بررسی روند تکاملی حریم خصوصی و امنیت در سامانه‌های مدیریت هویت

محمد خدیوی کاشانی[1] و محمد علی دوستاری[2]

[1] کارشناسی ارشد، دانشگاه شاهد تهران، وزارت علوم و فناوری اطلاعات، تهران، ایران
m.khadivi@yahoo.com

[2] استادیار، عضو هیئت علمی دانشگاه شاهد تهران، وزارت علوم و فناوری اطلاعات، تهران، ایران
Doostari@shahed.ac.ir

چکیده

سامانهٔ مدیریت هویت (IDM) 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. در سامانه مدیریت هویت با توجه به ذخیره‌شدن ویژگی‌های هویتی کاربر در تأمین‌کنندهٔ هویت، کاربران کنترل فیزیکی و سنتی خود را بر روی اطلاعات شخصی هویتی خود از دست خواهند داد، و از طرف دیگر ویژگی‌ها و صفات کاربر در معرض حملات بیشتری از سوی قسمت‌های داخل سامانه و نفوذگران خارجی است؛ لذا برای اطمینان از کنترل حریم خصوصی کاربر در حفظ و آگاهی از انتشار اطلاعات هویتی خود ، ارائه سازوکارهای امنیتی در حوزهٔ حفظ حریم خصوصی، امری ضروری است. سازوکارهای فعلی، نتوانسته اعتماد کاربران را از حفظ امنیت و حریم خصوصی مرتبط با اطلاعات هویتی‌شان، برآورده سازد. طرح های ارائه‌شده در این زمینه، مداخله و درگیری کاربر را در حین تعاملات سامانه زیاد می‌کند و کاربر بایستی به عنوان نقش واسط عمل کند. از مشکلات طرح‌های ارائه‌شده، بار محاسباتی بالا بر روی یک بخش سامانه است. در این مقاله روند تکاملی کنترل حفظ حریم خصوصی و آگاهی کاربر در جهت حل مشکلات بررسی و تحلیل شده است.

واژگان کلیدی: سامانه‌های مدیریت هویت، هویت دیجیتال، امنیت، حریم خصوصی، سیاست حریم خصوصی

۱- مقدمه

در حوزه اینترنت، افراد نیاز دارند بتوانند خدمات مبتنی بر فناوری اطلاعات را در همه‌جا و در هر زمان دریافت کنند. در فضای مجازی کاربر با حوزه‌های[1] مختلف ارائهٔ خدمت مواجه است. مانند خدمات بانکی، سلامت، آموزشی، دولتی و غیره. هر حوزه به‌صورت کاملاً جزیره‌ای و مستقل به تعریف هویت خاص آن حوزه[2] و روش خاصی برای احراز هویت کاربر می‌پردازد. ازجمله این روش‌ها می‌توان به گذرواژه، توکن، بیومتریک و رمز یک‌بارمصرف اشاره کرد؛ بنابراین کاربر در هر حوزه خدماتی باید هویت ویژه آن حوزه را داشته باشد و از روش خاص احراز هویت آن حوزه تبعیت کند. از سوی دیگر در اغلب روش‌های متداول کنونی، تمرکز بر شناسایی و احراز هویت کاربر است؛ درحالی‌که شناسایی و احراز هویت خدمتگزار نیز به همان درجه و حتی بیشتر اهمیت دارد؛ بنابراین کاربر از طرفی سهولت لازم را ندارد و از سوی دیگر به‌دلیل عدم وجود سازوکار یکپارچه‌ای برای شناسایی خدمت‌گزار، همواره با تردید به انتخاب ارائه‌دهندهٔ خدمت می‌پردازد. افزون بر این، همواره نگرانی از حفظ امنیت داده‌ها و البته رعایت حریم خصوصی وجود دارد. از دیدگاه خدمت‌گزار نیز نگرانی از جعل و سرقت هویت کاربر مطرح است و به‌خصوص انجام این امر در سطح وسیع، خسارات زیادی به خدمت‌گزاران و همچنین کاربران وارد می‌کند. سازوکارهای فعلی ارائه‌شده، نتوانسته اعتماد کاربران را از حفظ امنیت و حریم خصوصی مرتبط با اطلاعات هویتی‌شان، برآورده سازد. همچنین طرح‌های ارائه‌شده در این زمینه، مداخله و درگیری کاربر را در حین تعاملات سامانه زیاد می‌کند و کاربر بایستی به‌عنوان نقش واسط عمل کند. از

