اطلاعات	-	✓
	صحت اطلاعات	-	✓
	حریم خصوصی	-	✓
	امنیت ارتباطات	-	✓
	امنیت برنامه‌های کاربردی	-	✓
اعتماد و اعتبار	اعتبار خدمات	✓	✓
	اعتماد خدمات	✓	✓
	حریم خصوصی	✓	✓
مدیریت زمینه	تازگی و صحت اطلاعات	-	✓
	محرمانگی اطلاعات حوزه کاربرد	-	✓
	دسترس‌پذیری اطلاعات	-	✓

۲-۳-۷- مقایسه با سایر پژوهش‌ها

در مقالات متعدد به موضوع آسیب‌پذیری‌ها، تهدیدات خانه هوشمند و اینترنت اشیاء پرداخته‌شده و یا راهکارهایی جهت امن سازی آن ارائه‌شده است. در این مقاله علاوه بر بررسی موضوعات فوق، به‌منظور ارائه راهکار استاندارد برای تأمین امنیت خانه‌های هوشمند از معماری مرجع IoT-A استفاده‌شده است. به‌کارگیری معماری مرجع اینترنت اشیاء در این پژوهش موجب ایجاد یک قالب واحد برای تمامی فعالیت‌ها و فرایندهای مربوط به این دامنه کاربردی خواهد شد. به این معنا که ارائه چارچوب امنیتی نه‌تنها موجب امن سازی دامنه کاربردی خانه هوشمند خواهد شد، بلکه کلیه فرایندها و سرویس‌ها و ارتباطات مبتنی بر معماری اینترنت اشیاء را پوشش خواهد داد.

مؤلفه مدیریت زمینه قبلاً در ساختمان‌های هوشمند بکار گرفته‌شده و کارایی آن آزموده شده است [۵۲]. در این مقاله با اندکی تغییر در نوع کاربرد، از مؤلفه فوق به‌عنوان تأمین‌کننده اصلی اطلاعات برای سایر مؤلفه‌های چارچوب امنیتی به‌منظور حفظ تازگی اطلاعات و جهت جلوگیری از برخی حملات استفاده‌شده است.

مؤلفه مدیریت آسیب‌پذیری و تهدیدات مشابه یک مرکز عملیات امنیت عمل می‌کند که به‌طور توزیع‌شده در بستر ابر و حوزه کاربرد پیاده‌سازی می‌شود. این مؤلفه با استفاده از سرویس‌های پایش، جمع‌آوری و تحلیل اطلاعات به امن سازی حداکثری حوزه کاربرد اقدام می‌کند. این روند با به‌کارگیری سیستم‌های مدیریت رخداد و رویدادهای امنیتی[۴۰] قبلاً در حوزه اینترنت اشیاء بررسی و آزموده شده است [۵۳].

۴- نتیجه‌گیری و پیشنهادها

این مقاله باهدف ارتقا امنیت در خانه‌های هوشمند مبتنی بر اینترنت اشیاء، به ارائه یک چارچوب امنیتی از طریق انجام تغییرات و اضافه کردن مؤلفه‌های لازم به چارچوب امنیتی معماری مرجع IoT-A پرداخته است. اضافه شدن مدیریت زمینه به مؤلفه‌های چارچوب امنیتی به شناسایی و جمع‌آوری اطلاعات منابع و اشیاء هوشمند و همچنین اطلاعات مربوط به پروتکل‌های ارتباطی خانه هوشمند کمک می‌کند. در چارچوب پیشنهادی تغییراتی در نحوه کار ارزیابی و صدور مجوز کنترل داده‌شده است به‌طوری‌که این مکانیسم با استفاده از مدیریت زمینه به‌صورت توزیع‌شده به‌صورت بهینه به فعالیت خود خواهد پرداخت. همچنین مؤلفه مدیریت آسیب‌پذیری و تهدیدات به این چارچوب اضافه‌شده که در مدیریت متمرکز امنیت کمک شایانی خواهد نمود. مدل ارائه‌شده با توجه به تحقیقات پیشین و جداول مقایسه و ارزیابی این مقاله، ازنظر تئوری موجب تأمین نیازهای امنیتی خانه هوشمند مبتنی بر معماری اینترنت اشیاءIoT-A می‌شود.

مطالعات انجام‌شده در این مقاله نشان می‌دهد که فقدان یک معماری استاندارد و مشترک برای این فنّاوری کاملاً محسوس است. با توجه به گستردگی زمینه فعالیت و پژوهش جهت ارائه روش‌های نوین و یا استانداردسازی در این حوزه اجرای طرح‌های مطالعاتی جامع‌تر پیشنهاد می‌شود. مؤلفه مدیریت هویت و احراز هویت در چارچوب ارائه‌شده با استفاده مکانیسم‌های پیشنهادشده توسط معماری مرجع پیاده‌سازی شده است. با توجه به ظهور و بروز شدن مکانیسم‌های ابری و استفاده روزافزون از آن‌ها در این زمینه، پیشنهاد می‌گردد برای تمرکز در مدیریت و ارتقاء امنیت در این زمینه و همچنین کاهش هزینه‌ها، از مدیریت هویت ابری[۴۱] یا شناسه به‌عنوان خدمت[۴۲] استفاده شود.

[40] SIEM (Security information and event management)

[42] Identity as a service

منابع

1. J. Zheng, C.D.S.R. Bisdikian, H. Mouftah, The internet of Things, IEEE Communications Magazine, 49(11) (2011) 30-31.
2. T. Fan, Y. Chen, A scheme of data management in the Internet of Things, in: 2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content, IEEE, 2010, pp. 110-114.
3. Y. Yu, J. Wang, G. Zhou, The exploration in the education of professionals in applied internet of things engineering, in: 2010 4th International Conference on Distance Learning and Education, IEEE, 2010, pp. 74-77.
4. Y. Huang, G. Li, Descriptive models for Internet of Things, in: Paper presented at the Intelligent Control and Information Processing (ICICIP), 2010 International Conference on, 2010.
5. K. Ashton, That ‘internet of things’ thing, RFID journal, 22(7) (2009) 97-114.
6. G.T. Ferguson, Have your objects call my objects, Harvard business review, 80(6) (2002) 138-144.
7. L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks, 54(15) (2010) 2787-2805.
8. G. Lawton, Machine-to-machine technology gears up for growth, computer, (9) (2004) 12-15.
9. A. Gandomi, M. Haider, Beyond the hype: Big data concepts, methods, and analytics, International journal of information management, 35(2) (2015) 137-144.
10. S. Zhang, S. Zhang, X. Chen, X. Huo, . Cloud computing research and development trend, in: Paper presented at the Future Networks. ICFN'10. Second International Conference on., 2010.
11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE communications surveys & tutorials, 17(4) (2015) 2347-2376.
12. A.K. Sangaiah, G. Li, A joint resource-aware and medical data security framework for wearable healthcare systems, Future Generation Computer Systems, 95 (2019) 382-391.
13. D. Vinodhan, A. Vinnarasi, IOT Based Smart Home, International Journal of Engineering and Innovative Technology (IJEIT), 10 (2016).
14. M. O’Neill, Insecurity by design: Today’s IoT device security problem, Engineering, 21(1) (2016) 48-49.
15. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges, Wireless Networks, 20(8) (2014) 2481-2501.
16. E. Nimmermark, A. Larsson, Comparison of IoT frameworks for the smart home, (2016).
17. G. Lobaccaro, S. Carlucci, E. Löfström, A review of systems and technologies for smart homes and smart grids, Energies, 9(5) (2016) 348.
18.H.K. Jonnalagadda, Secure Communication Scheme in Smart Home Environment, (2016).
19.F. Johari, The security of communication protocols used for Internet of Things, LU-CS-EX 2015-42, (2015).
20.F. Kausar, E. Al Eisa, I. Bakhsh, Intelligent home monitoring using RSSI in wireless sensor networks, International Journal of Computer Networks & Communications, 4(6) (2012) 33.
21.S. Marzano, The new everyday: Views on ambient intelligence, 010 Publ., 2003.
22.A. Saad al-sumaiti, M.H. Ahmed, M.M. Salama, Smart home activities: A literature review, Electric Power Components and Systems, 42(3-4) (2014) 294-305.
23.W. Granzer, W. Kastner, G. Neugschwandtner, F. Praus, A modular architecture for building automation systems, na, 2006.

24.M.A. Al-Qutayri, J.S. Jeedella, Integrated wireless technologies for smart homes applications, in: Smart Home Systems, IntechOpen, 2010.
25.B.L.R. Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, Journal of Cleaner Production, 140 (20.١٤٦٤-١٤٥٤ (١٧
26.T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, Security Challenges in the IP-based Internet of Things, Wireless Personal Communications, 61(3) (2011) 527-542.
27.G. Gan, Z. Lu, J. Jiang, Internet of things security analysis, in: 2011 international conference on internet technology and applications, IEEE, 2011, pp. 1-4.
28.M. Katagi, S. Moriai, Lightweight cryptography for the internet of things, Sony Corporation, (2008) 7-10.
29.S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE, 2011, pp. 1-5.
30.R. Roman, P. Najera, J. Lopez, Securing the internet of things, Computer, (9) (2011) 51-58.
31.M.M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: 2015 IEEE World Congress on Services, IEEE, 2015, pp. 21-28.
32.P. Sarigiannidis, E. Karapistoli, A.A. Economides, VisIoT: A threat visualisation tool for IoT systems security, in: 2015 IEEE International Conference on Communication Workshop (ICCW), IEEE, 2015, pp. 2633-2638.
33.H. Lin, N. Bergmann, IoT privacy and security challenges for smart home environments, Information, 7(3) (2016) 44.
34.Z.A. Almusaylim, N. Zaman, A review on smart home present state and challenges: linked to context-awareness internet of things (IoT), Wireless Networks, 25(6) (2019) 3193-3204.
35.I. Lee, K. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, 58(4) (2015) 431-440.
36.J. Bugeja, A. Jacobsson, P. Davidsson, On privacy and security challenges in smart connected homes, in: 2016 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2016, pp. 172-175.
37.S.C. Mukhopadhyay, N. Suryadevara, Internet of things: Challenges and opportunities. In Internet of Things (pp. 1-17), Springer, 2014.
38.M. Younas, Research challenges of big data, (2019).
39.O. Olayemi, V. Antti, H. Keijo, T. Pekka, Security issues in smart homes and mobile health system: threat analysis, possible countermeasures and lessons learned, (2017).
40.R. Billure, V.M. Tayur, V. Mahesh, Internet of Things-a study on the security challenges, in: 2015 IEEE International Advance Computing Conference (IACC), IEEE, 2015, pp. 247-252.
41.A. Riahi ,E. Natalizio, Y. Challal, N. Mitton, A. Iera, A systemic and cognitive approach for IoT security, in: 2014 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2014, pp. 183-188.
42.C. Lee, L. Zappaterra, K. Choi, H.-A. Choi, Securing smart home: Technologies, security challenges, and security requirements, in: 2014 IEEE Conference on Communications and Network Security, IEEE, 2014, pp. 67-72.

43.H.A. Abdul-Ghani, D. Konstantas, A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective, Journal of Sensor and Actuator Networks, 8(2) (2019) 22.
44.D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, G. Baldini, Security and privacy issues for an IoT based smart home, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2017, pp. 1292-1297.
45.M. Dabbagh, A. Rayes, Internet of things security and privacy, in: Internet of Things From Hype to Reality, Springer, 2019, pp. 211-238.
46.I. Yaqoob, E. Ahmed, M.H. ur Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the Internet of Things, Computer Networks, 129 (20 (۱۷ .٤٥٨-٤٤٤
47.T. Bhattasali, R. Chaki, N. Chaki, Study of security issues in pervasive environment of next generation internet of things, in: IFIP International Conference on Computer Information Systems and Industrial Management, Springer, 2013, pp..۲۱۷-۲۰٦
48.P. Fremantle, A reference architecture for the internet of things, WSO2 White paper, (2014).
49.S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, A vision of IoT: Applications, challenges, and opportunities with china perspective, IEEE Internet of Things journal, 1(4) (2014) 349-359.
50.I. FhG, S.H. SAP, E.H. HSG, C. Jardak, A.O. CEA, A. Serbanati, J.W. Walewski, Internet of things-architecture iot-a deliverable d1. 3–updated reference model for iot v1. 5 (2012).
51.A. Torkaman, M.A. Seyyedi, Analyzing IoT reference architecture models, International Journal of Computer Science and Software Engineering, 5(8) (2016) 154.
52.J.L. Hernández-Ramos, M.V. Moreno, J.B. Bernabé, D.G. Carrillo, A.F. Skarmeta, SAFIR: Secure access framework for IoT-enabled services on smart buildings, Journal of Computer and System Sciences, 81(8) (2015) 1452-1463.
53.N. Miloslavskaya, A. Tolstoy, New SIEM System for the Internet of Things, in: In World Conference on Information Systems and Technologies (pp. 317-32 (۷ Springer, Cham. April., 2019.

فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص: ۴۳- ۵۶

سامانه تشخیص ارقام فارسی در نوشتار هوایی مبتنی بر تصویر عمق

رضا ملکی* شهرام محمدی**

*دکتری برق- الکترونیک، دانشگاه زنجان، سازمان تنظیم مقررات و ارتباطات رادیویی، تبریز، ایران

** استادیار، دانشکده مهندسی برق، دانشگاه زنجان

تاریخ دریافت: ۱۳۹۸/۹/۱۸ تاریخ پذیرش:۱۳۹۸/۱۱/۰۵

چکیده

تشخیص دست‌نوشته از روی کاغذ، صفحه‌نمایش و یا در هوا از چالش‌هایی هستند که در بینایی ماشین وجود دارند. تشخیص نوشتار هوایی به خاطر سه‌بعدی بودن دارای چالش‌های زیادی است. در این کار تحقیقی تشخیص ارقام فارسی در نوشتار هوایی مدنظر است که در آن، کاربر ارقام صفر تا نه را در مقابل حس‌گر کینکت در هوا می‌نویسد و سامانه با استفاده از اطلاعات عمق حس‌گر قادر به تشخیص ارقام فوق است. در سامانه پیشنهادی، برای جداسازی دست و نوک انگشت از پس‌زمینه از روش خوشه‌بندی خودکار k-means، برای استخراج ویژگی از روش تغییر علامت شیب‌خط پیشنهادی و جهت تشخیص ویژگی و تعیین رقم از دسته‌بند مدل مارکوف مخفی (HMM) استفاده‌شده است. دقت تشخیص سامانه پیشنهادی برای ارقام فارسی با دیتابیس محلی و بااعتبار سنجی متقابل ۱۰ برابری ۹۸ درصد است. سامانه پیشنهادی با نتایج چندین کار مشابه مقایسه گردید، این مقایسه‌ها نشان می‌دهند که سامانه پیشنهادی به‌صورت نسبی بهتر از سامانه‌های تحت مقایسه کار می‌کند.

واژه‌های کلیدی: حس‌گر کینکت، تصویر عمق، تغییرات علامت شیب‌خط، مدل مارکوف مخفی

۱- مقدمه

پیشرفت‌های عظیمی در حوزه‌های فناوری محاسباتی، ارتباطی و نمایشگرها انجام‌شده‌اند؛ اما پیشرفت چندانی در حوزه تعامل با این تجهیزات، حاصل نشده است؛ بنابراین، لازم است تنگناهای موجود مرتفع شوند. این الزام باعث شده است که در چند سال گذشته حوزه تعامل انسان - کامپیوتر[1] (HCI) به یک حوزه تحقیقی فعالی تبدیل گردد. اگرچه در طراحی و ساخت صفحه‌کلیدها و موشواره‌ها پیشرفت‌های زیادی انجام‌شده است؛ اما هنوز این تجهیزات، مخصوصاً در تعامل با فضاهای سه‌بعدی جهت HCI مناسب نیستند. موشواره‌ها که دارای آزادی دوبعدی هستند نمی‌توانند فضای سه‌بعدی را تقلید نمایند. استفاده از ژست‌های دست، جایگزین جذاب و طبیعی برای تجهیزات واسط دوبعدی در محیط‌های مجازی هستند. یک ژست به‌عنوان حرکت فیزیکی دست، بازو، صورت و بدن باهدف انتقال اطلاعات بامعنی تعریف می‌شود [۱]. طبق تحقیقی که انجام‌شده است، دست به‌صورت گسترده‌ای در مقایسه با سایر اجزای بدن جهت تعامل استفاده می‌شود [۲]. ژست‌های دست توسط تجهیزات تماسی و غیر تماسی قابل‌تشخیص هستند. تجهیزات غیر تماسی به خاطر طبیعی

1. Human-Computer Interaction

نویسنده عهده‌دار مکاتبات: رضا ملکی r.maleki@znu.ac.ir

بودن تعامل، ارجحیت بالاتری برای کاربر و محققین دارند. از مهم‌ترین کاربردهای تعامل با تجهیزات غیرتماسی نوشتار هوایی[1] است که مانند صفحه‌کلید سه‌بعدی عمل می‌کند. سامانه تشخیص نوشتار هوایی در محیط‌هایی که امکان استفاده از موشواره و صفحه‌کلید وجود ندارد مانند محیط‌های روغنی، گازی قابل‌استفاده است. سامانه تشخیص نوشتار هوایی می‌تواند کاراکترهای خیلی بیشتری نسبت به صفحه‌کلید عادی منتقل کند. این سامانه می‌تواند در حوزه بازی و گیم، صدور دستورات کنترلی، تعامل با ربات و ماشین‌ها به‌صورت گسترده استفاده گردد. در حوزه تشخیص نوشتار هوایی کاراکترهای فارسی کار معتبری تابه‌حال گزارش نشده است؛ بنابراین، در کار حاضر تلاش و تمرکز ما روی تشخیص نوشتار هوایی ارقام فارسی صفرتا نه است و در کارهای آینده روی تشخیص حروف فارسی، اعداد و کلمات و عبارت‌های فارسی نوشته‌شده در هوا متمرکز می‌شویم.این مقاله به‌صورت زیر تنظیم‌شده است. در بخش دوم کارهای مرتبط با تشخیص نوشتار هوایی کاراکترها بیان می‌شود. در بخش سوم الگوریتم‌های استفاده‌شده در بلوک‌های ساختاری سامانه تشریح می‌گردد. در بخش چهارم نتایج عملی سامانه پیشنهادی بیان می‌گردد و در قسمت پنجم نتیجه‌گیری و کارهای آینده و در انتها مراجع ارائه می‌شوند.

۲- کارهای مرتبط با تشخیص نوشتار هوایی کاراکتر

برای حوزه تشخیص نوشتار هوایی مقالات و سامانه‌های زیادی گزارش شده‌اند. استفان و همکاران از یک دوربین رنگ با وضوح ۲۴۰×۳۲۰ و دسته‌بند DSTW[2] برای شناسایی نوشتار هوایی ژست‌های دست ارقام انگلیسی استفاده کردند [۳]. استرن با استفاده از مفهوم MDS[3] (بخشی از ژست کاراکتر است که از بخش‌های ژست‌های دیگر متفاوت است) و دسته‌بندMDSLCS (توسعه‌یافته LCS است) ارقام انگلیسی نوشته‌شده در هوا را با حس‌گر PrimeSense 3D تشخیص دادند [۴]. المازین و همکاران برای تشخیص نوشتار هوایی اعداد انگلیسی از تصاویر رنگ و عمق دوربین استریو استفاده کردند [۵]. آنها برای انجام این کار از دسته‌بند HMM استفاده کرده‌اند. چون از تصویر رنگ برای جداسازی دست در کار آنها استفاده‌شده است؛ بنابراین، تشخیص ارقام در کار آنها به شرایط نوری محیط شدیداً وابسته است. در کار دیگری، تصاویر رنگ و عمق دوربین کینکت برای آشکارسازی ارقام انگلیسی صفرتا نه نوشته‌شده در هوا مقایسه می‌شوند [۶]. نتایج نشان می‌دهند که استفاده از تصویر عمق برای جداسازی دست و تشخیص ارقام، خطای کمتری را ایجاد می‌کند. نتایج ارزیابی سامانه‌های گزارش‌شده در حوزه تشخیص نوشتار هوایی نشان دادند که استفاده از تصویر عمق بجای تصویر رنگ دقت تشخیص بالاتری را ارائه می‌دهد؛ بنابراین از روی نتایج سامانه‌های گزارش‌شده فوق، در این کار تحقیقی از تصویر عمق ژست دست استفاده می‌شود که با استفاده از خوشه بند خودکار k-means، دست و نوک انگشت از پس‌زمینه در هر فریم جداسازی می‌شود و درنهایت، خط سیر از اتصال نقاط نوک انگشت هر فریم حاصل می‌گردد. روش استخراج ویژگی از خط سیر ژست دست نیز مهم‌ترین مسئله‌ای است که به‌صورت مستقیم روی دقت تشخیص ژست‌ها مؤثر است. مهم‌ترین ویژگی‌هایی که می‌توانند بردار ویژگی را از خط سیر استخراج کنند عبارت‌اند از: شیب منحنی، طول، نقاط ماکزیمم و می نیمم منحنی و تعداد نقاط برخورد با منحنی. بردار تشخیص مؤثر، بردار تشخیصی است که نسبت به‌اندازه، انتقال و چرخش ژست یا خط سیر مقاوم است، ابعاد بسیار کمی را ایجاد می‌کند و همچنین برای هر ژست منحصربه‌فرد است. در کار حاضر روشی پیشنهاد می‌شود که برای هر ژست دست، بردار تشخیص مؤثری را ایجاد می‌کند که این بردار به‌عنوان ورودی برای دسته‌بند HMM جهت تشخیص ژست دست استفاده می‌گردد. مشابه کارهای [۵] [۱۲-۱۳]،در سامانه پیشنهادی از دسته‌بند HMM استفاده‌شده است. HMM دارای تئوری ریاضی بسیار قوی است و درصورتی‌که خوب آموزش ببیند دارای دقت بالا در تشخیص کلاس‌ها است. زمان آموزش HMM نسبت به دسته‌بندهای دیگر مانند SVM و KNN بسیار بالا است؛ اما بعدازاین که آموزش دید زمان تشخیص نسبت به دسته‌بندهای فوق بسیار پایین‌تر خواهد بود.

---

1. Air-writing
2. Dynamic Space Time Warping
3. Most Discriminating Segments

۳- الگوریتم‌های بلوک‌های ساختاری سامانه

در حالت کلی سامانه‌های گزارش‌شده در حوزه تشخیص نوشتار هوایی از چهار بلوک اصلی تشکیل‌شده‌اند که عبارت‌اند از: ۱- بلوک اخذ داده: وظیفه تبدیل کردن ژست‌های دست به تصاویر را انجام می‌دهد. ۲- پیش‌پردازش و جداسازی دست: وظیفه استخراج دست، نوک انگشت و خط سیر ژست دست را دارد و همچنین نویز و پس‌زمینه را حذف می‌کند. ۳- استخراج ویژگی: وظیفه استخراج بردار ویژگی از خط سیر را دارد. ۴- دسته‌بند: شناسایی کاراکتر از روی بردار ویژگی را انجام می‌دهد. در پیاده‌سازی سامانه پیشنهادی دقیقاً چهار بلوک فوق در نظر گرفته‌شده است. شکل ۱ بلوک دیاگرام سامانه پیشنهادی را نشان می‌دهد؛ که در ادامه، ساختار سامانه پیشنهادی تشریح می‌گردد.

۳-۱- بلوک اخذ داده

در کار حاضر، حس گر استفاده‌شده برای تبدیل ژست دست به تصویر، دوربین کینکت XBOX360 مایکروسافت است. این حس‌گر در ابتدا توسط شرکت مایکروسافت برای کنسول بازی ساخته شده بود؛ اما محققان موفق شدند بعد از هک کردن درایورهای این حس‌گر، آن را برای کارهای تحقیقاتی و بخصوص در حوزه بینایی ماشین بکار بگیرند. خروجی دوربین کینکت تصاویر رنگ، عمق، اسکلتی و مادون‌قرمز است. در این کار تحقیقاتی از تصویر عمق کینکت که دارای ۳۰ فریم بر ثانیه با وضوح ۶۴۰×۴۸۰ است استفاده می‌شود. برای استفاده از داده‌های عمق حس‌گر کینکت، از کلاس‌ها و متدهای خاصی که در چارچوب Kinect SDK وجود دارند استفاده شد.

