فصلنامه علمی امنیت ملی
سال یازدهم، شماره چهلم، تابستان ۱۴۰۰
مقاله پنجم از صفحات ۱۵۴-۱۲۱

مقاله پژوهشی: ارائه چارچوب مدیریت هویت دیجیتال در فضای سایبر با رویکرد آمیخته

20.1001.1.33292538.1400.11.40.5.1

هاتف رسولی [۱]، چنگیز والمحمدی [۲]، ناصر آزاد [۳] و قنبر عباس‌پور اسفدن [۴]

تاریخ دریافت: ۱۳۹۸/۱۲/۱۶ **تاریخ پذیرش: ۱۳۹۹/۰۷/۰۱**

چکیده

هویت دیجیتال به‌عنوان یکی از زیرساخت‌های اصلی و اساسی فضای سایبر باعث تقویت امنیت و حاکمیت کشور در فضای سایبر می‌شود. مدیریت هویت دیجیتال یکی از راهبردی‌ترین بحث‌های امنیت سایبری و پایه و اساس ایجاد اعتماد در فضای سایبر است. هدف این مقاله شناسایی و اولویت‌بندی معیارها و شاخص‌های هویت دیجیتال در قالب چارچوبی جامع برای مدیریت هویت دیجیتال در فضای سایبر کشور است. این تحقیق از لحاظ هدف کاربردی با رویکرد بنیادین و روش انجام توصیفی- اکتشافی است. روش گردآوری اطلاعات، مطالعات کتابخانه‌ای و میدانی از طریق پرسشنامه و مصاحبه است. با مرور ادبیات نظری تحقیق، عوامل اثرگذار شناسایی و سپس به روش دلفی- فازی غربالگری شد. جهت تعیین روابط بین عوامل اصلی و عوامل فرعی و همچنین وزن‌دهی و اولویت‌بندی آن ها از روش ترکیبی فرایند تحلیل شبکه و دیمتل استفاده شد. نتایج تجزیه وتحلیل داده‌ها نشان داد که عامل «برنامه‌ریزی راهبردی» تأثیرگذارترین عامل در مدیریت هویت دیجیتال است. در حل مسئله به روش ترکیبی فرایند تحلیل شبکه و دیمتل نیز «مدیریت دسترسی» در عوامل اصلی و «کنترل دسترسی به کلیه منابع و اطلاعات تنها از طریق سیستم مدیریت هویت دیجیتال» در عوامل فرعی اولویت اول را کسب کردند.

۱. دانش‌آموخته دوره دکتری - رشته مدیریت فناوری اطلاعات - دانشگاه آزاد اسلامی - واحد تهران- جنوب - تهران - ایران Hatef.rasouli@gmail.com

۲. دانشیار دانشکده مدیریت - گروه مدیریت صنعتی - دانشگاه آزاد اسلامی - واحد تهران- جنوب - تهران - ایران، (نویسنده مسئول) ch_valmohammadi@azad.ac.ir

۳. استادیار دانشکده مدیریت - گروه برنامه‌ریزی علوم اداری و مدیریت - دانشگاه آزاد اسلامی - واحد تهران- جنوب - تهران - ایران a_azad@azad.ac.ir

٤. استادیار دانشکده مدیریت - گروه مدیریت صنعتی- دانشگاه آزاد اسلامی - واحد تهران- جنوب - تهران - ایران gh_abbaspour@azad.ac.ir

کلیدواژه‌ها: هویت دیجیتال، مدیریت هویت دیجیتال، فضای سایبر، مدیریت هویت، احراز هویت

۱. مقدمه و بیان مسئله

تحولات دیجیتال رخ داده در حوزه اینترنت و فضای سایبر موجب شده است تا شاهد تغییرات عظیم و شگرفی در حوزه هویت دیجیتال باشیم. مفاهیم جدیدی مانند اکوسیستم هویت نشان می‌دهد که حاکمیت هویت دیجیتال افراد، دیگر بر عهده دولت‌ها نیست، بلکه در اکوسیستمی که موجودیت‌های مختلف اعم از افراد، سازمان‌های دولتی و سازمان‌های خصوصی فعال هستند، دولت‌ها تنها یک موجودیت از این اکوسیستم به شمار می‌روند که به اندازه خود بر این اکوسیستم تأثیرگذار هستند. تحولات فضای سایبر، نگرانی‌ها و چالش‌هایی را در حوزه هویت دیجیتال ایجاد کرده است. برای نمونه یکی از نگرانی‌هایی که در حوزه هویت دیجیتال وجود دارد، بحث حریم خصوصی است. در ادبیات موضوع، به این موضوع تحت عناوینی مانند حفاظت حریم خصوصی مربوط به دسترسی، حریم خصوصی هویت، حریم خصوصی داده، حریم خصوصی مکان فیزیکی و نظایر آن اشاره شده است (زنگ[1] و دیگران، ۲۰۲۰: ۳۲۷). یکی از دلایل اصلی که افراد به قوانین حریم خصوصی اهمیت می‌دهند، ایجاد بستر برای مدیریت و حفاظت از هویت دیجیتال و ایجاد احساس امنیت برای آن‌ها در فضای سایبر است (پترونیو[2] و چیلد[3]، ۲۰۱۹: ۲۵). اگر تحولات فضای سایبر و دگردیسی دیجیتالی به درستی درک شود و از آن به عنوان فرصت استفاده شود، قطعاً موجب تقویت حاکمیت برای دولت‌ها فراهم می‌شود، اما اگر به این تغییرات بی‌توجهی شود و به آن به‌عنوان تهدید نگریسته شود می‌تواند به تضعیف حاکمیت بینجامد؛ چراکه تغییرات فضای مجازی و تحولات دیجیتال از بُعد منفی خود می‌تواند باعث افزایش سرعت ارتکاب افراد به جرائم هویتی مجازی شده و از سویی دیگر باعث تهدید حاکمیت جمهوری اسلامی می‌شود؛ بنابراین باید از روش‌ها و ابزارهایی استفاده کرد تا علاوه بر جلوگیری از تضعیف حاکمیت، موجبات تقویت آن نیز فراهم گردد. برای این کار، لازم است هویت دیجیتال افراد (و همچنین اشیا) در فضای مجازی مدیریت شود. با توجه به

1. Zhang.
2. Petronio.
3. Child.

تحولات فضای سایبر، یک سیستم مدیریت هویت دیجیتال لازم است تـا مـدیریت هویـت را به صورت کلی و جامع مدنظر قرار دهد؛ ازجمله اثبات هویت، مـدیریت هویـت‌هـای متنـوع، احراز هویت قوی با استفاده از داده‌های بیومتریک یا زیست‌سنجی، حفظ حـریم خصوصـی و همچنین اتخاذ رویکرد امنیتی جهت جلوگیری از حملات سایبری (برنابـل[1] و دیگـران، ۲۰۲۰: ٤۱۰). درواقع از مهم‌ترین عوامل مهم و تقویت‌کننـده فضـای سـایبر در کشـور، هویـت دیجیتـال است. مدیریت هویت دیجیتال به‌عنوان یکی از زیرساخت‌های اصلی و اساسی فضای سایبر به جهت ارائه خدمات الکترونیک و برقراری تعامل میان افراد است. اهمیت این موضوع در حدی است که بسیاری از کشورها در این زمینه راهبردهای کلان ارائه داده‌اند و پروژه‌هـای تحقیقاتی و عملیاتی قابل توجهی را انجام داده‌اند. امروز، شناخت این فضای جدید و درک الگوهای مورد استفاده در دنیـا و بـومی‌سـازی ایـن مفـاهیم و برنامـه‌ریـزی بـرای اجـرا و به‌کارگیری آن‌ها در کشور ایران اهمیت بسیار زیادی دارد. درواقع موضوع مدیریت هویـت دیجیتال در حال حاضر یکی از راهبردی‌ترین بحث‌های امنیت سایبری در دنیا است. اعتماد پیش‌نیاز تعاملات و تبادلات در فضای سایبر است و هویت دیجیتـال پایـه و اسـاس ایجـاد اعتماد در فضای سایبر است. اگر کشور ما از یک نظام مدیریت هویت دیجیتـال قابـل اتکـا در فضای سایبر برخوردار نباشد:

- از جایگاه مناسب در فضای سایبر برخوردار نبوده و با خطر تسـلیم کـردن کنتـرل هویت خود بـه عوامـل خـارجی و بـرون‌مـرزی مواجـه اسـت. در ایـن صـورت ارزش‌های غیراسلامی و غیرایرانی جایگزین ارزش های والای اسلامی – ایرانی در فضای سایبر خواهد شد و حاکمیت بر این فضا و تـأمین امنیـت ملـی در فضـای سایبر ممکن نخواهد بود؛
- افزایش مخاطرات کلاه‌برداری و سرقت هویت اتفاق می‌افتد و با عقـب افتـادن از سایر کشورها در بحث امنیت سایبری، ممکن است کشور بـه هـدفی آسـان بـرای مهاجمان بدل شود؛

1. Bernable.

- قادر به مشارکت در جهانی که هر روز بیشتر دیجیتالی می شود نخواهد بود؛ چراکه به علت وجود مقررات غیرمترقی و همچنین فقدان زیرساخت، مجبور است از شیوه‌های غیردیجیتال استفاده نماید؛
- برتری رقابتی ملی در فضای سایبر تحلیل رفته و از دست دادن استعدادهای باارزش (فرار مغزها) اتفاق می‌افتد؛
- احتمال از دست دادن کارآفرینان و سرمایه گذاری ها در فضای سایبر افزایش چشم‌گیری خواهد داشت که در عوض ممکن است به پیشرفت کسب‌وکار در سایر کشورها کمک نمایند.

اما در مقابل، برخی از منافع ملی حاصل از یک نظام مدیریت هویت دیجیتال در کشور عبارت‌اند از:

- ایجاد اعتماد به هویت در سراسر کشور و ضمانت استقلال کشور در عرصه دیجیتال و اقتصاد دیجیتال؛
- حل چالش های امنیت فضای سایبر شامل سرقت هویت و عدم وجود روابط شفاف مبتنی بر اعتماد؛
- ارتقاء جایگاه سطح راهبردی فناوری اطلاعات در سطح ملی و حتی فراملی؛
- حرکت به سمت احراز هویت برخط و افزایش تقاضا برای به کارگیری افراد ماهر و فناوری‌های جدید؛
- تقویت حاکمیت دیجیتال در فضای سایبر از طریق به کارگیری حلقه مفقوده مدیریت هویت دیجیتال در کشور به واسطه هماهنگ‌سازی و رگلاتوری طرح‌ها و پروژه های دولت الکترونیک با محوریت هویت دیجیتال و نیز همراه کردن ذی‌نفعان متعدد در قالب یک زیست‌بوم هویت دیجیتال؛
- ایجاد شغل به واسطه تقاضا برای راهکارهای نوآورانه در عرصه انواع فناوری‌ها برای مدیریت هویت دیجیتال؛

- ایجاد یک عرصه برابر جهت فعالیت آحاد جامعه در فضای سایبر از طریق شناسایی و احراز هویت دیجیتال؛
- ایجاد فرصت‌های کسب‌وکار جدید در فضای سایبر هم برای دولت و هم برای بخش خصوصی و درنتیجه تعامل‌پذیری مطلوب میان ذی نفعان دولتی و غیردولتی و همچنین افزایش توانمندی برای رقابت در عرصه اقتصاد و کسب‌وکار دیجیتال.

