دوفصلنامه محاسبات و سامانه های توزیع شده
سال ۵، شماره ۱، شماره پیاپی ۹، صفحه ۶۴ تا ۷۳، سال ۱۴۰۱

مروری بر مدل‌های مدیریت هویت دیجیتال در بانکداری دیجیتال

محسن راجی*[۱]، بابک میرزاخانی[۲]
[۱]دانشیار دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران.
[۲]کارشناسی ارشد، دانشکده آموزش‌های الکترونیکی، دانشگاه شیراز، شیراز ، ایران.

چکیده

بانکداری دیجیتال پارادایم جدیدی است که مصالح فراوانی را برای بانک، عرضه داشته و سبب افزایش بهره وری و سودآوری به نفع بانک و مشتری می‌گردد. در بانکداری دیجیتال با توجه به ذخیره‌شدن ویژگی‌های هویتی کاربر در تعیین هویت، کاربران کنترل فیزیکی و سنتی خود را بر روی اطلاعات شخصی هویتی خود از دست خواهند داد، و لذا به منظور پذیرش گسترده بانکداری دیجیتال، مشتریان باید مطمئن باشند که هویت آن‌ها ربوده نخواهد شد. در جهت حل مشکل هویت‌های متعدد کاربران، سیستم‌های مدیریت هویت دیجیتال، پیشنهاد شده است. سامانه مدیریت هویت دیجیتال به‌عنوان مجموعه‌ای از سیاست‌ها، قوانین، روش‌ها و سامانه‌هایی است که مدیریت احراز هویت، کنترل دسترسی و عملیات حسابرسی بر اساس هویت دیجیتال را بر عهده دارد. کاربردی‌ترین مدل‌های مدیریت هویت به ۵ دسته، مدل مجزا مدل متمرکز ، مدل وابسته ، کاربر محور و مدیریت ترکیبی دسته‌بندی می‌شوند. در این مقاله، مروری بر مدل‌های مختلف مدیریت هویت دیجیتال در حوزه بانکداری دیجیتال ارائه می شود و مزایا و معایب هر کدام ارائه می‌گردد.

کلمات کلیدی: امنیت، سیستم‌های مدیریت هویت، مدل کاربر محور، مدل مدیریت ترکیبی، هویت دیجیتال.

A Survey on Digital Identity Management Models in Digital Banking

Mohsen Raji*[1], Babak Mirzakhani[2]
[1] Associate Professor, School of Electrical and Computer Engineering, Shiraz, Iran.
[2] M.Sc., Faculty of Electronic Learning, Shiraz University, Shiraz, Iran.

Abstract

Digital banking is a new paradigm that provides a lot of materials for the bank and increases productivity and profitability for the benefit of the bank and the customer. In digital banking, due to the storage of the user's identity characteristics in determining the identity, users will lose their physical and traditional control over their personal identity information, and therefore, in order to widely accept digital banking, customers must be sure that their identity Will not be kidnapped. In order to solve the problem of multiple user identities, digital identity management systems have been proposed. Digital identity management system is a set of policies, rules, methods and systems that manage authentication, access control and audit operations based on digital identity. The most practical identity management models are classified into 5 categories, separate model, centralized model, dependent model, user-oriented model, and mixed management. In this article, an overview of different models of digital identity management in the field of digital banking is presented and the advantages and disadvantages of each are presented.

Keywords: Security, Identity management systems, User-centric model, Hybrid management model, Digital identity

تاریخچه مقاله:

تاریخ ارسال: ۱۴۰۱/۰۵/۱۱
تاریخ اصلاحات: ۱۴۰۱/۰۶/۲۰
تاریخ پذیرش: ۱۴۰۱/۰۶/۲۵
تاریخ انتشار: ۱۴۰۱/۰۶/۲۹

Keywords:

Security
Identity management systems
User-centric model
Hybrid management model
Digital identity

* ایمیل نویسنده مسئول:
mraji@shirazu.ac.ir

۱ – مقدمه

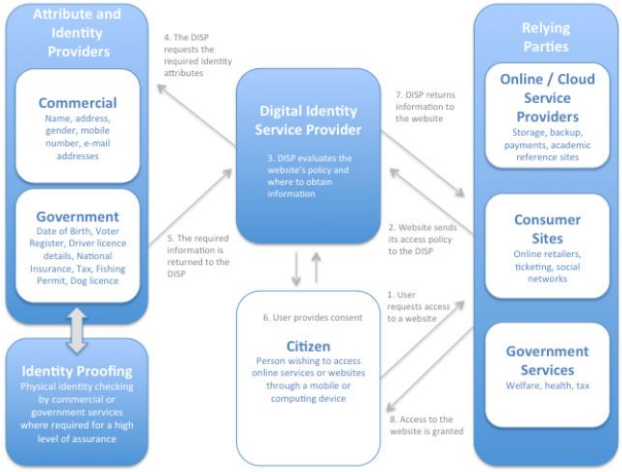
نفوذ گسترده فناوری‌های دیجیتالی در زندگی روزمره انسان‌ها سبب بوجود آمدن تغییرات گسترده در سبک زندگی مردم و مدل کسب و کارهای امروزی گردیده است. بانک‌ها نیز به عنوان یک سازمان مردم نهاد از این قاعده مستثنی نیستند[۱]. مشتری‌مداری و حرکت بر مدار خواسته‌های مشتریان از مهم‌ترین عوامل موفقیت در صنعت بانکداری است که فناوری‌های تحول آفرین دیجیتالی با فراهم آوردن امکان ارائه خدمات شخصی‌سازی شده، عملا پارادایم جدیدی پیش روی بانک‌های پیشرو برای دستیابی به این مفهوم، ایجاد نموده است. در سال‌های اخیر نسل جدید بانکداری تحت عنوان بانکداری دیجیتال، در بانک‌های مطرح اروپایی و آمریکایی عملیاتی شده و طبق آمارها و گزارش‌های منتشر شده، بخش عمده‌ای از فعالیت‌ها و برنامه‌ریزی‌های بانک‌های پیشرو، حول محور تحول دیجیتالی ، معطوف گردیده است[۳]. بانکداری دیجیتال به عنوان بانکداری آینده، راهکاری برای ایجاد تحول دیجیتال در صنعت بانکداری است[۲].

بانکداری دیجیتال را می‌توان به این صورت تعریف نمود: «استفاده از فناوری برای اطمینان از یکپارچگی ابتدا تا انتهای پردازش تراکنش‌ها یا عملیات بانکی است. عملیاتی که با درخواست مشتری آغاز شده، حداکثر بهینه‌سازی در آن لحاظ شده؛ برای مشتری: در دسترس بودن، سودمندی و صرفه؛ و برای بانک: کاهش هزینه‌های عملیاتی، عاری از خطا و خدمات بهبود یافته را به ارمغان می‌آورد» [۳]. اما یکی از چالش‌های بانکداری دیجیتال، کسب یا حفظ اعتماد مشتریان است. به منظور پذیرش گسترده بانکداری دیجیتال توسط مشتریان، اعتماد، پیش‌نیاز اصلی است؛ مشتریان باید مطمئن باشند که هویت آنها ربوده نخواهد شد[۲].