۳-۲- پیش‌پردازش و جداسازی دست

نوشتار هوایی توسط نوک انگشت یا به‌وسیله مرکز دست انجام می‌شود. برای استخراج نقاطی که نوشتار هوایی را انجام می‌دهند، لازم است که دست از پس‌زمینه تصویر در هر فریم استخراج شود. برای استخراج دست از پس‌زمینه روش‌های مختلفی در مقالات پیشنهاد شده است که مهم‌ترین این روش‌ها استفاده از آشکارسازی پوست در تصاویر رنگی، استفاده از اطلاعات عمق دست در تصاویر عمق، استفاده از نقاط مفصل در تصاویر اسکلتی و یا استفاده از اطلاعات رنگ و عمق همزمان دست در تصاویر رنگ و عمق هستند. تصاویر رنگی شدیداً به شرایط نوری محیط وابسته می‌باشند؛ بنابراین، آشکارسازی و جداسازی دست در تصاویر رنگی با تغییرات روشنایی و سایه‌ها دچار خطای زیادی است. استفاده تنها از تصاویر اسکلتی برای آشکارسازی دست نیز در شرایط خاص امکان‌پذیر است و معمولاً استفاده از تصویر اسکلتی برای آشکارسازی دست، همراه با تصاویر رنگی انجام می‌شود[۱۴]. تصاویر عمق در مقایسه با تصاویر رنگ جزئیات کاملی از ژست دست را انتقال نمی‌دهند؛ اما چون جزئیات انتقالی شامل نوک انگشت و مرکز دست را به‌صورت کامل شامل می‌باشند و این نقاط مستقل از تغییرات روشنایی محیط هستند گزینه بسیار عالی برای جداسازی دست در تصاویر هستند؛ به همین دلیل، در این کار تحقیقی از تصویر عمق ژست دست استفاده می‌شود. در اینجا، برای استخراج ناحیه دست از پس‌زمینه خوشه‌بند k-means تصویر عمق بکار گرفته‌شده است. خوشه‌بندی k-means روش تقریب سازی برداری است که نقاط تصویر را به چندین ناحیه اختصاص می‌دهد. هر ناحیه یک خوشه نامیده می‌شود. نقاط داخل هر خوشه برچسب‌های برابری دارند. چگونگی قرار دادن یک نقطه در داخل یک خوشه وابسته به نزدیک بودن آن نقطه به مرکز خوشه است. رابطه (۱) شرط قرار دادن نقاطی مانند X_p را در درون خوشه S_i نشان می‌دهد[۷]. در این رابطه k و m به ترتیب تعداد خوشه‌ها و مرکز خوشه‌ها هستند.

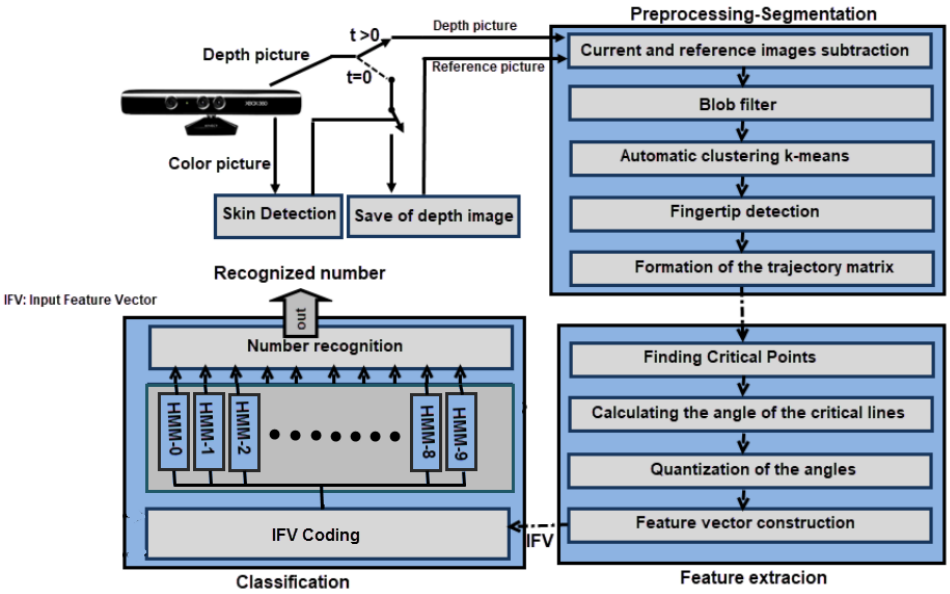
مرکز خوشه توسط متوسط گیری نقاط درون خوشه‌ها به دست می‌آید؛ که این موضوع در رابطه (۲) نشان داده‌شده است. در شروع، مرکز خوشه‌ها به‌صورت تصادفی روی تصویر انتخاب می‌شوند. سپس بروز رسانی خوشه‌ها با استفاده از

روابط (۱) و (۲) انجام می‌شود. در بروز رسانی، مراکز خوشه‌ها حرکت می‌کنند. زمانی که تعداد نقاط در داخل خوشه‌ها تقریباً ثابت ماند، حرکت خوشه‌ها متوقف می‌شود و خوشه‌بندی همگرا می‌شود.

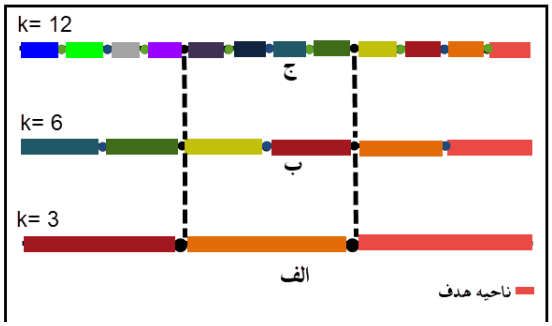
استخراج ناحیه هدف از تصویر کامل با استفاده از خوشه‌بندی k-means به‌صورت شدید وابسته به تعداد خوشه‌ها است. در فاصله نزدیک که ناحیه هدف بیشترین سطح تصویر را پوشش می‌دهد، ناحیه هدف می‌تواند با تعداد کمی از خوشه‌ها استخراج شود؛ اما زمانی که فاصله افزایش پیدا می‌کند با خوشه‌های کم نمی‌توان ناحیه هدف را استخراج کرد. شکل ۲ این موضوع را نشان می‌دهد. چنانچه از این شکل دیده می‌شود، جهت آشکارسازی صحیح ناحیه هدف باید تعداد خوشه‌ها متناسب با فاصله ناحیه هدف از دوربین باشد.

$$S_i^{(t)} = \{X_p : ||X_p - m_i^{(t)}||^2 \le ||X_p - m_j^{(t)}||^2 \forall_j, 1 \le j \le k\} \quad (1)$$

$$m_i^{t+1} = \frac{1}{S_i^{(t)}} \sum_{X_j \in S_i^{(t)}} X_j \quad (2)$$



شکل ۱- بلوک دیاگرام سامانه پیشنهادی برای شناسایی ارقام فارسی در نوشتار هوایی.



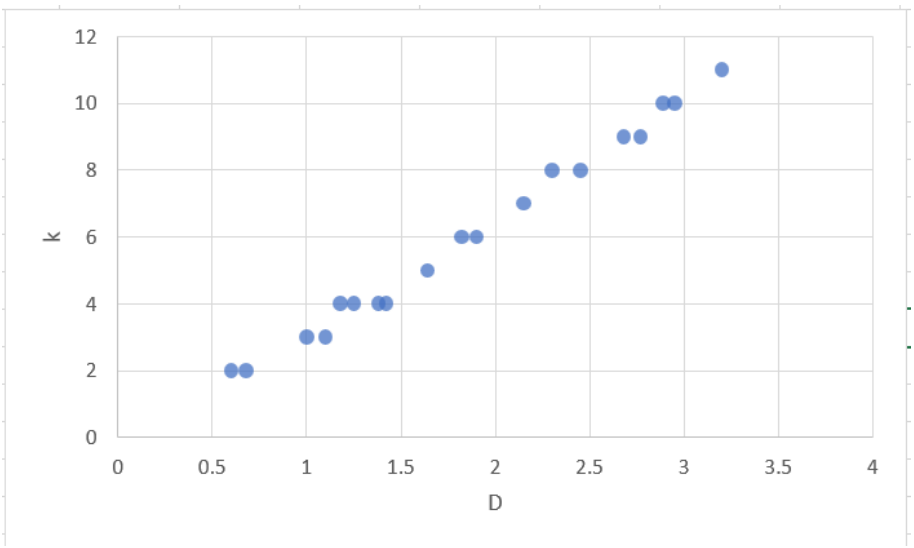
شکل ۲- ارتباط تعداد خوشه‌ها با فاصله ناحیه هدف از دوربین، الف) ناحیه هدف در فاصله نزدیک، ب) ناحیه هدف در فاصله دور، ج) ناحیه هدف در فاصله دورتر.

اگر تعداد خوشه‌ها متناسب با فاصله ناحیه هدف از دوربین نباشد امکان استخراج ناحیه هدف وجود نخواهد داشت. شکل ۳ این مطلب را نشان می دهد. دراین شکل ناحیه هدف که دست کاربر است درصورتی‌که $k=7$ باشد قابل‌استخراج است (شکل ۳.الف) اما اگر $k=3$ باشد علاوه بر دست، صورت کاربر نیز استخراج می‌شود (شکل ۳.ب) همچنین اگر $k=9$ انتخاب شود فقط قسمتی از دست استخراج می‌شود (شکل۳.ج). در این مقاله، برای پیاده‌سازی ارتباط بین تعداد خوشه‌ها و فاصله ناحیه هدف از دوربین، خوشه‌بندی خودکار k-means پیشنهاد می‌شود. در این روش، تعداد خوشه‌ها متناسب با فاصله کاربر از دوربین است و تعداد خوشه‌ها با دور شدن کاربر از دوربین به‌صورت خودکار افزایش پیدا می‌کند. نتیجه ۲۰ آزمایش عملی که توزیع آن در شکل ۴ آمده است، نشان داد که رابطه تعداد خوشه‌ها نسبت به نزدیک‌ترین نقطه به دوربین از رابطه (۳) به دست می‌آید. در این رابطه k، D و$[.]$ به ترتیب تعداد خوشه‌ها، نزدیک‌ترین فاصله دوربین از کاربر برحسب متر و جزء صحیح عدد هستند. رابطه (۳) از طریق درون‌یابی خطی با روش حداقل مربعات به‌دست‌آمده است [۱۵].

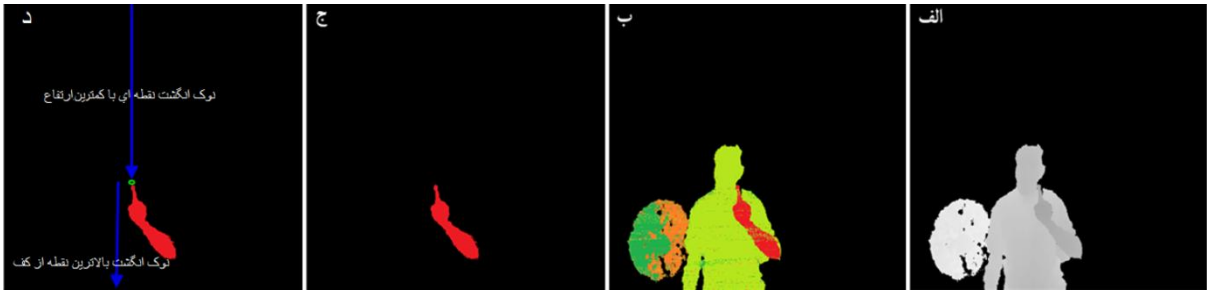
$$K = [D \times 3.56 - 0.1] \qquad (۳)$$

یک مثال از خوشه‌بندی خودکار در شکل ۵ نشان داده‌شده است. چنانچه از این شکل دیده می‌شود، برای یک شخص در فاصله ۱۵۹ سانتی‌متری از دوربین تعداد خوشه‌ها طبق رابطه (۳) برابر $k=[5.66-0.1]=5$ خواهد بود. در اینجا، خوشه‌بندی توسط روابط (۱) و (۲) انجام‌شده و کوچک‌ترین مقدار عمق در هر خوشه به‌عنوان برچسب آن خوشه انتخاب می‌شود. چون دست نزدیک‌ترین ناحیه به دوربین است بنابراین بعد از خوشه‌بندی خودکار، خوشه با برچسب کمینه انتخاب می‌شود. این خوشه، نزدیک‌ترین خوشه به دوربین است و ناحیه نوک انگشت نیز در این ناحیه خواهد بود. بالاترین نقطه این تصویر نسبت به کف که دارای کمترین پهنا است به‌عنوان نوک انگشت خواهد بود (شکل ۵.د). اتصال نقاط نوک انگشت پیداشده در فریم‌های متوالی، خط سیر نوک انگشت را تشکیل می‌دهد. این خط سیر درواقع همان ژست دست کاربر است که نوشتار هوایی ارقام را انجام داده است. در کار حاضر، برای حذف اشیایی که در مقایسه با دست به دوربین نزدیک‌تر است از تفریق هر فریم از تصویر مرجع استفاده‌شده است که در آن، تصویر مرجع تصویری است که قبل از نوشتار هوایی از صحنه گرفته می‌شود. خروجی تفریق ممکن است شامل یک سری حباب‌های کوچک ناشی از حرکت‌های جزئی اشیای فوق و یا انعکاست نوری باشد که برای حذف آن از فیلتر حباب استفاده‌شده است که این موضوع در شکل ۶ نشان داده‌شده است.

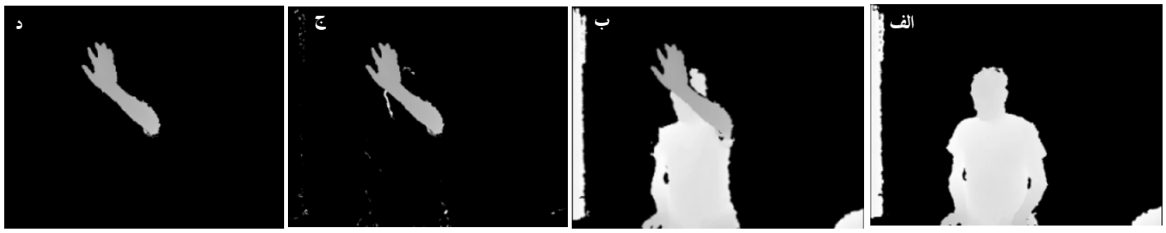
شکل ۳- نقش انتخاب k صحیح در خوشه‌بندی k-means برای استخراج ناحیه هدف، الف) خوشه‌بندی با تعداد خوشه صحیح (k=7)، ب) خوشه‌بندی با تعداد خوشه کمتر از خوشه صحیح (k=3)، ج) خوشه‌بندی با تعداد بیشتر از خوشه صحیح (k=9).



شکل ۴- توزیع تعداد خوشه‌ها نسبت به کمترین فاصله نقطه تصویر از دوربین



شکل ۵- نحوه استخراج نقطه نوک انگشت الف) تصویر عمق در فاصله ۱۵۹ سانتی‌متری از دوربین، ب) نتیجه خوشه‌بندی خودکار، ج) انتخاب نزدیک‌ترین خوشه به دوربین د) تعیین نقطه نوک انگشت.



شکل ۶- استفاده از فیلتر Blob برای حذف حباب های ریز در تصویر الف) تصویر مرجع ب) تصویر جاری، ج) تفریق تصویر جاری از تصویر مرجع، د) نتیجه اعمال فیلتر Blob.

۳-۳- استخراج بردار ویژگی

خط سیر استخراج‌شده دارای یکسری ویژگی است که این ویژگی‌ها، خط سیر مذکور را از خط سیرهای دیگر جدا می‌کند. طول، زاویه، شیب، نقاط شکست، سرعت تغییرات نقاط خط سیر از مهم‌ترین ویژگی‌های یک خط سیر هستند.

یکی از متداول‌ترین روش‌های استخراج بردار ویژگی که در بیشتر مقالات استفاده‌شده است روش کدهای زنجیره‌ای است [۵] [۸]. در این روش، زاویه خط اتصال نقاط مجاور نسبت به افق پیدا می‌شود و با سطوح کوانتیزه مقایسه می‌گردد و برچسب مربوط به آن تعیین می‌گردد. شکل ۷،

این روش را به‌صورت ساده نشان می‌دهد. چنانچه از شکل ۷.ج مشاهده می‌گردد، این روش ابعاد زیادی را برای بردار ویژگی ایجاد می‌کند و همچنین این روش شدیداً وابسته به اندازه خط سیر و نرخ فریم است. ما از این روش استفاده کرده و روشی را توسعه دادیم که ابعاد خیلی کمی را برای بردار ویژگی ایجاد می‌کند و همچنین بردار ویژگی که از این روش تولید می‌شود مستقل از اندازه، انتقال، چرخش خط سیر و نرخ فریم است. شکل ۷.د روش پیشنهادی را روی یک خط سیر نمونه نشان می‌دهد. در کار حاضر، برای استخراج ویژگی خط سیر از روش پیشنهادی آشکارساز تغییرات شیب[1] (SVD) استفاده می‌شود. در این روش، تانژانت‌های خطوطی که از نقاط قبلی و بعدی یک نقطه در روی خط سیر عبور می‌کنند ارزیابی می‌شوند. شکل ۸ این خطوط را برای نقطه (X1, Y1) نشان می‌دهد. در اینجا، نقاط (Xi,Yi) به ازای i=0, 1, 2 ,…,n مختصات نوک انگشت در فریم i از n فریم هستند که روی خط سیر قرار دارند. (XCj, YCj) مختصات نقطه بحرانی j روی خط سیر را نشان می‌دهند- α و β شیب یا تانژانت خطوط هستند. تانژانت‌ها از رابطه (۴) محاسبه می‌شوند.

$$\begin{cases} \alpha = \tan\theta 1 = f'(x)|_{(X1.Y1)} = \frac{Y1-Y0}{X1-X0} = \frac{\Delta Y0}{\Delta X0} \\ \beta = \tan\theta 2 = f'(x)|_{(X2.Y2)} = \frac{Y2-Y1}{X2-X1} = \frac{\Delta Y1}{\Delta X1} \end{cases} \quad (۴)$$

اگر علامت تانژانت‌ها در نقطه فرضی یکسان نباشند. این نقطه، به‌عنوان یک نقطه بحرانی عمل می‌کند. برای ارزیابی تغییرات علامت تانژانت‌ها از پارامتری بنام k استفاده می‌شود که در آن، $k = \alpha \times \beta$ است. اگر در یک نقطه، k منفی، صفر یا بی‌نهایت باشد این نقطه، یک نقطه بحرانی خواهد بود؛ اما اگر نقطه مورد ارزیابی نقطه بحرانی نباشد یعنی $k > 0$ باشد در این حالت، پردازش بر روی نقطه بعدی انجام می‌شود؛ بنابراین، (X1, Y1) = (X0, Y0)، (X2, Y2) = (X1, Y1) و (X3, Y3) = (X2, Y2) خواهد بود و این عمل ادامه پیدا می‌کند تا نقطه بحرانی (XC1, YC1) پیدا شود. پردازش در هر لحظه روی سه نقطه انجام می‌شود. شکل ۹، سه‌نقطه بحرانی E، F و M را که با استفاده از این روش پیداشده‌اند نشان می‌دهد. تانژانت‌های معکوس خطوط مابین نقاط A با E، E با F و F با M به ترتیب اولین، دومین و سومین مؤلفه از بردار ویژگی ورودی (IFV) هستند؛ بنابراین بردار ویژگی برای این خط سیر به‌صورت زیر خواهد بود:

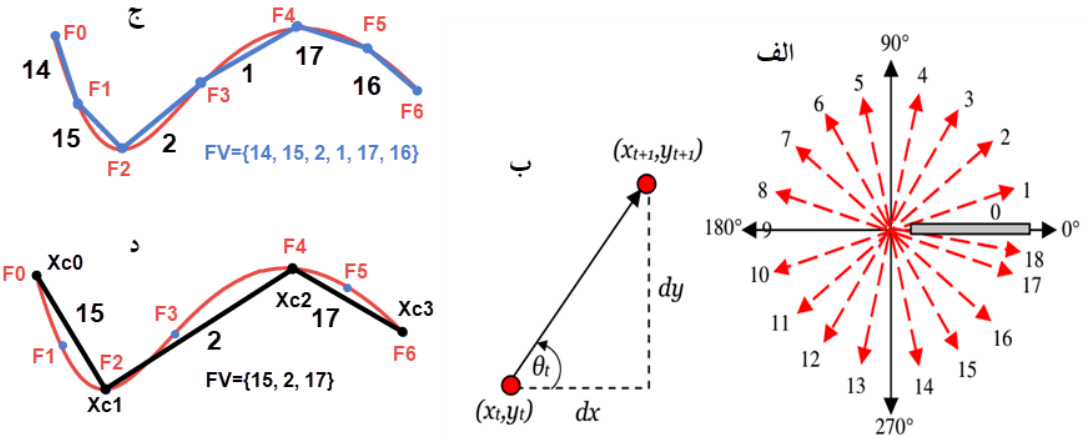
IFV= {θ1, θ2, θ3}

برای محدود کردن تعداد زاویه‌ها، می‌توان از کوانتایزر[2] یا تقریب کننده استفاده کرد [۸]. ساده‌ترین روش تقریب، تقسیم کردن کل زاویه ۰ تا ۳۶۰ درجه به قسمت‌های مساوی و اختصاص یک برچسب برای هریک از نواحی است. یک مثال نمونه از تقریب زاویه در شکل ۱۰ نشان داده‌شده است. در این شکل ناحیه ۳۶۰ درجه به قسمت‌های ۳۰ درجه تقسیم‌شده است؛ و برای هریک از نواحی و همچنین محورهای افقی و عمودی برچسب‌های ۱ تا ۱۶ استفاده گردیده است. استفاده از بلوک تقریب کننده باعث می‌شود که بردار با مؤلفه‌های زاویه‌ای به بردار با مؤلفه‌های عددی محدود تبدیل شوند. شکل ۱۱ بردار ویژگی که با روش SVD برای رقم ۵ به دست می‌آید را نشان می‌دهد. زاویه نرمال از تقسیم کردن مؤلفه‌های زاویه‌ای بردار ویژگی به ۳۶۰ درجه به دست می‌آید. بردار ویژگی که با روش SVD به دست می‌آید، به‌صورت کامل به اندازه و انتقال خط سیر مقاوم است. این در حالی است که به چرخش خط سیر فقط تا ۳۰ درجه مقاوم است. ارزیابی ریاضی نشان می‌دهد که برای مقاوم بودن به ۳۶۰ درجه، کافی است که مؤلفه‌های مجاور بردار ویژگی مطابق با رابطه (۵) از هم دیگر تفریق گردند. در اینجا $0 \le j < L$ است و L طول بردار IFV است. مقاوم بودن روش SVD با رابطه (۵) در قالب یک مثال در شکل ۱۲ نشان داده‌شده است. در اینجا، بردار ویژگی IFVD6 یک نسخه

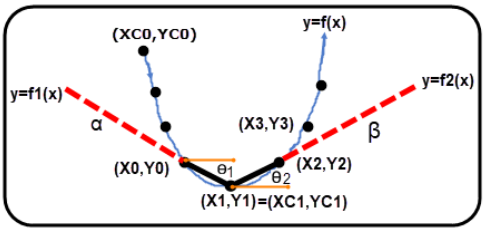
1.Slope Variations Detection
2.Quanrizer

اصلاحی از IFV6 است که مستقل از چرخش خط سیر خواهد بود. شکل ۱۳ استقلال بردار ویژگی را از اندازه، انتقال و چرخش خط سیر نشان می‌دهد.در این شکل با توجه به تغییرات اندازه خط سیر، تغییرات محل شروع خط سیر و همچنین چرخش خط سیر همواره بردار ویژگی به‌صورت ذیل است:

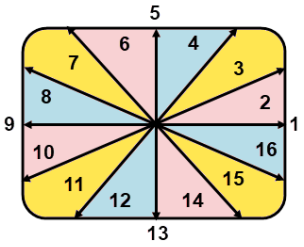
IFV2= {12, 9, 7, 14}



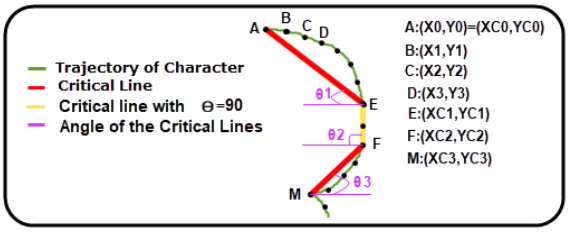
شکل ۷- مقایسه روش زنجیره کد با روش SVD پیشنهادی، الف) سطوح کوانتیزه برای تعیین برچسب خط، ب) روش تعیین زاویه خط دونقطه مجاور نسبت به افق، ج) استفاده از روش زنجیره کد برای تعیین ویژگی برای خط سیر نمونه، د) تعیین بردار ویژگی برای خط سیر نمونه با استفاده از روش پیشنهادی SVD



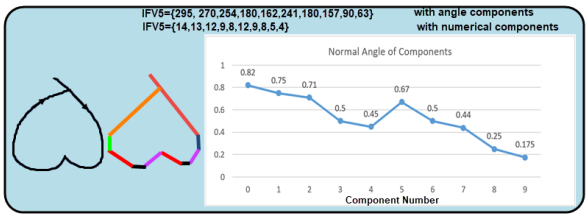
شکل ۸- خطوط گذرنده از نقاط مجاور نقطه فرضی برای تعیین نقطه بحرانی در روی خط سیر.