طراحی و به کارگیری نظام هویت دیجیتال این فرصت را ایجاد می‌کند تا تعاملاتی که در گذشته به صورت حضوری و با استفاده از اسناد شناسایی فیزیکی انجام می‌شد، به صورتی امن و قابل اعتماد به صورت برخط قابل انجام باشد. این نظام، یکپارچگی بخش های دولتی و خصوصی را نیز ممکن خواهد کرد. این نظام باید قابل اتکا، امن و گسترش‌پذیر[1] باشد و هیچ‌گونه مخاطره‌ای برای اطلاعات شخصی و حریم خصوصی افراد ایجاد ننماید. در حقیقت لازم است تا به ارائه الگوی راهبردی بومی برای مدیریت هویت و احراز هویت دیجیتال در فضای سایبر پرداخت. در این مقاله، قصد آن است تا مهم ترین و کلیدی‌ترین موضوعات حوزه مدیریت هویت دیجیتال در قالب شناخت الگو و نیازمندی‌های به‌کارگیری و پیاده‌سازی آن‌ها، مورد بررسی و مداقه قرار گیرد. درواقع هدف این پژوهش تدوین چارچوبی جامع برای مدیریت هویت دیجیتال است که به شناسایی و اولویت‌بندی معیارها و شاخص‌های هویت دیجیتال بپردازد. این چارچوب می‌تواند مبنایی آکادمیک برای دیگر فعالیت هایی باشد که در زمینه مدیریت هویت دیجیتال در کشور انجام می‌شود. نتایج این تحقیق به حاکمیت و دولت و مراکز دولتی کمک می‌کند تا از چارچوب معرفی‌شده به منظور تبیین سیاست‌ها و راهبردهای هویت دیجیتال از ابعاد گوناگون بپردازند و به دنبال پیاده‌سازی راهکارهای عملیاتی و اجرایی باشند. اجرای چنین چارچوبی نیازمند اقدام مشترک و هماهنگ کلیه نهادها و دستگاه های دولتی و خصوصی است. نیاز به همکاری با یکدیگر در این سطح یک امتیاز مثبت به شمار نمی‌آید، بلکه یک الزام مهم و

1. Scalable.

حیاتی، جهت‌گذار کشور به فضای مجازی امن و اقتصاد دیجیتالی تلقی می‌شود. پرسش‌های این تحقیق که در پایان به آن‌ها پاسخ داده شده است عبارت‌اند از:

- عوامل مؤثر در حوزه مدیریت هویت دیجیتال کدام‌اند؟
- روابط و اثرگذاری و اثرپذیری عوامل مؤثر در مدیریت هویت دیجیتال چگونه است؟
- وزن و اهمیت (اولویت) عوامل مؤثر در مدیریت هویت دیجیتال چگونه است؟

در کشور ما موضوعات جدید مرتبط با فضای مجازی یکی از مهم‌ترین و در عین حال بکرترین حوزه‌های تحقیقاتی است. موضوع مدیریت هویت دیجیتال در فضای مجازی نیز یکی از این حوزه‌ها است که نه تنها در ایران، بلکه در دنیا جزو مباحث روز فضای مجازی بوده و فعالیت‌های تحقیقاتی قابل توجه در کشورهای مختلف در حال اجرا است. با توجه به جدید بودن موضوع این پژوهش که طبیعتاً می‌تواند مبنایی برای دیگر پژوهش‌های آکادمیک باشد، نتایج حاصل از این تحقیق شامل ارائه چارچوب جامع مدیریت هویت دیجیتال، غربالگری و بومی‌سازی این چارچوب و ارائه الگو و مدل فازی برای آن نیز جدید و نوآورانه است.

۲. مبانی نظری

هویت به چیستی یک شخص یا چیز می‌گویند. هویت معانی است که خود شخص یا دیگران به او نسبت می‌دهند (نیکویستا[1] و ماخرجیا[2]، ۲۰۱۶: ۸۵۳). هویت دیجیتالِ منحصربه‌فرد افراد در فضای سایبر و در شبکه‌هایی مانند اینترنت اشیا، می‌تواند رفتارهای مالی آن‌ها را رصد کرده و موجب بهبود ارائه محصولات و خدمات ارائه شده به آن‌ها شود (خانبوبی[3] و دیگران، ۲۰۱۹: ۸۰). تلاش‌ها و اقدامات انجام‌شده برای مدیریت هویت دیجیتال توانمندسازهایی حیاتی در جهت شناسایی و رفع نیازهای امنیت سایبری هستند. کشورها و

1. Nykvista.
2. Mukherjeea.
3. Khanboubi.

دولت‌های مختلف بر اهمیت مدیریت هویت دیجیتال در امنیت فضای سایبر تأکید بسیاری دارند (فدرال کانسیل[1]، ۲۰۱۱). مدیریت هویت دیجیتال و موضوعات مرتبط با آن در سال‌های اخیر مورد توجه پژوهشگران و محققان بوده است. در ادامه برخی مطالعات بررسی‌شده معرفی اجمالی می‌شوند.

۲-۱. پژوهش‌های داخلی

خدیوی کاشانی در پایان‌نامه خود موضوع حریم خصوصی و امنیت در سیستم‌های مدیریت هویت را بررسی کرده است و چارچوبی را برای ارتقای حریم خصوصی و امنیت در این سیستم‌ها ارائه داده است (کاشانی، ۱۳۹۵). پیغله (۱۳۹٤) در رساله خود یک مدل مدیریت هویت برای کاربردهای تجارت الکترونیکی ارائه داده است. در این پژوهش عنوان شده است که مهم ترین مبحث در تجارت الکترونیکی، شناسایی هویت کاربر و صدور مجوز برای تعیین سطح دسترسی کاربر و اعتبارسنجی و مدیریت تعیین هویت در یک سازمان جهت حفاظت از داده‌ها در برابر حملات و افراد غیرمجاز است. چالش دیگری که پژوهشگر معرفی کرده است ابعاد مختلف مدیریت هویت، مرکز صدور گواهی ملی و بین‌المللی، مراکز صدور گواهی میانی، نظامی برای کنترل اعتبارسنجی و تهیه تجهیزات بستر زیرساختی را عنوان کرد. برای رفع این چالش‌ها این پژوهش روشی را ارائه داده است تا از ساخت و توزیع پروفایل های مشتریان واقعی یا ردگیری تراکنش های آنان توسط نهادهای غیرمجاز جلوگیری شود. مهم‌ترین جنبه‌های این پژوهش تلفیق دو نظریه امنیت و حریم خصوصی در مقابل یک مدل تهاجم مبتنی بر دنیای واقعی است تا بتوان تعریفی جدید و عملی‌تر از حریم خصوصی را ارائه نمود که قابلیت استفاده در بسیاری از فعالیت‌های کاربردی را داشته باشد (پیغله، ۱۳۹٤).

1. Federal Chief Information Officers Council.

۲-۲. پژوهش‌های خارجی

میتینن[1] در پایان‌نامه خود موضوع مدیریت هویت متمرکز در سازمان‌های غیرمتمرکز را بررسی کرده است. او ابتدا فرایندهای فعلی و آتی را بررسی کرده و نقص‌های امنیتی آن‌ها را بررسی کرده است. بر اساس مسائل شناسایی‌شده میتینن معتقد است که در آینده تغییر در فرایندهای مدیریت هویت دیجیتال اجتناب ناپذیر خواهند بود (میتینن، ۲۰۱۷). راسیواسا[2] در پایان‌نامه خود چارچوبی را برای پیاده‌سازی پروتکل OpenID [3] در هم‌پیمانی‌های هویتی طراحی کرده است. به دلیل دخالت سازمان‌های مختلف، داده‌های حساس کاربران و مسائل امنیتی بی‌شمار اجرای پروتکل‌های FIM [4] و SSO[5] پیچیده است. موارد متعددی از پیاده‌سازی‌های نامناسب وجود دارد که به دلیل عدم هدایت مناسب، امنیت را به خطر انداخته‌اند تا پیاده‌سازی را تسهیل کنند (راسیواسا، ۲۰۱۷). در پایان‌نامه دیگری، هدف تجزیه وتحلیل نقش هویت دیجیتال در افزایش اثربخشی خدمات عمومی در کشورهای در حال توسعه است (اولانی[6]، ۲۰۱۷). ویتانن[7] در پایان‌نامه خود موضوع یکپارچه‌سازی مدیریت هویت و مدیریت دسترسی را بررسی کرده است. او در این پژوهش یک مدیریت هویت منبع باز را در سیستم مدیریت دسترسی یکی از شرکت‌ها ادغام نموده است (ویتانن، ۲۰۱۵). در ادامه این پژوهش، بر اساس مطالعات انجام‌شده در ادبیات موضوع، مجموعه عوامل اصلی و عوامل فرعی مدنظر در حوزه مدیریت هویت دیجیتال در جدول ۱ ارائه شده است.

1. Antti Miettinen.
2. Akshay Rasiwasia.
3. Open Identity.
4. Federated Identity Management.
5. Single Sign On.
6. Olaniyi.
7. Samu Viitanen.