موضوع«هویت»، یکی از موضوعات مهم و مطرح در این فضا (فضای مجازی) است که با عنوان«هویت دیجیتال» مطرح می‌شود. هویت دیجیتال به معنی مجموعه ویژگی‌ها و خصوصیات یک موجود است که آن را به صورت منحصر به فردی در فضای سایبری توصیف می کند[۵]. مشکلی فعلی این است که کاربر با حوزه‌های مختلف ارائه خدمت مواجه است. بنابراین کاربر در هر حوزه‌ی خدماتی از جمله بانکداری دیجیتال، باید هویت ویژه آن حوزه را داشته باشد و از روش خاص احراز هویت آن حوزه تبعیت کند. در جهت حل مشکل هویت‌های متعدد کاربران، سیستم‌های مدیریت هویت دیجیتال پیشنهاد شده است [۶]. سیستم مدیریت هویت دیجیتال به عنوان مجموعه‌ای از سیاست‌ها، قوانین، روش‌ها و سیستم-هایی است که مدیریت احراز هویت، کنترل دسترسی و عملیات حسابرسی بر اساس هویت دیجیتال را بر عهده دارد. سیستم‌های مدیریت هویت امکان تعریف کاربر و انتساب هویت به آن کاربر و نحوه اعطای نقش و مجوزهای دسترسی به هویت و محافظت از اطلاعات هویت را فراهم می‌کنند و برای اینکار از فناوری‌های مختلف مانند پرونکل‌های امنیتی شبکه، گواهینامه‌های امنیتی، روش‌های مختلف گذرواژه و غیره استفاده می کنند[۹] [۳] [۱۰]. کاربردی‌ترین مدل‌های مدیریت هویت به پنج دسته، مدل مجزا، مدل متمرکز، مدل وابسته، کاربر محور و مدیریت ترکیبی دسته‌بندی می شوند[۹] [۳] [۱۰]. لذا لازم است این مدل‌ها بررسی گردد و مزایا و معایب آن‌ها مقایسه کرد و بهترین مدل از لحاظ بالا بودن امنیت، سادگی، هزینه و قابلیت اطمینان برای بانکداری دیجیتال پیشنهاد شود.

۲ – پیشینه تحقیق

شکل ۱ نشان می‌دهد که هویت دیجیتال فقط یک روش ساده برای تأیید اعتبار و کنترل دسترسی نیست، بلکه بیشتر به یک مجموعه اطلاعات پیچیده در چارچوب قابل اعتماد شباهت دارد[۱۱]. علاوه بر این، مدیریت هویت نیز یک عنصر اساسی برای امنیت اطلاعات است. این مبنای بسیاری از انواع کنترل دسترسی و ایجاد مسئولیت آنلاین است. بنابراین، با کاهش خطرات دسترسی غیر مجاز به اطلاعات شخصی، نقض داده‌ها و سرقت هویت، به محافظت از حریم خصوصی کمک می‌کند[۱۲].



(شکل ۱): دسترسی به وب سایت با استفاده از هویت دیجیتال[۱۱].

در دنیای فیزیکی، مدیریت هویت به رفع خطرات مرتبط با فعل و انفعالات انسانی کمک می‌کند و باعث افزایش اطمینان بین طرفین تعامل می‌شود. بنابراین برای زندگی اقتصادی و اجتماعی لازم است. همین امر در فضای مجازی صدق می‌کند، جایی که فقدان ارتباط قابل

اثبات بین شخص فیزیکی و هویت دیجیتالی می‌تواند عدم اطمینان بیشتری ایجاد کند که در حال حاضر وجود ندارد[۱۳].

۱-۲-دسته‌های مدیریت هویت دیجیتال

پنج دسته مدیریت هویت دیجیتال وجود دارد که به طور گسترده در دسترس هستند[۱۴]: منفرد، متمرکز، وابسته، کاربر محور و ترکیبی. در این پژوهش مروری بر مدل‌ها مدیریت هویت دیجیتال می‌شود و مزایا و معایب آن‌ها مورد بررسی قرار می‌گیرد.

۲-۲-سیر تکامل مدل‌های مدیریت هویت

مدل‌های مدیریت هویت متنوعی برای کنترل هویت دیجیتال ایجاد شده‌اند. هویت دیجیتال به یکی از عناصر حیاتی عصر حاضر تبدیل شده است. سرویس‌های اینترنتی نیازمند شناسایی امن هویت کاربران از طریق نام کاربری و رمز عبور، تراشه‌های روی کارت، توکن‌های امنیتی و شناسه‌های الکترونیک می‌باشند. علاوه بر افراد، شناسایی هویت دیجیتال موجودیت‌های غیرانسانی مانند دستگاه‌ها و تجهیزات فنی نیز از اهمیت بالایی در تبادل داده و ارزش برخوردار است. هویت دیجیتال یک تصویر لحظه‌ای از هویت واقعی فرد، شرکت، دستگاه، اتومبیل و در حالت کلی، یک موجودیت است. هویت واقعی شامل تمامی ویژگی‌های قابل تشخیص یک موجودیت است که آن موجودیت را از دیگران متمایز می‌سازد. هر هویت دیجیتال معمولاً دربردانده بخشی از هویت است و برای اهداف خاص در حوزه‌های مشخص ایجاد می‌شود. هویت‌های دیجیتال یک فرد در سطح جزییات تحت پوشش، دقت توصیفات و درجه انتزاع با یکدیگر متفاوتند. علاوه بر این، هویت دیجیتال دارای نقطه مرجع زمانی مشخصی است و ویژگی‌های موجودیت در طول زمان تغییر می‌کنند. هر انسان، هر سیستم، هر حسگر یا به عبارتی هر موجودیت دارای یک هویت است ولی می‌تواند تعداد نامحدودی هویت دیجیتال داشته باشد.

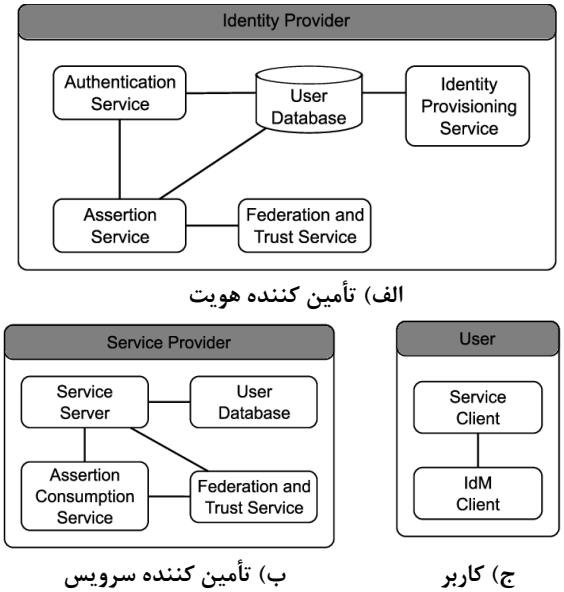
در گذر زمان، مدل‌های مختلفی برای مدیریت هویت توسعه داده شده‌اند. دلایل متعددی در پیشرفت مدل‌های مدیریت هویت دخیل بوده است با این وجود، تکامل هویت دیجیتال تأثیر شایانی از تلاش‌های صورت گرفته برای برآورده‌سازی سه نیاز عمده زیر پذیرفته است.