شکل ۱۰- تقریب سازی ۳۰ درجه‌ای.

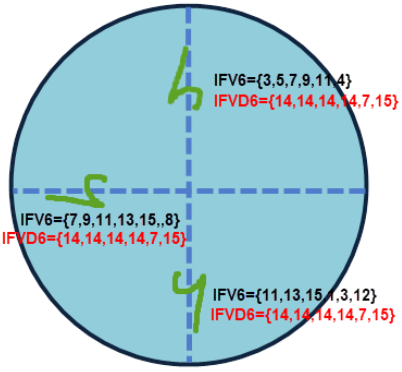


شکل ۹- سه‌نقطه بحرانی پیداشده روی خط سیر با روش SVD.

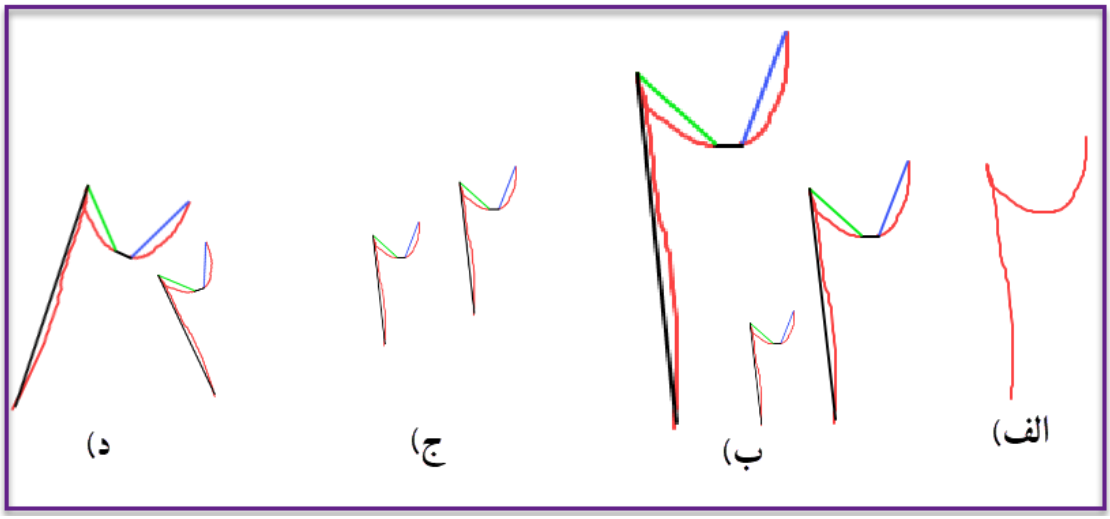


شکل ۱۱- خطوط بحرانی، بردارهای ویژگی و منحنی زاویه نرمال برای رقم ۵.

$$\begin{cases} \Delta IFV[j]=IFV[j]-IFV[j+1] & \\ IFVD[j]=\Delta IFV[j] & \text{if} \quad \Delta IFV[j]\geq 0 \;\&\delta\; 0\leq j\leq L-2 \\ IFVD[j]=\Delta IFV[j]+16 & \text{if} \quad \Delta IFV[j]<0 \;\&\delta\; 0\leq j\leq L-2 \\ IFVD[j]=IFV[0]-IFV[L-1] & \text{if} \quad (IFV[0]-IFV[L-1])\geq 0 \\ IFVD[j]=IFV[0]-IFV[L-1]+16 & \text{if} \quad (IFV[0]-IFV[L-1])<0 \end{cases} \tag{5}$$



شکل ۱۲- مقاوم بودن بردار ویژگی اصلاحی IFVD6 در چرخش‌های ۹۰ و ۱۸۰ درجه‌ای در جهت عقربه‌های ساعت برای رقم شش.



شکل ۱۳- مقاوم بودن بردار ویژگی به اندازه، انتقال و چرخش خط سیر، الف) خط سیر اصلی رقم ۲ ب) خطوط بحرانی و تغییر اندازه خط سیر، ج) تغییر محل خط سیر (انتقال)، د) چرخش خط سیر.

۴-۳- دسته‌بند HMM

مدل مارکوف مخفی (HMM) یک مدل ریاضی برای فرآیندهای استاتیکی است. HMM توسط پارامترهای زیر نشان داده می‌شود[۹].

- سری حالت‌ها $S=\{s_1, s_2,\ldots, s_N\}$ که در آن N تعداد کل حالت‌ها است.
- احتمال اولیه π_i برای هر حالت که $i=0,1,\ldots,N$ است و $\pi_i = P(s_i)$
- ماتریس گذر $A=\{a_{ij}\}$، $N\times N$ که a_{ij} احتمال گذر از حالت S_i به S_J که $1\leq i \leq N, J$ است؛ که جمع ورودی‌ها

در هر ردیف از ماتریس A برابر با یک است.

- سری انتشار (مشاهده) $O= \{o_1,o_2, \ldots, o_T\}$ که T طول مسیر ژست است.
- سری نمادهای گسسته $V= \{v_1, v_2, \ldots., v_M\}$ که M تعداد نمادهای گسسته را بیان می‌کند.
- ماتریس مشاهده N در M، $B=\{ b_{im} \}$ که b_{im} احتمال انتشار نماد v_m از حالت s_i است. جمع ورودی‌ها در هر ردیف ماتریس B برابر با یک است.

برای HMM سه نوع توپولوژی تعریف‌شده است.

۱. ارگودیگ: هر حالت به هر حالت دلخواهی می‌تواند وصل شود.

۲. مدل چپ به راست: هر حالت می‌تواند به خودش و یا به حالت‌های مستقیم وصل شود.

۳. مدل چپ به راست محدود: هر حالت می‌تواند به خودش و یا به حالت بعدی خود وصل شوند.

برای ساخت بلوک دسته‌بند برای هر رقم، باید تعداد حالت‌ها و تعداد نمادهای گسسته مشخص شوند. بقیه پارامترها یعنی ماتریس گذر A، ماتریس احتمال اولیه π و ماتریس مشاهده B از طریق آموزش با استفاده از نمونه‌های آموزشی به دست می‌آیند. انتخاب تعداد حالت‌ها برای بلوک‌های HMM موضوعی چالشی است که هنوز جوابی قطعی برای آن ارائه نشده است. در کار حاضر، حالت‌ها از روی بیشینه خطوط بحرانی هریک از ارقام مشخص‌شده‌اند. بیشینه خطوط بحرانی برای کلیه ارقام فارسی از روی نمونه‌های آموزشی مشخص می‌گردند. تعداد نمادهای گسسته برابر دامنه تغییرات مشاهدات هستند. درکار حاضر، چون از روش SVD برای استخراج بردار ویژگی استفاده می‌گردد؛ بنابراین، تعداد نمادهای گسسته ۱۶ (۱ تا ۱۶) نماد با تقریب ۳۰ درجه خواهد بود. توپولوژی HMM برای رقم فارسی دو در شکل ۱۴ نشان داده‌شده است. چنانچه از این شکل دیده می‌شود تعداد حالت‌ها ۸ و تعداد نمادها ۱۶ هستند و توپولوژی از نوع چپ به راست محدود است. در اینجا، برای پیدا کردن پارامترهای A، B و π از الگوریتم آموزش باوم– ولش روی نمونه های آموزشی استفاده‌شده است [۹].

فرآیند کلی کار برای به دست آوردن کلاس بردار ویژگی، به‌صورت ذیل است:

۱. آموزش هریک از بلوک‌های دسته‌بند هر رقم از روی نمونه‌های آموزشی جمع‌آوری‌شده برای آن کلاس از روی الگوریتم باوم- ولش.

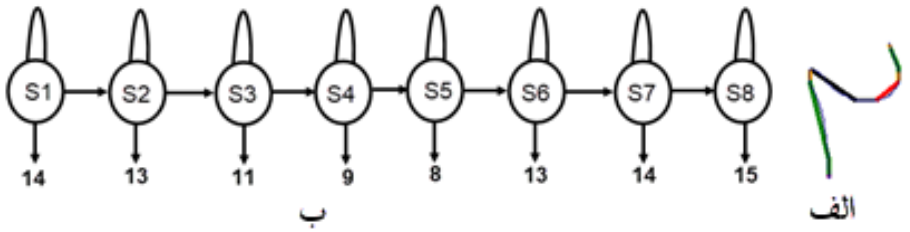
۲. به دست آوردن بیشینه احتمال کلاس‌ها برای بردار مشاهده از روی ضرایب پیشرو یا پسرو.

۳. انتخاب کلاسی که بالاترین احتمال را برای بردار مشاهده نشان می‌دهد.

در مورد دسته‌بندی HMM کارهای تحقیقی زیادی گزارش شده و کدهای برنامه‌نویسی برای پیاده‌سازی این دسته‌بند در قالب ماژول‌های نرم‌افزاری موجود است. در کار حاضر، برای پیاده‌سازی HMM از چارچوب Accord.net استفاده می‌شود. این چارچوب درواقع یک چارچوب یادگیری ماشینNET. است که ترکیبی از کتابخانه‌های پردازش تصویر و صوت است که در زبان C# نوشته‌شده است و چارچوب کاملی برای ساخت پروژه‌های بینایی ماشین با کمترین کدهای برنامه‌نویسی است. همچنین برای کاربردهای استاتیکی، پردازش سیگنال و حتی استفاده تجاری مناسب است. برای استفاده از این چارچوب کافی است که کتابخانه Statistics.DLL را به پروژه اصلی اضافه کرده و از کلاس‌ها و توابع آن استفاده کرد. استفاده از این ماژول حجم کد نویسی و همچنین زمان پردازش را بسیار کاهش می‌دهد.HMM چون از خاصیت جمع استفاده می‌کند و نسبت به جابجایی مؤلفه‌ها حساس نیست

بنابراین HMM برای بردار ویژگی ورودی مثلاً {۱۳و ۷و ۱۰} و {۱۰و ۱۳و ۷} احتمال یکسانی را در نظر می‌گیرد (تداخل بین برداری). این امر باعث می‌شود که دقت تشخیص دسته‌بند بسیار پایین باشد. برای حل این مشکل از کد کردن بردار ویژگی استفاده کردیم که در آن، به بردار ویژگی ارقام، موقعیت مؤلفه، طول بردار و تعداد مؤلفه‌های برچسب ۹ اضافه شد. شکل ۱۵ روش کد کردن مؤلفه با مقدار ۱ را نشان می‌دهد؛ بنابراین، برای مؤلفه با مقدار ۱ اگر طول بردار ویژگی ۲ و تعداد مؤلفه‌های ۹ قبل از مؤلفه مذکور، صفر و مؤلفه با مقدار ۱ اولین باشد مؤلفه کد شده طبق شکل ۱۵ برابر ۷ خواهد بود. کد کردن برای مؤلفه با مقدار ۲ نیز همانند شکل ۱۵ است فقط نقطه شروع از ۱۶۶ خواهد بود. در حالت کلی، مؤلفه کد شده هر مؤلفه بردار ویژگی، با اعمال ویژگی‌های ذکرشده، از رابطه (۶) به دست می‌آید. در این رابطه، C_IFV بردار ویژگی کد شده است. همچنین sum، L، com9 و i به ترتیب برابر $sum = \sum_{n=0}^{L-1} n$ ، طول بردار، تعداد برچسب‌های ۹ قبل از مؤلفه مفروض و شماره مؤلفه هستند. کد کردن بردار ویژگی باعث می‌شود که تداخلی بین بردارهای ویژگی حذف شود و درنتیجه دقت تشخیص دسته‌بند HMM افزایش پیدا کند. بردارهای کد شده برای {۱۳و ۷و ۱۰} و {۱۰و ۱۳و ۷} از روی رابطه (۶) به ترتیب {۱۹۹۶و ۱۰۰۳و ۱۴۹۵} و {۱۵۰۱و ۱۹۹۳و ۱۰۰۰}هستند و چنانچه دیده می‌شود تداخل بین برداری مابین آنها توسط کدینگ حذف می‌شود. ماکزیمم تعداد حالت برای ارقام فارسی از روی نمونه‌های آموزشی ۱۰ می‌باشد؛ بنابراین، طبق رابطه (۶) نماد یا سمبل بیشینه ۲۷۱۱ خواهد بود.

$$C\_IFV[i]= (sum\times3+1) +3\times i+com9[i]+(IFV[i]-1) \times 165 \quad (۶)$$



شکل ۱۴- مدل مارکوف مخفی الف) خطوط بحرانی رقم فارسی ۲، ب) توپولوژی HMM برای رقم فارسی ۲.

تعداد مولفه 9 قبل از مولفه	طول بردار	مولفه 0			مولفه 1			مولفه 8			مولفه 9		
		0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3									
	2	4	5	6	7	8	9						
	3	10	11	12	13	14	15						
	4	19	20	21	22	23	24						
	5	31	32	33	34	35	36						
	6	46	47	48	49	50	51						
	7	64	65	66	67	68	69						
	8	85	86	87	88	89	90						
	9	109	110	111	112	113	114	133	134	135			
	10	136	137	138	139	140	141	160	161	162	163	164	165

شکل ۱۵- جدول کد کردن مؤلفه بردار ویژه با مقدار ۱.

۴- نتایج عملی

درکار تحقیقی حاضر، کل پیاده‌سازی‌های نرم‌افزاری الگوریتم‌ها با استفاده از زبان برنامه‌نویسی C# و فایل‌های DLL مربوط به کتابخانه‌های Accord.net و A Forge.net انجام شده‌اند. سخت‌افزار استفاده‌شده لپ‌تاپ با مشخصات Core i7-1.73GHz اینتل است. برای

اندازه‌گیری دقت دسته‌بند، پایگاه داده محلی با ۱۰۰۰ نمونه آموزشی تشکیل گردید که این نمونه‌ها توسط ۱۰ کاربر که هر رقم را به تعداد ۱۰ بار در مقابل دوربین به‌صورت موفقیت‌آمیز انجام داده بودند جمع‌آوری‌شده است. نتایج عملی روی دسته‌بند HMM با بردار ویژگی کد شده و کد نشده با اعتبارسنجی متقابل ۱۰ برابری پایگاه داده محلی در جدول ۱ نشان داده‌شده است. این جدول نشان می‌دهد که دقت تشخیص متوسط HMM ارقام برابر ۹۸ درصد است که نرخ قابل قبولی برای یک سامانه تشخیص ارقام است. زمان تشخیص در HMM با بردار ویژگی کد شده به خاطر استفاده از ۲۷۱۱ سمبل، طولانی است؛ اما مدت‌زمان آموزش به خاطر این‌که سریع همگرا می‌شود پایین است. سامانه پیشنهادی با نتایج چندین سامانه مشابه که کار تشخیص ارقام انگلیسی را انجام می‌دهد مقایسه گردید که این مقایسه در جدول ۲ نشان داده‌شده است. جدول ۲ نشان می‌دهد که سامانه پیشنهادی به‌صورت نسبی بهتر از سامانه‌های گزارش‌شده عمل می‌کند. فریم‌هایی از نوشتار هوایی برای رقم ۳ در شکل ۱۶ نشان داده‌شده است.

جدول ۱- مقایسه دقت تشخیص متوسط HMM با بردار ویژگی کد شده و کد نشده.

نوع کلاس‌بندی	دقت	مدت‌زمان آموزش	مدت‌زمان تشخیص
HMM with SVD	68	5.3 s	20 ms
HMM with Coded SVD	98	4.5 s	62 ms

جدول ۲- مقایسه سامانه پیشنهادی با نتایج چندین کار مشابه گزارش‌شده.

روش	اعتبارسنجی متقابل دو برابری	اعتبارسنجی متقابل ۱۰ برابری
Kane and Khanna [10]	-	95.5
Feng [11]	86	100
Stern [4]	-	92.6
Proposed approach	92	98

شکل۱۶- فریم‌هایی از نوشتار هوایی رقم ۳.

۵- نتیجه‌گیری

برای تشخیص نوشتار هوایی ارقام فارسی با استفاده از تصویر عمق حس‌گر کینکت، سامانه‌ای پیشنهاد شد که در این سامانه برای استخراج دست و نوک انگشت از خوشه‌بندی خودکار k-means استفاده شد. استفاده از این روش علاوه بر افزایش دقت شناسایی، حساسیت شناسایی به تغییرات روشنایی محیط را نیز حذف می‌کند. برای استخراج ویژگی از خط سیر در این سامانه، از روش پیشنهادی تغییرات علامت شیب‌خط استفاده شد. مقاوم بودن در برابر انتقال، اندازه و چرخش خط سیر و تولید بردار

ویژگی منحصربه‌فرد با ابعاد کم از مهم‌ترین مزایای روش پیشنهادی در استخراج بردار ویژگی است. برای شناسایی خط سیر از روی بردار ویژگی از دسته‌بند HMM استفاده گردید. دقت تشخیص متوسط در HMM به خاطر تداخل بین برداری نمونه‌های آموزشی بسیار پایین است؛ بنابراین، برای افزایش آن از کدینگ برداری روی نمونه‌ها استفاده شد. نتایج عملی نشان می‌دهند که دقت تشخیص متوسط سامانه پیشنهادی ۹۸ درصد است. سامانه پیشنهادی با نتایج چندین کار گزارش‌شده مقایسه گردید و نتایج مقایسه نشان دادند که سامانه پیشنهادی عملکرد بهتری دارد. کارهای آینده ما روی تشخیص حروف، اعداد و کلمات فارسی با استفاده از حس‌گرهای سه‌بعدی جدید و ارزان متمرکز خواهد بود.

منابع

1. Mitra, S., Acharya, T. 2007. Gesture recognition: a survey. IEEE Trans Syst Man Cybern (SMC)Part C Appl Rev 37(3), pp:311–324.

2. Karam, M. 2006. A framework for research and design of gesture-based human computer interactions. PhD Thesis, University of Southampton.

3. Stefan, A., Athitsos, V., Alon, J., Sclaroff, S. 2008. Translation and scale invariant gesture recognition in complex scenes. in Proc. 1st ACM Int. Conf. PErvasive Technol. Related Assist. Environ., Art. no. 7.

4. Stern, H., Shmueli, M., Berman, S. 2013. Most discriminating segment Longest common subsequence (MDSLCS) algorithm for dynamic hand gesture classification. Pattern Recognit. Lett., vol. 34, no. 15, pp:1980–1989.

5. Elmezain, M., AlHamadi, A., Michaelis, B. 2009. Hand trajectory-based gesture spotting and recognition using HMM. In using HMM. In Proc. 16th IEEE Int.Conf. Image Process., pp: 3577–3580.

6. Doliotis, P., Stefan, A., McMurrough, C., Eckhard, D., Athitsos, V. 2011. Comparing gesture recognition accuracy using color and depth information. in Proc. 4th ACM Int. Conf. Pervasive Technol. Related Assist. Environ., Art. no. 20.

7. Mackay, D. 2003. Information Theory, Inference and Learning Algorithms. Cambridge University Press. pp. 284–292. ISBN 0-52 64298-1.MR 2012999.

8. Liu, N., Lovell, B. C., Kootsookos, P. J. 2003. Evaluation of HMM training algorithms for letter hand gesture recognition. Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology.

9. Rabiner, LR. 1989. A Tutorial on Hidden Markov Models and Selected Application in Speech Recognition. Proc. of the IEEE, Vol.77, No.2, pp:257—286

10. Kane, L., Khanna, P. 2017. Vision-Based Mid-Air Unistroke Character Input Using Polar Signatures. IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS.

11.Based Mid-Air Unistroke Character Input Using Polar Signatures. IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS.

11. Feng, Z., Xu, S., Zhang, X., Jin, L., Ye, Z. 2012. Real-time Fingertip Tracking and Detection using Kinect Depth Sensor for a New Writing-in-the Air System. The 4th International Conference on Internet Multimedia Computing and Service (ICIMCS), China.

12. Elmezain, M., Alhamadi, A., Appenrodt, J., Michaelis, B. 2008. A

Hidden Markov Model-Based Isolated and Meaningful Hand Gesture Recognition. PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY.

13. Liu, N., Lovell, B. C., Kootsookos, P. J. 2003. Evaluation of HMM training algorithms for letter hand gesture recognition. Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology.

14. Liu, F., Du, B., Wang, Q., Wang, Y., Zeng, W. 2017. Hand Gesture Recognition Using via Deterministic Learning. 29th Chinese Control and Decision Conference (CCDC)

۱۵. رضایی و ذهابی، ۱۳۸۹، اندازه‌گیری الکترونیکی، انتشارات دانش نگار، تهران

فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص: ۵۷- ۷۴

شناسایی و اولویت‌بندی پارامترهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات

(مطالعه موردی: شعب تامین‌اجتماعی استان گیلان)

اسدالله شاه‌بهرامی [*] رامین رفیع‌زاده‌کاسانی [**] حسین پوریوسفی‌درگاه [***]

* گروه مهندسی کامپیوتر، دانشکده فنی دانشگاه گیلان

** مدرس دانشگاه جامع علمی و کاربردی گیلان

*** گروه مدیریت فناوری اطلاعات، دانشگاه آزاد واحد الکترونیکی تهران

تاریخ دریافت: ۱۳۹۶/۰۴/۲۶ تاریخ پذیرش: ۱۳۹۷/۰۱/۱۸

چکیده

اطلاعات و حفاظت از آن یکی از ارکان مهم بقای سازمان‌های امروزی است از اینرو دستاوردهای مطالعاتی‌سیستم مدیریت امنیت اطلاعات(ISMS) ، حفاظت از اطلاعات را در سه مفهوم خاص محرمانه بودن اطلاعات، صحت وجامعیت اطلاعات و در دسترس بودن اطلاعات تعریف می‌کند و بسیاری از شکست‌های پیاده سازی ISMS را ریشه در مسائل سازمانی و بی‌توجهی به وضعیت آمادگی سازمان قبل از پیاده‌سازی آن می‌داند. لذا ارزیابی وضعیت و اولویت‌بندی مخاطرات امنیت اطلاعات و ایجاد دید کلی و سلسله مراتبی از آن، در استقرار موفق سیستم امنیت اطلاعات حائز اهمیت است. اما به لحاظ ابعاد و آثار و علل متعدد مخاطرات امنیت و با توجه به تعدد شاخص‌ها و پارامترهای تاثیرگذار پیاده‌سازی ISMS، لزوم استفاده از مدل‌های تصمیم‌گیری چند شاخصه را در ارزیابی و رتبه‌بندی آنها مطرح می‌نماید. در این پژوهش تلاش شده است عوامل موثر بر سیستم مدیریت امنیت اطلاعات را به دو گروه عوامل نرم و سخت طبقه‌بندی نموده و به منظور رتبه‌بندی دقیق و تمرکز بیشتر علی‌الخصوص در شرایط عدم قطعیت که در ذات اخذ تصمیمات انسانی است، به روش تحلیل سلسله مراتبی فازی(FAHP) اقدام گردید. بر این اساس و به کمک پرسشنامه به جهت کمی نمودن نتایج از نظرات خبرگان فن شامل خبرگان دانشگاهی، مدیران و کارکنان بخش فناوری اطلاعات شعب تامین اجتماعی استان گیلان به‌عنوان مطالعه موردی این پژوهش استفاده شده‌است. نتایج حاصل نشان می‌دهد، عوامل نرم شامل عوامل مدیریتی و فرهنگی/ اجتماعی نسبت به عوامل سخت شامل عوامل مالی و فنی/ فناورانه درسیستم مدیریت امنیت اطلاعات از اهمیت بیشتری برخوردار بوده و عوامل مدیریتی نسبت به سایر عوامل نرم و همچنین عوامل فنی/ فناورانه نسبت به سایر عوامل سخت دارای بیشترین اهمیت هستند.

واژه‌های کلیدی : امنیت اطلاعات، سیستم مدیریت امنیت اطلاعات، تحلیل سلسله مراتبی فازی، عوامل نرم، عوامل سخت

۱- مقدمه

ارائه سرویس مداوم و داشتن توانایی پاسخگویی به انتظارها، یکی از نیازمندی‌های کسب‌وکار مطمئن سازمانها در شرایط پر از تحول و مخاطرات امروزی است، به همین دلیل داشتن ساختار شبکه‌ای قوی، مؤثر و ایمن در سازمان‌ها بسیار مهم است. گسترش روزافزون استفاده از اینترنت، تبادلات اطلاعات درون سازمانی و برون سازمانی

نویسنده عهده‌دار مکاتبات: اسدالله شاه‌بهرامی shahbahrami@guilan.ac.ir

و هزینه‌های صرف شده برای یکپارچگی اطلاعات، کسب آمادگی کافی جهت مقابله یا اتخاذ تصمیمات مناسب در مقابل حوادث فیزیکی، جرائم سایبری و غیره در هر دو لایه زیرساخت و کاربرد فناوری اطلاعات، رهیافتی اجتناب‌ناپذیر برای تضمین پایایی کسب‌وکاراست [۲۶].