جدول ۱- عوامل اصلی و عوامل فرعی به‌دست‌آمده از مطالعات کتابخانه‌ای

ردیف	عوامل اصلی	ردیف فرعی	عوامل فرعی	منابع
۱	مدیریت هویت	۱-۱	ثبت نام بر اساس الزامات مدیریت هویت دیجیتال	(عثمان اقلو[1]، ۲۰۱٤)، (نیست[2]، ۲۰۱۳)، (وایت هاوس[3]، ۲۰۱۱)، (دیاک[4]، ۲۰۱۵)، (اس‌ای‌آیدی[5]، ۲۰۱۵)
		۱-۲	امکان غربال هویت	(فدرال کانسیل، ۲۰۱۱)، (اس‌ای‌آیدی، ۲۰۱۵)
		۱-۳	ثبت اطلاعات هویتی برای موجودیت‌های غیرانسانی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (اس‌ای‌آیدی، ۲۰۱۵)، (نیست، ۲۰۱۳)، (دیاک، ۲۰۱۵)
		۱-٤	به‌روز بودن داده‌های هویتی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (اس‌ای‌آیدی، ۲۰۱۵)، (نیست، ۲۰۱۳)، (دیاک، ۲۰۱۵)
		۱-۵	شناسایی تمام منابع هویتی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (اس‌ای‌آیدی، ۲۰۱۵)، (نیست، ۲۰۱۳)، (دیاک، ۲۰۱۵)
۲	مدیریت اعتبارنامه	۲-۱	ثبت‌نام تنها از طریق الزامات مدیریت هویت دیجیتال	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (اس‌ای‌آیدی، ۲۰۱۵)، (نیست، ۲۰۱۳)، (دیاک، ۲۰۱۵)
		۲-۲	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت دیجیتال	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام[6]، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری[7]، ۲۰۱۳)، (نیست، ۲۰۱۳)
		۲-۳	مکانیزم‌های قانونی برای ابطال ضروریِ اعتبارنامه	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)

1. Osmanoglu.
2. NIST.
3. White House.
4. DIACC.
5. SeID.
6. WA IdAM.
7. Rountree.

ردیف	عوامل اصلی	ردیف فرعی	عوامل فرعی	منابع
۳	مدیریت دسترسی	۳-۱	سیاست دسترسی برای همه منابع	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		۳-۲	درخواست دسترسی به منابع تنها از طریق سیستم مدیریت هویت دیجیتال	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		۳-۳	کنترل دسترسی به کلیه منابع تنها از طریق سیستم مدیریت هویت دیجیتال	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		۳-٤	پشتیبانی از ورود به سیستم‌ها از طریق یک‌بار ورود	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		۳-۵	احراز هویت دستگاه‌های مورد استفاده کاربران	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
٤	هم‌پیمان‌سازی/ فدریشن	٤-۱	وجود سیاست برای هم‌پیمانی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		٤-۲	تبادل اطلاعات هویتی بین سرویس‌ها و دستگاه‌ها	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		٤-۳	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت دیجیتال	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)

ردیف	عوامل اصلی	ردیف فرعی	عوامل فرعی	منابع
۵	حاکمیت	۵-۱	سیاست‌ها و مکانیسم‌های بازگشت از حوادث	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (رونتری، ۲۰۱۳)
		۵-۲	برنامه‌ریزی مدون برای ممیزی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
٦	موضوعات راهبردی	٦-۱	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (فدرال کانسیل، ۲۰۱۱)، (وی‌ای‌آی‌دی‌ام، ۲۰۰۵)، (دیاک، ۲۰۱۵)، (رونتری، ۲۰۱۳)، (نیست، ۲۰۱۳)
		٦-۲	متمرکز بودن مدیریت اطلاعات هویتی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (رونتری، ۲۰۱۳)
		٦-۳	امکان مشارکت همه ذی‌نفعان در برنامه‌ریزی	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (رونتری، ۲۰۱۳)
		٦-٤	یکپارچه بودن سیستم مدیریت هویت دیجیتال با سایر سیستم‌ها	(عثمان اقلو، ۲۰۱٤)، (وایت هاوس، ۲۰۱۱)، (رونتری، ۲۰۱۳)
		٦-۵	تعریف راهبرد و چشم‌انداز	(عثمان اقلو، ۲۰۱٤)، (رونتری، ۲۰۱۳)

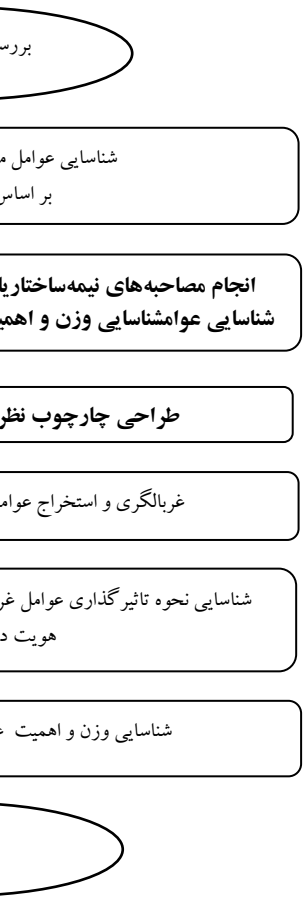
۳. روش‌شناسی تحقیق

پژوهش حاضر در قالب یک پژوهش کاربردی با رویکرد بنیادین اجرا شده است و از حیث چگونگی پردازش و تحلیل داده‌ها از نوع توصیفی –تحلیلی اکتشافی و حل مسئله از نوع تصمیم‌گیری چندمعیاره فازی است. به‌طور کلی روش اجرای تحقیق به‌صورت شکل ۱ نمایش داده شده است. در این پژوهش از روش آمیخته استفاده شده است. در گام نخست به بررسی و شناسایی موضوع هویت دیجیتال در ادبیات موضوع پرداخته شد. مؤلفه‌های شناسایی‌شده در این مرحله از طریق مصاحبه‌های نیمه‌ساختاریافته از خبرگان مورد پرسش

قرار گرفت. در این مرحله الگوی اولیه تحقیق پیشنهاد شد. در ادامه با توجه به بافت محتوایی پژوهش و برحسب نظرات خبرگان، الگوی اولیه تعدیل شده است و متغیرهایی که تناسب بیشتری با موضوع پژوهش برخوردار بودند برای طراحی چارچوب نظری پژوهش و تبیین چارچوب مدیریت هویت دیجیتال مورد استفاده قرار گرفتند. جمع‌آوری داده‌ها به دو صورت مطالعات کتابخانه‌ای شامل مقالات منتشرشده در مجلات معتبر بین‌المللی، رساله‌ها، پایان‌نامه‌ها، کتاب‌ها و نشریات داخلی معتبر و پایگاه‌های اطلاعاتی و سایت‌های اینترنتی و میدانی (مصاحبه و پرسشنامه) است. در بخش مصاحبه، مصاحبه‌های نیمه‌ساختاریافته بر اساس مطالعات اولیه صورت گرفته در این تحقیق با خبرگان حوزه هویت دیجیتال ترتیب داده شد تا چه‌بسا زوایای پنهانی که در ادبیات موضوع وجود داشت و در بررسی‌های کتابخانه‌ای و اسناد موجود مورد بررسی قرار نگرفت را آشکار نماید. همچنین در این تحقیق دو پرسشنامه مورد استفاده قرار گرفت. پرسشنامه اول برای انتخاب عوامل شناسایی‌شده و غربالگری آن‌ها استفاده شد که در آن هر یک از خبرگان به میزان اهمیت هر یک از عوامل شناسایی‌شده بر اساس طیف لیکرت پنج گزینه ای پاسخ می‌دهند. پرسشنامه دوم جهت بررسی روابط درونی میان عوامل و شدت تأثیر آن ها بر یکدیگر از طریق رویکرد دیمتل[1] فازی و همچنین وزن‌دهی به معیارها و شاخص‌ها با استفاده از روش ترکیبی فازی فرایند تحلیل شبکه‌ای و دیمتل[2] تدوین شده است. جامعه خبرگان این پژوهش متخصصان حوزه امنیت سایبری با تخصص مدیریت هویت دیجیتال می‌باشند که به دلیل تخصصی بودن موضوع و محدودیت در شناسایی خبرگان، بر اساس روش قضاوتی هدفمند انتخاب شدند. تعداد خبرگان به‌عنوان مصاحبه‌شونده نباید زیاد باشد و در کل پنج الی پانزده نفر را پیشنهاد می‌شود (اصغرپور، ۱۳۸۲). جامعه خبرگان این پژوهش به دو گروه تقسیم شده‌اند. گروه اول به تعداد ده نفر از کارشناسان ارشد و مدیران (شاغل در بانک مرکزی، بانک سپه، وزارت کشور، مرکز ملی فضای سایبر و دو شرکت نیمه‌دولتی با

1. DEMATEL.
2. FDANP.

تخصص هویت دیجیتال و کارت هوشمند) است که برای غربالگری عوامل و بومی‌سازی الگو از طریق روش دلفی- فازی مورد استفاده قرار گرفتند. گروه دوم متشکل از هفت نفر از گروه اول هستند که برای حل مدل‌های ریاضی پژوهش به روش ترکیبی فازی فرایند تحلیل شبکه‌ای و دیمتل مورد پرسش قرار گرفتند. همان طور که اشاره شد، با توجه به محدودیت‌های شناسایی خبرگان، این هفت نفر به این دلیل انتخاب شدند که دارای سابقه کاری بالاتری بوده و پست‌های مدیریتی بیشتری را تجربه کرده بودند، ضمن اینکه به حوزه تخصصی مدیریت هویت دیجیتال تسلط بیشتری داشتند. همچنین افراد گروه دوم، به‌عنوان مصاحبه‌شونده جهت انجام مصاحبه‌های نیمه‌ساختاریافته مورد پرسش قرار گرفته‌اند.



شکل ۱- مراحل و متدولوژی اجرای تحقیق

٤. تجزیه‌وتحلیل یافته‌ها

٤-١. تحلیل مصاحبه‌ها

روش پژوهش جهت تحلیل داده‌های مرتبط با مصاحبه‌ها، بر مبنای تحلیل مضمون یا تم[1] است؛ به این معنی که تحلیل داده‌های گردآوری‌شده طی مصاحبه‌ها، بر اساس روش تحلیل مضمون (تم) مورد تجزیه‌وتحلیل قرار گرفته‌اند (عابدی[2] و دیگران، ۲۰۱۱: ١٦٣). در بخش کیفی این پژوهش از طریق مصاحبه با هفت متخصص در حوزه هویت دیجیتال که دارای مدرک کارشناسی ارشد و دکتری بودند و در زمینه هویت دیجیتال، تجربه و دانش کافی داشتند از روش تحلیل تم، جهت تکمیل و تدوین نهایی طرح اولیه چارچوب مدیریت هویت دیجیتال در فضای سایبر استفاده شد. ساختار مصاحبه‌ها بر اساس مطالعات اولیه صورت گرفته در این پژوهش با خبرگان هویت دیجیتال و امنیت سایبری ترتیب داده شد تا چه‌بسا زوایای پنهانی که در ادبیات موضوع وجود داشت و در بررسی‌های کتابخانه‌ای و اسناد موجود مورد بررسی قرار نگرفت را آشکار نماید. درمجموع صدوپنجاه عبارت کلیدی با کدهای نشانگر طی مصاحبه‌ها استخراج شده است. در گام بعدی این عبارات کلیدی در قالب مفاهیم انتزاعی مفهوم‌سازی شده‌اند (مضامین فرعی). بر اساس مضامین فرعی به‌دست‌آمده و با حذف موارد مشابه و ادغام برخی دیگر، درنهایت ۱۷ مضمون فرعی حاصل شده است که این تعداد نیز درنهایت شش مضمون پایه پژوهش را بر اساس ادبیات تحقیق و بینش پژوهشگر تشکیل داده‌اند. در ادامه، دو مضمون اصلی از طریق تبیین و ارتباط‌دهی میان آن‌ها پدید آمده است. به‌منظور افزایش پایایی و اعتبار یافته‌ها، فرایند تجزیه‌وتحلیل داده‌ها طی این پژوهش، هم‌زمان با جمع‌آوری اطلاعات صورت پذیرفته است. به این صورت که با به دست آمدن اطلاعات مربوط به هر مصاحبه، تحلیل محتوای مربوط به آن بخش صورت می‌پذیرفت. جمع‌بندی مصاحبه‌های انجام‌شده در جدول ۲ نمایش داده شده است.