[1] Domain

[2] Domain Specific ID

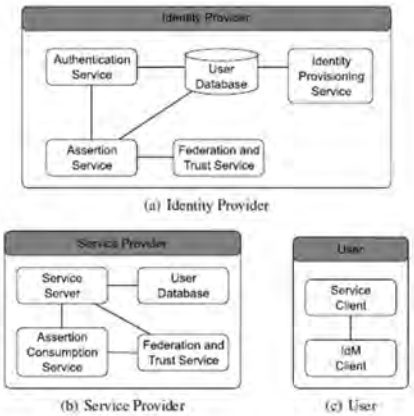
مشکلات طرح‌های ارائه‌شده بار محاسباتی بالا بر روی یک بخش سامانه است و درگیری زیاد کاربر در حین تعاملات سامانه است. در این مقاله روند تکاملی کنترل حفظ حریم خصوصی و آگاهی کاربر در جهت حل مشکلات بررسی و تحلیل شده است.

۲- مفاهیم و مدل‌های اساسی در سامانه مدیریت هویت

مدیریت هویت یک روش متمرکز و خودکار است که دسترسی به منابع را برای کارمندان و افراد مجاز در شرکت فراهم می‌کند که با هدف افزایش امنیت و بهره‌وری و همچنین کاهش هزینه‌ها، زمان و وظایف تکراری صورت می‌گیرد. درواقع مدیریت هویت وظیفه کنترل اطلاعات کاربران را برعهده دارد، که این اطلاعات شامل اطلاعات مورد نیاز برای احراز هویت یک کاربر، و اطلاعاتی، عملیات و کارهایی را که کاربران مجاز به انجام آن هستند، توصیف می‌کند.

۲-۱- مفاهیم اساسی

قبل از اینکه مدل‌ها و الگوهای مدیریت هویت را بررسی کنیم، باید مفاهیم و عناصر کلیدی موجود در آن را بشناسیم. در شکل (۱) نمایی از معماری مرجع IDM آورده شده است[3].



(شکل-۱): معماری مرجع IDM [3]

- ✓ مهیاکنندهٔ خدمات(SP): این مؤلفه در مدیریت هویت وظیفهٔ مهیاکردن خدمات را برای کاربر دارد. افراد می‌توانند از خدمات متفاوتی مانند e-bank و e-shopping استفاده کنند. واحد خدمات سرور[1]، خدمات موجود و در دسترس را برای خدمات فراهم می‌کند. خدمات تأیید هویت مورد ادعای کاربر[2]، هویت ادعایی کاربر را جهت احراز هویت به‌وسیله اعتماد به یک IDP ممکن می‌سازد. SP به IDP با توجه به رابطه اعتمادی که از قبل ایجاد شده و موجود است، اعتماد می‌کند. این روال توسط خدمات اعتماد و فدرال، صورت می‌پذیرد.
- ✓ مهیاکنندهٔ هویت(IDP): این مؤلفه به‌عنوان هسته سامانه‌های مدیریت هویت شناخته می‌شوند. مهیاکنندهٔ هویت سطوح امنیتی متفاوتی را به کاربران مختلف ارائه می‌کند. برای مثال یک کاربر عادی و یک مدیر باید سطوح اعتماد متفاوتی را در یک سازمان داشته باشند. IDP دارای دو وظیفه کلی است: ۱- پیاده‌سازی خدمات برای کاربران مانند ثبت نام کاربر، بررسی هویت کاربر و فضای هویت کاربران. ۲- دریافت درخواست‌های احراز هویت از کاربران و SPها. در IDP اعتبارسنجی کاربران بر عهده خدمات احراز هویت[3] است. IDP در پروتکل احراز هویت و ردوبدل‌کردن اطلاعات و تأیید صحت اطلاعات کاربر از پایگاه دادهٔ کاربر[4] استفاده می‌کند. پایگاه داده‌ای کاربر شامل فهرستی از هویت کاربران مانند: شناسه هویت، صفات و ویژگی‌های مرتبط با کاربر و متادیتاهایی[5] در مورد کاربر (به‌عنوان مثال: تاریخ قبلی استفاده از هویت) است. خدمات تأمین هویت[6] ، پایگاه داده‌ای کاربر را پر می‌کند. پس از ایجاد هویت جدید، آن را وارد پایگاده دادهٔ کاربر می‌کند. بنابر این رابطه ایجادشده از قبل بین IDP و SP باعث محافظت در ردوبدل‌شدن اطلاعات می‌شود. این موضوع بر عهده خدمات اعتماد و فدرال[7] می‌شود. بر طبق رابطه اعتماد ایجادشده، SP اثبات هویت را با استفاده از سرویس ادعاکننده[8] درخواست می‌کند.
- ✓ کاربر(User). کاربران مشتریان مهیاکنندگان خدمات و مهیاکنندگان هویت هستند که می‌توانند یک سازمان عمومی، یک شخص، یک نهاد مجازی مانند نرم‌افزار یا غیره باشد.کاربر با هویت خود از SP خدمات می‌گیرد. کاربر احراز هویت خود را از IDP و به‌وسیله IDM Client می‌گیرد. پس از احراز هویت کاربر توسط IDP کاربر در موقعیت استفاده از خدمات قرار می‌گیرد.