برای حل مسئله امنیت اطلاعات، سازمان نیازمند بکارگیری مجموعه گسترده‌ای از فناوری، دانش و قوانین سازمانی است و باید توجه داشت فناوری به تنهایی، قادر به حفاظت از سازمان نیست، چرا که امنیت اطلاعات یک مشکل صرفاً فنی نیست و اجزای کلیدی دیگر امنیت اطلاعات، شامل فرآیندها و کارکنان است که خود یک مسئله مدیریتی و کسب‌وکار است. به همین دلیل با تدوین اولین استاندارد مدیریت امنیت اطلاعات درسال۱۹۹۵، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات جایگزین نگرش فنی گردید [۲۷].

بر اساس این نگرش، هر سازمان برای تأمین امنیت فضای تبادل اطلاعات درون مجموعه خود براساس یک روش مشخص و برنامه‌ریزی شده به کنترل و نظارت بر پیدایش، جابجایی و تبادلات اطلاعات می پردازد وبدلیل نیاز به صرف زمان و هزینه زیاد و عدم امکان پیاده‌سازی یکباره سیستم مدیریت امنیت اطلاعات(ISMS)، لازم است امنیت در یک چرخه مداوم ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح تامین گردد [۱۵].

از طرفی مطالعات متعدد نشان داده است که شناسایی کلیه پارامترهای تاثیرگذار درپیاده سازی ISMS شامل مولفه های مدیریتی، محیطی، فنی، آموزشی، اقتصادی، ساختاری، فردی و فرهنگی و زیرمؤلفهٔ آن و نیز داشتن دید کلی و سلسله مراتبی از وضعیت موجود امنیت اطلاعات، در استقرار موفق سیستم امنیت اطلاعات موثر است. از اینرو برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات، رتبه‌بندی میزان تاثیرات عوامل یا موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات، در سازمان‌ها نقش بسزایی دارد [۱].

از اینرو هدف از این پژوهش، ایجاد سلسله مراتب و اولویت‌بندی عوامل موثر بر پیاده سازی سیستم مدیریت امنیت در سازمان موصوف به جهت کسب نتایج بهتر و مطلوبتر درتحقق رسالت امنیت اطلاعات است. در این راستا نظر به اینکه تعدادی از عوامل اساسی موفقیت پیاده سازی ISMS، عواملی نظیر حمایت مدیریت ارشد، خط مشی امنیتی سازمان، ایجاد مدیریت مرکزی با نفوذ (مدیرامنیت)، آگاهی ودانش کارکنان از امنیت اطلاعات، آگاهی وپایبندی به سیاست ها، رویه‌ها و عملیات سازمان، گزارش‌دهی وقایع امنیتی سازمان، سیاست ها و استراتژی‌های فناوری اطلاعات و امنیت سازمان، تعیین قلمرو امنیت سازمان، فرهنگ سازمانی، فرهنگ امنیت اطلاعات در سازمان، نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان، آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات، آموزش مداوم استفاده کنندگان در زمینه فناوری و امنیت اطلاعات، تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت افزار، نرم‌افزار و شبکه)، شناسایی و ارزیابی مخاطرات امنیت اطلاعات، مدیریت مخاطرات (ریسک‌ها) سازمان ، تدوین و نگهداری مستندات امنیت اطلاعات، نظارت، ارزیابی، کنترل و ممیزی داخلی، شناخت دارایی‌ها و تعیین ارزش آنها، تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات، تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و ارتباطات و امنیت اطلاعات وغیره لحاظ شده است نسبت به سنجش و طبقه بندی پارامترهایی مانند عوامل مدیریتی و عوامل فرهنگی در طبقه عوامل نرم و پارامترهایی مانند عوامل مالی و عوامل فنی/ فناورانه در طبقه عوامل سخت اقدام گردید [۸] و ادامه مطالب درقالب مباحث کمی وکاربردی، نتایج حاصل این تحقیق را به روش فرایند تحلیل سلسله مراتبی فازی نشان می‌دهد.

۲- مبانی نظری پژوهش

در این بخش تعاریفی که دراین مقاله در زمینه سیستمهای مدیریت امنیت اطلاعات مطرح هستند تعریف شده و به‌طور مختصر شرح داده می‌شوند.

۲-۱- امنیت اطلاعات: طبق تعریف استاندارد، امنیت اطلاعات به منظور تضمین سه اصل مورد نیاز است: ۱- محرمانگی: اطمینان از اینکه منابع فقط برای افراد مجاز سازمان در دسترس هستند. ۲- یکپارچگی: تامین دقت لازم

و کامل بودن منابع و داده‌ها و روش‌های پردازش آنها. ۳- دسترس‌پذیری: اطمینان از این که افراد مجاز در تمامی زمان‌های تعیین شده، به منابع و داده‌ها و سرمایه‌های موجود دس ترسی داشته باشند [۱۵].

۲-۲- سیستم مدیریت امنیت اطلاعات: سیستم مدیریت امنیت اطلاعات بخشی از سیستم کلی مدیریت به‌شمار می‌رود و مبتنی بر رویکرد ریسک تجاری بوده و هدف از آن ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات است [۱۶].

سیستم مدیریت امنیت اطلاعات یک مفهوم مستقل نیست، بلکه مشتقاتی از استانداردهای مختلف از جمله ISO/IEC17799 (سری استانداردهای BS7799 در امنیتIT) و ایزو ۹۰۰۰ در مدیریت کیفیت جامع است. بررسی و مرور مفاهیم و ادبیات موجود در زمینه مدیریت کیفیت جامع و مدیریت امنیت اطلاعات، نشان می‌دهد، عوامل مؤثر بر سیستم مدیریت امنیت اطلاعات در دو طبقه کلی عوامل نرم و عوامل سخت قابل طبقه‌بندی است [۲۰].

۲-۳- عوامل نرم: عوامل نرم آنهایی هستند که اندازه‌گیری و ارزیابی آنها نسبتاً دشوار بوده و بر بلندمدت تأکید دارند. فرهنگ، آگاهی، روابط‌کاری و انسانی، اعتماد، مقاومت، تغییرپذیری، آموزش، هماهنگی، امنیت، تصمیم‌گیری، سازماندهی و موضوعاتی از این دست، از جمله عوامل نرم به شمار می‌آیند [۲۱].

۲-۴- عوامل سخت : عوامل سخت، بیشتر سیستم‌گرا بوده و نقش حمایتی برای اعمال عوامل نرم دارند. زیرساخت‌های فنی و اقتصادی، تأمین هزینه‌های توسعه شبکه، سرمایه‌گذاری‌ها، تهیه نرم‌افزارها و سخت‌افزارهای مربوطه و مسائلی از این دست، از جمله عوامل سخت به‌شمار می‌آیند [۱۷].

۲-۵- مدل‌های تصمیم گیری چند شاخصه: مدل‌های تصمیم‌گیری چند شاخصه مجموعه‌ای از تکنیک‌ها هستند که اجازه می‌دهد طیفی از شاخص‌های وابسته به یک مبحث، امتیازدهی و وزن‌دهی شده و سپس رتبه‌بندی شوند و پتانسیل زیادی را به منظور کاهش دادن هزینه و زمان و بالابردن دقت در تصمیم‌گیری‌ها دارا می‌باشد و می‌تواند چارچوب مناسبی را برای بهبود مدیریت مخاطرات امنیت اطلاعات فراهم آورد[۲۸] مانند روش ویکور، روش الکتر، روش لین مپ، روش مجموع وزین وغیره.

اما یکی از پرکاربردترین و در عین حال مناسب‌ترین روش‌های تصمیم‌گیری چند شاخصه، روش فرایند تحلیل سلسله مراتبی است. به زبان ساده اگر ساختار مساله شامل سطوح مختلفی از شاخص‌های ارزیابی و به شکل سلسله مراتبی باشد و بخواهیم اهمیت تجمیعی و نهایی گزینه‌ها را با توجه به هر شاخص یا زیر شاخص بسنجیم و به اولویت آنها بپردازیم، روش فرایند سلسله مراتبی مناسب‌ترین روش تحلیل مساله است [۲]. و نیز به منظور رتبه‌بندی دقیق و تمرکز بیشتر بر مباحث امنیت اطلاعات علی‌الخصوص در شرایط عدم قطعیت که در ذات اخذ تصمیمات انسانی است، از تکنیک‌های تحلیل فازی کمک گرفته می‌شود که مدلی بنام تحلیل سلسله مراتبی فازی (FAHP) شکل می‌گیرد که نتیجه آن حصول نتایج مطلوب‌تر و دقیق‌تر و در نهایت بهبود رتبه‌بندی عوامل مخاطرات امنیت اطلاعات خواهد بود که سبب پیاده‌سازی موفق ISMS و اعمال کنترل‌های لازم در تمام سطوح سازمانی (راهبردی، تاکتیکی و عملیاتی) می‌گردد.

۳- پیشینه پژوهش (پیشینه تجربی)

با توجه به هدف تحقیق در خصوص بررسی عوامل تاثیرگذار بر سیستم مدیریت امنیت، به جهت ارتباط موضوع در ادامه برخی از تحقیقات انجام شده در این خصوص آورده شده است که همگی به این مطلب تاکید دارند که پیاده‌سازی اثربخش امنیت اطلاعات در سازمان‌ها، نیازمند رویکردی مدیریتی و یکپارچه براساس مدلهای ارزیابی و رتبه بندی شاخصها و عوامل مطرح در امنیت اطلاعات است.

تاج‌فر و دیگران(۱۳۹۳) در مطالعه ایی تلاش کرده‌اند موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات برحسب میزان اهمیت، رتبه‌بندی و میزان آمادگی سازمان در پیاده‌سازی سیستم مدیریت امنیت اطلاعات مشخص نمایند. نتایج پژوهش مهمترین مانع در راه پیاده‌سازی سیستم مدیریت امنیت اطلاعات را ناهمخوانی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات

دانسته و ترس کارکنان از سخت شدن فرآیندهای کار با اجرای سیستم مدیریت امنیت اطلاعات را کم‌اهمیت‌ترین مانع معرفی کرده است؛ ضمن آن‌که میزان آمادگی مدیریت اکتشاف در پیاده‌سازی سیستم مدیریت امنیت اطلاعات پایین‌تراز حد متوسط است[۱].

قرایی و آقا محی‌الدین(۱۳۹۳) در پژوهشی به معرفی امکان بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل تصمیم‌گیری چند شاخصه پرداختند و این مدل را روشی کاربردی جهت ارزیابی و بهبود اقدامات مخاطرات امنیت دانسته‌اند [۲].

بهرامی (۱۳۹۰) در پژوهشی ضمن معرفی برخی از استانداردهای معتبر در زمینه مدیریت امنیت اطلاعات و ارتباطات، با ارائه یک چرخه مدیریت امنیت مناسب، شاخص‌های مدیریت امنیت را جهت طراحی و پیاده‌سازی در یک سازمان بزرگ، معرفی نمودند [۴].

زنده‌دل نوبری (۱۳۸۹) مدلی برای رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها ارائه نمود. بدین منظور، پس از تعیین شاخص‌های امنیت اطلاعات در قالب دو دسته‌ی کلی فنی و مدیریتی و با توجه به معیارهای سه‌گانه‌ی «امنیت»، «ایمنی» و «پایداری»، نظرهای خبرگان فناوری اطلاعات بخش‌های انفورماتیک در سه سازمان مطالعه شد [۷].

آرام (۱۳۸۸) شاخص‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی را مورد سنجش قرار داد. نتایج پژوهش حاکی از تأثیرگذاری بیشتر عوامل انسانی از دیدگاه کارشناسان فناوری اطلاعات بود و پس از آن شاخص‌های مربوط به عوامل مدیریتی، فنی و مالی قرار داشت [۳].

صالحیان (۱۳۸۸) در پژوهشی به بررسی استقرار نظام مدیریت امنیت اطلاعات در دستگاه‌های دولتی پرداخت. نتایج پژوهش بیان می‌دارد، استقرار نظام مدیریت امنیت اطلاعات در سازمان‌های دولتی براساس استاندارد خانواده بی.اس.۷۷۹۹ نشان‌دهنده اهمیت پیاده‌سازی سیاست کنترلی مشخص برای افراد سازمان و حفاظت از اطلاعات سازمان است [۵].

طاهری (۱۳۸۶) در پژوهشی به مطالعه نقش عوامل انسانی در امنیت نظام اطلاعاتی پرداخت. نتایج نشان می‌دهد، داشتن چارچوبی مناسب برای ایفای درست نقش عوامل انسانی در امنیت نظام اطلاعاتی، به عنوان یکی از مولفه‌های مهم ایجاد امنیت، متغیرهایی مانند آموزش، فرهنگ و مهارت امنیتی و خودباوری‌های افراد به‌عنوان عوامل اثرگذار معرفی شده‌اند [۶].

تحقیقی دیگر توسط نیکرک و سُلمز (۲۰۰۹) شکل‌گیری فرهنگ امنیت اطلاعات در سازمان و تفاوت آن با فرهنگ سازمانی ارائه شد، و به این نتیجه رسید که در ایجاد فرهنگ امنیت اطلاعات علاوه بر مصنوعات و ارزش‌های پذیرفته شده و احساسات و اعتقادات کارمندان، دانش و آگاهی کارمندان از امنیت اطلاعات تأثیر بسزایی دارد [۲۲].

در تحقیقی که توسط چوی و دیگران (۲۰۰۸) در زمینه امنیت اطلاعات انجام شد، یافته‌ها حاکی از آن بود که افزایش میزان مدیریت آگاهی و دانش کاربران از امنیت اطلاعات تأثیری مستقیم بر نحوه مدیریت عمل و رفتار امنیتی کارکنان خواهد گذاشت و در نتیجه، عملکرد سازمان بهبود خواهد یافت [۱۲].

در تحقیق دیگری که توسط کریت‌زینگ و المی (۲۰۰۸) انجام شد، نمای کلی برای مدیریت امنیت اطلاعات (مستخرج از اسناد امنیت اطلاعات همچون استانداردها، گزارش‌ها و غیره) به دو قسمت موضوعات فنی و غیرفنی تقسیم شد، که از جمله موضوعات غیرفنی تأثیرگذار برای مدیریت امنیت اطلاعات، موضوع عوامل انسانی بود [۱۸].

در پژوهش دیگری توسط چانگ (۲۰۰۷) نیز نتیجه گرفته شد که فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. از جمله مؤلفه‌های سازمانی شامل همکاری، نوآوری، سازگاری، کارایی و تأثیربخشی بر روی اصول امنیت اطلاعات یعنی محرمانگی، در دسترس بودن، صحت و پاسخگویی بررسی شد و یافته‌ها نشان داد که تمام عوامل فرهنگ سازمانی برمؤلفه‌های امنیت اطلاعات تأثیر مثبتی دارد [۱۱].

کراگر و کرنی (۲۰۰۶) در تحقیقی در زمینه ارزیابی میزان آگاهی کارکنان از امنیت اطلاعات در شرکت‌های بین‌المللی معادن، نتایج مهمی در موارد مختلف امنیتی به دست آوردند. آنها سطوح آگاهی از امنیت اطلاعات را درسه سطح دانش، نگرش و رفتار تقسیم کردند و نواحی مورد ارزیابی در این سه سطح، شامل پایبندی به سیاست‌ها، ایجاد و نگهداری رمزهای مطمئن، اصول اینترنت و ایمیل، ایمنی تجهیزات سیار در انتقال اطلاعات، گزارش‌دهی وقایع امنیتی و اقدامات عملیاتی مناسب بود. این پژوهشگران پس از ارزیابی‌های خود به این نتیجه رسیدند که در کل، سطح آگاهی کارمندان از امنیت اطلاعات در حد متوسطی قرار دارد و به آموزش و توجه بیشتری نیاز است و برای بالا بردن سطح آگاهی از امنیت اطلاعات لازم است در هرکدام از حیطه‌های دانش، نگرش تلاش بیشتری انجام دهند [۱۹].

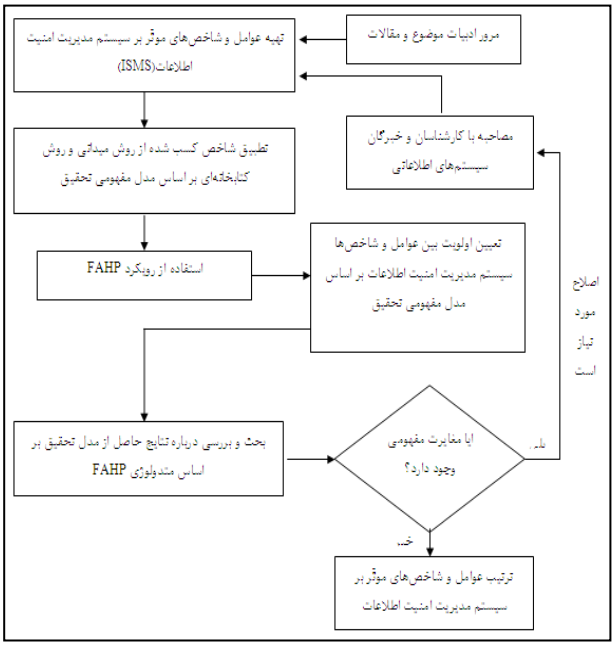
۴- مدل مفهومی

در این پژوهش با توجه به مبانی نظری و پیشینه مطالعات صورت گرفته و مصاحبه با متولیان امر و محدودیتهای محقق در سازمان مورد نظر، عوامل نرم موثر برسیستم مدیریت امنیت اطلاعات در قالب دو دسته کلی عوامل فرهنگی/ اجتماعی و عوامل مدیریتی و عوامل سخت نیز در دو دسته، عوامل فنی/ فناورانه و عوامل مالی طبقه‌بندی شده‌اند. شکل ۱ مدل مفهومی این پژوهش را نشان می‌دهد.

شکل ۱ – مدل مفهومی پژوهش، عوامل‌های نرم و سخت موثر بر سیستم مدیریت امنیت

۴-۱- روش‌شناسی پژوهش

پس از جمع‌آوری مهمترین عوامل و شاخص‌های تاثیر گذار بر سیستم مدیریت امنیت اطلاعات از طریق مرور پیشینه تحقیق، کتب، مقالات و پایان‌نامه‌ها، و منابع اینترنتی معتبر داخلی و خارجی و انطباق آن با مدل مفهومی پژوهش، پرسش‌نامه‌های مقایسات زوجی تنظیم شده سپس با استفاده از رویکرد فرآیند تحلیل سلسله مراتبی فازی این عوامل و میزان اهمیت آن مشخص شد. برای سنجش روایی پرسشنامه از نظر خبرگان دانشگاهی استفاده گردید، بدین ترتیب روایی پرسشنامه‌ها مورد تایید قرار گرفت و در تعیین پایایی ابزار جمع‌آوری داده‌ها از نرخ سازگاری استفاده شده است. شکل۲ فرایند اجرایی تحقیق را نشان می‌دهد.



شکل۲ – فرایند اجرایی تحقیق

باید توجه داشت در این فرآیند عامل مهم‌تر، کیفیت نظر خبرگان است. در این پژوهش برای برقراری روش فرآیند تحلیل سلسله مراتبی فازی (FAHP) از نظرات بیست خبره از خبرگان دانشگاهی و مدیران و کارکنان در حوزه مدیریت فناوری اطلاعات و مدیریت امنیت اطلاعات استفاده شده است. انتخاب نمونه‌های پژوهش، بر مبنای معیارهایی

همچون سابقه آنها در حوزه فناوری اطلاعات و مدیریت امنیت اطلاعات با حداقل پنج سال به بالا و شناخت عوامل مورد استفاده در این پژوهش بوده است.

۴-۲- فرایند تحلیل سلسله مراتبی فازی

یکی از روش‌هایی که در تصمیم‌گیری مورد استفاده قرار می‌گیرد، فرآیند تحلیل سلسله مراتبی فازی است. تمامی مقایسه‌ها در فرآیند تحلیل سلسله مراتبی، به‌صورت مقایسات زوجی انجام می‌شود [۱۳]. اعداد فازی استفاده شده در این فرایند معمولاً اعداد فازی مثلثی یا ذوزنقه‌ای است که به‌دلیل راحتی محاسبات از اعداد فازی مثلثی (T.F.N) استفاده می‌گردد. عدد فازی مثلثی به‌وسیله سه نقطه (l,m,u) نشان داده می‌شود. تابع عضویت یک عدد فازی مثلثی را می‌توان به‌وسیله معادله زیرنشان داد [۹].

$$\mu_x(x)=\begin{cases}(x-l)/(m-l), & l\le x<m\\ (u-x)/(u-m), & m<x\le u\\ 0 & otherwise\end{cases} \qquad (۱)$$

پاسخ خبرگان به مقایسه‌های زوجی، بر مبنا اصطلاحات (متغیر) زبانی و معیار نه نقطه‌ای صورت می‌گیرد. جدول ۱ اعداد فازی متناظر با اصطلاحات زبانی استفاده شده را نشان می‌دهد.

جدول۱- مقایسه‌های زبانی برای بیان درجه اهمیت

معکوس عدد فازی	مقیاس عددی فازی مثلثی	اصطلاحات(متغیر) زبانی	عدد
(۱/۹ ،۱/۹ ،۱/۹)	(۹،۹،۹)	شدیدا قوی	۹
(۱/۷ ،۱/۸ ،۱/۹)	(۷،۸،۹)	متوسط	۸
(۱/۶ ،۱/۷ ،۱/۸)	(۶،۷،۸)	بسیار قوی	۷
(۱/۵ ،۱/۶ ،۱/۷)	(۵،۶،۷)	متوسط	۶
(۱/۴ ،۱/۵ ،۱/۶)	(۴،۵،۶)	قوی	۵
(۱/۳ ،۱/۴ ،۱/۵)	(۳،۴،۵)	متوسط	۴
(۱/۲ ،۱/۳ ،۱/۴)	(۲،۳،۴)	نسبتا قوی	۳
(۱ ،۱/۲ ،۱/۳)	(۱،۲،۳)	متوسط	۲
(۱،۱،۱)	(۱،۱،۱)	دارای اهمیت	۱

پس از تبدیل جواب‌های خبرگان به اعداد فازی، برای یکپارچه‌سازی جواب‌های خبرگان از روشی که باکلی [۱۰] پیشنهاد داده، استفاده شده‌است. بنا به گفته باکلی برای تلفیق نظرات خبرگان از فرمول‌های زیر استفاده می‌شود. در اینجا U_{ij} یک عدد فازی مثلثی است [۱۱].

$$U_{ij}=(l_{ij},m_{ij},u_{ij}):l_{ij}\le m_{ij}\le u_{ij}\in[1/9.9]$$
$$l_{ij}=\min(B_{ijk})$$
$$m_{ij}=\sqrt[n]{\prod_1^b B_{ijk}} \qquad (۲)$$
$$u_{ij}=\max(B_{ijk})$$

قبل محاسبه وزن معیارها با استفاده از تحلیل سلسله مراتبی فازی ابتدا باید نرخ سازگاری پاسخهای خبرگان حساب شود [۲۳]. شاخص سازگاری (CI) و نرخ سازگاری (CR) را به‌منظور تأیید ماتریس مقایسات زوجی مطرح کرد.

A = ماتریس مقایسات زوجی — CR= نرخ سازگاری

RI= شاخص تصادفی — CI= شاخص سازگاری

λ_{Max} = بزرگترین مقدار ویژه ماتریس A — W= بردار وزنی

$$Aw=\lambda_{max}w$$
$$CI=\frac{\lambda_{max}-n}{n-1} \qquad (۳)$$
$$CR=\frac{CI}{RI}$$

ساعتی (۱۹۹۴) ذکر کرده‌است که بیشترین مقدار قابل قبول نرخ سازگاری باید مطابق جدول ۲ باشد.

جدول ۲-حداکثر مقدار قابل پذیرش نرخ ناسازگاری در ارتباط با شمار معیارها(n) [۲۴]

n	۳×۳	۴×۴	n>۴
RI	۰/۰۵	۰/۰۸	۰/۱

مطابق مباحث فوق به منظور اندازه‌گیری روابط بین عوامل و شاخص‌های مؤثّر بر سیستم مدیریت امنیت اطلاعات، ابتدا باید نرخ سازگاری پاسخ خبرگان حساب گردد. جدول۳ نرخ سازگاری عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر یکی از خبرگان) را نشان می‌دهد.