1. Theme.
2. Abedi.

جدول ۲- جمع‌بندی مضامین فرعی به‌دست‌آمده از مصاحبه‌ها

ردیف	مضامین اصلی	مضامین پایه	ردیف	مضامین فرعی
۱	حوزه عملیاتی مدیریت هویت دیجیتال	مدیریت هویت	۱-۱	فرایند مدون برای اثبات هویت
			۱-۲	یکپارچه‌سازی اطلاعات هویتی فرد
			۱-۳	وجود چرخه حیات برای داده‌های هویتی
۲		مدیریت اعتبارنامه	۲-۱	فعال‌سازی اعتبارنامه از راه دور
			۲-۲	وجود چرخه حیات برای اعتبارنامه‌ها
۳		مدیریت دسترسی	۳-۱	راهکار برای مدیریت دسترسی حساب‌های ممتاز
			۳-۲	پشتیبانی از احراز هویت چندعاملی
			۳-۳	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان
٤		هم‌پیمان‌سازی/ فدریشن	٤-۱	وجود فرمت استاندارد برای درک اعتبارنامه‌ها
			٤-۲	الزامات حقوقی- قضایی برای جبران خسارت
۵	حوزه راهبردی مدیریت هویت دیجیتال	حاکمیت	۵-۱	راهبردها و الزامات برای حریم خصوصی
			۵-۲	مکانیزم پاسخ‌گویی مشکلات و شکایات
			۵-۳	پایش مستمر سیستم‌ها و فرایندها
٦		موضوعات راهبردی	٦-۱	وجود مدل بلوغ مدیریت هویت دیجیتال
			٦-۲	تعهد در کل سازمان
			٦-۳	رعایت الزامات مدیریت هویت دیجیتال برای استفاده سایر نرم‌افزارها
			٦-٤	جامعیت برنامه مدیریت هویت دیجیتال

با توجه به نتایج حاصل معیارها و شاخص‌های احصاشده درنتیجه مطالعات کتابخانه‌ای و همچنین نتایج به‌دست‌آمده از مصاحبه‌ها، از ترکیب این دو نتیجه، جدول ۳ را جهت ترسیم چارچوب نظری مدنظر قرار داد.

جدول ۳- عوامل اصلی و عوامل فرعی احصاشده در پژوهش جهت ترسیم چارچوب مدیریت هویت دیجیتال

ردیف	دسته‌های کلی	عوامل اصلی	ردیف فرعی	عوامل فرعی
۱	حوزه عملیاتی	مدیریت هویت	۱-۱	ثبت‌نام بر اساس الزامات مدیریت هویت دیجیتال
			۱-۲	فرایند مدون برای اثبات هویت
			۱-۳	امکان غربال هویت
			۱-٤	ثبت اطلاعات هویتی برای موجودیت‌های غیرانسانی
			۱-۵	یکپارچه‌سازی اطلاعات هویتی فرد
			۱-٦	وجود چرخه حیات برای داده‌های هویتی
			۱-۷	به‌روز بودن داده‌های هویتی
			۱-۸	شناسایی تمام منابع هویتی
۲		مدیریت اعتبارنامه	۲-۱	ثبت‌نام تنها از طریق الزامات مدیریت هویت دیجیتال
			۲-۲	فعال‌سازی اعتبارنامه از راه دور
			۲-۳	وجود چرخه حیات برای اعتبارنامه‌ها
			۲-٤	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت دیجیتال
			۲-۵	مکانیزم‌های قانونی برای ابطال ضروریِ اعتبارنامه
۳		مدیریت دسترسی	۳-۱	سیاست دسترسی برای همه منابع
			۳-۲	درخواست دسترسی به منابع تنها از طریق سیستم مدیریت هویت دیجیتال
			۳-۳	کنترل دسترسی به کلیه منابع تنها از طریق سیستم مدیریت هویت دیجیتال
			۳-٤	راهکار برای مدیریت دسترسی حساب‌های ممتاز
			۳-۵	پشتیبانی از ورود به سیستم‌ها از طریق یک‌بار ورود
			۳-٦	پشتیبانی از احراز هویت چندعاملی
			۳-۷	احراز هویت دستگاه‌های مورد استفاده کاربران
			۳-۸	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان
٤		هم‌پیمان سازی/ فدریشن	٤-۱	وجود سیاست برای هم‌پیمانی
			٤-۲	تبادل اطلاعات هویتی بین سرویس‌ها و دستگاه‌ها
			٤-۳	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت دیجیتال
			٤-٤	وجود فرمت استاندارد برای درک اعتبارنامه‌ها
			٤-۵	الزامات حقوقی- قضایی برای جبران خسارت

ردیف	دسته‌های کلی	عوامل اصلی	ردیف فرعی	عوامل فرعی
۵	حوزه راهبردی	حاکمیت	۵-۱	سیاست‌ها و مکانیسم‌های بازگشت از حوادث
			۵-۲	راهبردها و الزامات برای حریم خصوصی
			۵-۳	برنامه‌ریزی مدون برای ممیزی
			۵-۴	مکانیزم پاسخ‌گویی مشکلات و شکایات
			۵-۵	پایش مستمر سیستم‌ها و فرایندها
٦		موضوعات راهبردی	٦-۱	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی
			٦-۲	متمرکز بودن مدیریت اطلاعات هویتی
			٦-۳	وجود مدل بلوغ مدیریت هویت دیجیتال
			٦-۴	امکان مشارکت همه ذی‌نفعان در برنامه‌ریزی
			٦-۵	یکپارچه بودن سیستم مدیریت هویت دیجیتال با سایر سیستم‌ها
			٦-۶	تعهد در کل سازمان
			٦-۷	تعریف راهبرد و چشم‌انداز
			٦-۸	رعایت الزامات مدیریت هویت دیجیتال برای استفاده سایر نرم-افزارها
			٦-۹	جامعیت برنامه مدیریت هویت دیجیتال

٤-۲. ارزیابی و انتخاب معیارها با استفاده از روش دلفی- فازی

به دلیل اینکه تعداد عوامل شناسایی‌شده (حاصل مطالعات کتابخانه‌ای و مصاحبه‌ها) قابل توجه است و به‌منظور انتخاب عوامل و کاهش تعداد آن‌ها برای محاسبات مراحل بعدی و همچنین تعیین میزان اهمیت عوامل نسبت به هم و غربالگری آن‌ها، از طریق روش دلفی- فازی، استفاده می‌شود. روش دلفی- فازی در دهه ۱۹۸۰ میلادی توسط کافمن و گویتا[1] ابداع شد (چینگ هاس[2] و لین[3]، ۲۰۰۲: ۱٤۷). کاربرد این روش به منظور تصمیم-گیری و اجماع بر مسائلی که اهداف و پارامترها به‌صراحت مشخص نیستند، منجر به نتایج

1. Kaufman And Gupta.
2. Ching-Hsue.
3. Lin.

بسیار ارزنده می‌شود. ویژگی مهم این روش، ارائه چارچوبی انعطاف‌پذیر است که بسیاری از موانع مربوط به عدم دقت و صراحت را تحت پوشش قرار می‌دهد (آذر و فرجی، ۱۳۸۱: ٥٦). به همین منظور پرسشنامه‌ای که در آن هر سؤال بیانگر یک عامل است طراحی گردید. تعداد ده پرسشنامه که به تعداد پاسخ‌دهندگان خبره است جهت پاسخگویی در اختیار آن‌ها قرار گرفت و تمامی پرسشنامه‌ها به صورت کامل تکمیل و بازگردانده شد. این پرسشنامه‌ها بر اساس طیف لیکرت پنج‌گزینه‌ای از خیلی بااهمیت تا بدون اهمیت تنظیم شد. در نظرسنجی مرحله نخست، عوامل اصلی و عوامل فرعی به همراه و با شرح و توضیحات به اعضای گروه خبره ارسال گردید و میزان موافقت آن ها با هر یک از عوامل اخذ گردید. همچنین نقطه‌نظرات پیشنهادی و اصلاحی آن ها مورد توجه قرار گرفت. میانگین قطعی به‌دست‌آمده نشان‌دهنده میزان شدت موافقت خبرگان با هر یک از عوامل در نظر گرفته‌شده در تحقیق است. در مرحله دوم پرسشنامه دیگری تهیه گردیده و همراه با نقطه‌نظرات قبلی هر خبره و میزان اختلاف آن ها با دیدگاه سایر خبرگان، دوباره به اعضای گروه خبره ارسال گردید و اعضای گروه خبره با توجه به نقطه‌نظرات سایر اعضای گروه، دوباره به سؤالات ارائه‌شده پاسخ دادند. با توجه به دیدگاه‌های ارائه‌شده در مرحله اول و مقایسه آن با نتایج این مرحله، در صورتی که اختلاف بین دو مرحله کمتر از حد آستانه ۰,۲ باشد، فرایند نظرسنجی متوقف می‌شود. در این مرحله نه عامل متوقف گردیده و نظرسنجی در مورد چهار عامل باقی‌مانده باید صورت بگیرد که در مرحله سوم انجام می‌شود. در مرحله سوم ضمن اعمال تغییرات لازم در شاخص‌های الگو، پرسشنامه سوم تهیه گردیده و همراه با نقطه‌نظرات قبلی هر فرد و نیز میزان اختلاف آن ها با میانگین دیدگاه سایر خبرگان، دوباره برای خبرگان ارسال گردید. جدول ٤ به صورت خلاصه، به سه مرحله روش دلفی- فازی اشاره شده است.