- امنیت: اطلاعات هویتی باید در مقابل افشای غیرعمدی محافظت شوند.
- کنترل: مالک داده باید دسترسی‌های افراد به داده‌های خود را کنترل و مدیریت نماید.
- قابلیت حمل: مالک داده باید از توانایی حمل داده‌های هویتی به هر مکانی برخوردار باشد.

غیرمتمرکزسازی یکی از روندهای پیش رو برای غلبه بر مشکلات مربوط به محدوده جهانی هویت‌های دیجیتال بوده است. اولین گام‌های مدیریت هویت با مدل‌های هویتی منفرد و سیلویی آغاز شد. در گام بعدی تلاش‌های برای متمرکزسازی مدیریت هویت انجام گرفت[۴]. در ادامه، مهم‌ترین مدل‌های مدیریت هویت توضیح داده شده‌اند.

۳ – مدل‌های مدیریت هویت دیجیتال

مدیریت هویت یک روش متمرکز و اتومات است که دسترسی به منابع را برای کارمندان و افراد مجاز در شرکت فراهم می‌آورد که با هدف افزایش امنیت و بهره‌وری و همچنین کاهش هزینه‌های زمان و وظایف تکراری صورت می‌گیرد. در واقع مدیریت هویت وظیفه کنترل اطلاعات کاربران را بر عهده دارد، که این اطلاعات شامل اطلاعات مورد نیاز برای احراز هویت کردن یک کاربر، و اطلاعاتی که عملیات و کارهایی را که کاربران مجاز به انجام آن هستند را توصیف می‌کند. قبل از اینکه مدل-ها و الگوهای مدیریت هویت را بررسی کنیم باید مفاهیم و معناصر کلیدی موجود در آن را بشناسیم. در شکل ۲ نمایی از معماری مرجع مدیریت هویت دیجیتال آورده شده است[۴].



الف) تأمین کننده هویت

ب) تأمین کننده سرویس **ج) کاربر**

(شکل ۲): معماری مرجع مدیریت هویت دیجیتال 4][۴].

- مهیا کننده خدمات[1]

این مولفه در مدیریت هویت وظیفه مهیا کردن سرویس‌ها را برای کاربر را دارد. افراد می‌توانند از سرویس‌های متفاوتی مانند بانکداری اینترنتی و خرید اینترنتی استفاده کنند. واحد خدمات سرور[2]، خدمات موجود و در دسترس را برای خدمات فراهم می‌کند. سرویس تایید هویت مورد ادعای کاربر[3]، هویت ادعایی کاربر را جهت احراز هویت بوسیله اعتماد به یک مهیا کننده هویت[4] صورت می‌دهد. مهیا کننده خدمات به مهیا کننده هویت با توجه به رابطه اعتمادی که از قبل ایجاد شده و موجود است، اعتماد می‌کند. این روال توسط سرویس اعتماد و وابسته، صورت می‌پذیرد.

- مهیا کننده هویت[5]

این مولفه به عنوان هسته سیستم‌های مدیریت هویت شناخته می‌شوند. مهیا کننده هویت سطوح امنیتی متفاوتی را به کاربران مختلف ارائه می‌دهد. برای مثال یک کاربر عادی و یک مدیر باید سطوح اعتماد متفاوتی را در یک سازمان داشته باشند. مهیا کننده هویت دارای ۲ وظیفه کلی است:

۱- پیاده‌سازی سرویس برای کاربران مانند ثبت نام کاربری بررسی هویت کاربر و فضای هویت کاربران.

۲- دریافت درخواست‌های احراز هویت را از کاربران و مهیا کننده خدمت‌ها. در مهیا کننده هویت اعتبارسنجی کاربران بر عهده سرویس احراز هویت[6] می‌باشد.

مهیا کننده هویت در پروتکل احراز هویت و رد و بدل کردن کردن اطلاعات و تایید صحت اطلاعات کاربر از پایگاه داده‌ای کاربر استفاده می‌کند. پایگاه داده‌ای کاربر[7] شامل لیستی از هویت کاربران مانند: شناسه هویت، صفات و ویژگی‌های مرتبط با کاربر و متادیتاهایی[8] در مورد کاربر (به عنوان مثال: تاریخ قبلی استفاده از هویت) می‌باشد. سرویس تامین هویت[9] پایگاه داده‌ای کاربر را پر می‌کند. پس از ایجاد هویت جدید، آن‌را وارد پایگاده داده‌ای کاربر می‌کند. بنابراین رابطه ایجاد شده از قبل بین مهیا کننده هویت و مهیا کننده خدمات باعث محافظت در رد و بدل شدن اطلاعات می‌شود. این موضوع بر عهده سرویس اعتماد و وابسته[10] می‌شود. بر طبق رابطه اعتماد ایجاد شده، مهیا کننده خدمات اثبات هویت را با استفاده از سرویس ادعاکننده[11] درخواست می‌دهد.

-کاربر[12]

کاربران مشتریان مهیا کنندگان سرویس‌ها و مهیا کنندگان هویت می‌باشند که می‌توانند یک سازمان عمومی، یک شخص، یک نهاد مجازی مانند نرم افزار یا غیره باشد. کاربر با هویت خود از مهیا کننده خدمات خدمات می‌گیرد. کاربر احراز هویت خود را از مهیا کننده هویت و بوسیله مهیا کننده هویت مشتری[13] می‌گیرد. پس از احراز هویت کاربر توسط مهیا کننده هویت کاربر در موقعیت استفاده از خدمات قرار می‌گیرد.

مهیا کننده هویت بر اساس عملکردشان به چهار نوع تقسیم می‌شوند[۱۵]:

۱- سرویس هویت معتبر[14]

این نوع مهیاکننده هویت برای احراز هویت کاربر از اعتبارنامه‌ها به عنوان هویت کاربر استفاده می‌کنند. اولین و محبوب‌ترین آن اعتبارنامه X.509، است.

۲- سرویس هویت شناسایی[15]

اطلاعاتی از کاربران است که می تواند شامل نام، ایمیل یا شماره آی دی کارت تخصیص یافته شناسایی کاربر باشد.