جدول۳ - نرخ سازگاری عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر یکی از خبرگان)

WSV (DM) = D × W(DM)									SV(DM)=WSV(DM)/W(DM)				/lmax	CI	CR=CI/RI(۰.۹۰)
DM۱	عوامل اصلی	C۱	C۲	C۳	C۴		W(DM)		WSV(DM		W(DM)		SV(DM)			
C۱	۱-مدیریتی	۱.۰۰	۲.۰۰	۳.۰۰	۴.۰۰		۰.۴۳۴		۱.۸۵۹		۰.۴۳۴		۴.۲۸۷			
C۲	۲-فرهنگی- اجتماعی	۰.۵۰	۱.۰۰	۳.۰۰	۴.۰۰	X	۰.۳۴۰	=	۱.۳۰۱	/	۰.۳۴۰	=	۳.۸۲۲		۴.۱۷۴	۰.۰۵۸	۰.۰۶۴
C۳	۳-فنی و فناورانه	۰.۳۳	۰.۳۳	۱.۰۰	۳.۰۰		۰.۱۶۰		۰.۶۱۶		۰.۱۶۰		۳.۸۵۷			
C۴	۴-مالی	۰.۲۵	۰.۲۵	۰.۳۳	۱.۰۰		۰.۰۶۶		۰.۳۱۳		۰.۰۶۶		۴.۷۲۸			

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، اکنون زمان آن فرا رسیده که وزن عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات محاسبه شود. جدول۴ ماتریس عوامل مؤثّر بر سیستم

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، اکنون زمان آن فرا رسیده که وزن عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات

جدول۴- عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر نهایی خبرگان- بر مبنا روش باکلی)

عوامل اصلی		C۱			C۲			C۳			C۴		
C۱	۱-مدیریتی	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۲.۰۰۰	۳.۰۴۳	۵.۰۰۰	۲.۰۰۰	۳.۴۸۰	۶.۰۰۰
C۲	۲-فرهنگی- اجتماعی	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۱۲۵	۴.۰۰۰	۱.۰۰۰	۲.۲۹۰	۶.۰۰۰
C۳	۳-فنی و فناورانه	۰.۲۰۰	۰.۳۲۹	۰.۵۰۰	۰.۲۵۰	۰.۴۷۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۱۲۵	۴.۰۰۰
C۴	۴-مالی	۰.۱۶۷	۰.۲۸۷	۰.۵۰۰	۰.۱۶۷	۰.۴۳۷	۱.۰۰۰	۰.۲۵۰	۰.۴۷۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰

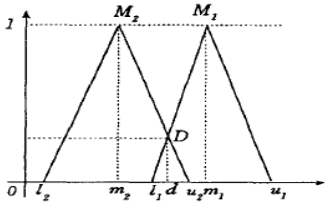
پس از اطمینان از سازگاری همه داده‌ها در جدول مقایسات زوجی، برای محاسبه وزن معیارها و زیر-معیارها، از روش تحلیل توسعه‌ای که توسط چانگ [۲۵] ارائه شده، استفاده شده‌است. اعداد فازی مورد استفاده در این روش اعداد فازی مثلثی هستند. مراحل تحلیل سلسله مراتبی فازی طبق روش تحلیل توسعه‌ای چانگ به‌صورت زیر می‌باشد [۱۴]:

***گام اول**: محاسبه ارزش هر یک از معیارها S_k است که برای هر یک از سطرهای ماتریس مقایسه‌های زوجی به‌صورت زیر تعریف می‌شود. k بیانگر شماره سطر و i و j به‌ترتیب نشان‌دهنده گزینه‌ها و شاخص‌ها هستند.

$$S_k = \sum_{j=1}^{n} M_{kj} * \left[\sum_{i=1}^{m}\sum_{j=1}^{n} M_{ij}\right]^{-1} \qquad (۴)$$

***گام دوم**: در روش تحلیل توسعه‌ای پس از محاسبه S_k هر سطر، درجه بزرگی ارزش هر معیار نسبت به هم به‌دست آید. به‌طور کلی اگر $M_1=(l_1,m_1,u_1)$ و $M_2=(l_2,m_2,u_2)$دو عدد فازی مثلثی باشند، درجه بزرگی M_1 نسبت به M_2 که با $V(M_1 \geq M_2)$ نشان داده می‌شود، به‌صورت زیر تعریف می‌شود:

$$\begin{cases} V(M_1 \geq M_2) = 1 & m_1 \geq m_2 \\ V(M_2 \geq M_1) = hgt(M_1 \cap M_2) = \dfrac{l_1 - u_2}{(m_2 - u_2) + (m_1 - l_1)} \end{cases}$$



(۵)

***گام سوم**: محاسبه میزان بزرگی یک عدد فازی مثلثی از k عدد فازی مثلثی دیگر است که از روابط زیر به‌دست می‌آید:

$$V(M_1 \geq M_2, \ldots, M_k) = V(M_1 \geq M_2), \ldots, V(M_1 \geq M_k) \qquad (۶)$$

محاسبه وزن شاخص‌ها در ماتریس مقایسه‌ها زوجی به‌صورت زیر عمل می‌شود:

$$W'(X_i)=\min\{V(S_i \geq S_k)\} \qquad k=1,2,.....,n, k\neq i \qquad (۷)$$

بر این اساس بردار وزن شاخص‌ها به‌صورت زیر خواهد بود که همان بردار ضرایب غیرنرمال تحلیل سلسله مراتبی فازی است:

$$W'=[W'(X_1),W'(X_2),....,W'(X_n)]^t \qquad (۸)$$

***گام چهارم**: اینک بر اساس رابطه زیر، مقدار اوزان نرمال شده شاخص‌ها به‌دست می‌آید.

$$W_i=\frac{W_i'}{\sum W_i'} \qquad (۹)$$

در این مقاله پیشنهاد انجام اهداف تحقیق به روش فوق توجه به این نکته بوده است که مخاطرات دارای ابعاد و اثرات مختلفی، با قابلیت رخداد در سطوح مختلف هستند و اقدامات پیشگیرانه خاص خود را در هر سطح می‌طلبند که روش فوق رتبه‌بندی مخاطرات امنیت اطلاعات در سازمان مورد نظر را با در نظرگرفتن علل بروز هر مخاطره و وزن و آثار آن مخاطره بنا به طبقه‌بندی انجام شده مطابق مدل مفهومی، رتبه‌بندی می‌کند که نتایج یافته‌های آماری آن بشرح ذیل می‌باشد:

۵- تجزیه و تحلیل یافته‌ها

با توجه به اینکه سازمان تامین‌اجتماعی یک سازمان بیمه‌گر و با خدمات متنوع رفاهی برای آحاد جامعه برشمرده می‌شود و تقریباً نیمی از جمعیت کشور را تحت پوشش خود دارد، استفاده هرچه بهتر و ایمن‌تر از تکنولوژی و سرویس‌ها و خدمات جدید می‌تواند تاثیر بسزایی در افزایش خدمت رسانی و در نتیجه افزایش رفاه اجتماعی و ایجاد رضایت‌مندی بیشتر در مخاطبان سازمان داشته باشد. نگاهی به پیشینه فعالیت‌های سازمان و مصاحبه با خبرگان امر شاهد این مدعاست که در هر دوره‌ای به فناوری اطلاعات و امنیت آن اهمیت داده شده و فضای رشد و توسعه مناسب فراهم شده باشد، خدمات ارائه شده به مخاطبان اعم از بیمه‌ای و درمانی جهش‌های چشمگیری را نشان داده و در هر دوره‌ای که به آن اهمیت جدی داده نشده است ارائه خدمات وسرویس‌های الکترونیکی با نقصان مواجه شده است. در این راستا نتایج حاصل ازیافته‌های آماری سئوالات محقق از خبرگان سازمانی در مطالعه موردی شعب تامین اجتماعی استان گیلان در سه بعد قابل ذکر است:

الف) شناسایی عوامل موثر بر امنیت اطلاعات بر اساس مدل مفهومی

با توجه به ادبیات پژوهش و نظر خبرگان، عوامل مؤثر بر سیستم مدیریت امنیت اطلاعات شناسایی و براساس مدل مفهومی تحقیق طبقه‌بندی گردید. جدول ۵ نظر نهایی حاصل از بازخورد خبرگان در مورد عوامل مؤثر، نرم و سخت بر سیستم مدیریت امنیت اطلاعات در شعب تامین‌اجتماعی استان گیلان را نشان می‌دهد.

جدول ۵- نظر نهایی حاصل از بازخورد خبرگان شعب تامین اجتماعی استان گیلان در مورد عوامل موثر نرم و سخت بر سیستم امنیت اطلاعات

عوامل اصلی	عوامل فرعی	شاخص‌ها	
عوامل نرم	۱-مدیریتی	۱-حمایت مدیریت ارشد ۲- خط‌مشی امنیتی سازمان ۳-ایجاد مدیریت مرکزی با نفوذ(مدیر امنیت) ۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان ۶- گزارش‌دهی وقایع امنیتی سازمان ۷-سیاستها و استراتژیهای فناوری اطلاعات و امنیت سازمان ۸-تعیین قلمرو امنیت سازمان
	۲-فرهنگی و اجتماعی	۱-فرهنگ سازمانی ۲-فرهنگ امنیت اطلاعات در سازمان ۳- نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۴- آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات ۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات
عوامل سخت	۱-فنی و فناورانه	۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت‌افزار، نرم‌افزار و شبکه) ۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۳-مدیریت مخاطرات (ریسک‌ها) سازمان ۴- تدوین و نگهداری مستندات امنیت اطلاعات ۵- نظارت، ارزیابی، کنترل و ممیزی داخلی
	۲-مالی	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها ۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات ۳- تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات	

ب) اولویت‌بندی عوامل اصلی و فرعی سیستم مدیریت امنیت اطلاعات:

همان‌گونه که در جدول۶ مشاهده می‌گردد، مطابق نظر خبرگان و بر اساس تحلیل سلسله مراتبی فازی، عوامل مدیریتی (وزن ۰/۳۸۵۱) دارای بیشترین اهمیت و عوامل مالی (وزن ۰/۰۸۷۳) داری کم‌ترین اهمیت را در بین عوامل موثر بر سیستم مدیریت امنیت اطلاعات دارند.

جدول ۶- وزن عوامل فرعی مؤثر بر سیستم مدیریت امنیت اطلاعات شعب تامین اجتماعی استان گیلان

عوامل اصلی	وزن نهایی	غیرنرمال	$V(S_1,S_2,S_3,S_4)$
۱- مدیریتی	۰/۳۸۵۱	۱	$V(S_1 \geq S_2,S_3,S_4)$
۲- فرهنگی- اجتماعی	۰/۳۱۳۷	۰/۸۱۴۶	$V(S_2 \geq S_1,S_3,S_4)$
۳- فنی و فناورانه	۰/۲۱۳۸	۰/۵۵۵۱	$V(S_3 \geq S_1,S_2,S_4)$
۴- مالی	۰/۰۸۷۳	۰/۲۲۶۷	$V(S_4 \geq S_1,S_2,S_3)$
		۲/۵۹۶۵	SUM

ج) اولویت‌بندی شاخصهای عوامل موثر بر سیستم مدیریت امنیت اطلاعات

پس از مشخص شدن اولویت عوامل اصلی و فرعی موثر بر سیستم مدیریت امنیت اطلاعات، نوبت تعیین اولویت شاخصهای شناسایی شده هریک از عوامل مدیریتی، فرهنگی- اجتماعی ، مالی و فنی در این سازمان است. نتایج حاصل از پاسخ خبرگان به پرسشنامه مقایسات زوجی، با در نظر گرفتن نرخ سازگاری ابتدا با روش باکلی ترکیب، سپس با روش تحلیل توسعه‌ای نسبت به اولویت‌بندی آن اقدام شد. نتایج حاصل از آن در جداول ۷ تا ۱۵ آورده شده که بیانگر لزوم اولویت بندی این عوامل در اخذ تصمیمات راهبردی در تامین امنیت فضای تولید و تبادل اطلاعات سازمانی است.

در این راستا بعنوان یک مثال، برای اندازه‌گیری روابط بین شاخص‌های مدیریتی بر اساس نظر خبرگان، مقایسات زوجی بعمل آمد و این نظریات به

ارزش‌های زبانی فازی متناظر تبدیل گردید. قبل از اینکه وزن شاخص‌های مدیریتی با استفاده از تحلیل سلسله مراتبی فازی حساب شود، ابتدا باید نرخ سازگاری پاسخ خبرگان حساب گردد. جدول۷ نرخ سازگاری شاخصهای مدیریتی (نظر یکی از خبرگان) را نشان می‌دهد.

جدول۷- نرخ سازگاری شاخص‌های مدیریتی (نظر یکی از خبرگان)

WSV (DM۱) = D x W(DM۱)													SV(DM۱)=WSV(DM۱)/W(DM۱)						
DM۱	شاخص‌های مدیریتی	C۱	C۲	C۳	C۴	C۵	C۶	C۷	C۸		W(DM۱)		WSV(DM۱)		W(DM۱)		SV(DM۱)	/lmax	CI	CR=CI/RI(۱.۴۱)
C۱	۱-حمایت مدیریت ارشد	۱.۰۰	۲.۰۰	۳.۰۰	۴.۰۰	۴.۰۰	۲.۰۰	۵.۰۰	۶.۰۰		۰.۲۸۲		۲.۵۵۰		۰.۲۸۲		۹.۰۵۳			
C۲	۲- خط مشی امنیتی سازمان	۰.۵۰	۱.۰۰	۲.۰۰	۲.۰۰	۴.۰۰	۳.۰۰	۴.۰۰	۴.۰۰		۰.۱۹۵		۱.۸۱۵		۰.۱۹۵		۹.۳۱۳			
C۳	۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰.۳۳	۰.۵۰	۱.۰۰	۳.۰۰	۲.۰۰	۲.۰۰	۳.۰۰	۴.۰۰		۰.۱۴۰		۱.۳۲۵		۰.۱۴۰		۹.۴۳۳			
C۴	۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰.۲۵	۰.۵۰	۰.۳۳	۱.۰۰	۳.۰۰	۳.۰۰	۳.۰۰	۴.۰۰	×	۰.۱۲۱	=	۱.۱۴۹	/	۰.۱۲۱	=	۹.۴۶۰	۸.۹۶۲	۰.۱۳۷۴	۰.۰۹۷
C۵	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۰.۲۵	۰.۲۵	۰.۵۰	۰.۳۳	۱.۰۰	۳.۰۰	۳.۰۰	۴.۰۰		۰.۰۹۴		۰.۸۵۵		۰.۰۹۴		۹.۱۲۰			
C۶	۶- گزارش‌دهی وقایع امنیتی سازمان	۰.۵۰	۰.۳۳	۰.۵۰	۰.۳۳	۰.۳۳	۱.۰۰	۳.۰۰	۶.۰۰		۰.۰۹۰		۰.۷۵۵		۰.۰۹۰		۸.۳۵۷			
C۷	۷-سیاست‌ها واستراتژی‌های فن‌آوری اطلاعات و امنیت سازمان	۰.۲۰	۰.۲۵	۰.۳۳	۰.۳۳	۰.۳۳	۰.۳۳	۱.۰۰	۴.۰۰		۰.۰۴۹		۰.۴۱۶		۰.۰۴۹		۸.۴۱۷			
C۸	۸-تعیین قلمرو امنیت سازمان	۰.۱۷	۰.۲۵	۰.۲۵	۰.۲۵	۰.۲۵	۰.۱۷	۰.۲۵	۱.۰۰		۰.۰۲۸		۰.۲۴۰		۰.۰۲۸		۸.۵۴۲			

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، سپس وزن شاخصهای مدیریتی محاسبه گردید. جدول۸ ماتریس شاخص‌های مدیریتی را که در نتیجه ترکیب پاسخهای بیست خبره بر مبنای روش باکلی حاصل شده‌اند، نشان می‌دهد.

جدول۸- ماتریس شاخص‌های مدیریتی (نظر نهایی خبرگان- بر مبنا روش باکلی)

شاخص‌های مدیریتی		C۱			C۲			C۳			C۴			C۵			C۶			C۷			C۸		
C۱	۱-حمایت مدیریت ارشد	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۳.۸۰۹	۵.۰۰۰	۲.۰۰۰	۳.۹۴۳	۵.۰۰۰	۱.۰۰۰	۲.۳۱۱	۵.۰۰۰	۲.۰۰۰	۳.۳۴۴	۶.۰۰۰	۲.۰۰۰	۵.۴۳۷	۷.۰۰۰
C۲	۲- خط مشی امنیتی سازمان	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۴۱	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۳.۰۲۶	۵.۰۰۰	۲.۰۰۰	۳.۷۷۶	۵.۰۰۰	۲.۰۰۰	۴.۰۳۲	۶.۰۰۰
C۳	۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۰.۲۵۰	۰.۴۹۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۹۴۰	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۲۳۲	۵.۰۰۰	۲.۰۰۰	۳.۰۴۳	۵.۰۰۰	۲.۰۰۰	۳.۹۸۷	۶.۰۰۰
C۴	۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰.۲۰۰	۰.۲۶۳	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۲۵۰	۰.۳۴۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۴.۲۸۳	۶.۰۰۰
C۵	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۰.۲۰۰	۰.۲۵۴	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۲.۱۵۶	۵.۰۰۰	۲.۰۰۰	۳.۰۸۸	۵.۰۰۰	۲.۰۰۰	۳.۰۸۸	۵.۰۰۰
C۶	۶- گزارش‌دهی وقایع امنیتی سازمان	۰.۲۰۰	۰.۴۳۳	۱.۰۰۰	۰.۲۰۰	۰.۳۳۱	۱.۰۰۰	۰.۲۰۰	۰.۴۴۸	۱.۰۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۹۴۰	۴.۰۰۰	۱.۰۰۰	۴.۶۷۹	۷.۰۰۰
C۷	۷-سیاست‌ها واستراتژی‌های فن‌آوری اطلاعات و امنیت سازمان	۰.۱۶۷	۰.۲۹۹	۰.۵۰۰	۰.۲۰۰	۰.۲۶۵	۰.۵۰۰	۰.۲۰۰	۰.۳۲۹	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۲۰۰	۰.۴۶۴	۱.۰۰۰	۰.۲۵۰	۰.۳۴۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۹۸۷	۶.۰۰۰
C۸	۸-تعیین قلمرو امنیت سازمان	۰.۱۴۲	۰.۱۸۴	۰.۵۰۰	۰.۱۶۷	۰.۲۴۸	۰.۵۰۰	۰.۱۶۷	۰.۲۵۱	۰.۵۰۰	۰.۱۶۷	۰.۲۲۳	۰.۵۰۰	۰.۲۰۰	۰.۳۲۴	۰.۵۰۰	۰.۱۴۳	۰.۲۱۴	۱.۰۰۰	۰.۱۶۷	۰.۲۵۱	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰

برای محاسبه وزن شاخص‌های مدیریتی، از روش تحلیل توسعه‌ای استفاده می‌گردد. همانگونه که بیان گردید اعداد مورد استفاده در این روش اعداد فازی مثلثی هستند. مراحل تحلیل سلسله مراتبی فازی طبق روش تحلیل توسعه‌ای چانگ به صورت زیر است:

گام اول: محاسبه S_k برای هر یک از سطرهای ماتریس مقایسه‌های زوجی به صورت زیر تعریف می‌شود. در اینجا k بیانگر شماره سطر و i و j به ترتیب نشان دهنده گزینه‌ها و شاخص‌ها هستند. جدول۹ ماتریسی S_k برای شاخص‌های مدیریتی را نشان می‌دهد.

گام دوم: مرحله دوم در روش تحلیل توسعه‌ای پس از محاسبه S_k مربوط به هر سطر، این است که درجه بزرگی آنها نسبت به هم به دست آید. جدول۱۰، درجه بزرگی S_k را نسبت به هم نشان می‌دهد.

جدول۹- مقدار S_k برای شاخص‌های مدیریتی

S_k			
S۱	۰.۰۷۸	۰.۲۴۰	۰.۶۱۰
S۲	۰.۰۶۱	۰.۱۵۸	۰.۴۰۷
S۳	۰.۰۵۶	۰.۱۴۵	۰.۳۹۸
S۴	۰.۰۶۲	۰.۱۳۴	۰.۳۲۲
S۵	۰.۰۵۵	۰.۱۱۴	۰.۳۰۵
S۶	۰.۰۲۷	۰.۱۰۱	۰.۲۷۱
S۷	۰.۰۳۳	۰.۰۷۴	۰.۱۹۵
S۸	۰.۰۱۴	۰.۰۲۶	۰.۰۸۵

جدول۱۰- درجه بزرگی S_k برای شاخص‌های مدیریتی

V۱		V۲		V۳		V۴		V۵		V۶		V۷		V۸	
V(S۱>=S۲)	۱.۰۰۰	V(S۲>=S۱)	۰.۸۰۱	V(S۳>=S۱)	۰.۷۷۱	V(S۴>=S۱)	۰.۶۹۷	V(S۵>=S۱)	۰.۶۴۳	V(S۶>=S۱)	۰.۵۸۲	V(S۷>=S۱)	۰.۴۱۳	V(S۸>=S۱)	۰.۰۲۹
V(S۱>=S۳)	۱.۰۰۰	V(S۲>=S۳)	۱.۰۰۰	V(S۳>=S۲)	۰.۹۶۳	V(S۴>=S۲)	۰.۹۱۶	V(S۵>=S۲)	۰.۸۴۸	V(S۶>=S۲)	۰.۷۸۷	V(S۷>=S۲)	۰.۶۱۵	V(S۸>=S۲)	۰.۱۵۲
V(S۱>=S۴)	۱.۰۰۰	V(S۲>=S۴)	۱.۰۰۰	V(S۳>=S۴)	۱.۰۰۰	V(S۴>=S۳)	۰.۹۶۰	V(S۵>=S۳)	۰.۸۹۰	V(S۶>=S۳)	۰.۸۳۱	V(S۷>=S۳)	۰.۶۶۳	V(S۸>=S۳)	۰.۱۹۷
V(S۱>=S۵)	۱.۰۰۰	V(S۲>=S۵)	۱.۰۰۰	V(S۳>=S۵)	۱.۰۰۰	V(S۴>=S۵)	۱.۰۰۰	V(S۵>=S۴)	۰.۹۲۵	V(S۶>=S۴)	۰.۸۶۵	V(S۷>=S۴)	۰.۶۹۰	V(S۸>=S۴)	۰.۱۷۵
V(S۱>=S۶)	۱.۰۰۰	V(S۲>=S۶)	۱.۰۰۰	V(S۳>=S۶)	۱.۰۰۰	V(S۴>=S۶)	۱.۰۰۰	V(S۵>=S۶)	۱.۰۰۰	V(S۶>=S۵)	۰.۹۴۴	V(S۷>=S۵)	۰.۷۷۷	V(S۸>=S۵)	۰.۲۵۱
V(S۱>=S۷)	۱.۰۰۰	V(S۲>=S۷)	۱.۰۰۰	V(S۳>=S۷)	۱.۰۰۰	V(S۴>=S۷)	۱.۰۰۰	V(S۵>=S۷)	۱.۰۰۰	V(S۶>=S۷)	۱.۰۰۰	V(S۷>=S۶)	۰.۸۶۱	V(S۸>=S۶)	۰.۴۳۵
V(S۱>=S۸)	۱.۰۰۰	V(S۲>=S۸)	۱.۰۰۰	V(S۳>=S۸)	۱.۰۰۰	V(S۴>=S۸)	۱.۰۰۰	V(S۵>=S۸)	۱.۰۰۰	V(S۶>=S۸)	۱.۰۰۰	V(S۷>=S۸)	۱.۰۰۰	V(S۸>=S۷)	۰.۵۱۹

گام سوم: محاسبه میزان بزرگی یک عدد فازی مثلثی از k عدد فازی مثلثی دیگر و در نهایت محاسبه وزن شاخص‌های مدیریتی می‌باشد.

جدول۱۱ وزن شاخص‌های مدیریتی (غیرنرمال، وزن نسبی و وزن نهایی) را نشان می‌دهد.

جدول ۱۱- وزن شاخص‌های عامل فرعی مـدیریتی از عامل اصلی نرم

شاخصهای مدیریتی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8)$
۱-حمایت مدیریت ارشد	۰/۰۷۸۰	۰/۲۰۳	۱/۰۰۰	$V(S_1 \geq S_2,S_3,S_4,S_5,S_6,S_7,S_8)$
۲-خط‌مشی امنیتی سازمان	۰/۰۶۲۵	۰/۱۶۲	۰/۸۰۱	$V(S_2 \geq S_1,S_3,S_4,S_5,S_6,S_7,S_8)$
۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰/۰۶۰۲	۰/۱۵۶	۰/۷۷۱	$V(S_3 \geq S_1,S_2,S_4,S_5,S_6,S_7,S_8)$
۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰/۰۵۴۴	۰/۱۴۱	۰/۶۹۷	$V(S_4 \geq S_1,S_2,S_3,S_5,S_6,S_7,S_8)$
۵-آگاهی و پایبندی به سیاستها، رویه‌ها و عملیات سازمانها	۰/۰۴۴۱	۰/۱۳۰	۰/۶۴۳	$V(S_5 \geq S_1,S_2,S_3,S_4,S_6,S_7,S_8)$
۶-گزارش‌دهی وقایع امنیتی سازمان	۰/۰۴۵۴	۰/۱۱۸	۰/۵۸۲	$V(S_6 \geq S_1,S_2,S_3,S_4,S_5,S_7,S_8)$
۷-سیاستها و استراتژی‌های فناوری اطلاعات و امنیت سازمان	۰/۰۳۲۲	۰/۰۸۴	۰/۴۱۳	$V(S_7 \geq S_1,S_2,S_3,S_4,S_5,S_6,S_8)$
۸-تعیین قلمرو امنیت سازمان	۰/۰۰۲۲	۰/۰۰۶	۰/۰۲۹	$V(S_8 \geq S_1,S_2,S_3,S_4,S_5,S_6,S_7)$
SUM			۴/۹۳۵	

همانگونه که در جدول ۱۱ مشاهده می‌گردد، شاخص حمایت مدیریت ارشد(وزن نسبی ۰/۲۰۳ و وزن نهایی ۰/۰۷۸۰) دارای بیشترین اهمیت و شاخص تعیین قلمرو امنیت سازمان(وزن نسبی ۰/۰۰۶ و وزن نهایی ۰/۰۰۲۲) داری کمترین اهمیت را در بین شاخص‌های مدیریتی در این سازمان است. سایر شاخصها نیز به همین سبک محاسبه و مورد ارزیابی قرارمی‌گیرند که جداول زیر بیانگر نتایج نهایی بدست آمده است.