جدول٤- نتایج نظرسنجی روش دلفی - فازی

عوامل اصلی	ردیف	مرحله	۱	۲			۳		
		زیرمعیارها - ارزش فازی	میانگین غیرفازی شده نظرات خبرگان	میانگین غیرفازی شده نظرات خبرگان	اختلاف میانگین پرسشنامه‌های اول و دوم	نتیجه	میانگین غیرفازی شده نظرات خبرگان	اختلاف میانگین پرسشنامه‌های اول و دوم	نتیجه
مدیریت هویت	۱	ثبت نام (تنها) بر اساس الزامات مدیریت هویت دیجیتال	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲	امکان غربال هویت	□□□□	□□□□	□□□□	رد	-	-	-
	۳	فرایند مدون برای اثبات هویت	□□□	□□□□	□□□□	پذیرش	-	-	-
	٤	یکپارچه‌سازی اطلاعات هویتی فرد	□□□□	□□□□	□□□	بعدی	□□□□	□□□□	پذیرش
	٥	ثبت اطلاعات هویتی برای همه موجودیت‌های غیرانسانی	□□□□	□□□□	□□□□	رد	-	-	-
	٦	وجود چرخه حیات برای داده‌های هویتی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۷	شناسایی تمام منابع هویتی در سازمان	□□□□	□□□□	□□□□	رد	-	-	-
	۸	به‌روز بودن داده‌های هویتی	□□□□	□□□□	□□□□	پذیرش	-	-	-
مدیریت اعتبارنامه	۹	ثبت‌نام اعتبارنامه تنها از طریق الزامات مدیریت هویت	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱۰	امکان فعال‌سازی/ غیرفعال‌سازی اعتبارنامه از راه دور	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱۱	وجود چرخه حیات برای اعتبارنامه‌ها	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱۲	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت	□□□□	□□□□	□□□	بعدی	□□□□	□□□□	پذیرش
	۱۳	وجود مکانیزم‌های قانونی برای ابطال اعتبارنامه	□□□□	□□□□	□□□□	پذیرش	-	-	-
مدیریت دسترسی	۱٤	وجود سیاست دسترسی برای همه منابع و اطلاعات	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱٥	کنترل دسترسی به کلیه منابع و اطلاعات تنها از طریق سیستم مدیریت هویت دیجیتال	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱٦	امکان ارائه درخواست دسترسی به منابع تنها از طریق سیستم مدیریت هویت دیجیتال	□□□□	□□□□	□□□□	رد	-	-	-
	۱۷	وجود راهکار برای مدیریت دسترسی حساب‌های ممتاز	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۱۸	پشتیبانی از ورود به سیستم‌ها از طریق یک‌بار ورود	□□□□	□□□□	□□□□	رد	-	-	-
	۱۹	امکان احراز هویت دستگاه‌های مورد استفاده کاربران	□□□□	□□□□	□□□□	رد	-	-	-

عوامل اصلی	ردیف	مرحله	۱	۲			۳		
		زیرمعیارها - ارزش فازی	میانگین غیرفازی شده نظرات خبرگان	میانگین غیرفازی شده نظرات خبرگان	اختلاف میانگین پرسشنامه‌های اول و دوم	نتیجه	میانگین غیرفازی شده نظرات خبرگان	اختلاف میانگین پرسشنامه‌های اول و دوم	نتیجه
	۲۰	پشتیبانی از احراز هویت چندعاملی	□□□	□□□□	□□□□	پذیرش	-	-	-
	۲۱	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان	□□□□	□□□□	□□□□	پذیرش	-	-	-
هم‌پیمان‌سازی	۲۲	وجود سیاست برای هم‌پیمانی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲۳	امکان تبادل اطلاعات هویتی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲٤	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت	□□□□	□□□□	□□□	بعدی	□□□□	□□□□	پذیرش
	۲۵	وجود فرمتی استاندارد برای درک اعتبارنامه‌ها	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲٦	وجود الزامات حقوقی- قضایی برای جبران خسارت	□□□□	□□□□	□□□□	پذیرش	-	-	-
حاکمیت	۲۷	وجود سیاست‌های بازگشت از حوادث	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲۸	وجود الزامات حریم خصوصی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۲۹	برنامه‌ریزی برای ممیزی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳۰	وجود مکانیزم پاسخ‌گویی به شکایات	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳۱	پایش مستمر فرایندها	□□□□	□□□□	□□□	بعدی	□□□□	□□□□	پذیرش
موضوعات راهبردی	۳۲	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳۳	وجود مدل بلوغ مدیریت هویت دیجیتال	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳٤	متمرکز بودن مدیریت اطلاعات هویتی	□□□□	□□□□	□□□□	رد	-	-	-
	۳۵	یکپارچه بودن سیستم مدیریت هویت دیجیتال با سایر سیستم‌ها	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳٦	امکان مشارکت همه ذی‌نفعان در برنامه‌ریزی	□□□□	□□□□	□□□□	رد	-	-	-
	۳۷	تعهد در کل سازمان	□□□□	□□□□	□□□□	پذیرش	-	-	-
	۳۸	رعایت الزامات مدیریت هویت دیجیتال برای استفاده از سایر نرم‌افزارها	□□□□	□□□□	□□□□	رد	-	-	-
	۳۹	تعریف راهبرد و چشم‌انداز	□□□□	□□□□	□□□□	پذیرش	-	-	-
	٤۰	جامعیت برنامه مدیریت هویت دیجیتال	□□□□	□□□□	□□□□	پذیرش	-	-	-

بنابراین در طی سه مرحله نظرسنجی از چهل عامل فرعی، نه عامل فرعی از الگوی اصلی حذف و الگوی نهایی شامل شش عامل اصلی و سی‌ویک عامل فرعی گردید که در جدول ۵ آمده است.

جدول ۵- عوامل اصلی و عوامل فرعی تأییدشده نهایی توسط خبرگان

عوامل اصلی	عوامل فرعی	نشان اختصاری
مدیریت هویت C1	ثبت‌نام (تنها) بر اساس الزامات مدیریت هویت دیجیتال	C11
	فرایند مدون برای اثبات هویت	C12
	یکپارچه‌سازی اطلاعات هویتی فرد	C13
	وجود چرخه حیات برای داده‌های هویتی	C14
	به‌روز بودن داده‌های هویتی	C15
مدیریت اعتبارنامه C2	ثبت‌نام اعتبارنامه تنها از طریق الزامات مدیریت هویت دیجیتال	C21
	امکان فعال‌سازی/ غیرفعال‌سازی اعتبارنامه از راه دور	C22
	وجود چرخه حیات برای اعتبارنامه‌ها	C23
	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت دیجیتال	C24
	وجود مکانیزم‌های قانونی برای ابطال اعتبارنامه	C25
مدیریت دسترسی C3	وجود سیاست دسترسی برای همه منابع و اطلاعات	C31
	کنترل دسترسی به کلیه منابع و اطلاعات تنها از طریق سیستم مدیریت هویت دیجیتال	C32
	وجود راهکار برای مدیریت دسترسی حساب‌های ممتاز	C33
	پشتیبانی از احراز هویت چندعاملی	C34
	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان	C35
هم‌پیمان سازی/ فدریشن C4	وجود سیاست برای هم‌پیمانی	C41
	امکان تبادل اطلاعات هویتی	C42
	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت دیجیتال	C43
	وجود فرمتی استاندارد برای درک اعتبارنامه‌ها	C44
	وجود الزامات حقوقی- قضایی برای جبران خسارت	C45
حاکمیت C5	وجود سیاست‌های بازگشت از حوادث	C51
	وجود الزامات حریم خصوصی	C52
	برنامه‌ریزی برای ممیزی	C53
	وجود مکانیزم پاسخ‌گویی به شکایات	C54
	پایش مستمر فرایندها	C55

عوامل اصلی	عوامل فرعی	نشان اختصاری
موضوعات راهبردی C6	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی	C61
	وجود مدل بلوغ مدیریت هویت دیجیتال	C62
	یکپارچه بودن سیستم مدیریت هویت دیجیتال با سایر سیستم‌ها	C63
	تعهد در کل سازمان (نسبت به سیاست‌های مدیریت هویت دیجیتال)	C64
	تعریف راهبرد و چشم‌انداز	C65
	جامعیت برنامه مدیریت هویت دیجیتال در پوشش همه جنبه‌ها	C66

٤-۳. بررسی نتایج حاصل از روش ترکیبی فازی فرایند تحلیل شبکه‌ای و دیمتل[1]

مروری بر مطالعات نشان می‌دهد که اغلب محققان، از روش‌های تصمیم‌گیری فازی ترکیبی از فرایند تحلیل شبکه‌ای[2] و دیمتل[3] برای انتخاب گزینه‌های مناسب در مسائل مختلف استفاده کرده‌اند (مدیری و همکاران،۱۳۹۳: ۱٤۳). در هنگام محاسبه وزن نسبی معیارها با استفاده از روش مرسوم فرایند تحلیل شبکه‌ای، سطح وابستگی میان معیارها به صورت ارزش‌های متقابل (دوطرفه) در نظر گرفته می‌شود؛ در حالی که در روش دیمتل، سطح وابستگی میان معیارها ارزش‌های متقابل نخواهد داشت که این به آنچه در دنیای واقعی وجود دارد نزدیک‌تر است؛ بنابراین جهت رفع این نقص که در روش مرسوم فرایند تحلیل شبکه‌ای وجود دارد، از ماتریس روابط کلی که از روش دیمتل به دست می‌آید، جهت محاسبه وزن نسبی معیارها استفاده می‌شود (یانگ[4] و تزنگ[5]، ۲۰۱۱: ۱٤۲۱). سنجش روایی پرسشنامه دیمتل از دو طریق روایی محتوا و روایی صوری آزمون گردیده است. از نظر روایی محتوا، متغیرهای پرسشنامه، به صورت کامل از ادبیات موضوع استخراج شده‌اند. از نظر روایی صوری نیز پرسشنامه مورد استفاده در این تحقیق توسط سه نفر از افراد خبره

1. FDANP.
2. ANP.
3. DEMATEL.
4. Yang.
5. Tzeng.

مورد ارزیابی قرار گرفته و اصلاحات لازم صورت پذیرفته است. در خصوص پایایی پرسشنامه نیز، به‌منظور تعیین پایایی از آزمون مجدد استفاده شده است. به همین منظور، پرسشنامه‌ها در بین سه نفر از افراد متخصص و خبرگان در دو بازه زمانی با اختلاف دو هفته توزیع گردید. نتایج حاصل نشان داد ضریب همبستگی به میزان ۰/۸۲٤ است. با توجه به اینکه همبستگی پاسخ‌ها بالاتر از ۰/۷ است، بنابراین می‌توان گفت که پایایی پرسشنامه قابل قبول است. برای بررسی عوامل از نظر هفت خبره استفاده شده است. در ابتدا ماتریس مستقیم فازی برای عوامل اصلی و فرعی تشکیل می‌شود. سپس جهت نرمالیزه کردن این ماتریس‌ها اقدام می‌شود. در ادامه ماتریس روابط کل فازی تشکیل می‌شود. در مرحله بعدی میزان اهمیت شاخص‌ها ($\widetilde{D}_i + \widetilde{R}_i$) و رابطه بین معیارها ($\widetilde{D}_i - \widetilde{R}_i$) مشخص می‌گردد. اگر $\widetilde{D}_i - \widetilde{R}_i > 0$ باشد معیار مربوطه اثرگذار و اگر $\widetilde{D}_i - \widetilde{R}_i < 0$ باشد معیار مربوطه اثرپذیر است. جداول ٦ و ۷ اعداد دیفازی شده مقادیر اثرگذاری D، اثرپذیری R، اهمیت ($\widetilde{D}_i + \widetilde{R}_i$) و اثرگذاری و اثرپذیری خالص ($\widetilde{D}_i - \widetilde{R}_i$) را برای عوامل اصلی و فرعی نشان می‌دهد.