۳- سرویس هویت صفات[16]

هویت صفات اطلاعاتی است که برای توصیف هویت کاربران می‌تواند استفاده شود. مانند آدرس، کد ملی، اطلاعات تماس و غیره.

۴- سرویس هویت الگویی[17]

شناساسس الگویی به این معنی است که یک مهیا کننده هویت از الگوها، شهرت، سوابق اعتمادی برای توصیف یا مشخص کردن هویت

[1] SP
[2] Service Server
[3] Assertion Consumption Service
[4] IDP
[5] IDP
[6] Authentication Service
[7] User Database
[8] meta-data
[9] Identity Provisioning Service
[10] Federation & Trust Service
[11] Assertion Service
[12] User
[13] IDM Client
[14] Credential Identity Service
[15] Identifier identity service
[16] Attribute Identity Service
[17] Pattern Identity Service

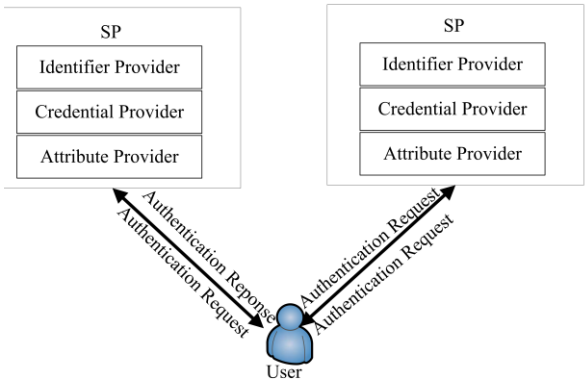
کاربران استفاده می‌کند. مثلا از مشخصات یک مدل حمله‌کننده می‌توانیم برای تشخیص حمله هکر استفاده کنیم. در واقع، اینکه از کدام سرویس هویت استفاده شود یا اینکه آیا نیاز به ترکیب دو یا چند سرویس است یا نه، به سطح امنیتی مورد نیاز برای مدیریت هویت دیجیتال بستگی دارد. مثلا برای دسترسی به وب یا سرویس‌های رایج دیگر شناسایی هویت کافی است. اما برای سرویس‌های سطح بالا مانند سرویس‌های بانکداری الکترونیکی، اعتبارنامه‌های مناسب نیز مورد نیاز است.

مدل‌های مدیریت هویت به ۵ دسته، مدل مجزا[18] مدل متمرکز[19]، مدل وابسته[20]، مدل کاربر محور[21] و مدل مدیریت ترکیبی[22] دسته‌بندی می‌شوند[۹] [۱۰].

۱-۳-مدل مجزا

در مدل مجزا واحد مهیا کننده خدمات وظیفه فراهم کردن سرویس و فراهم کردن هویت را دارد به این معنی که تمام فضای ذخیره‌سازی هویت و عملکردهای کاربران به وسیله یک سرور صورت می‌گیرد. تخصیص هویت منحصر به فرد، حذف، اصلاح، تصدیق هویت و اختیار دادن در مهیا کننده سرویس پیاده سازی می‌شود. هر کاربر باید گواهی‌نامه‌های مجزا مانند کلمه عبور یا بیومتریک مرتبط با هویت داشته باشد. واحد مهیا کننده خدمات به عنوان ارائه دهنده شناسه"، ارائه‌دهنده اعتبار و ارائه‌دهنده صفات (ویژگی) عمل می‌کند. این مدل در شکل ۳ نشان داده شده است. این مدل بسیار ساده است، اما مشکلات زیادی دارد. با رشد انفجاری خدمات آنلاین، کاربران باید اطلاعات شناسایی بیشتری را مدیریت کنند. اعتبارنامه‌های بیشتری مانند نام کاربری و کلمه عبور باید به درستی توسط کاربران مدیریت شود. ترس از فراموش کردن اعتبارنامه‌ها به ویژه رمزعبور موانع زیادی را برای استفاده کاربران ایجاد می‌کند. هزینه بازیابی رمز عبور باعث افزایش هزینه مهیا کننده خدمات می‌شود به ویژه اگر سطح امنیتی بالایی مورد نیاز باشد.

یکی از اهداف مهم از اجرای طرح تحمل پذیری خطا در محاسبات ابری، افزایش قابلیت اطمینان در محیط ابر می باشد. تحمل پذیری خطا در محاسبات ابری مولفه ای بسیار مهم است، که آن را به عنوان تضمین کننده در دسترس بودن، قابلیت اطمینان و عملکرد برنامه های کاربردی در نظر خواهند گرفت. در برخی از مواقع، حجم کار زیاد و نوسانی محیط ابر به گونه ای است که ممکن است وضعیت اجرای برنامه ها به یک حالت نامعقول تبدیل شود. مولفه خطا برای دستیابی به قابلیت اطمینان، در دسترس بودن، عملکرد و استحکام محیط ابری امری ضروری است. حتی اگر خطاهای موجود در محاسبات ابری شناخته شده هم باشند، باز هم امکان بروز مشکلات وجود دارد.

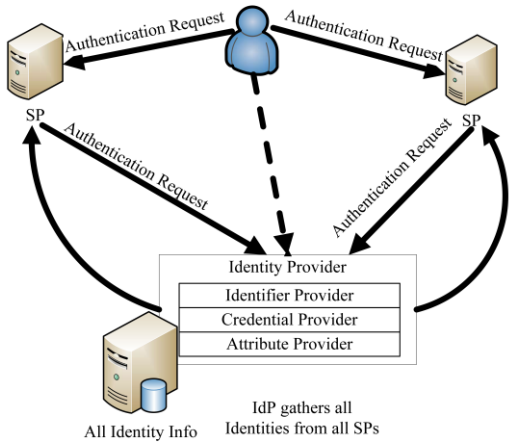


(شکل ۳): مدل مجزا .Error! Reference source not found

۲-۳-مدل متمرکز

مدل متمرکز در یک مدل C/s پیاده سازی می‌شود، فضای ذخیره هویت کاربران و تصدیق هویت کاربران هر دو در سمت سرور که مهیا کننده هویت نامیده می‌شود، پیاده‌سازی می‌شود. برخلاف مدل مجزا، این مدل عملکردهای مهیا کننده خدمات و مهیا کننده هویت را از هم جدا می‌کند. تمام هویت‌ها باید برای ذخیره‌سازی و دنبال کردن تصدیق هویت به مرکز مهیا کننده هویت فرستاده شود. شکل۴ مدل متمرکز را نشان می‌دهد، تمامی هویت‌های موجود در هر مهیا کننده خدمات در مهیا کننده هویت ذخیره می‌شود، زمانی که مهیا کننده خدمات نیاز به تصدیق هویت یک کاربر دارد اطلاعات کاربر را برای اتمام فرآیند به مهیا کننده هویت ارسال می‌کند. سیستم‌های مدیریت هویت زیادی در مدل متمرکز پیاده‌سازی شده‌اند، مانند پی کی آی، کربروس کاس و غیره این مدل معایب زیادی دارد، ذخیره تمام هویت‌ها در یک مهیا کننده هویت مشکلات حفاظت از حریم خصوصی را به وجود می‌آورد. همچنین این مدل نمی‌تواند از تفویض امتیاز کاربر[23] و دسترسی متقابل دامنه[24] به‌خوبی پشتیبانی کند.