مطابق جدول ۱۲ شاخص فرهنگ سازمانی(وزن نسبی ۰/۲۳۳ و وزن نهایی ۰/۰۷۳۰) دارای بیشترین اهمیت و شاخص آموزش مداوم استفاده کنندگان در زمینه فناوری و امنیت اطلاعات (وزن نسبی ۰/۰۹۸ و وزن نهایی ۰/۰۳۰۶) داری کم‌ترین اهمیت، در بین شاخص‌های فرهنگی- اجتماعی است.

جدول ۱۲- وزن شاخص‌های عامل فرعی فرهنگی- اجتماعی از عامل اصلی نرم

شاخصهای فرهنگی و اجتماعی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5)$
۱-فرهنگ سازمانی	۰/۰۷۳۰	۰/۲۳۳	۰/۹۱۲	$V(S_1 \geq S_2,S_3,S_4,S_5)$
۲-فرهنگ امنیت اطلاعات در سازمان	۰/۰۸۰۰	۰/۲۵۵	۱/۰۰۰	$V(S_2 \geq S_1,S_3,S_4,S_5)$
۳-نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۰/۰۷۰۷	۰/۲۲۵	۰/۸۸۳	$V(S_3 \geq S_1,S_2,S_4,S_5)$
۴-آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات	۰/۰۵۹۴	۰/۱۸۹	۰/۷۴۲	$V(S_4 \geq S_1,S_2,S_3,S_5)$
۵-آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۰/۰۳۰۶	۰/۰۹۸	۰/۳۸۳	$V(S_5 \geq S_1,S_2,S_3,S_4)$
			۳/۹۲۰	SUM

وزن شاخصهای فنی و فناورانه نیز در جدول۱۳ نشان داده شده است. که بر اساس این جدول شاخص شناسایی و ارزیابی مخاطرات امنیت اطلاعات (وزن نسبی ۰/۳۰۲ و وزن نهایی ۰/۰۶۴۶) دارای بیشترین اهمیت و شاخص نظارت، ارزیابی، کنترل و ممیزی داخلی (وزن نسبی ۰/۰۵۵ و وزن نهایی ۰/۰۱۱۸) داری کم‌ترین اهمیت، در بین شاخص‌های فنی و فناورانه است.

جدول ۱۳- وزن شاخص‌های عامل فرعی فنی و فناورانه از عامل اصلی سخت

شاخصهای فنی و فناورانه	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5)$
۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت‌افزار، نرم‌افزار و شبکه)	۰/۰۵۰۸	۰/۲۳۷	۰/۷۸۶	$V(S_1 \geq S_2,S_3,S_4,S_5)$
۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۰/۰۶۴۶	۰/۳۰۲	۱/۰۰۰	$V(S_2 \geq S_1,S_3,S_4,S_5)$
۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۰/۰۵۰۱	۰/۲۳۴	۰/۷۷۵	$V(S_3 \geq S_1,S_2,S_4,S_5)$
۴-تدوین و نگهداری مستندات امنیت اطلاعات	۰/۰۳۶۵	۰/۱۷	۰/۵۶۵	$V(S_4 \geq S_1,S_2,S_3,S_5)$
۵-نظارت، ارزیابی، کنترل و ممیزی داخلی	۰/۰۱۱۸	۰/۰۵۵	۰/۱۸۲	$V(S_5 \geq S_1,S_2,S_3,S_4)$
			۳/۳۰۸	SUM

مطابق جدول ۱۴ شاخص شناخت دارایی‌ها و تعیین ارزش آن‌ها (وزن نسبی ۰/۵۷۰ و وزن نهایی ۰/۰۴۹۸) دارای بیشترین اهمیت و شاخص تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات (وزن نسبی ۰/۲۱۳ و وزن نهایی ۰/۰۱۸۶) داری کم‌ترین اهمیت، در بین شاخص‌های مالی هستند.

جدول ۱۴- وزن شاخص‌های عامل فرعی مالی از عامل اصلی سخت

شاخصهای مـــالی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3)$
۱-شناخت دارایی‌ها و تعیین ارزش آن‌ها	۰/۰۴۹۸	۰/۵۷۰	۱	$V(S_1 \geq S_2,S_3)$
۲-تخصیص بودجه مناسب در زمینه فن‌آوری اطلاعات و امنیت اطلاعات	۰/۰۱۸۹	۰/۲۱۶	۰/۳۷۹۵	$V(S_2 \geq S_1,S_3)$
۳-تامین هزینه‌های آموزش در زمینه فن‌آوری اطلاعات و امنیت اطلاعات	۰/۰۱۸۶	۰/۲۱۳	۰/۳۷۴۳	$V(S_3 \geq S_1,S_2)$
			۱/۷۵۳۹	SUM

درجدول ۱۵ وزن های (نسبی و نهایی) عوامل و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات، به تفکیک نشان داده می‌شود.

جدول ۱۵- اوزان نسبی و نهایی عوامل اصلی و شاخص‌های فرعی مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان

عوامل اصلی	وزن	عوامل فرعی	وزن نهایی	شاخص‌ها	وزن	
					نسبی	نهایی
عوامل نرم	۰/۶۹۸۹	مدیریتی	۰/۳۸۵۱	۱-حمایت مدیریت ارشد	۰/۲۰۳	۰/۰۷۸۰
				۲- خط مشی امنیتی سازمان	۰/۱۶۲	۰/۰۶۲۵
				۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰/۱۵۶	۰/۰۶۰۲
				۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰/۱۴۱	۰/۰۵۴۴
				۵- آگاهی وپایبندی به سیاستها، رویه‌ها و عملیات سازمان	۰/۱۳۰	۰/۰۴۴۱
				۶- گزارش‌دهی وقایع امنیتی سازمان	۰/۱۱۸	۰/۰۴۵۴
				۷-سیاستها واستراتژیهای فناوری اطلاعات وامنیت سازمان	۰/۰۸۴	۰/۰۳۲۲
				۸-تعیین قلمرو امنیت سازمان	۰/۰۰۶	۰/۰۰۲۲
		فرهنگی و اجتماعی	۰/۳۱۳۷	۱-فرهنگ سازمانی	۰/۲۳۳	۰/۰۷۳۰
				۲-فرهنگ امنیت اطلاعات در سازمان	۰/۲۵۵	۰/۰۸۰۰
				۳- نهادینه شدن رفتارسازمانی و رفتارهاامنیتی در کارکنان	۰/۲۲۵	۰/۰۷۰۷
				۴- آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات	۰/۱۸۹	۰/۰۵۹۴
				۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۰/۰۹۸	۰/۰۳۰۶
عوامل سخت	۰/۳۰۱۱	فنی و فناورانه	۰/۲۱۳۸	۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت افزار، نرم‌افزار و شبکه)	۰/۲۳۷	۰/۰۵۰۸
				۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۰/۳۰۲	۰/۰۶۴۶
				۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۰/۲۳۴	۰/۰۵۰۱
				۴- تدوین و نگهداری مستندات امنیت اطلاعات	۰/۱۷۱	۰/۰۳۶۵
				۵- نظارت، ارزیابی، کنترل و ممیزی داخلی	۰/۰۵۵	۰/۰۱۱۸
		مالی	۰/۰۸۷۳	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها	۰/۵۷۰	۰/۰۴۹۸
				۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات	۰/۲۱۶	۰/۰۱۸۹
				۳- تامین هزینه‌های آموزش درزمینه فناوری اطلاعات و امنیت اطلاعات	۰/۲۱۳	۰/۰۱۱۸

در بین سازمان‌ها، سازمان تامین اجتماعی با توجه به اهمیت و تنوع فعالیت‌های آنها و به لحاظ تردد کارفرمایان و بیمه‌شدگان و سایر متقاضیان و همچنین اقدامات سازمان در انتقال حجم زیادی از داده‌های خود در ارتباط به لیست حق بیمه و پرداخت وجه بیمه از طریق سیستم‌وب؛ حساسیت امنیت بستر وب، نگهداری داده‌ها، تهیه پشتیبان و محل نگهداری پشتیبان‌ها را بسیارحائز اهمیت نموده است که داشتن رویکرد اساسی به سیستم مدیریت امنیت اطلاعات درآن اساسی بنظر می رسد و از طرفی با توجه به اینکه این دستگاه مطابق چشم‌انداز تعیین شده درسند راهبردی امنیت فضای تبادل اطلاعات کشور (سندافتا- سال ۱۳۸۶) یعنی"- تأمین امنیت فضای تولید و تبادل اطلاعات کشور، عدم بروز اختلال درزیرساخت‌های حیاتی کشور واعتماد وآسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی ازجمله فعالیت‌های اقتصادی، اجتماعی و فرهنگی به منظور صیانت ازحاکمیت واقتدار ملی درافق سال۱۴۰۴" و طبق مفاد بندهای ترتیبات اجرایی سند افتا درجهت لزوم انجام مطالعات فضای تولید و تبادل اطلاعات توسط کلیه دستگاه‌های اجرایی، ملزم است در تدوین اسناد بالادستی خود به بررسی مخاطرات فناوری اطلاعات و ارایه راه حل‌هایی درخصوص افزایش عملکرد بهینه سامانه‌ها و رده‌بندی دارایی‌های اطلاعاتی مانند بانک‌های اطلاعاتی، سرویس‌های الکترونیکی، اسناد مکتوب یا دارایی‌های فیزیکی (مانند رایانه‌ها، سرورها، شبکه وسایر تجهیزات)، درقالب استانداردهای امنیتی به ممیزی وتدوین سیاست نامه‌ها وقوانین و دستورالعملهای امنیتی بپردازد که بنابراین ضرورت اینگونه مطالعات در این سازمان و شعب تابعه آن را دو چندان نموده است و از طرفی سیاست سازمان تامین اجتماعی در خصوص برونسپاری خدمات و همچنین واگذاری برخی از امور به بخش خصوصی سازمان تحت نام کارگزاری‌ها اخیراً سرعت گرفته است که در سایه شناسایی و اولویت‌بندی این ملاحظات امنیتی، شاهد تعالی سازمان در جهت جلب رضایت ارباب رجوع و کاهش دغدغه‌های مدیریتی در حفظ جایگاه رقابتی سازمان خواهیم بود.

جدول ۱۶- اولویت‌بندی عوامل نرم و سخت و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان

عوامل اصلی	اولویت	عوامل فرعی	اولویت	شاخص‌ها	اولویت
عوامل نرم	۱	مدیریتی	۱	۱-حمایت مدیریت ارشد	۱
				۲- خط‌مشی امنیتی سازمان	۲
				۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۳
				۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۴
				۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۵
				۶- گزارش‌دهی وقایع امنیتی سازمان	۶
				۷-سیاست‌ها واستراتژی‌های فناوری اطلاعات و امنیت سازمان	۷
				۸-تعیین قلمرو امنیت سازمان	۸
		فرهنگی و اجتماعی	۲	۱-فرهنگ سازمانی	۲
				۲-فرهنگ امنیت اطلاعات در سازمان	۱
				۳- نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۳
				۴- آگاهی ذینفعان و مشتریان ازمزایای امنیت اطلاعات	۴
				۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۵
عوامل سخت		فنی و فناورانه	۳	۱-تجهیزات و زیرساختهای امنیت اطلاعات (سخت‌افزار، نرم‌افزار وشبکه)	۲
				۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۱
				۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۳
				۴- تدوین و نگهداری مستندات امنیت اطلاعات	۴
				۵- نظارت، ارزیابی، کنترل و ممیزی داخلی	۵
		مالی	۴	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها	۱
				۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات	۲
				۳- تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات	۳

با بررسی یافته‌های تحقیق حاضر از طریق طبقه‌بندی و رتبه‌بندی عوامل موثر بر سیستم مدیریت امنیت اطلاعات در قالب عوامل نرم و سخت براساس رویکرد تحلیل سلسله مراتبی فازی در شعب تامین اجتماعی گیلان نشان می‌دهد که در بین عوامل اصلی، عوامل نرم با وزن ۰/۶۹۸۹ در رتبه اولویت اول و عوامل سخت با وزن ۰/۳۰۱۱ در رتبه اولویت دوم قرار دارد. عوامل اصلی نرم و سخت به عوامل فرعی، مدیریتی، فرهنگی، فنی و مالی تقسیم شدند. نتایج تحقیق نشان داد که در بین عوامل فرعی، عامل مدیریتی با وزن ۰/۳۸۵۱ در رتبه اول و عامل مالی با وزن ۰/۰۸۷۳ در رتبه چهارم قرار دارد. همچنین از بین شاخص‌های هر یک از عوامل فرعی، حمایت مدیریت ارشد، فرهنگ امنیت اطلاعات در سازمان، شناسایی و ارزیابی مخاطرات امنیت اطلاعات و شناخت دارایی‌ها و تعیین ارزش آن‌ها، دارای بیشترین اهمیت در بین بقیه شاخص‌ها به ترتیب در عوامل فرعی مدیریتی، فرهنگی، فنی و مالی هستند. درجدول ۱۶، اولویت‌بندی عوامل و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان به تفکیک نشان داده شده‌است.

براساس مطالعات انجام شده شرط موفقیت سازمان‌های امروزی در ارایه خدمات متنوع و انجام وظایف بطور مطمئن و ایمن با استفاده از ابزارهای فناوری اطلاعات، نگاه ویژه به پیاده سازی سیستم مدیریت امنیت اطلاعات و استمرار چرخه امنیت اطلاعات است که ارتباط مستقیم با شهرت سازمان دارد. از اینرو اگر اولویت پیاده‌سازی و استمرار چرخه امنیت اطلاعات در سازمان کمرنگ شود، به جرات می‌توان ادعا کرد سیستم مدیریت امنیت اطلاعات در سایر مشغله‌های مدیران و کاربران محو خواهد شد. همچنین باید توجه داشت که سیاست ارتقای امنیت سیستم، راهبردی مؤثر در جهت افزایش اطمینان و اعتماد مشتریان است. زیرا آن چیزی که بیشتر مشتریان به آن اهمیت می‌دهند حفاظت از اطلاعات شخصی آنان است. لازم است سازمان بر روی عوامل نرم شامل عوامل مدیریتی و فرهنگی تمرکز بیشتری نموده و از حمایت مدیریت ارشد در تصویب و آموزش قوانین مرتبط با امنیت اطلاعات و تشکیلات امنیت بهره‌مند شود و خط مشی، اهداف بلندمدت و کوتاه‌مدت اطلاعاتی در جهت افزایش فرهنگ امنیت اطلاعات در سازمان را مشخص نماید. با توجه به این‌که هر گونه تغییرات یا اصلاحات در عوامل نرم، مشمول صرف زمان و سرمایه است لازم است به‌صورت برنامه‌ریزی شده به آن توجه شود. از این رو حمایت مدیریت ارشد، ایجاد یا بازنگری تشکیلات امنیت اطلاعات، انتخاب مناسب مدیر امنیت اطلاعات و نظارت مستمر مدیر ارشد سازمان در برقراری سیستم امنیت اطلاعات بسیار حائز اهمیت است. سازمان‌ها بایستی علاوه بر سرمایه‌گذاری بر راه‌حل‌های فنی برای حفظ امنیت اطلاعات، به عوامل غیرفنی و انسانی از جمله ارتقاء سطح آگاهی کلیه کارمندان از مؤلفه‌های امنیت اطلاعات، توجه بیشتری داشته باشند. برای این منظور لازم است مسئولین ذیربط در حیطه فناوری اطلاعات، یک چارچوب مناسب در جهت ارزیابی میزان آگاهی کارمندان و آموزش امنیت اطلاعات داشته باشند و با استفاده از این چارچوب و با در نظر گرفتن اولویت مؤلفه‌ها و سطوح (دانش، نگرش و رفتار) برنامه‌های آموزشی آگاهی از امنیت اطلاعات را به نحوی مؤثرتر و مفیدتر ارائه دهند.

منابع

۱. تاج‌فر، امیرهوشنگ، محمد محمودی میمند، فاطمه رضاسلطانی و پوریا رضاسلطانی. (۱۳۹۳). رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف. مدیریت فناوری اطلاعات. ۶ (۴): ۵۶۶-۵۵۱.

۲. قرایی، حسین و مهسا آقا محی الدین. (۱۳۹۳). بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخه. پردازش علائم و داده‌ها. ۲ (۲۲): ۱۴-۳.

۳. آرام، محمدرضا. (۱۳۸۸). بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

۴. بهرامی، مجتبی. (۱۳۹۰). ارائه روشی مناسب برای بهبود و توسعه شاخص های مدیریت امنیت اطلاعات جهت طراحی و پیاده سازی در سازمان ها. هشتمین کنفرانس بین المللی انجمن رمز ایران.

۵. صالحیان، مهران. (۱۳۸۸). بررسی استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در دستگاه‌های دولتی. پایان‌نامه کارشناسی ارشد. دانشگاه شیراز.

۶. طاهری، مهدی. (۱۳۸۶). ارائه چارچوبی برای نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی. پایان‌نامه کارشناسی ارشد. دانشگاه تربیت مدرس. تهران.

۷. زنده دل نوبری، بابک. (۱۳۸۹). ارائه مدلی جهت رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها. پایان‌نامه کارشناسی ارشد. دانشگاه آزاد اسلامی واحد علوم تحقیقات. تهران.

۸. شاه بهرامی، اسدا.. رفیع زاده کاسانی، رامین. (۱۳۹۴). امنیت منابع فناوری اطلاعات، انتشارات جهاد دانشگاهی- تهران.

۹. مومنی، منصور (۱۳۸۵)، مباحث نوین تحقیق در عملیات، انتشارات دانشکده مدیریت، دانشگاه تهران.

10. Buckley, J. (1985). Fuzzy Hierarchial Analysis. Fuzzy Sets and Systems. 17. 233-247.

11. Chang, E., Lin, C. (2007). Exploring organizational culture for information security Management. Industrial Management & Data Systems. 107. 1-10.

12. Choi, N. Dan, K and Jahyun G. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action, Information Management & Computer Security. 16. 484-485.

13. Deng, H.(1999). Multicriteria analysis with fuzzy pairwise comparisons. International Journal of Approximate Reasoning. 21. 231–215.

14. Hua, B. (2008). A Fuzzy AHP Based Evaluation Method for Vendor-Selection. Shenzhen Tourism College. Jinan University. Shenzhen. 518053. China.

15. ISO/IEC 27001. (2005). Information technology-Security techniques-Information security management systems–Requirements (First edition).

16. ISO/IEC 27005. (2008). Information technology - Security techniques-Information security risk management (First edition).

17. Hubacek, K. Dabo G. and Anamika B. (2007). Changing Lifestyles and Consumption Patterns in Developing Countries: A Scenario Analysis for China and India. Sustainability Research Institute (SRI). 45-62.

18. Kritzinge, E and Elme S. (2008). Information security management: An information security retrieval and awareness model for industry. Computer & security. 27. 224-231.

19. Kruger, H and Kearney, W. D. (2006). A prototype for assessing information security awareness, Computer & security, 25, 289-296.

20. Lau, H. C. and Mohd Awang, I. (2001). The Soft Foundation of The Critical SuccessFactors on TQM Implementation in Malaysia, The TQM magazine , Vol.13 , No. 1, PP. 51-62.

21. Lewis W. Pun, K. Fai. L. (2006). Exploring Soft versus Hard Factors for TQM Implementation in Small and Medium-Sized Enterprises, International Journal of Productivity and Performance Management, Vol. 55, No. 7, PP. 539-554.

22. Nikrerk, J. and Solms, V. (2009). Information security culture: a management perspective, Computer & security, 5, 142-144.

23. Saaty, T.L., (1980). The Analytic Hierarchy Process, New York, Mc GrawHill.

24. Saaty, T.L.(1994).How to Make a Decision:The Analytic Hierarchy Process, Interfaces 24(6):19-43.

25. Chang, D. (1996). Applications of the Extent Analysis Method on Fuzzy AHP. European Journal of Operational Research. 95(3). 649-655.

26. Sungho, K. Jang, S. Lee, J and Kim,S.(2007).Common defects in information security management system of Korean companies. The Journal of Systems and Software. 80(10). 1631–1638.

27. Broderick, J. S. (2006). ISMS, security standards and security regulations, information security technical report. 11: 26 –31.

28. Meer, J. van der (Jeroen). (2012). Multi-criteria decision model inference and application in information security risk classification

فصلنامه علمی- پژوهشی

فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷

صص: ۷۵- ۸۸

کشف گزارش‌های نقص محصول از متن نظرات آنلاین کاربران

[*] نرگس نعمتی فرد [*]محرم منصوری‌زاده [*]مهدی سخایی‌نیا

* گروه مهندسی کامپیوتر، دانشگاه بوعلی سینا، همدان، ایران

تاریخ دریافت: ۱۳۹۷/۰۳/۱۰ تاریخ پذیرش:۱۳۹۸/۰۱/۰۹

چکیده

با توسعه وب ۲ و شبکه‌های اجتماعی، مشتریان و کاربران نظرهای خود را درباره‌ی محصولات مختلف با یکدیگر به اشتراک می‌گذارند. این نظرها به عنوان یک منبع ارزشمند، جهت تعیین جایگاه کالا و موفقیت در بازاریابی، می‌تواند مورد استفاده قرار گیرد. استخراج نواقص گزارش شده از میان حجم زیاد نظرهایی که توسط کاربران تولید شده از مشکلات عمده این زمینه تحقیقاتی است. مشتریان و مصرف‌کنندگان با مقایسه محصولات تولیدکنندگان مختلف نقاط قوت و ضعف محصولات را در قالب نظرهای مثبت و منفی بیان می‌نمایند. طبقه‌بندی نظرات بر اساس واژگان حسی مثبت و منفی در متن نظر به اسناد حاوی گزارش نقص و فاقد آن نتیجه درست و دقیقی در پی ندارد. چون گزارش نواقص صرفاً در نظرات منفی صورت نمی‌گیرد. ممکن است که مشتری نسبت به یک کالا حس مثبتی داشته باشد و با این حال در نظر خود یک نقص را گزارش نماید. بنابراین چالش دیگر این زمینه تحقیقاتی طبقه‌بندی درست و دقیق نظرات است. برای حل این مشکلات و چالش‌ها، در این مقاله روشی موثر و کارا برای استخراج نظرهای حاوی گزارش نقص محصول از نظرهای آنلاین کاربران ارائه گردیده است. بدین منظور طبقه‌بند جنگل تصادفی برای تشخیص گزارش نقص و تکنیک بدون ناظر مدل‌سازی موضوعی تخصیص پنهان دیریکله را برای ارائه‌ی خلاصه‌ای از گزارش نقص بکار گرفته شدند. برای تحلیل و ارزیابی روش پیشنهادی از داده‌های وب‌سایت آمازون استفاده شده است. نتایج نشان داد جنگل تصادفی حتی با تعداد کم داده‌های آموزشی عملکرد قابل قبولی برای کشف گزارش نقص دارد. نتایج و خروجی‌های استخراج شده از اسناد حاوی گزارش نقص، شامل خلاصه‌ی گزارش نقص جهت سهولت در تصمیم‌گیری تولیدکنندگان، یافتن الگوهای وجود گزارش نقص در متن به صورت خودکار و کشف جنبه‌هایی از محصول که بیشترین گزارش نقص مربوط به آنها می‌باشد، نشان‌دهنده توانایی روش تخصیص پنهان دیریکله است.

واژه‌های کلیدی: تشخیص گزارش خرابی، نظر کاوی، تحلیل حسی، تحلیل نظر کاربران، متن کاوی.

نویسنده عهده‌دار مکاتبات : محرم منصوری‌زاده mansoorm@basu.ac.ir

۱- مقدمه

گسترش وب۲، کاربران اینترنتی را در تعامل با یکدیگر و همچنین در تشکیل شبکه‌های اجتماعی برای تولید اطـلاعات و انتشـار دادگان با حجم زیاد و محـتوای مفید بر روی وب توانمند ساخته است. یکی از مهمترین محتوایی که کاربران اینترنتی تولید می‌کنند، اظهار نظر[1] پیرامون یک موضوع، شی، رویداد یا حتی شخص است. این نقد و بررسی‌ها[2] عامل مهم و اثرگذاری در فرایند تصمیم‌گیری کاربران اینترنتی در زمینه‌های مختلف است [۱].