جدول ٦- اهمیت و اثرگذاری عوامل اصلی مربوط به مدیریت هویت دیجیتال

عوامل اصلی	نشان اختصاری	D	R	D+R	D-R	نتیجه
مدیریت هویت	C1	□□□□	□□□□	□□□□	□□□□	اثرگذار
مدیریت اعتبارنامه	C2	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
مدیریت دسترسی	C3	□□□□	□□□□	□□□□	□□□□□	اثرپذیرترین
هم-پیمان-سازی	C4	□□□□	□□□□	□□□□	□□□□	اثرگذار
حاکمیت	C5	□□□□	□□□□	□□□□	□□□□	اثرگذار
برنامه-	C6	□□□□	□□□□	□□□□	□□□□	اثرگذارترین

ریزی راهبردی						

در بین عوامل اصلی «برنامه‌ریزی راهبردی» با مقدار اثرگذاری تأثیرگذارترین و «مدیریت دسترسی» با مقدار اثرپذیری خالص برابر تأثیرپذیرترین عامل است. به طور کلی ($\widetilde{D}_i - \widetilde{R}_i$) مثبت، عامل علی و ($\widetilde{D}_i - \widetilde{R}_i$) منفی عامل معلول اثرپذیر محسوب می‌شود؛ بنابراین عوامل «مدیریت هویت»، «هم‌پیمان‌سازی» و «حاکمیت» و «برنامه‌ریزی راهبردی» علت هستند که بیشتر موجب هدایت می‌شوند و خود کمتر وابستگی دارند. عوامل «مدیریت اعتبارنامه» و «مدیریت دسترسی» معلول هستند که خود تحت تأثیر عوامل علی می‌باشند. این عوامل دارای وابستگی شدید هستند و کمتر باعث هدایت می‌شوند. همچنین D_i+R_i میزان اهمیت شاخص را نشان می‌دهد، به نحوی که هر چه این مقدار بیشتر باشد نشان‌دهنده اهمیت و تعامل بیشتر با دیگر شاخص‌ها است (والمحمدی[1] و خاکی[2]، ۲۰۱۹). در بین عوامل اصلی، عامل مدیریت هویت با مقدار ۷/۷۶ بیشترین اهمیت را نسبت به دیگر عوامل اصلی دارا است. این نشان‌دهنده این است که عامل مدیریت هویت، بیشترین تعامل را با دیگر عوامل اصلی دارد و همچنین مدیریت اعتبارنامه با مقدار ۷/۰۹ کمترین اهمیت را دارد و این نشان‌دهنده کمترین تعامل این عامل با دیگر عوامل است.

جدول ۷- اهمیت و اثرگذاری عوامل فرعی مربوط به مدیریت هویت دیجیتال

عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
مدیریت هویت	ثبت‌نام (تنها) بر اساس الزامات مدیریت هویت دیجیتال	C11	□□□□	□□□□	□□□□	□□□□	اثرگذار

1. Valmohammadi.
2. Khaki.

عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
	فرایند مدون و تعریف‌شده برای اثبات هویت	C12	□□□□	□□□□	□□□□	□□□□	اثرگذار
	یکپارچه‌سازی اطلاعات هویتی فرد	C13	□□□□	□□□□	□□□□	□□□□	اثرگذار
	وجود چرخه حیات تعریف‌شده برای نگهداری داده‌های هویتی	C14	□□□□	□□□□	□□□□	□□□□	اثرگذار
	به‌روز بودن کلیه داده‌های هویتی افراد	C15	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
مدیریت اعتبارنامه	ثبت‌نام برای اعتبارنامه معتبر از طریق الزامات مدیریت هویت	C21	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	امکان فعال‌سازی (غیرفعال‌سازی) اعتبارنامه از راه دور	C22	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	وجود چرخه حیات	C23	□□□□	□□□□	□□□□	□□□□□	اثرپذیر

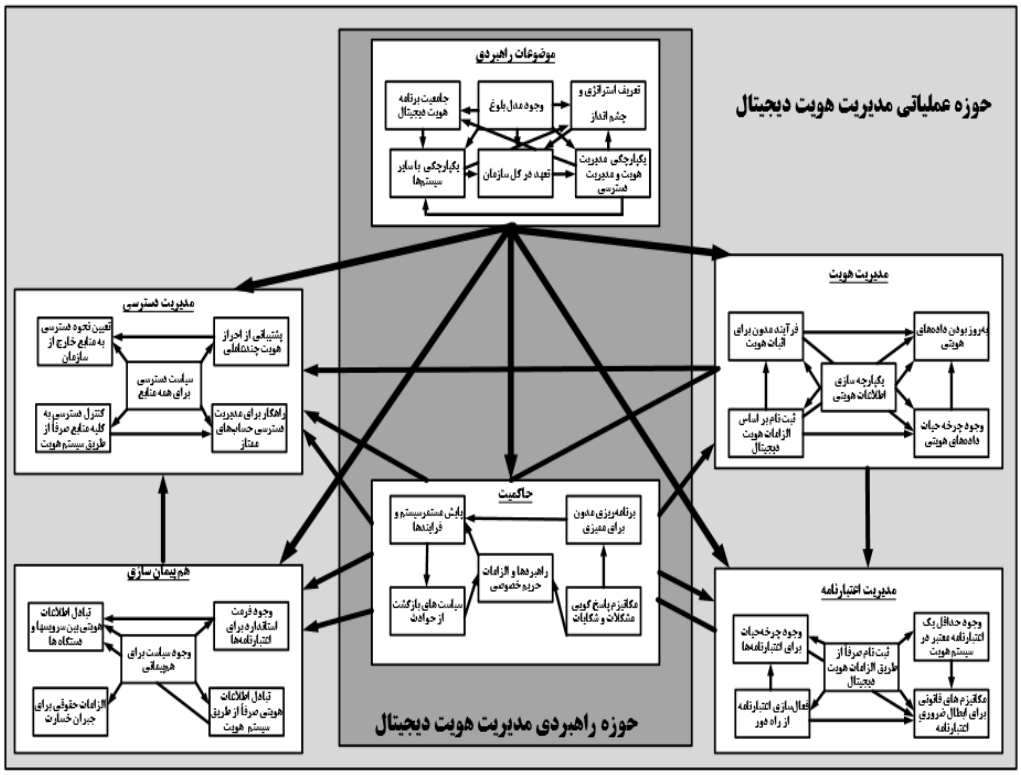
عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
	تعریف‌شده برای اعتبارنامه‌ها						
	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت	C24	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	وجود مکانیزم های قانونی برای ابطال ضروریِ اعتبارنامه	C25	□□□□	□□□□	□□□□	□□□□□	اثرپذیرترین
مدیریت دسترسی	وجود سیاست دسترسی برای همه منابع و اطلاعات	C31	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	کنترل دسترسی به کلیه منابع تنها از طریق سیستم مدیریت هویت	C32	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	وجود راهکار برای مدیریت دسترسی حساب‌های ممتاز	C33	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	پشتیبانی از احراز هویت	C34	□□□□	□□□□	□□□□	□□□□□	اثرپذیر

عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
	چندعاملی						
	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان	C35	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
هم‌پیمان‌سازی	وجود سیاست مشخص برای هم‌پیمانی	C41	□□□□	□□□□	□□□□	□□□□	اثرگذار
	امکان تبادل اطلاعات هویتی بین سرویس‌ها و دستگاه‌ها	C42	□□□□	□□□□	□□□□	□□□□	اثرگذار
	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت	C43	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	وجود فرمتی مشترک و استاندارد برای درک اعتبارنامه‌ها	C44	□□□□	□□□□	□□□□	□□□□	اثرگذار
	وجود الزامات حقوقی- قضایی برای جبران خسارت	C45	□□□□	□□□□	□□□□	□□□□	اثرگذار
حاکمیت	وجود سیاست ها و مکانیسم‌های	C51	□□□□	□□□□	□□□□	□□□□□	اثرپذیر

عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
	بازگشت از حوادث						
	وجود راهبردها و الزامات تعریف شده برای حریم خصوصی	C52	□□□□	□□□□	□□□□	□□□□	اثرگذار
	برنامه‌ریزی مدون برای ممیزی	C53	□□□□	□□□□	□□□□	□□□□	اثرگذار
	وجود مکانیزم مشخص برای بررسی و پاسخ گویی مشکلات	C54	□□□□	□□□□	□□□□	□□□□□	اثرپذیر
	پایش مستمر سیستم ها و فرایندهای مربوط به هویت	C55	□□□□	□□□□	□□□□	□□□□	اثرگذار
برنامه‌ریزی راهبردی	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی	C61	□□□□	□□□□	□□□□	□□□□	اثرگذار
	وجود مدل بلوغ مدیریت هویت دیجیتال	C62	□□□□	□□□□	□□□□	□□□□	اثرگذار
	یکپارچه بودن سیستم	C63	□□□□	□□□□	□□□□	□□□□	اثرگذار

عوامل اصلی	عوامل فرعی	نشان اختصاری	D	R	D+R	D-R	نتیجه
	مدیریت هویت دیجیتال با سایر سیستم‌ها						
	تعهد در کل سازمان	C64	□□□□	□□□□	□□□□	□□□□	اثرگذار
	تعریف راهبرد و چشم‌انداز	C65	□□□□	□□□□	□□□□	□□□□	اثرگذارترین
	جامعیت برنامه مدیریت هویت دیجیتال	C66	□□□□	□□□□	□□□□	□□□□	اثرگذار

با توجه به غربال عوامل اصلی و فرعی اشاره‌شده در پژوهش و بر اساس نتایج به‌دست‌آمده از دیمتل، چارچوب بومی‌شده مدیریت هویت دیجیتال در فضای سایبر در شکل ۲ آمده است.



شکل ۲- چارچوب بومی‌شده مدیریت هویت دیجیتال در فضای سایبر

در این تحقیق بر اساس ماتریس روابط کلی که میزان اثرگذاری و اثرپذیری عوامل را نشان می‌دهد، اقدام به حل فرایند تحلیل شبکه ای فازی با رویکرد دیمتل می‌شود. بعد از نرمالیزه شدن ماتریس ارتباطات کل، سوپرماتریس موزون را همگرا کرده تا سوپرماتریس حددار تشکیل شود. در این پژوهش در توان پنج سوپرماتریس همگرا شده و ماتریس حددار تشکیل شده است. درنهایت با به دست آمدن سوپرماتریس حددار، وزن عوامل اصلی و فرعی مشخص و به دست آمد که در جدول ۸ نشان دادن داده شده است.