[18] Isolated
[19] Centralized
[20] Federate
[21] User Centric Identity
[22] Hybrid Identity Management
[23] user privilege delegation
[24] cross domain access



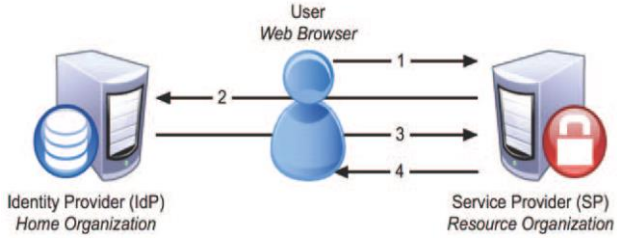
(شکل ۴): مدل متمرکز[۱۵]

۳-۳-مدل وابسته

در مدل متمرکز کاربران نمی‌توانند به سرویس‌های موجود در دامنه-های دیگر دسترسی یابند. مدل وابسته دامنه‌های زیادی را با یکدیگر یکپارچه می‌کند و آن را تقریبا به یک دامنه منحصر به فرد جهانی تبدیل می‌کند.

این مدل در اصل گسترش مدیریت هویت به چندین دامنه امنیتی است. هدف این است که یک کاربر بتواند یکبار احراز هویت شود و سپس به برنامه‌ها و منابع چندین دامنه بتواند دسترسی پیدا کند[۱۶]. مدل وابسته می‌تواند به عنوان مجموعه‌ای از توافق نامه‌ها، استانداردها و تکنولوژی‌ها تعریف شود که گروهی از مهیا کننده خدمات‌ها را توانا می‌سازد تا هویت‌های کاربران را از دیگر مهیا کننده خدمات‌ها تشخیص دهند. پروتکل‌ها که شامل سیاست‌ها و استانداردها و تکنولوژی هستند بین مهیا کننده خدمات‌ها ایجاد می‌شوند به طوریکه هویت‌ها از دامنه‌های هویتی متفاوت می‌تواند در بین همه دامنه‌ها شناخته شود.

سازمان هویت وابسته شامل گروهی از سازمان هاست که به منظور تبادل اطلاعات شناسه دیجیتال و حفظ جامعیت و محرمانگی اطلاعات شخصی کاربران ارتباطات قابل اعتمادی را میان یکدیگر ایجاد کرده‌اند. سازمان هویت وابسته مهیا کنندگان شناسه و مهیا کنندگان خدمات را در یک ساختار اعتماد و بوسیله کانال‌های ارتباطی امن شده و قراردادهای تجاری درگیر می‌سازد. مهیا کننده هویت اطلاعات شناسه کاربران را مدیریت می‌کند و فرآیند احراز شناسه به منظور معتبر ساختن شناسه انجام می‌دهد. سازمان هویت وابسته می‌تواند شامل یک مهیا کننده هویت (مدل متمرکز) یا چندین مهیا کننده هویت (مدل توزیع شده[۲۵]) باشد. مزیت مدل متمرکز این است که اطلاعات شناسه منتشر نمی‌شود و حفظ محرمانگی و جامعیت اطلاعات آسان‌تر می-باشد. اما می‌تواند باعث ایجاد تنگنا و یک نقطه خرابی شود. در مدل توزیع شده، فرآیند احراز شناسه می‌تواند در هر مهیا کننده هویت صورت گیرد که باعث ایجاد انعطاف و تعادل بار می‌شود. اگر چه این روش به مکانیزم‌های امن و پیچیده‌تری برای تبادلات نیاز دارد، ولی اطلاعات شناسه را مدیریت می‌کند و دارای مشکل یک نقطه خرابی نیست در شکل ۵ یک سناریوی ساده از مدیریت هویت وابسته را بیان می‌کنیم. اگر یک کاربر از یک سازمان بخواهد از منابع سازمان دیگر استفاده کند، او ممکن است در مدیریت هویت وابسته از همان شناسه-ای که در حوزه سازمانی خودش استفاده می‌کند، استفاده کند.



(شکل ۵): سناریوی ساده مورد استفاده در مدیریت هویت وابسته17]][۱۷].

در این سناریو در ابتدا کاربر درخواست خود را در جهت دسترسی به سرویس در دامنه سازمانی دیگر، درخواست می‌دهد[۱۵]. مهیا کننده خدمات در این زمان با مهیا کننده هویت در جهت احراز هویت کاربر، ارتباط برقرار می‌کند[۱۸]. در این زمان مهیا کننده هویت، نشانه امنیتی احراز هویت را به مهیا کننده خدمات اعلام می‌کند[۴]. در آخرین گام [۱۰]، کاربر اجازه دسترسی به سرویس را می‌گیرد[۱۷].

یک معماری شناسه یکپارچه باید عملکردهای اصلی زیر را از دیدگاه کاربران، مهیا کنندگان شناسه و مهیا کنندگان خدمات داشته باشد:

- ✓ **ورود یکپارچه**[۲۶]: به کاربران اجازه می‌دهد که با یک مهیا کننده هویت احراز شناسه شوند و سپس بدون احراز شناسه مجدد به خدمات مهیا شده بوسیله چندین مهیا کننده سرویس دسترسی داشته باشند.
- ✓ **تبادل صفت**[۲۷]: یکبار که کاربر بوسیله مهیا کننده هویت احراز شناسه شد، مهیا کننده خدمات برای مهیا کردن سرویس‌های شخصی‌سازی شده به صفات بیشتری نیاز دارد. بنابراین سازمان هویت

[25] Distributed
[26] SSO Single - sign - on
[27] Attribute exchange

وابسته باید تبادل صفات را بین مهیا کننده هویت و مهیا کننده خدمات آسان کند.

- ✓ **حفظ اطلاعات شخصی:** محرمانگی و جامعیت اطلاعات شخصی کاربران باید به روشی که ارائه صفات شناسه بوسیله کاربر کنترل شود، تضمین شود.
- ✓ **مدیریت چرخه عمر شناسه:** چه مدل متمرکز باشد و چه توزیع شده ایجاد، نگه‌داری و حذف شناسه دیجیتال باید ساده باشد و هزینه اجرایی بالایی نداشته باشد.
- ✓ **معماری استاندارد شده:** سازمان هویت وابسته باید برای ادغام راحت مهیا کننده خدمات‌ها و مهیا کننده هویت‌های جدید بر اساس استانداردها بنا شده باشد.