اخیراً در زمینه‌ی استخراج ریز اطلاعات از جمله استخراج جنبه‌هایی از محصول که مشتری درباره‌ی آنها نظر خود را بیان کرده است و همچنین نرخ امتیاز دهی، کارها و تحقیقات زیادی صورت گرفته است [۱]. این اطلاعات در تصمیم‌گیری مشتریان هنگام خرید و آگاهی تولیدکننده از حس مشتری نسبت به محصول کمک‌کننده هستند. اما در این میان استخراج گزارش نقص و خرابی کالا به رغم اهمیت فراوان آن، کمتر مورد توجه قرار گرفته است.

در بسیاری از بازخوردهای[3] مشتریان نسبت به محصول، اطلاعاتی وجود دارد که کشف آنها برای اخذ تصمیمات عملی بسیار مؤثر است. این نوع اطلاعات گزارش‌های نقص محصولات هستند که توسط کاربران فضای مجازی بر اساس تجربه‌ها استفاده از محصول، نوشته می‌شوند. مسلماً شرکت-های تولیدکننده در فرآیند تولید، محصول را از جهات مختلف مورد آزمایش قرار می‌دهند، اما تجربه‌های مشتریان در استفاده از محصول برای تصمیم‌گیری و برنامه‌ریزی مدیران شرکت‌ها از اهمیت بالایی برخوردار است. از طرفی آگاهی از اینگونه اطلاعات می‌تواند برای مشتریان نیز مفید باشد و از تکرار وقوع خرابی محصول در هنگام استفاده از آن جلوگیری شود. بنابراین استخراج گزارش‌های نقص از متن نظر، یعنی نظر کاوی، هم برای تولیدکننده و هم برای مصرف‌کننده از اهمیت فراوانی برخوردار است [۲].

حجم زیاد نظرات و عدم ساخت‌یافتگی آن، تحقیق در زمینه‌ی نظرکاوی را همواره با مشکلاتی روبرو می‌نماید که رسیدن به دقت بالا در استخراج اطلاعات را دشوار می‌سازد[۳]. پژوهش در خصوص استخراج گزارش‌های نقص[4] نه تنها از این مشکلات مستثنا نیست، بلکه به دلیل نوع اطلاعات استخراجی با مشکلات دیگری نیز مواجه است. اغلب کاربران برای ابراز حس خود از واژگان حسی[5] استفاده می‌کنند. بنابراین با تشخیص این لغات کلیدی در متن می‌توان نظر کاربر را استخراج کرد. اما برای کشف گزارش خرابی وجود لغات بیان‌کننده‌ی احساس کافی نیست. گاهی دیده می‌شود که مشتری حس مثبتی نسبت به محصول دارد اما بنابر مشکلی که در حین استفاده از محصول مواجه شده است، گزارشی از نقص محصول را نیز مطرح می‌کند. همچنین در بسیاری از نقد و بررسی‌ها با اینکه مشتری احساسات منفی ابراز کرده است، گزارشی از خرابی و نقص محصول در متن نظر وجود ندارد و فقط سلیقه‌ی شخصی خود را مطرح کرده است. بنابراین صرفاً نمی‌توان گفت گزارش نقص فقط در نقد و بررسی‌ها با قطبیت منفی وجود دارد. به همین دلیل کلاس‌بندی نقد و بررسی‌ها به اسناد حاوی گزارش نقص و فاقد آن، با چالش‌های جدی روبه‌رو است.

[1] Opinion
[2] Reviews
[3] feedback
[4] defect
[5] Opinion words

استخراج گزارش نقص از متن نظرات کاربران یک موضوع جدید است که راه حل‌های خیلی زیادی در این زمینه ارائه نشده است. یکی از راه حل‌هایی که وجود دارد استفاده از کلماتی که به اصطلاح رنگی[۶] گفته می‌شود، است. کلمات رنگی می‌توانند مجموعه‌ای از جنبه‌های یک محصول باشند که ممکن است دچار خرابی و نقص شده‌اند. اما استفاده از این لغات ما را در تشخیص اینکه آیا نظر حاوی گزارش نقص هست یا خیر کمک نمی‌کند، بلکه فقط امکان استخراج نقص در نظری که حاوی گزارش نقص است را فراهم می‌نماید. همچنین این روش وابسته به دامنه است که کاربرد عمومی آن را محدود می سازد.

روشی دیگر جهت تشخیص گزارش نقص در متن نظر مشتری استفاده از ایده‌ای است که در تکنیک نظارت از راه دور وجود دارد. تکنیک نظارت از راه دور روشی برای تولید مجموعه‌ی داده‌های آموزشی است. این تکنیک از نشانه‌های تقریبی[۷] به عنوان برچسب‌های مثبت در متن برای آموزش کلاس‌بندی استفاده می‌کند. عباراتی که مشتریان معمولاً برای بیان نقص محصول به کار می‌برند مانند" *not allow, not let, no ability, bug, crash, ...*" می‌تواند در تشخیص اسناد حاوی گزارش نقص کمک کننده باشد. اما این نشانه‌های تقریبی باعث افزایش پاسخ مثبت کاذب هم می‌شوند.

روش پیشنهادی در این مقاله با استفاده از طبقه‌بند جنگل تصادفی، گزارش‌های نقص را از مجموعه نظرات به صورت خودکار استخراج نموده و خلاصه‌سازی می‌کند. با توجه به هزینه‌ی زیاد و زمانبر بودن برچسب زنی حجم عظیم نظرها، به عنوان بخشی از فرایند پیش پردازش از تعداد کمی داده‌ی آموزشی جهت کلاس‌بندی اسناد حاوی گزارش نقص استفاده شده است. سپس خروجی‌های مثبت آن را برای خلاصه‌سازی و ارائه اطلاعات کاربردی از اسناد حاوی گزارش نقص، به کمک تکنیک بدون ناظر، تخصیص پنهان دیریکله، به کار برده شده است. نکته حائز اهمیت دیگر اینکه روش پیشنهادی در این مقاله مستقل از دامنه می‌باشد.

ساختار مقاله به این شرح است. پس مقدمه در بخش دوم کارهای مرتبط و مشابه بررسی خواهد گردید و سپس در بخش سوم روش پیشنهادی با تاکید بر انگیزه‌ها و کاربردهای آن ارائه می‌گردد. در بخش چهار نتایج آزمون و ارزیابی روش پیشنهادی را روی مجموعه دادگان وسیع گزارش شده است و با مقاله با بخش نتیجه‌گیری به پایان خواهد رسید.

۲- کارهای مرتبط

در طول دهه‌ی گذشته، تعداد زیادی از تحقیقات روی نظر-کاوی به صورت عام و همچنین تشخیص و استخراج جنبه متمرکز بوده‌اند که اطلاعات مفیدی هم از متن نظر مشتری‌ها استخراج کردند [۴]. با این حال مطالعات بسیار کمی (تنها یک مورد[۵]) برای استخراج گزارش نقص محصول از متن نظر آنلاین مشتری صورت گرفته است.

از سوی دیگر پایگاه داده‌ای به همراه برچسب حاوی گزارش نقص و غیر آن نیز در دسترس نمی‌باشد، بنابراین استخراج گزارش نقص یک مسئله‌ی جوان است. در ادامه به کارهایی اشاره می‌کنیم که اهداف آنها تا حدودی به مساله مورد تمرکز ما نزدیک است. عمدتاً وجه مشترک این کارها با کار ما این است که آنها نیز به استخراج ریز اطلاعات می‌پردازند.

از اولین تحقیقات انجام شده در این زمینه روش‌های مبتنی بر فرکانس است که به کمک تکنیک‌های متفاوت فیلتر کردن، عبارات اسمی را که فرکانس بالاتری داشته باشند به عنوان جنبه استخراج می‌کنند [۶] [۷] مسئله‌ی تولید خلاصه از نظرات کاربران براساس جنبه‌ی محصول، در [۸] مورد مطالعه قرار گرفت. برای این کار به تشخیص تعداد تکرار جنبه‌ها می‌پردازد و گروه‌های اسمی پر تکرار را به

---

[6] Smoky در لغت به معنی دود کننده است. از آنجایی که دود برای نشان دادن و اطلاع رسانی یک وضعیت استفاده می شود، از کلمه«رنگی» به جای آن استفاده کردیم

[7] noisy signals

عنوان جنبه درنظر می‌گیرد. نقطه قوت این روش‌ها این است که در عین سادگی بسیار موثر عمل می‌کنند. اما نقطه‌ی ضعف آنها در تولید تعداد زیادی غیرجنبه است و جنبه‌هایی که تعداد کمتری تکرار شده‌اند، از دست می‌روند. همچنین نیاز به تنظیمات دستی دارد که برای هر پایگاه داده‌ای متفاوت خواهد بود.

کارهایی که اخیراً انجام شده از تکنیک‌هایی بر پایه‌ی مدل‌سازی استفاده شده است. بعضی روش‌های با ناظر مدل‌سازی آماری مانند (HMM, CRF) هستند [۹] [۱۰] و بعضی تکنیک‌های بدون ناظر مدل‌سازی موضوعی مانند تخصیص پنهان دیریکله (LDA) می‌باشند که جنبه‌های محصول و نرخ آنها را استخراج می‌کنند و اطلاعات مفیدی در اختیار مشتریان هنگام تصمیم‌گیری خرید محصول قرار می‌دهند [۱۱] [۱۲] [۱۳]. مدل تخصیص پنهان دیریکله که در [۱۴]. مطرح شد یک ابزار مفید برای خلاصه‌سازی متن است. خانم مقدم و همکاران نیز به کشف گزارش نقص محصول از متن نظرات مشتریان آنلاین پرداخته‌اند که جهت خلاصه‌سازی گزارش‌های نقص از LDA با مجموعه ویژگی‌های کیسه واژگانی[8]، اسم‌ها، فعل‌ها، عبارات اسمی، عبارات فعلی و دو-گرمی استفاده کرده‌اند. خانم مقدم تکنیک نظارت از راه دور را برای ساخت داده‌های آموزشی به کار گرفت و برای این‌کار الگوهایی به صورت دستی به عنوان نشانه‌هایی از وجود گزارش نقص در متن نظرها، استخراج کرد او کار خود را روی بازخوردهای " eBay App Reviews " انجام داده است [۱۴].

یک روش احتمالی برای تشخیص نقص از شکایات مردم در [۱۵] پیشنهاد شده است که هدفش فرموله کردن شکایات است. این کار وابسته به دامنه است و کارش را درباره‌ی مدل‌های مختلف خودرو ارائه می‌دهد و نقص‌هایی که در شکایات آمده است را خلاصه و سازمان‌دهی می‌کند. به منظور استخراج نقص‌ها از پایگاه‌داده، چهار موجودیت کلیدی تعریف می‌کند از جمله مدل موتور و سال، اجزای موتور، علائم و تاریخ تصادف که این چهار موجودیت توسط ماژول‌های استخراج موجودیت بدست آورده است. در مدل احتمالی نقص فرض می‌کند شکایت ثبت شده در مجموعه‌ی شکایات از توزیع نقص‌ها، تولید شده است که می‌توان روابط بین آنها را توسط روش احتمالی مولد، مدل کرد. سپس کار بعدی را به صورت یک مدل دامنه گرا با تکنیک تخصیص پنهان دیریکله پیشنهاد دادند. برای تعریف یک نقص حوزه‌گرا، مدل تخصیص پنهان دیریکله استاندارد را به تخصیص پنهان دیریکله دوبعدی برای خلاصه کردن نقص‌ها از نظرهای مشتریان توسعه دادند. روش پیشنهاد شده بر مشکل خوشه‌بندی‌های بدون ناظر با استفاده از تعداد زیادی ویژگی مخصوص یک حوزه که در شناسایی نقص شرکت دارند، غلبه می‌کند. این مدل به عنوان یک فرایند قابل توسعه ابتدا اجزای محصول سپس توصیفی از نقص را تولید می‌کند [۱۶]. هردو روش دامنه‌گرا هستند و از طرفی فقط شکایات را درنظر می‌گیرند که همگی حاوی گزارش خرابی هستند و خلاصه‌ای از گزارش خرابی را به صورت ساخت‌یافته ارائه می‌دهند ولی در روشی پیشنهاد ما اسناد با حس و عقیده‌های متفاوت مورد بررسی قرار می‌گیرند. زیرا ممکن است سند با اینکه عقیده‌ی مثبتی درباره‌ی کالا داشته باشد نقصی را نیز گزارش کند و سندی که حاوی حس منفی نسبت به محصول است گزارشی از خرابی محصول مطرح نکرده باشد. هدف ما این است که اگر سندی حاوی گزارش نقص است بتوان آن را کشف کرد. از سوی دیگر کار ما وابسته به دامنه نیست هرچند کارهای دامنه‌گرا نتایج دقیق‌تر خواهند داشت.

در [۱۷] یک سیستم پیشنهاددهنده با هدف استخراج پیشنهادهای مشتریان برای بهبود محصول توسط طراحی شده است؛ با این بینش که پیشنهادات با استفاده از کلمه‌های ''wishes'' یا ''regret'' در نظرات کاربران ظاهر می‌شوند. بنابراین تشخیص پیشنهاد، متکی به الگوهای نحوی- معنایی جهت بدست‌آوردن اینگونه عبارات است.

[8] Bag of Words

۳-روش پیشنهادی

۳-۱- انگیزش

از آنجایی که حجم اسناد تولید شده بر بستر وب بسیار عظیم و به صورت پویا درحال رشد است، جنگل تصادفی را جهت تشخیص اسناد حاوی گزارش نقص درنظر گرفتیم. جنگل تصادفی روی داده‌های بسیار بزرگ قابل اجرا است و می‌تواند هزاران متغیر را بدون حذف آنها مدیریت نماید. از سوی دیگر جنگل تصادفی یک طبقه‌بند با ناظر است که نیاز به داده‌های برچسب خورده دارد.

جهت خلاصه سازی و ارائه اطلاعات کاربردی از اسناد حاوی گزارش نقص، تخصیص پنهان دیریکله (LDA) را که یک روش مدل‌سازی موضوعی است استفاده کردیم. این روش بدون ناظر است و نیازی به داده‌های برچسب خورده ندارد. با توجه به اینکه اسناد تحت بررسی گزارش‌های نقص هستند؛ انتظار داریم LDA در موضوع‌بندی این اسناد نوع نقص گزارش شده در آنها را به عنوان متغیر پنهان در نظر گرفته و اسناد را بر اساس آن دسته‌بندی نماید.

۳-۲- نمادها، مفاهیم و اصطلاحات

مجموعه$P=\{P_1, P_2, P_3,...,P_M\}$ شامل محصولاتی که توسط شرکت‌ها تولید می‌شوند. $R_p= \{r_1, r_2, r_3,...,r_n\}$ نیز برای هر محصول، مجموعه‌ی از نقد وبررسی‌هایی است که توسط مشتریان در بستر وب قرار گرفته است. در مجموعه‌ی R برخی از نقد و بررسی‌ها حاوی گزارش نقص محصول هستند که این نظرها را با D(Defect) و سایر بازخوردها را با O(Others) نشان می‌دهیم.

سند: منظور از سند در این پژوهش متن کامل یک نظر است. مثلا شکل (۲) و همچنین شکل (۳) نمونه‌هایی از نظرهای موجود در مجموعه تحت بررسی هستند. یک نظر می‌تواند کوتاه (در حد یکی دو جمله) یا بلند (در حد ده‌ها جمله) باشد. نظرات بلند معمولا حاوی اطلاعات متنوعی مانند تجربه خرید، معرفی محصولات مشابه، بیان نقاط قوت و ضعف محصول و حتی گاهی مطالب بی‌ربط به محصول مورد بحث هستند.

گزارش نقص: بازخوردهایی که به طور واضح به سختی در استفاده، خطا، اشکال و ناتوانی محصول اشاره دارند به عبارت دیگر مشتری جنبه‌هایی از محصول را که درست کار نمی‌کنند یا نیاز به ترمیم دارند گزارش می‌کند. گزارش نقص معمولا در قالب چند جمله متوالی یک نظر ارائه می شود. مثلا در شکل(۱) جملات و عبارات "*It's heavy, hard to push, a 1-day battery life, freeze up and crashes all the time*" نقص موجود در کتابخوان الکترونیکی مد نظر را گزارش می‌کنند.

I am still waiting for the perfect ebook reader. I bought the Nook for these reasons: 1) It reads industry-standard ePub-format ebooks, 2) it's tightly integrated with the B&N; ebook store, 3) the ebooks are encrypted in a well-documented easily-understood format that is portable across multiple devices so they can be decrypted and read in, say, your iPad's Nook reader software, or even in a Sony Reader (with the very latest firmware), without having to be re-purchased because of DRM nonsense.The problem is that the Nook simply doesn't live up to its promise. The \"paper-white\" display is more an off-beige, and reflects light in a way that makes it hard to read with a reading light (necessary because it has no backlight, as is true for all ePaper devices). It's heavy and the buttons to change pages are hard to push, especially with gloved hands as you might have while reading outdoors on a cool day. The \"5 day battery life\" in reality for me has been a 1-day battery life, read a book, and it needs to be recharged, and be darn sure to turn it off. The thing freezes up and crashes all the time even with the very latest software, and is excruciatingly slow even with the very latest software. The latest software added classifications for the ebooks so you could sort them into pseudo-folders, which is necessary given how excruciatingly slow the Nook is to scroll through its book list (get about 50 books on the list and you're in for major pain), but the clunky way they implemented this makes those of us who've gotten used to modern user interfaces frown and shake our heads.Sad to say, I really can't recommend any current eBook reader. Either they're too clumsy to use (Nook), have no books available for them (Sony), or have a proprietary eBook format that locks you into a single vendor (Kindle). I'm seriously considering buying an iPad, yes, it will only work for 9 hours or so on a battery charge, but that's true of the Nook too in real actual use and the iPad is usable for a lot of other things too. It's just disappointing that I can't get an ePaper-based reader that meets my criteria (non-proprietary ebook format, long battery life, compact, decent user interface), and instead have things either crippled by bad design decisions or crippled by having a proprietary ebook format that locks you into a single vendor. Well, I don't like

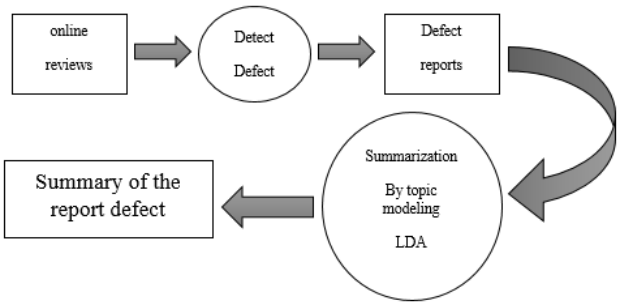
crippled, so I'll look elsewhere, thank you very much...

شکل۱- نمونه یک نظر درباره یک کتابخوان الکترونیکی

موضوع: منظور از موضوع نظر نوع نقص گزارش شده در آن است. مثلا سختی یافتن یک منو یا کلید خاص در واسط کاربری برنامه یک نوع نقص است و کاهش سریع باتری نقصی از نوع دیگر است. گزارش نقص‌هایی که مشابه دارند در یک دسته قرار می گیرند. این دسته بندی کار مطالعه و ارزیابی نظرات کاربران را خیلی آسان می سازد. مثلا اگر تعداد قابل توجهی از نظرات کاربران در ذیل موضوع «کاهش سریع توان باتری» قرار بگیرند، می‌توان نتیجه گرفت که مساله محصول مورد بحث جدی است.

۳-۳- تشریح روش پیشنهادی

کلاس‌بندی اسناد به گزارش نقص و سایر با روش جنگل تصادفی و داده‌هایی که به صورت دستی برچسب زده شده، با مجموعه ویژگی کیسه واژگانی انجام گردید. جنگل تصادفی یک روش باناظر است که برای طبقه‌بندی دو کلاسی عملکرد خوبی دارد [۱۸]. اما استخراج گزارش نقص از متن نظر کاربران اینترنتی نوعاً مسئله‌ای است که نمی‌توان آن را به صورت با ناظر حل کرد، به دلیل اینکه حجم نظرها بسیار زیاد است و برای تکنیک‌های با ناظر برچسب زنی این حجم عظیمی از متن‌ها زمان‌گیر، هزینه بر و مستعد خطاست. به جهت بهره‌گیری از مزایای کلاس بندی با ناظر، در این پژوهش از تعداد داده‌های آموزشی کمی جهت کلاس‌بندی استفاده شد و در واقع یک کلاس‌بندی ضعیف روی اسناد انجام گردید. بعد از کلاس‌بندی اسناد و مشخص شدن اسناد حاوی گزارش نقص توسط جنگل تصادفی از بین حجم عظیمی از اسناد، مهمترین مرحله نحوه‌ی ارائه‌ی گزارش نقص محصول است، زیرا مطالعه‌ی کل اسناد حاوی گزارش نقص که اطلاعات اضافی دیگری نیز دارند برای مدیران و تولیدکنندگان خسته‌کننده و زمان‌بر است. هدف، ارائه‌ی خلاصه‌ای کاربردی از گزارش‌های نقص می‌باشد. تکنیک تخصیص پنهان دیریکله (LDA) با مجموعه ویژگی دوگرمی را به منظور خلاصه‌سازی بعد از کشف اسناد حاوی گزارش نقص استفاده گردید. مراحلی که برای ارائه‌ی گزارش نقص باید انجام شود در شکل (۲) آمده است.



شکل ۱)گام‌های اصلی کشف گزارش نقص

۴- آزمون و ارزیابی

۴-۱- معرفی روش آزمون

دقت[9]، بازنمایی[10] و اندازه F[11] معیارهای کاربردی در حوزه بازیابی اطلاعات هستند که میزان تناسب اسناد بازیابی شده توسط سیستم را با نیاز کاربر تعیین می‌کنند. این سه معیار به صورت زیر تعریف می شوند.

$\text{Precision} = \frac{Q_{related}}{Qretrieved}$	رابطه(۱)
$\text{Recall} = \frac{Q_{related}}{N_{related}}$	رابطه(۲)
$\text{F\_Score} = 2\frac{Precisoin \times Recall}{Precision + Recall}$	رابطه(۳)

[9] Precision
[10] Recall
[11] F-Score/ Measure

در این روابط N تعداد کل اسناد پیکره، $N_{related}$ تعداد اسناد مرتبط با پرس و جوی خاص، $Q_{retrieved}$ تعداد اسناد بازیابی شده برای این پرس و جو و $Q_{related}$ تعداد اسناد بازیابی شده مرتبط با پرس و جو هستند. دو معیار دقت و بازنمایی معمولا در حالت تقابل با همدیگر هستند و افزایش یکی سبب کاهش دیگری می‌شود. از این رو مقایسه دو سیستم بازیابی بر اساس اندازه F که ترکیبی از هر دوی این معیارهاست؛ انجام می‌گیرد. لازمه‌ی محاسبه دقت و بازنمایی داشتن داده‌های برچسب خورده هست و از طرفی کار با حجم عظیمی از اسناد هزینه‌ی برچسب‌زنی بالایی را می‌طلبد. از آنجایی که در این پژوهش برای کلاس‌بندی از تعداد داده‌های آموزشی کم استفاده شده است و روش خلاصه سازی یک تکنیک بدون ناظر می‌باشد، از اینرو نیازی به برچسب زنی کل اسناد نیست. برای ارزیابی نتایج کلاس-بندی، ۱۰درصد از کل اسناد به صورت تصادفی انتخاب و برچسب زنی شدند. بر اساس نسبت تعداد اسناد حاوی گزارش نقص در این مجموعه، تعداد اسناد حاوی گزارش نقص در کل پیکره بر اساس روابط (۴) و (۵) تخمین زده شد.

$N_d = \alpha N_{total}$	رابطه(۴)
$\alpha = \frac{N_{defect}}{N_{random}}$	رابطه(۵)

در روابط فوق N_{random} تعداد اسنادی است که به صورت دستی برچسب خورده‌اند. از این میان N_{defect} تعداد اسنادی است که برچسب مثبت دارند. با توجه به انتخاب تصادفی و یکنواخت اسناد برای برچسب زنی دستی، می‌توان این نسبت را به کل پیکره تعمیم داد. از این رو برآورد می‌شود تعداد N_d سند در پیکره حاوی گزارش نقص باشند. در محاسبات و تصمیم‌گیری‌های بعدی این تعداد لحاظ شده است. همچنین برای ارزیابی دقت جنگل تصادفی ده درصد از اسناد پیکر به صورت تصادفی انتخاب و برچسب زنی شدند. سپس این مجموعه با جنگل تصادفی به دو کلاس گزارش نقص و سایر طبقه‌بندی شدند. نهایتا دقت جنگل تصادفی، β، معادل با نسبت تعداد اسنادی که درست طبقه‌بندی شدند؛ بدست آمد. مشابه قبل، می‌توان این دقت را بر روی کل پیکره هم تعمیم داد. یعنی اگر جنگل تصادفی M سند از کل پیکره را گزارش نقص تشخیص دهد؛ می‌توان انتظار داشت که حدود $\beta \cdot M$ تای آنها واقعا گزارش نقص باشند. با توجه به مقادیر α وβ ، معیارهای دقت و بازنمایی و اندازه F محاسبه گردیده است.