[1] Service Server
[2] Assertion Consumption Service
[3] Authentication Service
[4] User Database
[5] meta-data
[6] Identity Provisioning Service
[7] Federation and Trust Service
[8] Assertion Service

مهیاکنندهٔ هویت(IDP) براساس عملکردشان به چهار نوع تقسیم می‌شوند[1] یک IDP می‌تواند به چهار روش برای کاربران هویت مشخص کند:

۱- Credential Identity Service
این نوع IDP برای احراز هویت کاربر از Credentialها (اعتبارنامه‌ها) به‌عنوان هویت کاربر استفاده می‌کند. نخستین و محبوب‌ترین Credential، X.509 است.

۲- Identifier identity service
Identifier نمایش کاربران است که می‌تواند شامل نام، رایانامه یا شماره ID-card تخصیص‌یافته به کاربر باشد.

۳- Attribute Identity Service
Attribute اطلاعاتی است که برای توصیف هویت کاربران می‌تواند استفاده شود. مانند نشانی، کد ملی، اطلاعات تماس و غیره.

۴- Pattern Identity Service
Pattern Identity به این معنی است که یک IDP از الگوها، شهرت، سوابق اعتمادی برای توصیف یا مشخص‌کردن هویت کاربران استفاده می‌کند. به‌عنوان مثال از مشخصات یک مدل حمله‌کننده می‌توانیم برای تشخیص حمله نفوذگر استفاده کنیم.

درواقع، اینکه از کدام Identity Service استفاده شود یا اینکه آیا نیاز به ترکیب دو یا چند خدمت است یا نه، به سطح امنیتی مورد نیاز برای IDM بستگی دارد. به‌عنوان مثال برای دسترسی به وب یا خدمات رایج دیگر Identifier identity service کافی است؛ اما برای خدمات سطح بالا مانند خدمات بانکداری الکترونیکی، credentialهای مناسب نیز مورد نیاز است.

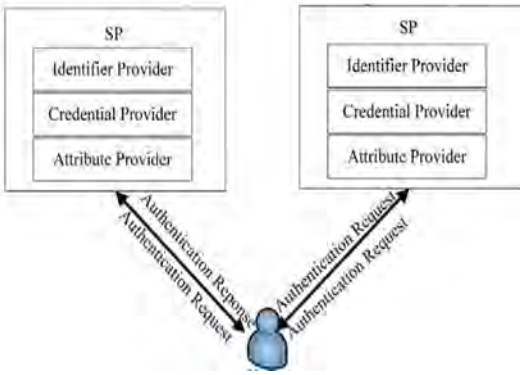
۲-۲- مدل‌های مدیریت هویت

مدل‌های مدیریت هویت به سه دسته، مدل isolated، مدل centralized و مدل federate دسته‌بندی می‌شوند [6]، [5]، [4].

۲-۲-۱- مدل isolated

در مدل isolated، واحدSP وظیفه فراهم‌کردن خدمت و فراهم‌کردن هویت را دارد به این معنی که تمام فضای ذخیره‌سازی هویت و عملکردهای کاربران توسط یک سرور صورت می‌گیرد. تخصیص هویت منحصربه‌فرد، حذف، اصلاح، تصدیق هویت و اختیاردادن در مهیاکننده خدمت پیاده‌سازی می‌شود. هر کاربر باید گواهی‌نامه‌های مجزا مانند کلمه عبور یا بیومتریک مرتبط با هویت داشته باشد. واحد SP به‌عنوان ارائه‌دهنده شناسه[1]، ارائه دهنده اعتبار[2] و ارائه‌دهنده صفات[3](ویژگی) عمل می‌کند. این مدل در شکل (۲) نشان داده شده است.