جدول ۸- وزن و اولویت عوامل و عوامل فرعی مؤثر در مدیریت هویت دیجیتال

وزن و اولویت عوامل اصلی	عوامل فرعی	نشان اختصاری	وزن و اولویت نسبی عوامل	وزن و اولویت نهایی عوامل

وزن و اولویت عوامل اصلی	عوامل فرعی	نشان اختصاری	وزن و اولویت نسبی عوامل		وزن و اولویت نهایی عوامل	
مدیریت هویت (٦) (۰/۱۵۸۸)	ثبت نام (تنها) بر اساس الزامات مدیریت هویت دیجیتال	C11	۳	□□□□□□□□	۲۰	□□□□□□
	فرایند مدون و تعریف شده برای اثبات هویت	C12	٤	□□□□□□□□	۲۲	□□□□□□
	یکپارچه‌سازی اطلاعات هویتی فرد	C13	٥	□□□□□□□□	۲۳	□□□□□□
	وجود چرخه حیات تعریف-شده برای نگهداری داده‌های هویتی	C14	۲	□□□□□□□	۱٤	□□□□□□
	به‌روز بودن کلیه داده‌های هویتی افراد	C15	۱	□□□□□□□□	۱۰	□□□□□□
مدیریت اعتبارنامه (۲) (۰/۱۷۳٦)	ثبت نام برای اعتبارنامه تنها از طریق الزامات مدیریت هویت دیجیتال	C21	۳	□□□□□□□	٦	□□□□□□
	امکان فعال‌سازی (غیرفعال سازی) اعتبارنامه از راه دور	C22	٤	□□□□□□□□	۲۱	□□□□□□
	وجود چرخه حیات تعریف‌شده برای اعتبارنامه‌ها	C23	۲	□□□□□□□□	٥	□□□□□□
	وجود حداقل یک اعتبارنامه معتبر در سیستم مدیریت هویت	C24	٥	□□□□□□□	۲٥	□□□□□□
	وجود مکانیزم‌های قانونی برای ابطال ضروریِ اعتبارنامه	C25	۱	□□□□□□□□	٤	□□□□□□
مدیریت دسترسی (۱) (۰/۱۸٤۳)	وجود سیاست دسترسی برای همه منابع و اطلاعات	C31	۲	□□□□□□□□	۲	□□□□□□
	کنترل دسترسی به کلیه منابع از طریق سیستم مدیریت هویت دیجیتال	C32	۱	□□□□□□□□	۱	□□□□□□
	وجود راهکار برای مدیریت دسترسی حساب‌های ممتاز	C33	٤	□□□□□□□□	۱۱	□□□□□□
	پشتیبانی از احراز هویت	C34	٥	□□□□□□□□	۲٦	□□□□□□

وزن و اولویت عوامل اصلی	عوامل فرعی	نشان اختصاری	وزن و اولویت نسبی عوامل		وزن و اولویت نهایی عوامل	
	چندعاملی					
	تعیین نحوه دسترسی کاربر به منابع خارج از سازمان	C35	۳	□□□□□□□	□□□□□□	۷
هم‌پیمان سازی (٤) (۰/۱٦۰۹)	وجود سیاست مشخص برای هم‌پیمانی	C41	٤	□□□□□□□□	□□□□□□	۱۸
	امکان تبادل اطلاعات هویتی بین سرویس‌ها و دستگاه‌های مختلف	C42	۲	□□□□□□□	□□□□□□	۱۳
	تبادل اطلاعات هویتی تنها از طریق سیستم مدیریت هویت دیجیتال	C43	۱	□□□□□□□□	□□□□□□	۳
	وجود فرمتی مشترک و استاندارد برای درک اعتبارنامه‌ها	C44	٥	□□□□□□□□	□□□□□□	۲۹
	وجود الزامات حقوقی- قضایی برای جبران خسارت	C45	۳	□□□□□□□□	□□□□□□	۱٦
حاکمیت (۳) (۰/۱٦۳۰)	وجود سیاست‌ها و مکانیسم‌های بازگشت از حوادث	C51	٥	□□□□□□	□□□□□□	۲٤
	وجود راهبردها و الزامات تعریف‌شده برای حریم خصوصی	C52	۲	□□□□□□□□	□□□□□□	۱۲
	برنامه‌ریزی مدون برای ممیزی	C53	۳	□□□□□□□□	□□□□□□	۱۷
	وجود مکانیزم مشخص برای بررسی و پاسخ‌گویی مشکلات	C54	٤	□□□□□□□□	□□□□□□	۱۹
	پایش مستمر سیستم‌ها و فرایندهای مربوط به هویت	C55	۱	□□□□□□□□	□□□□□□	۹
برنامه‌ریزی راهبردی (٥) (۰/۱٥۹۳)	یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی	C61	۲	□□□□□□□	□□□□□□	۱٥
	وجود مدل بلوغ مدیریت هویت دیجیتال	C62	٦	□□□□□□□□	□□□□□□	۳۱
	یکپارچه بودن سیستم	C63	۳	□□□□□□□	□□□□□□	۲۷

وزن و اولویت عوامل اصلی	عوامل فرعی	نشان اختصاری	وزن و اولویت نسبی عوامل		وزن و اولویت نهایی عوامل	
	مدیریت هویت دیجیتال با سایر سیستم‌ها					
	تعهد در کل سازمان	C64	٥	□□□□□□□□□	۳۰	□□□□□□
	تعریف راهبرد و چشم‌انداز	C65	٤	□□□□□□□□□	۲۸	□□□□□□
	جامعیت برنامه مدیریت هویت دیجیتال	C66	۱	□□□□□□□□□	۸	□□□□□□

۵. نتیجه‌گیری و پیشنهادها

هدف این پژوهش تدوین چارچوبی جامع برای مدیریت هویت دیجیتال بود که به شناسایی و اولویت‌بندی معیارها و شاخص‌های هویت دیجیتال بپردازد. در این پژوهش، عوامل اصلی و فرعی مرتبط با مدیریت هویت دیجیتال در فضای مجازی شناسایی شدند. سپس با نظرخواهی از خبرگان و بومی‌سازی کلیه این عوامل، تأثیرگذاری آن ها بر یکدیگر مشخص شد و به این ترتیب هدف پژوهش محقق گردید. سؤال «عوامل مؤثر در حوزه مدیریت هویت دیجیتال کدام٤اند؟» این گونه پاسخ داده شد که چارچوب مدیریت هویت دیجیتال در فضای سایبر، از شش عامل اصلی «موضوعات راهبردی»، «حاکمیت»، «مدیریت هویت»، «مدیریت دسترسی»، «مدیریت اعتبارنامه» و «هم‌پیمان‌سازی» تشکیل شده است. این عوامل هر یک نقش تأثیرگذاری در مدیریت هویت دیجیتال داشته و بر یکدیگر نیز تأثیرگذار هستند. در فضای سایبر و حوزه‌هایی نظیر دولت الکترونیک، مجموعه عوامل اصلی و عوامل فرعی مرتبط با آن‌ها باید به‌صورت هم‌زمان و توأمان مورد توجه قرار بگیرند. برای پاسخگویی به سؤال «روابط و اثرگذاری و اثرپذیری عوامل مؤثر در مدیریت هویت دیجیتال چگونه است؟» نتایج تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده از طریق پرسشنامه دیمتل و در حل آن از طریق نرم‌افزار اکسل استفاده شد. «برنامه ریزی راهبردی» به‌عنوان اثرگذارترین معیار شناخته شد. درواقع این معیار، عمده‌ترین نقطه قوت مدیریت هویت دیجیتال به شمار می‌رود. بدیهی است شاخص‌های مرتبط با این حوزه به عنوان

شاخص‌های راهبردی و اثرگذار هستند و جهت تدوین الزامات و طراحی سیستم‌های مدیریت هویت دیجیتال می‌بایست با اولویت اثرگذاری بالا مورد بررسی قرار بگیرند. همچنین لازم است به صورت دقیق و شفاف نسبت به تعریف و تدقیق هر یک از شاخص‌های حوزه برنامه‌ریزی راهبردی اقدام شود. در مورد شاخص‌های «برنامه‌ریزی راهبردی»، تعیین راهبرد و چشم‌انداز اثرگذارترین شاخص به حساب می‌آید. واقعیت آن است که لازم است تا با نگرش و رویکرد راهبردی و بلندمدت به موضوع مدیریت هویت دیجیتال نگریسته شود. نگاه‌های کوتاه‌مدت و مبتنی بر فناوری به این موضوع، تضمین‌کننده موفقیت آن در بلندمدت نیست. باید پذیرفت که مدیریت هویت دیجیتال به‌طور اساسی حوزه‌ای راهبردی است و عملیات و اجرا در مرحله دوم اهمیت قرار می‌گیرد. شاخص «استفاده از مدل بلوغ مدیریت هویت دیجیتال» شاخص اثرگذار دوم و شاخص‌های «تعهد در کل سازمان»، «یکپارچه بودن سیستم مدیریت هویت دیجیتال با سایر سیستم‌ها»، «جامعیت برنامه مدیریت هویت دیجیتال» و «یکپارچه بودن دو بُعد مدیریت هویت و مدیریت دسترسی» به ترتیب اثرگذار هستند. جهت برنامه‌ریزی راهبردی می‌بایست کلیه این شاخص‌ها با توجه به تأثیری که در اجرای موفقیت‌آمیز این سیستم دارند مدنظر قرار بگیرند. معیار برنامه‌ریزی راهبردی، بیشترین تأثیر را به ترتیب بر معیارهای «مدیریت هویت»، «هم‌پیمان‌سازی»، «حاکمیت»، «مدیریت اعتبارنامه» و «مدیریت دسترسی» دارد که نشان از اهمیت بالای این عامل مهم است. همچنین نتایج نشان داد که در بین معیارها، «مدیریت دسترسی» به عنوان اثرپذیرترین معیار باید در نظر گرفته شود. درواقع این معیار به‌عنوان عمده‌ترین نقطه ضعف به شمار می‌آید؛ بنابراین به جهت تبدیل آن به نقطه قوت تمرکز زیادی لازم است. با توجه به نقش و جایگاه مدیریت دسترسی و اهمیت آن، باید پذیرفت که برنامه‌ریزی راهبردی، مدیریت هویت، مدیریت اعتبارنامه، حاکمیت و هم‌پیمان‌سازی بر آن تأثیر دارند. برای پاسخگویی به سؤال «وزن و اهمیت (اولویت) عوامل مؤثر در مدیریت هویت دیجیتال چگونه است؟» باید توجه داشت که در حل مسئله به روش ترکیبی فرایند تحلیل شبکه‌ای و دیمتل نتایج تحقیق نشان می‌دهد که در بین عوامل