یکی از روش‌های ارزیابی و آزمون موضوع‌های بدست آمده از LDA استفاده از داوری خبرگان است. اگر چه به نظر می‌رسد که این یک فرض قوی است که فضای پنهان و نامعلومی که توسط مدل‌سازی موضوعی پیدا شده است معنادار و مفید باشد ولی ارزیابی هر یک از این فرض‌ها کار دشواری است. زیرا پیدا کردن موضوعات یک فرآیند بسیار دشوار و هزینه بر است. یعنی یک لیست استاندارد کامل از موضوعات برای هر متنی وجود ندارد. بنابراین با مطالعه‌ی اسناد در هر گروه ارزیابی صورت خواهد گرفت.

مدل‌سازی موضوعی به این نحو است که واژه‌ها و ترکیب‌هایی به عنوان موضوع اسناد استخراج می‌شوند. سپس خبرگان این واژه‌ها و عبارت‌ها را در قالب موضوعات قابل فهم و استنباط پالایش و معرفی می‌کنند. پس از استخراج واژگان و عبارات اولیه، در هر موضوع واژه یا عبارتی را که با سایر واژه‌ها پیوستگی معنایی ندارد حذف نموده و موضوعات نهایی با توجه به سایر واژه‌ها مشخص می‌گردد. سپس به جهت تشخیص مرتبط بودن یا نبودن اسناد به موضوع، اسناد بررسی می‌گردند.

۴-۲- معرفی دادگان و ابزارها

تعداد ۲۰ هزار نظر مشتریان درباره‌ی محصولات الکتریکی از سایت آمازون گرفته شده است. برچسب زنی اسناد به صورت دستی و تحت نظر خبره صورت گرفته است و به اسناد برچسب حاوی گزارش نقص (D) و سایر (O) زده شده است.

پیش‌پردازش و نرمال‌سازی متن به کمک ابزار متن پردازی سنتی GnuWin32 انجام گردید. این فرایند شامل حذف کلمات بی‌اثر، حذف کارکترهای غیر الفبای انگلیسی مانند #، $ و ...، ریشه‌یابی و کوچک کردن تمام

کردن تمام حروف می‌باشد. سپس واژه‌نامه‌ای[12] از واژه‌های اسناد ایجاد گردید. به این دلیل این واژه‌نامه را ایجاد شد که امروزه کاربران اینترنتی در نوشته‌های خود از واژه‌هایی استفاده می‌کنند که ممکن است حتی در لغت‌نامه‌های مفصل نیز موجود نباشند، مانند mer30، goooood-5، starو ... . در نهایت جهت خلاصه‌سازی توسط مدل‌سازی موضوعی (LDA) از کتابخانه‌ی gensim[13] در زبان python استفاده گردید.

۴-۳- نتایج آزمایش‌ها

۱-۴-۳- ارزیابی تشخیص اسناد حاوی گزارش نقص

مقادیر معیارهای دقت، بازنمایی و اندازه F برای کلاس‌بندی اسناد در جدول (۱) آمده است.

جدول۱: نتایج ارزیابی جنگل تصادفی

روش	معیارF	دقت	بازنمایی
نظارت از راه دور	۰,۵۶	۰,۴۰	۰,۹۱
جنگل تصادفی	۰,۵۴	۰,۷۲	۰,۴۳

ردیف اول این جدول نتایج کار مقدم و همکاران است که با روش نظارت از دور خرابی‌های گزارش شده را استخراج می‌نماید [۵]. در این روش از ۵۰ هزار نظر برچسب خورده (به صورت دستی) استفاده شده است. به دلیل متفاوت بودن اندازه و محتوای مجموعه دادگان نمی‌توان بین این دو مطالعه مقایسه دقیق و قاطعی انجام داد اما می توان برخی از جوانب قدرت و ضعف هر دو روش را برشمرد.

I've had my NST since last July, and I've been very happy with it.Pros:- Battery life when wifi is off is as good as advertised.- The page turn rate was already fast, but the update last November made it super speedy. Seriously, I've played with the current e-ink Kindles, and the difference in refresh rate might SEEM small on paper, but in practice it's a very noticeable difference.- I never had the wifi problems others did after the November firmware update, but I understand that the latest firmware update should solve it.- The NST feels really nice when you're holding it, and I really like that there are physical page turn buttons in addition to the onscreen touch turning - I use both, depending on whether I'm sitting up or lying down when I read, etc.- Navigation is very intuitive.- I bought a $5 4gb micro SD card and have had no problems using it with the NST.- Sideloading non-DRMed, non-B&N; content downloaded from places like Project Gutenburg is very easy, and it all goes into the same library as your B&N; downloaded content.Cons:- The user interface is easy to use, but it's also VERY basic, and there are very few features. You can organize your books into \"shelves,\" but only on the device itself, and it's a cumbersome process. You can sort books by title, author, and date added, and... that's pretty much it. The NST isn't a tablet and I don't want it to be, but there are still some pretty simple features that don't seem like it would have been that hard to add, and more flexible organization is one of them.- Once a book's in the library, you can't really see anything about it besides the title and author. Metadata from sideloaded content doesn't show up, and even purchased content requires you to be on wifi to see more information.That's about it. My cons list is really more of a wishlist, and I wouldn't hesitate to recommend the NST to anyone, especially at the lowered $99 price. I imagine a new touch reader will probably be released within the next few months, but unless the user interface is majorly updated, it's hard to imagine I'd feel the need to upgrade, since the current version meets almost all of my needs perfectly well.

شکل ۳ : دیدگاه یک مشتری درباره یک محصول الکترونیکی

روش مقدم و همکاران [۵] به دلیل استفاده از نشانه‌های نویزی نتایج مثبت کاذب به تعداد زیادی رخ داده است، اما این روش اکثر اسناد حاوی گزارش نقص را یافته است. این

[12] Vocabulary
[13] https://pypi.python.org/pypi/lda

روش جزو دسته عمومی روش‌های بازنمایی زیاد[14] قرار می‌گیرد. گرچه کشف همه نواقص گزارش شده اهمیت زیادی دارد، اما تعداد زیاد نمونه‌های مثبت کاذب سبب می‌شود که مدل‌سازی موضوعی LDA موضوعات حاشیه‌ای و پس زمینه متعددی تولید کند [۱۳] برای درک بهتر این رویداد تصور کنید که همه نظرات اعم از گزارش نقص و سایرین را تحلیل موضوعی نماییم. با توجه به اینکه تنوع محصولات و اشیا مورد بحث در این نظرها، تفکیک موضوعی به تفکیک نظرات بر اساس نوع محصول مورد بحث متمایل خواهد شد. یعنی بیش از اینکه وجود یا عدم وجود گزارش نقص در یک نظر معیار تخصیص آن نظر به موضوع خاصی باشد، نوع و مدل محصول سبب خواهد شد تا نظرات در گروه‌های مختلف قرار بگیرند. ما به عنوان مطالعه اولیه چنین فعالیتی را انجام دادیم و دریافتیم که استفاده از موضوع‌بندی بدون توجه به ماهیت نظر گمراه کننده است.

در مقابل روش‌هایی که هدفشان بازنمایی بالاست، روش‌های دارای دقت بالا[15] بر این حقیقت تاکید دارند که نظراتی که تفکیک و طبقه‌بندی موضوعی می‌شوند اصولا جزو گروه هدف (در اینجا گزارش نقص) باشند. بر اساس این فرض می‌توان امیدوار بود که تفکیک موضوعی انجام شده روی این نظرات بیانگر تفکیک انواع نقص‌های گزارش شده می‌باشد.

جنگل تصادفی به صورت ذاتی دادگان دارای تنوع زیاد را به خوبی دسته‌بندی می‌کند. دلیل این توانایی این است که این روش با انتخاب تصادفی زیرمجموعه‌های متنوع از ویژگی‌ها، تعداد زیادی درخت می‌سازد که هر یک از آنها می‌تواند بخشی از دادگان را به خوبی طبقه‌بندی نماید. تجمیع نتایج این درخت‌ها در یک قالب ساده اما کارآمد به تولید نتایج طبقه‌بندی دقیقی و کارآمدی منجر می‌شود. اسناد متنی اعم از نظر و غیر آن معمولا در قالب بردارهای واژگانی بیان می‌شود. از این رو برای هر سند تعداد زیادی ویژگی استخراج می‌شود که طبقه‌بندی‌هایی مثل جنگل تصادفی می‌توانند از آن بهره ببرند. نتایج آزمایش‌های ما نیز نشان می‌دهد جنگل تصادفی تقریباً نیمی از اسناد حاوی گزارش نقص را بازیابی کرده است. کلاس‌بندی جنگل تصادفی با تعداد داده‌های آموزشی کم در کشف گزارش نقص نیز نتیجه‌ی مطلوبی دارد و با وجود تعداد داده‌های آموزشی کم توانسته دقت بالایی در عملکرد خود داشته باشد. بررسی اسنادی که به اشتباه کلاس‌بندی شده‌اند (مانند شکل (۳)) نشان داد این اسناد با وجود اینکه مشتری به نقص کالا اشاره کرده‌است، به محصول علاقه زیادی داشته و از لغاتی که حس مثبت را ابراز می‌کنند استفاده زیادی کرده است. در جدول (۲) تعدادی از جملات این نظر همراه با برچسب‌شان آمده است. می‌توان دید که مشتری علاقه زیادی به محصول داشته و بسیار از آن تمجید کرده است. همچنین در ضمن این تعریف و تمجید نواقصی را هم گزارش نموده است.

جدول ۲: نمونه‌هایی از جملات نظر شکل، حاوی نظر مثبت و گزارش نقص

گروه	موضوع	مجموعه واژه‌های مرتبط
اول	برنامه‌های نرم‌افزاری	Card, software, app, memory tablet,install,window,android,format, driver,download,comput
دوم	بازگشت محصول	Back, return, got, bought, amazon, didn
سوم	رسانه‌ی ذخیره سازی	Tape , disk , record, clean, drive, vcr, cassett, floppy, cleaner, maxel
چهارم	باتری و شارژر	Batteri, charg, charger, usb, plug, power, recharge, garmin, adapt, Connect , cord, port,fit
پنجم	دستگاه پخش کننده موسیقی و فیلم	Player , dvd, soni, disc, year, rio, skip, mp3, panason, movi, repair
ششم	پخش کننده صدا	Radio, sound, speaker, good, headphone, better, like, even, much Look , volum
هفتم	پانل نگهدارنده‌ی تلویزیون	Case , lock, mount, palm, cover, plastic
هشتم	کتاب خوان الکترونیکی	Nook, book, kindl, read, purchas, barn, custom, nobl, screen, Service

[14] High Recall

[15] High Precision

تحلیل موضوعی گزارش‌های نقص با بردارهای دو گرمی قابلیت توصیف و تفسیر بهتری دارد. زیرا اغلب نواقص ونارضایتی‌ها با ترکیب‌ها و اصطلاحات دو کلمه‌ای بیان شده‌اند. مثلاً افعال منفی معمولا با پیشوندهای don't و can't استفاده شده‌اند. همچنین صفات ساده‌ای مثل bad, worst, low که بیانگر دیدگاه منفی هستند پیش از نام محصول یا جنبه‌ای از آن آمده‌اند.

بعضی از واژگان مختص یک یا دو موضوع هستند. این واژگان کم تکرار معمولاً عنوان یک محصول یا جنبه خاصی از آن هستند. در مقابل، برخی از واژگان پر تکرار هستند. یعنی در سه موضوع یا بیشتر ظاهر شده‌اند. این گروه نشان‌دهنده نوع نقص یا نارضایتی هستند.

پرتکرارترین واژگان افعال کمکی منفی هستند. استفاده از افعال کمکی منفی در بیان نقص و خرابی محصول در زبان انگلیسی رایج و مطابق دستور زبان است. البته لغات isn't و aren't خیلی متمایزکننده نیستند، چون در اکثر جملات وجود دارند. این واژگان به نوعی بیانگر موضوع عمومی موسوم به موضوع پس‌زمینه[16] هستند. موضوع پس‌زمینه حوزه عمومی مورد بحث همه اسناد تحت بررسی را نشان می‌دهد. به عنوان یک نتیجه جنبه‌ای می‌توان گفت که گزارش نقص محور نظرهای تحت بررسی بوده است. ظهور barn_noble به عنوان واژه پرتکرار نشان می‌دهد که اکثر شکایات از شرکت barn&noble بوده است. همچنین پرتکرارهایی مثل battery power و battery life از بین جنبه‌های گوناگون یک محصول بر این حقیقت تاکید می‌کنند که اکثر مشتریان عمر باتری محصول را مورد نقد و بررسی قرار داده‌اند. به صورت مشابه، واژگانی مثل (cd-player, sound-quality) نیز جزء جنبه‌هایی هستند که زیاد مورد نقد و بررسی مشتریان قرار گرفته‌اند. ترکیب پر تکرارcustomer service گویای این است که افراد به دلیل وجود نقص به خدمات پس از فروش مراجعه کرده‌اند.

جدول (۴) سه گروه از واژگان قابل توجه در موضوعات را نشان می‌دهد. گروه اول الگوهایی هستند که مستقیما به نوع نقص اشاره نمی‌کنند اما از حضور آنها می توان به وجود گزارش نقص در یک نظر پی برد. این واژگان را نیز می‌توان به عنوان نشانگرهای نویزی نقص و جزو موضوع پس‌زمینه برشمرد. وجود این نشانگرها در اغلب موضوعات حاکی از عملکر مناسب جنگل تصادفی در کلاس‌بندی و استخراج گزارش‌های نقص است.

جدول۴: نشانگرهای گزارش نقص، نوع نقص و جنبه هدف بدست آمده از تحلیلی موضوعی

گروه	واژگان عضو
نشانگر گزارش نقص	a lot-defect, another-one, another-problem, biggest-complaint, big-wast, bung-buck, buy-another, buyer-beware, cant-use, cheap-feel, cheaply-made, common-problem, didn't-expect, disappoint-experience, don't-buy, don't-recommand, dosen't-allow, explain-problem, first-time, frustrate-try, main-problem, money-back, never-able, notic-problem, piece-junk, return product, send-back, s-shame, try-get, try-use, wast-money, wast-time
نشانگر نوع نقص	slow-type, low-power, crash-often, adapt-fail, soft-reset, permanent-damage, defect-camera, background-hiss, sort-problem, player-stop, difficult-remove, background-noise, sound-horrible, poor-sound, drain-battery, bad-connect, start-freez, radio-faulty, get-hot, badly-written, start-skip, read-bad, give-break, bad-patch, stop-play, really-slow, got-stuck, battery-diy, stop-work, screen-freez, hit-pause, brock-first, whip-antenna, short-antenna, horizont-line, camera-eat, , simply-stop, lot-noise, come-dark

[16] Background topic

جنبه هدف	Battery-compartment, diamond-rio, extern-antena, flash-card, graphic-card, lcd-screen, memori-card, page-turn, nook-tablet, usb-cable, cell-phone, floppy-disk, image-quality, mp3-s, phone-jack, power-cord, dvd-player, recharge-battery, e-reader,mp3-player, nook-color, touch-screan

واژگان گروه اول به نوعی بیانگر عقیده، دیدگاه، تصمیم و توصیه نظردهنده هم می باشند. برای روشن شدن این مطلب مفهوم تعدادی از آنها توضیح داده شده است.

Don’t-buy: مشتری که از محصولی راضی نباشد، حال به دلیل نقصی که دارد یا اینکه عقیده شخصی وی نسبت به محصول منفی باشد دیگران را نیز از خرید محصول منصرف می‌کند.

buy-another, another-one: مشتری محصولی را خریداری کرده است به دلیل نقصی که داشته مجبور شده است یکی دیگر تهیه کند. در برخی اسناد مشتری از محصول دوم راضی است اما در برخی دیگر به نقص مشابه قبلی اشاره کرده است.

Cant-use: به دلیل وجود نقص آن‌گونه که باید از محصول نتوانسته‌اند استفاده کنند مثلاً محصولی علیرغم تبلیغی که کرده است با دستگاه خاصی سازگاری ندارد و مشتری نتوانسته از محصول بهره‌ی کامل ببرد.

First-time: برخی مشتریان از وجود نقص و خرابی محصول در ابتدای استفاده و یا دریافت محصول شکایت کردند.

Send-back, return product: خیلی از مشتریان محصولی که نقص دارد را بازپس می‌دهند.

Try-use, try-get: این دو-گرمی نیز نشانه‌ادی از وجود نقص است. زیرا اسنادی که این لغات را دارند به این نکته اشاره می‌کنند که مشتری با روش‌های مختلف سعی در استفاده از محصول داشته است اما به دلیل نقصی که دارد موفق نشده است.

Wast-money, wast-time: وقتی مشتری از محصول راضی نیست صرف زمان و هزینه برای آن را هدر رفت می‌داند.

Never-buy: به دلیل عدم رضایت، مشتری اعلام می‌کند که دیگر از این نوع محصول یا محصولات شرکتی هرگز خریداری نکند.

Didn’t-expec: مشتری علیرغم تبلیغی که برای محصول شده انتظار چنین نقصی را ندارد.

گروه دوم واژگان به صورت مستقیم نوع نقص را نشان می‌دهند. شاید این گروه را بتوان مهمترین دست‌آورد تحلیل موضوعی قلمداد کرد. در جدول (۴) گروه با عنوان نشانگرهای نقص مشخص شده‌اند.

گروه سوم واژگان جنبه‌هایی از محصولات را نشان می‌دهند که بیشتر مورد بحث بوده اند. این گروه از دو جهت اهمیت ویژه دارند. نخست اینکه نشان می‌دهد کاربران در مقایسه و گزینش محصولات به چه ویژگی‌هایی توجه دارند. مثلاً با اینکه اغلب گوشی‌های تلفن همراه و ادوات الکترونیکی پوشیدنی ضدآب یا ضد ضربه نیستند اما این جنبه‌ها کمتر مورد توجه بوده‌اند اما در مقابل باتری، صفحه نمایش و کابل شارژ در مرکز توجه قرار داشته اند. دلیل دوم اهمیت این جنبه ها این است که با کاوش قواعد انجمنی[17] بین نشانگرهای نقص و این جنبه‌ها می‌توان نقاط قوت و ضعف محصولات مختلف را به صورت خودکار استخراج و دسته‌بندی کرد.

۵- دسته‌بندی

اخیراً تمرکز پژوهشگران حوزه نظرکاوی بیشتر روی استخراج جنبه‌های محصول و تخمین امتیاز آنها از بازخوردها می‌باشد. گرچه استخراج جنبه و تخمین امتیاز آن می‌تواند به مشتریان جهت تصمیم‌گیری در خرید

[17] Association rules

محصول کمک کند؛ مدیران شرکت‌ها و تولیدکنندگان برای اخذ تصمیمات عملی و برنامه‌ریزی‌های تجاری خود نیاز به اطلاعات دقیق‌تری دارند. کشف نقص محصول نقش موثری در ارائه‌ی سریع راه حل کارا و درنتیجه راضی نگهداشتن مشتریان دارد. در این مقاله روشی پیشنهاد گردیده است که بتوان اطلاعات کاربردی از بازخورد مشتریان استخراج کرد. روش پیشنهادی مزایای زیر را داراست :

- به صورت خودکار گزارش‌های نقص را از متن نظرهای مشتریان استخراج می‌کند،
- مستقل از دامنه است،
- برای هر پایگاه داده‌ای قابل اجرا می‌باشد و
- به دلیل اینکه مدیران شرکت‌ها مجبور به خواندن کل متن نظر نباشند خلاصه‌ای از گزارش‌های نقص کشف شده را ارائه می‌دهد.

نتایج روی مجموعه داده‌های واقعی از سایت آمازون نشان داد برای کشف گزارش خرابی بررسی وصرفاً تحلیل لغات حسی مفید نیست. اما طبقه‌بندی مثل جنگل تصادفی با دادگان آموزشی کم نیز می تواند کلاس‌بندی قابل قبول داشته باشد. تخصیص پنهان دیریکله با مجموعه ویژگی دو-گرمی خلاصه‌ای از گزارش‌های نقص پرتکرار و اطلاعاتی نظیر اینکه بیشتر کدام جنبه‌های محصول مورد نقد و بررسی هستند را ارائه داد. همچنین روش پیشنهادی توانست به طور خودکار کشف الگو داشته باشد. فهرست واژگان تشکیل‌دهنده موضوع پس زمینه یکبار دیگر بر موفقیت جنگل تصادفی در تشخیص گزارش نقص تاکید دارد.

نشانگرهای نقص بدست آمده را می‌توان در مطالعات جدید برای پیش پردازش و فیلتر نظرهای حاوی نقص استفاده کرد. همچنین می توان این الگوها را در مطالعات مبتنی بر نظارت از راه دور [۱] بکارگرفت.

می‌توان از تکنیک نظارت از راه دور با استفاده از الگوهایی که به صورت خودکار در این پژوهش استخراج شد جهت بهبود نتایج کلاس‌بندی استفاده نمود. با توجه به روشی که در این پژوهش مطرح شد برای استخراج اطلاعات دیگری همچون استخراج نظرهایی که از محصول یا سرویس‌های خدماتی ناراضی هستند، نظراتی که عقیده‌ی مثبتی دارند، استخراج نظرهایی که دو یا چند کالا را مقایسه کرده‌اند و استخراج اطلاعات از مقایسه‌ها و نظرهایی که حاوی پیشنهادات مشتریان است می‌توان استفاده کرد.

منابع

1. B. Liu and L. Zhang, "A survey of opinion mining and sentiment analysis," in *Mining text data*, Springer, 2012, pp. 415-463.

2.S. Moghaddam and M. Ester, "Opinion digger: an unsupervised opinion miner from unstructured product reviews," in *Proceedings of the 19th ACM international conference on Information and knowledge management*, 2010.

3.B. Liu, M. Hu and J. Cheng, "Opinion observer: analyzing and comparing opinions on the web," in *Proceedings of the 14th international conference on World Wide Web*, 2005.

4.E. Cambria, B. Schuller, Y. Xia and C. Havasi, "New avenues in opinion mining and sentiment analysis," *IEEE Intelligent Systems*, vol. 28, pp. 15-21, 2013.

5.S. Moghaddam, "Beyond sentiment analysis: mining defects and improvements from customer feedback," in *European Conference on Information Retrieval*, 2015.

6.L.-W. Ku, Y.-T. Liang and H.-H. Chen, "Opinion extraction, summarization and tracking in news and blog corpora," in *Proceedings of AAAI*, 2006.

7.M. Hu and B. Liu, "Mining opinion features in customer reviews," in *AAAI*, 2004.

8.W. Jin, H. H. Ho and R. K. Srihari, "OpinionMiner: a novel machine

learning system for web opinion mining and extraction," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009.

9.F. Li, C. Han, M. Huang, X. Zhu, Y.-J. Xia, S. Zhang and H. Yu, "Structure-aware review mining and summarization," in *Proceedings of the 23rd international conference on computational linguistics*, 2010.

10.S. Moghaddam and M. Ester, "The FLDA model for aspect-based opinion mining: addressing the cold start problem," in *Proceedings of the 22nd international conference on World Wide Web*, 2013.

11.W. X. Zhao, J. Jiang, H. Yan and X. Li, "Jointly modeling aspects and opinions with a MaxEnt-LDA hybrid," in Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing, 2010.

12.S. Brody and N. Elhadad, "An unsupervised aspect-sentiment model for online reviews," in Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics,

2010.

13.D. M. Blei, A. Y. Ng and M. I. Jordan, "Latent dirichlet allocation," Journal of machine Learning research, vol. 3, pp. 993-1022, 2003.

14.Z. Qiao, X. Zhang, M. Zhou, G. A. Wang and W. Fan, "A Domain Oriented LDA Model for Mining Product Defects from Online Customer Reviews," 2017.

15.C. Brun and C. Hagege, "Suggestion Mining: Detecting Suggestions for Improvement in Users' Comments.," Research in Computing Science, vol. 70, pp. 199-209, 2013.

16.L. Zhang and B. Liu, "Aspect and entity extraction for opinion mining," in Data mining and knowledge discovery for big data, Springer, 2014, pp. 1-40.

17.X. Zhang, Z. Qiao, L. Tang, W. Fan, E. Fox and G. Wang, "Identifying Product Defects from User Complaints: A Probabilistic Defect Model," 2016.

18.A. Liaw, M. Wiener and others, "Classification and regression by randomForest," R news, vol. 2, pp. 18-22, 2002.

.