این مدل بسیار ساده است؛ اما مشکلات زیادی دارد. با رشد انفجاری خدمات برخط، کاربران باید اطلاعات شناسایی بیشتری را مدیریت کنند. اعتبارنامه‌های بیشتری مانند نام کاربری و کلمه عبور باید به‌درستی توسط کاربران مدیریت شود. ترس از فراموش‌کردن اعتبارنامه‌ها به‌ویژه رمز عبور موانع زیادی را برای استفاده کاربران ایجاد می‌کند. هزینه بازیابی رمز عبور باعث افزایش هزینه SP می‌شود؛ به‌ویژه اگر سطح امنیتی بالایی مورد نیاز باشد.



(شکل-۲): مدل isolated [1]

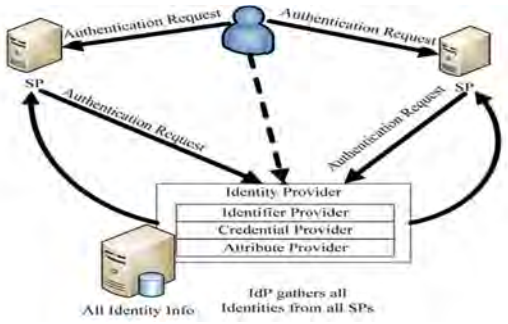
۲-۲-۲- مدل Centralized

مدل Centralized در یک مدل C/S[4] پیاده‌سازی می‌شود. فضای ذخیرهٔ هویت کاربران و تصدیق هویت کاربران هر دو در سمت سرور که مهیاکنندهٔ هویت (IDP) نام دارد، پیاده‌سازی می‌شود. برخلاف مدل isolated، این مدل عملکردهای SP و IDP را از هم جدا می‌کند. تمام هویت‌ها باید برای ذخیره‌سازی و دنبال‌کردن تصدیق هویت به مرکز IDP فرستاده شود. شکل (۳) مدل Centralized را نشان می‌دهد؛ تمامی هویت‌های موجود در هر SP در IDP ذخیره می‌شود، زمانی که SP نیاز به تصدیق هویت یک کاربر دارد، اطلاعات کاربر را برای اتمام فرآیند به IDP ارسال می‌کند.

سامانه‌های مدیریت هویت زیادی مانند PKI، Kerberos، CAS و ... در مدل Centralized پیاده‌سازی

[1] identifier provider
[2] credential provider
[3] attribute provider
[4] client/server

شده‌اند. این مدل معایب زیادی دارد؛ ذخیره تمام هویت‌ها در یک IDP مشکلات حفاظت از حریم خصوصی را به‌وجود می‌آورد. همچنین این مدل نمی‌تواند از user privilege delegation و cross domain access به‌خوبی پشتیبانی کند.



(شکل-۳): مدل Centralized [1]

۲-۲-۳-مدل Federated

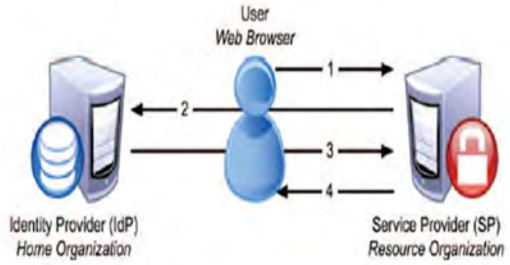
در مدل Centralized کاربران نمی‌توانند به خدمات موجود در دامنه‌های دیگر دسترسی یابند. مدل Federated دامنه‌های زیادی را با یکدیگر یکپارچه و آن را به‌طورتقریبی به یک دامنهٔ منحصربه‌فرد جهانی تبدیل می‌کند.

Identity Federation در اصل گسترش مدیریت هویت به چندین دامنه امنیتی است. هدف این است که یک کاربر بتواند یک بار احراز هویت شود و سپس به برنامه‌ها و منابع چندین دامنه بتواند دسترسی پیدا کند [9].

مدل Federated می‌تواند به‌عنوان مجموعه‌ای از توافق‌نامه‌ها، استانداردها و فناوری‌ها تعریف شود که گروهی از SPها را توانا می‌سازد تا هویت‌های کاربران را از دیگر SPها تشخیص دهند. پروتکل‌ها که شامل سیاست‌ها و استانداردها و فناوری‌ها هستند، بین SPها ایجاد می‌شوند؛ به‌طوری‌که هویت‌ها از دامنه‌های هویتی متفاوت در بین همه دامنه‌ها می‌تواند شناخته شود.