اصلی «مدیریت دسترسی»، با وزن ۰/۱۸٤۳، اولویت اول را در بین دیگر عوامل اصلی دارد. بدیهی است که لازم است توجه ویژه‌ای به این عامل شود. طبیعتاً یکی از مهم ترین اهداف مدیریت هویت دیجیتال این است که دسترسی به خدمات و منابع برای افراد و دیگر موجودیت‌ها امکان‌پذیر شود. اولویت دوم در بین عوامل اصلی به مدیریت اعتبارنامه با وزن ۰/۱۷۳٦ اختصاص دارد. بدیهی است که یکی از اهداف مهمی که در یک نظام مدیریت هویت دیجیتال دنبال می‌شود، دراصل مدیریت هویت موجودیت‌ها و ارائه دسترسی به آن‌ها از طریق یک ابزار مناسب (همان اعتبارنامه) است که باید مورد توجه باشد. عامل «حاکمیت» با وزن ۰/۱٦۳۰ در جایگاه سوم قرار می‌گیرد. عامل «هم‌پیمان‌سازی» با وزن ۰/۱٦۰۹ در جایگاه چهارم اهمیت، «برنامه‌ریزی راهبردی» با وزن ۰/۱۵۹۳ در جایگاه پنجم و «مدیریت هویت» با وزن ۰/۱۵۸۸ در جایگاه ششم اهمیت قرار گرفت. از آنجایی که برخی از اوزان عوامل به هم نزدیک هستند، به صورت کلی می‌توان اذعان داشت که مدیریت دسترسی حدود ۱۹ درصد از اهمیت را به خود اختصاص داده است. مدیریت اعتبارنامه حدود ۱۷ درصد از اهمیت عوامل اصلی را دارد. حاکمیت و هم‌پیمان‌سازی، برنامه‌ریزی راهبردی و مدیریت هویت نیز تقریباً به طور مساوی هر یک حدود ۱٦ درصد از اهمیت کل عوامل را از آن خود کرده‌اند.

٤-۱. پیشنهادهای عملی

در مقاله حاضر به چند راه‌حل پیشنهادی در خصوص به کارگیری راهکارهایی جهت توسعه مدیریت هویت دیجیتال پرداخته شده است:

- با توجه به اهمیت و میزان تأثیرگذاری بالای عامل «برنامه‌ریزی راهبردی» لازم است تا نسبت به تدوین طرح راهبردی دسترسی در سازمان به عنوان یک سند بالادستی و راهبردی اقدام شود که در آن راهبرد و چشم‌انداز طرح تعریف شده و

با نگرش و رویکرد راهبردی و بلندمدت موضوع مدیریت هویت دیجیتال مدنظر قرار بگیرد.

- تدوین و به کارگیری مدل بلوغ مدیریت هویت دیجیتال یکی از فعالیت‌های مهم است. از روش‌های کمی و قابل اندازه‌گیری در تدوین این مدل باید بهره‌برداری شود. در حوزه مدیریت هویت دیجیتال، هر سازمان در هر زمان در یک سطح یا لایه بلوغ قرار می‌گیرد. با انجام پروژه‌های بهبود، طی مرور زمان بلوغ افزایش پیدا کرده و سازمان در این حوزه ارتقا پیدا می‌کند.
- تدوین برنامه های فرهنگی و آموزشی جهت آشنایی مدیران و افراد اثرگذار در سازمان و دیگر کارکنان بدنه سازمان در قالب سمینارها و کلاس‌های آموزشی باید در اولویت‌های کاری قرار بگیرد. در حقیقت پیاده‌سازی موفق هر سیستم مبتنی بر فناوری اطلاعات در سازمان، مستلزم حمایت و تعهد مدیران ارشد آن سازمان است. اگر مدیران ارشد به مزایا و منافعی که یک نظام مدیریت هویت دیجیتال به ارمغان می‌آورد ایمان داشته باشند و با حمایت خود این موضوع را جدی بگیرند، زمینه فرهنگ‌سازی و پذیرش آن در سازمان فراهم آمده و دیگر افراد در دیگر سطوح سازمان نیز آن را می‌پذیرند و خود را در اجرای موفق آن سهیم و شریک می‌دانند.
- در خصوص تدوین متدلوژی برای ارزیابی وضعیت موجود سازمان در خصوص عوامل مهم و مؤثر در مدیریت هویت دیجیتال و بررسی امکان‌سنجی یکپارچگی سیستم مدیریت هویت دیجیتال با سایر سیستم‌های سازمان و ایجاد اطمینان از بابت حفظ جامعیت برنامه مدیریت هویت دیجیتال باید اقدام شود.

٤-۲. پیشنهادهای تحقیقی

به منظور ادامه تحقیقات و توسعه پژوهش‌های مرتبط با مدیریت هویت دیجیتال، موضوعات زیر به پژوهشگران و علاقه‌مندان پیشنهاد می‌گردد:

- تعیین عوامل مؤثر بر پذیرش یک سیستم مدیریت هویت دیجیتال در سازمان با توجه به مدل‌های جدید پذیرش فناوری در سازمان؛
- انتخاب صنایع مختلف در جهت پژوهش میدانی و مقایسه نتایج حاصله در این پژوهش؛
- تعیین تأثیر فناوری‌های نوظهور مانند بلاک‌چین، هوش مصنوعی، پرینترهای چندبُعدی و نظایر آن بر الگوهای مدیریت هویت دیجیتال؛
- تبیین الزامات معماری عملیاتی جهت پیاده‌سازی یک سیستم مدیریت هویت دیجیتال در سازمان و
- بررسی تأثیر به کارگیری مدیریت هویت دیجیتال بر بهبود عملکرد سازمان‌ها یا کسب‌وکارها.

فهرست منابع ومآخذ

الف. منابع فارسی

- آذر، عادل و فرجی، حجن (۱۳۸۱)، علم مدیریت فازی، مرکز مطالعات و بهره‌وری ایران، انتشارات اجتماع.
- اصغرپور، محمدجواد (۱۳۸۲)، تصمیم‌گیری و نظریه بازی‌ها با نگرش تحقیق در عملیات، انتشارات دانشگاه تهران، چاپ اول، ۱٤۰-۱۳۲.
- پیغله، فریده (۱۳۹٤)، ارائه یک مدل مدیریت هویت برای کاربردهای تجارت الکترونیکی، پایان-نامه دکترا در دانشگاه گیلان.
- کاشانی، محمد (۱۳۹۵)، ارتقاء حریم خصوصی و امنیت در سیستم‌های مدیریت هویت، پایان‌نامه ارشد دانشگاه شاهد.
- مدیری، محمود؛ میرزایی خاکی، مریم و کریمی شیرازی، حامد (۱۳۹۳)، تعیین اولویت کاربردهای فناوری نانو در بخش صنایع خودرو با مدل تصمیم‌گیری فازی ترکیبی، فصلنامه مدیریت توسعه فناوری، دوره دوم، شماره ۱.

ب. منابع انگلیسی

- Abedi Jafari, H., Taslimi, M., Faghihi, A., & Sheykhzadeh, M. (2011), Theme and theme analysis. "A simple and effective way to explain patterns in qualitative data", Strategic Management Thought, 151-198, (2) 5. (In Persian)
- Bernabe, J. B., David, M., Moreno, R. T., Cordero, J. P., Bahloul, S., & Skarmeta, A. (2020). Aries: Evaluation of a reliable and privacy-preserving European identity management framework. Future Generation Computer Systems, 102, 409-425.
- Cheng, Ching-Hsue & Lin, Yin. (2002) "Evaluating the best mail battle tank using fuzzy decision theory with linguistic criteria evaluation", European Journal of Operational Research, vol.142, p.147
- DIACC. (2015). Building Canada's Digital Identity Future. By: Digital Identification and Authentication Council of Canada.
- Federal Chief Information Officers Council. (2011). Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance. Federal Chief Information Officers Council AND Federal Enterprise Architecture.
- Hu, S. K., Lu, M. T., & Tzeng, G. H. (2015). Improving mobile commerce adoption using a new hybrid fuzzy MADM model. International Journal of Fuzzy Systems, 17(3), 399-413.
- Khanboubi, F., Boulmakoul, A., & Tabaa, M. (2019). Impact of digital trends using IoT on banking processes. Procedia Computer Science, 151, 77-84.

- Miettinen, A. (2017). Centralized Identity Management in a Decentralized Organization. THESIS in Karelia University of Applied Sciences.
- NIST. (2013). National Institute of Standards and Technology - NIST SP 800-63-2. NIST.
- Nykvista, S., & Mukherjeea, M. (2016). Who am I? Developing pre-service teacher identity in a digital World. Procedia - Social and Behavioral Sciences, 217, 851 – 857.
- OLANIYI, E. O. (2017). THE ROLE OF NATIONAL ELECTRONIC IDENTITY CARDS IN ENHANCING PUBLIC SERVICE EFFECTIVENESS THE NIGERIAN CASE.
- Osmanoglu, E. (2014). Identity and Access Management. Waltham, USA: Elsevier.
- Petronio, S., & Child, J. T. (2019). Conceptualization and Operationalization: Utility of Communication Privacy Management Theory. Current opinion in psychology.
- Rasiwasia, A. (2017). A Framework To Implement OpenID Connect Protocol For Federated Identity Management In Enterprises. Master Theses in Luleå University of Technology.
- Rountree, D. (2013). Federated Identity Primer. Oxford: Elsevier.
- SeID. (2015). Swiss eID-Ökosystem Modell. By: Berner Fachhochschule & SECO.
- Valmohammadi, C., & Khaki, M. M. (2019). Determinants for selection of projects for exploitation of mines in Iran. Resources Policy, 63, 101424.
- Viitanen, S. (2015). Integrating an Open Source Identity Management System into Access Management Software. Bachelor's Thesis in Hagaa-Helia University of applied science.
- WA IdAM. (2005). Western Australia Identity & Access Management Framework (WA Id&AM). By: WESTERN AUSTRALIAN GOVERNMENT OFFICE OF e-GOVERNMENT.
- White House. (2011). National Strategy for Trusted Identities in Cyberspace. White House.
- Yang, J. L., & Tzeng, G. H. (2011). An integrated MCDM technique combined with DEMATEL for a novel cluster-weighted with ANP method. Expert Systems with Applications, 38(3), 1417-1424.
- Zhang, C., Zhu, L., Xu, C., Sharif, K., Zhang, C., & Liu, X. (2020). PGAS: Privacy-preserving graph encryption for accurate constrained shortest distance queries. Information Sciences, 506, 325-345.