چندین روش و الگو برای پیاده سازی معماری سازمان هویت وابسته وجود دارد که در قسمت زیر معماری، عناصر و عملکردهای اصلی آن‌ها توصیف شده است و مورد مقایسه قرار گرفته است[۱۹].

پروتکل های استانداردها و سیستم‌ها برای مدل وابسته شامل اس ای ام ال[۲۰]. آسیس[۲۱] و سرویس وب وابسته[۲۸] [۲۲] می‌باشد. به عنوان نمونه امنیت موکد زبان نشانه‌گذاری (امنیت موکد زبان نشانه-گذاری) مجموعه‌ای از پروتکل‌های استاندارد خدمات وب است که توسط کمیته فنی خدمات امنیت (آسیس) انجام شده است. امنیت موکد زبان نشانه‌گذاری نسخه 1/0 و 1/1، در سال ۲۰۰۲ و ۲۰۰۵ منتشر شد، نسخه فعلی امنیت موکد زبان نشانه‌گذاری سهم زیادی از آزادی تجمیع دارد. امنیت موکد زبان نشانه‌گذاری استانداردXML برای تبادل احراز هویت و مجوز داده‌ها بین خدمات است. امنیت موکد زبان نشانه‌گذاری توسط بسیاری از کارشناسان امنیتی پیشرو صنعت و دانشگاه، به منظور ارائه قابلیت همکاری بین محصولات قابل ثبت نام تحت وب ایجاد شد. مورد استفاده معمولی شامل یک کاربر است که توسط یک مهیا کننده هویت، برای کاربران حساب می‌سازد. این استاندارد XML دو مشکل یکبار ورود و هویت‌های متمرکز را حل کرده و بیشتر برای شرکای کسب و کار که می‌خواهند یک استاندارد برای تبادل اطلاعات امنیتی در نظر بگیرند، مناسب است. فن‌آوری هویت وابسته اجازه می‌دهد تا سازمان با استفاده از احراز هویت و مجوز روش متفاوت برای همکاری، توانایی ارائه خدمات موجود در هر سازمان را به جای اجبار به جایگزینی آن‌ها، گسترش دهد. همچنین هویت وابسته به کاربران با استفاده از آشنایی با سیستم‌های ورود موجود و کاهش تعداد رمز عبور آن‌ها، کمک می‌کند.

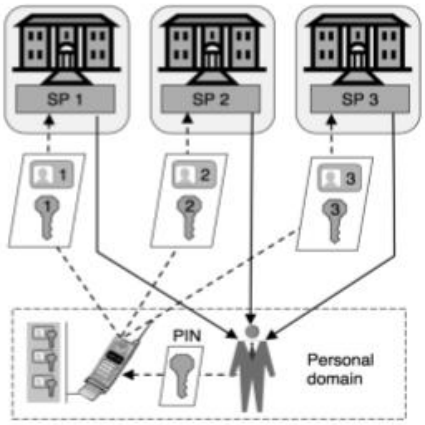
به طور خلاصه این مدل به کاربران اجازه می‌دهد تا بر اساس یک تأیید اعتبار به چندین سرویس دسترسی پیدا کنند. از نظر مفهومی، این شامل گروهی از سازمان‌ها است که روابط اعتماد را ایجاد می‌کنند که به آن‌ها امکان می‌دهد ادعاها را در مورد هویت کاربر به اشتراک بگذارند، و به کاربران اجازه دسترسی به منابع خود را بدهند. کاربر یکبار ثبت نام می‌کند تا به همه خدمات ارائه شده توسط شرکای مختلف در سراسر شرکت وابسته دسترسی یابد[۲۳]. مهیا کننده هویت، هویت کاربر را مدیریت کرده و فرایند احراز هویت را برای تأیید هویت کاربر انجام می‌دهد. مهیا کننده خدمات یک یا چند سرویس به کاربران درون سازمان وابسته ارائه می‌دهد. با این حال، این دسته هنوز به مکانیزم متمرکز متکی هستند. به منظور نزدیک شدن به کاربر با اجازه دادن به وی در انتخاب هویت‌های مورد استفاده برای برنامه‌های مختلف، هویت کاربر محور ارائه شده است.

۴-۳-مدل هویت کاربر محور

در این سیستم، کاربران می‌توانند از هر یک از هویت‌های خود برای هر برنامه استفاده کنند. این به کاربران اجازه می‌دهد تا شناسه‌ها و مدارک مربوط به ارائه دهندگان خدمات مختلف را در یک دستگاه سخت افزاری مقاوم در برابر دستکاری، که می‌تواند یک کارت هوشمند یا سایر دستگاه‌های شخصی قابل حمل باشد، ذخیره کنند[۲۴]. این مدل کاربر محور را می‌توان از مدل وابسته متمایز کرد زیرا تمرکز بیشتر کاربران روی متن در مقایسه با سازمان‌ها یا شرکت‌ها بیشتر است. پیشرفت عملی بیشتر این نوع سیستم، هویت مبتنی بر ویژگی است. این رویکرد با هدف حل مشکلات مربوط به امنیت و حریم خصوصی با استفاده از تکنیک اعتبار سنجی مبتنی بر ویژگی[۲۹] انجام می‌شود. فناوری اعتبار سنجی مبتنی بر ویژگی دیدگاه متفاوتی از هویت و مجوز دارد. ویژگی‌ها را می‌توان با موضوع داده (فرد) صادر و ذخیره کرد. علاوه بر این، فقط زیرمجموعه مربوط و غالباً غیر مشخص این ویژگی‌ها باید در متن یک نمونه خاص از تأیید و مجوز نشان داده شود. فرد نمی‌تواند مقادیر صفات خود را تغییر دهد. این اطمینان را به سیستم-هایی می‌دهد که از اعتبارسنجی مبتنی بر ویژگی برای تصمیم‌گیری در مورد دسترسی استفاده می‌کنند[۲۶].

[28] WS-Federation

[29] Attribute-Based-Credentials



(شکل ۶): مدل هویت کاربر محور[۲۴].

۵-۳-مدل مدیریت هویت ترکیبی

این رویکرد زمانی جایگزین می‌شود که هم رویکردهای سازمان وابسته و هم کاربر محور به راحتی با شرایط خاصی کنار نیایند. به عنوان مثال، در حالات مراقبت‌های بهداشتی، فرآیندهای تبادل و تفویض ویژگی نمی‌توانند کاملاً کاربر محور باشند، زیرا در موارد تصادفات حیاتی، کاربران نمی‌توانند رضایت خود را اعلام کنند. از طرف دیگر، مدل‌های سازمان وابسته نگرانی‌های مربوط به حریم خصوصی را ایجاد می‌کنند زیرا سوابق پزشکی ممکن است در دسترس هر نهادی در حلقه اعتماد باشد، حتی اگر موارد اضطراری وجود نداشته باشد. از این رو، مدل ترکیبی پیشنهادی به کاربران امکان می‌دهد تا از پرونده پزشکی خود اطمینان و ردیابی کنند، در حالی که ارائه دهندگان هویت اطلاعات کاربری را ذخیره و مدیریت می‌کنند[۲۵].

۴- بررسی و مقایسه روش ها

مدیریت هویت دیجیتال افراد را به هویت آنلاین مربوط به آن‌ها مرتبط می کند. این ویژگی از چندین ویژگی تشکیل شده است: نهادها، ویژگی‌ها، چرخه حیات، سیاست‌ها و فناوری‌ها. این ویژگی‌ها به یک راه حل دقیق و دقیق برای استقرار مدیریت هویت دیجیتال کمک می‌کنند. نقش هویت دیجیتال یکی از عناصر مهم امنیت اطلاعات است. این مبنای بسیاری از انواع کنترل دسترسی و ایجاد مسئولیت آنلاین است. بنابراین، با کاهش خطرات دسترسی غیرمجاز به اطلاعات شخصی، نقض داده‌ها و سرقت هویت، به محافظت از حریم خصوصی کمک می‌کند. راه حل‌های هویت دیجیتال را می‌توان در ۵ نوع مجزا، متمرکز، وابسته، کاربر محور و ترکیبی دسته‌بندی کرد. هر دسته دارای طرح‌های مختلف و گزینه‌های معماری است.

مدل مجزا ساده است، اما مشکلات زیادی دارد. با رشد انفجاری خدمات آنلاین، کاربران باید اطلاعات شناسایی بیشتری را مدیریت کنند. اعتبارنامه‌های بیشتری مانند نام کاربری و کلمه عبور باید به درستی توسط کاربران مدیریت شود. ترس از فراموش کردن اعتبارنامه‌ها به ویژه رمزعبور موانع زیادی را برای استفاده کاربران ایجاد می‌کند. هزینه بازیابی رمز عبور باعث افزایش هزینه سرویس خدمات دهنده می‌شود به ویژه اگر سطح امنیتی بالایی مورد نیاز باشد. سیستم‌های مدیریت هویت زیادی در مدل متمرکز پیاده‌سازی شده‌اند، مانند، گواهی کلید عمومی، سی‌ای‌اس، کربرس و غیره این مدل معایب زیادی دارد، ذخیره تمام هویت‌ها در یک ابزار پردازشگر داده‌ها مشکلات حفاظت از حریم خصوصی را به وجود می‌آورد. همچنین این مدل نمی‌تواند از کاربر دارای امتیازو دسترسی متقابل دامنه به خوبی پشتیبانی کند. هرچند در مدل متمرکز کاربران نمی‌توانند به سرویس‌های موجود در دامنه-های دیگر دسترسی یابند. اما جامع‌ترین و بهترین مدل از سیستم‌های مدیریت هویت دیجیتال، یعنی مدل وابسته، می‌تواند دامنه‌های زیادی را با یکدیگر یکپارچه کند و آن را تقریبا به یک دامنه منحصر به فرد جهانی تبدیل کند. مدل شناسایی وابسته در اصل گسترش مدیریت هویت به چندین دامنه امنیتی است. هدف این است که یک کاربر بتواند یکبار احراز هویت شود و سپس به برنامه‌ها و منابع چندین دامنه بتواند دسترسی پیدا کند. مدل وابسته می‌تواند به عنوان مجموعه‌ای از توافق نامه‌ها، استانداردها و تکنولوژی‌ها تعریف شود که گروهی از اس-پی‌ها را توانا می‌سازد تا هویت‌های کاربران را از دیگر اس‌پی‌ها تشخیص دهند. با این حال، این مدل هنوز به مکانیزم متمرکز متکی هستند. به منظور نزدیک شدن به کاربر با اجازه دادن به وی در انتخاب هویت‌های مورد استفاده برای برنامه‌های مختلف، هویت کاربر محور ارائه شده است. این مدل به‌ویژه بر روی سازمان کاربر و نه سازمان یا شرکت متمرکز است. آخرین نوع، مدیریت هویت ترکیبی است. این امر به دلیل شرایط خاص موجود در سیستم و رفتار نامتعارف بین هویت وابسته و کاربر محور، قابلیت اطمینان زیادی را فراهم می‌کند و نسبت به روش‌های دیگر ایمن‌تر و مطمئن‌تر است و لذا این مدل برای بانکداری دیجیتال پیشنهاد می‌گردد.

(جدول ۱): مزایا و معایب مدل‌های مدیریت هویت دیجیتال

مدل	مزایا	معایب
مجزا	✓سادگی ✓ذخیره‌سازی هویت و عملکردهای کاربران به وسیله یک سرور ✓تخصیص هویت منحصر به فرد، حذف، اصلاح، تصدیق هویت و اختیار دادن در مهیا کننده سرویس	✓مدیریت اطلاعات زیاد توسط کاربران ✓استفاده از اعتبارنامه‌های زیاد ✓مشکلات فراموشی رمز عبور و هزینه‌های بازیابی اعتبارنامه‌ها توسط کاربران
متمرکز	✓پیاده‌سازی سیستم‌های مدیریت هویت زیاد	✓مشکلات حفاظت از حریم خصوصی ناشی از ذخیره تمام هویت‌ها در یک ابزار پردازشگر داده‌ها ✓عدم پشتیبانی از کاربر دارای امتیاز و دسترسی متقابل دامنه
وابسته	✓یکپارچه کردن دامنه‌ها و تبدیل به یک دامنه منحصر به فرد جهانی ✓گسترش مدیریت هویت به چندین دامنه امنیتی ✓کافی بودن تنها یکبار احراز هویت ✓دسترسی به برنامه‌ها و منابع چندین دامنه	✓متکی بودن به مکانیزم متمرکز
کاربرمحور	✓نزدیک شدن به کاربر با اجازه دادن به وی در انتخاب هویت-های مورد استفاده برای برنامه-های مختلف	✓تمرکز بر روی سازمان کاربر و نه سازمان یا شرکت
ترکیبی	✓قابلیت اطمینان بالا ✓ایمن‌تر و مطمئن‌تر	-

۵- نتیجه گیری

بانکداری دیجیتال به عنوان بانکداری آینده، راهکاری برای ایجاد تحول دیجیتال در صنعت بانکداری است. یکی از چالش‌های بانکداری دیجیتال، کسب یا حفظ اعتماد مشتریان است. به منظور پذیرش گسترده بانکداری دیجیتال توسط مشتریان، اعتماد، پیش‌نیاز اصلی است؛ مشتریان باید مطمئن باشند که هویت آنها ربوده نخواهد شد.موضوع «هویت»، یکی از موضوعات مهم و مطرح در این فضا (فضای مجازی) است که با عنوان «هویت دیجیتال» مطرح می‌شود. مشکلی فعلی این است که کاربر با حوزه‌های مختلف ارائه خدمت مواجه است. بنابراین کاربر در هر حوزه‌ی خدماتی از جمله بانکداری دیجیتال، باید هویت ویژه آن حوزه را داشته باشد و از روش خاص احراز هویت آن حوزه تبعیت کند. در جهت حل مشکل هویت‌های متعدد کاربران، سیستم‌های مدیریت هویت دیجیتال پیشنهاد شده است. در این مقاله به معرفی روش‌های مختلف مدیریت هویت دیجیتال در سیستم بانکداری پرداختیم و مزایا و معایب این روش‌ها را مطرح کردیم.

۶ – مراجع

[۱]خدیوی کاشانی، م.، و دوستاری، م. ع. (۱۳۹۵). بررسی روند تکاملی حریم خصوصی و امنیت در سامانه‌های مدیریت هویت، ۵ ۱۵-۳۴

[۲]سلامتی طبا، س.، بیگی، م.، و اکبری، ع. (۱۳۹۶). بانکداری دیجیتالی، انقلابی در صنعت بانکداری. هفتمین همایش سالانه بانکداری الکترونیک و نظام¬های پرداخت. صص ۱-۱۹.

[3]Larsson, A., & Viitaoja, Y. (2017). Building customer loyalty in digital banking. International Journal of Bank Marketing

[4]Marc Andreas Barisch "Design and Evaluation of a System to Extend Identity Management to Multiple Devices" PhD diss., der Universität Stuttgart zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.) genehmigte Abhandlung, 2012

[5]Vial, G. (2019). Underst&ing digital transformation: A review & a research agenda. The Journal of Strategic Information Systems, 28(2), 118-144.

[6]Yang, X., & Li, W. (2020). A Zero-Knowledge-Proof-Based Digital Identity Management Scheme in Blockchain. Computers & Security, 102050

[7]Cross, D. B., Hallin, P. J., Jones, T. C., & Thomlinson, M. W. (2019). Digital Identity Management. Google Patents

[8]Tajbakhsh, M., Homayounvala, E., & Shokouhyar, S. (2017). Forensically ready digital identity management systems, issues of digital identity life cycle & context of usage. International Journal of Electronic Security & Digital Forensics, 9(1), 62-83.

[9]Jsang, and S. Pope, "User centric identity management," In Australian Computer Emergency Response Team Conference, Royal Pines Resort, Australia. 2005

[10]Miyata, Y. Koga, P. Madsen, and S. Adachi, "A Survey on Identity Management Protocols and Standards," IEICE - Transactions on Information and Systems, vol E89-D, pp. 112-123, January 2006

[11]Piran. Digital Iden-tity: An Introduction. Dec. 2014. url: http://piranpartners. com/wp-

content/uploads/2014/12/An-Introduction-to-Digital-Identity. Pdf

[12] Smedinghoff, Thomas J. "Introduction to Online Identity Management" (2011).

[13] Oecd. "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers". 186 (2011). url: http://EconPapers.repec.org/RePEc:oec:stiaab:186-en

[14] Halim, Roohul, Shaharyar, Syed Atif, and Vapen, A. "Digital Identity Management" (2009).

[15] Cao, Y., & Yang, L. (2010). A survey of identity management technology, in Information Theory & Information Security (ICITIS), IEEE International Conference on, December 2010, pp. 282 –293.

[16] Eran Hammer-Lahav, "Introducing OAuth 2.2," 15 May 2010.

[17] Malik, H. Anwar, and M. A. Shibli. Federated identity management (FIM): Challenges and opportunities. In 2015 Conference on Information As-surance and Cyber Security (CIACS), pages 25–82, Dec 2015

[18] Maryline Laurent, uciel fragoso, jose incera. "Federated Identity Management" International Conference on Availability, Reliability and Security (ARES 29.), Fukuoka, Japan, 2006 Marc Andreas Barisch

[19] Tobias Kolsch, Jan Zibuschka, and Kai Rannenberg, "Digital privacy. Chapter: Privacy and Identity Management Requirements: An Application Prototype Perspective," pages 235–249. Springer-Verlag, Berlin, Heidelberg, 2011

[20] Birrell and F. Schneider, "Federated identity management systems: A privacy-based characterization," Security Privacy, IEEE, vol. 11, no. 5, Sept 2013, pp. 36–48.

[21] Corella and K. Lewison, "Privacy postures of authentication technologies," in The Internet Identity Workshop, ser. IIW 2213, Mountain View, CA, 2213, [retrieved: September, 2015

[22] Alshehri, "Toward Effective Access Control Using Attributes and Pseudoroles," PhD diss., Rochester Institute of Technology, 2014.

[23] Kahate, "Cryptography and network security," Tata McGraw-Hill Education, ISBN:2-22-249483-5, 2013

[24] Jøsang, Audun and Pope, Simon. "User centric identity management". AusCERT Asia Pacific Information Technology Security Conference (2005), p. 77.

[25] Sánchez-Guerrero, Rosa et al. "An event driven hybrid identity management approach to privacy enhanced e-health". Sensors 12.5 (2019), pp. 6129–6154.

[26] Ahn, G.-J., & Ko, M. User-centric privacy management for identity management. In 2007,

محسن راجی مدرک دکتری خود را در رشته مهندسی کامپیوتر از دانشگاه صنعتی امیرکبیر، تهران، ایران، در سال ۱۳۹۴ دریافت کرد. وی از سال ۱۳۹۴ تاکنون در دانشکده مهندسی برق و کامپیوتر دانشگاه شیراز مشغول به کار است. علایق تحقیقاتی فعلی او شامل محاسبات قابل اطمینان، زیرساخت‌های سخت‌افزاری برای یادگیری عمیق، طراحی خودکار سیستم های دیجیتال و هوش مصنوعی Edge است.

نشانه رایانامه ایشان عبارتند از:

raji@shirazu.ac.ir

بابک میرزاخانی مدرک کارشناسی ارشد خود را در رشته مهندسی فناوری اطلاعات در سال ۱۳۹۹ از دانشکده آموزش‌های الکترونیکی دانشگاه شیراز اخذ کرده است. زمینه پژوهشی مورد علاقه ایشان عبارتند از: بانکداری اینترنتی، امنیت در سیستم‌های فناوری اطلاعات و هویت دیجیتال می باشد.

نشانه رایانامه ایشان عبارتند از:

bmirzakhani@shirazu.ac.ir

روش ارجاع به مقاله : م. راجی، ب. میرزاخانی. مروری بر مدل‌های دیریت هویت در بانکداری دیجیتال، دوفصلنامه محاسبات و سامانه های توزیع شده سال ۵، شماره ۱، شماره پیاپی ۹، صفحه ۶۴ تا ۷۳، سال ۱۴۰۱

How to cite: Mohsen Raji, Babak Mirzakhani. A Suvery on Digital Identitiy Management in Digital Banking, Journal of Distributed Computing and Systems(JDCS), Vol 5, Issue1, Page 64-73. 2022.