FIA شامل گروهی از سازمان‌هاست که به‌منظور تبادل اطلاعات شناسهٔ دیجیتال و حفظ جامعیت و محرمانگی اطلاعات شخصی کاربران ارتباطات قابل اعتمادی را میان یکدیگر ایجاد کرده‌اند. FIA مهیاکنندگان شناسه و مهیاکنندگان خدمات را در یک ساختار اعتماد و به‌وسیلهٔ کانال‌های ارتباطی امن‌شده و قراردادهای تجاری درگیر می سازد. IDP اطلاعات شناسه کاربران را مدیریت می‌کند و فرآیند احراز شناسه به‌منظور معتبرساختن شناسه انجام می‌دهد. FIA می‌تواند شامل یک IDP (مدل Centralized) یا چندین IDP (مدل Distributed) باشد. مزیت مدل Centralized این است که اطلاعات شناسه منتشر نمی‌شود و حفظ محرمانگی و جامعیت اطلاعات آسان‌تر است؛ اما می‌تواند باعث ایجاد Bottleneck و یک نقطه خرابی شود. در مدل Distributed، فرآیند احراز شناسه در هر IDP می‌تواند صورت گیرد که باعث ایجاد انعطاف و تعادل بار می‌شود. اگرچه این روش به سازوکارهای امن و پیچیده‌تری برای تبادلات نیاز دارد، ولی اطلاعات شناسه را مدیریت می‌کند و دارای مشکل یک نقطه خرابی نیست.

در شکل (۴) یک طرح ساده از مدیریت هویت فدرال را بیان می‌کنیم. اگر یک کاربر از یک سازمان بخواهد از منابع سازمان دیگر استفاده کند، او ممکن است در مدیریت هویت فدرال از همان شناسه‌ای که در حوزه سازمانی خودش استفاده می‌کند، استفاده کند.



(شکل-۴): طرح ساده مورد استفاده در مدیریت هویت فدرال [7]

در این طرح در ابتدا کاربر درخواست خود را در جهت دسترسی به سرویس در دامنه سازمانی دیگر، درخواست می‌دهد (۱). SP در این زمان با IDP در جهت احراز هویت کاربر، ارتباط برقرار می کند (۲). در این زمان IDP، نشانه امنیتی احراز هویت را به SP اعلام می کند (۳). در آخرین گام(۴)، کاربر اجازه دسترسی به خدمات را می‌گیرد [7].

۲-۳- عملکردهای اصلی سامانه مدیریت هویت

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

- ✓ Single-sign-on: SSO به کاربران اجازه می‌دهد که با یک IDP احراز شناسه شوند و سپس بدون احراز شناسه مجدد به خدمات مهیاشده به‌وسیله چندین مهیاکننده خدمات دسترسی داشته باشند.
- ✓ Attribute exchange: یک بار که کاربر به‌وسیله IDP احراز شناسه شد، SP برای مهیاکردن خدمات

شخصی‌سازی‌شده به صفات[1] بیشتری نیاز دارد. بنابراین FIA باید تبادل صفات را بین IDP و SP آسان کند.

- ✓ حفظ اطلاعات شخصی: محرمانگی و جامعیت اطلاعات شخصی کاربران باید به روشی که ارائه صفات شناسه به‌وسیله کاربر کنترل شود، تضمین شود.
- ✓ مدیریت چرخه عمر شناسه: چه مدل Centralized باشد و چه Distributed، ایجاد، نگه‌داری و حذف شناسه دیجیتال باید ساده و هزینه اجرایی بالایی نداشته باشد.
- ✓ معماری استانداردشده: FIA باید برای ادغام راحت SPها و IDPهای جدید بر اساس استانداردها بنا شده باشد.

۳- انواع سامانه‌های مدیریت هویت

۳-۱-۱- معرفی و مقایسه سامانه‌های مدیریت هویت

در این بخش به معرفی شش سامانه مدیریت هویت که دارای موقعیت بالا و مشهورتر در بین سامانه‌های مدیریت هویت هستند، پرداخته شده است.

سامانهٔ مدیریت هویت Windows CardSpace

مایکروسافت پیش‌بینی کرده است که یکابرسامانهٔ هویتی[2](سامانه‌ای از سامانه‌ها) که بتواند تمام فناوری‌های موجود را در روشی استاندارد جا دهد می‌تواند راه حل بهتری را برای کاهش تعداد زیادی از مشکلات مدیریت هویت مهیا کند [13]. متأسفانه مایکروسافت پروژه CardSpace خود را قطع کرده است. یک مقدمه کوتاه به ویندوز CardSpace را می توان در یافت کرد [14].

سامانهٔ مدیریت هویت OpenID

OpenID یک سامانه مدیریتی غیرمتمرکز برای هویت دیجیتال کاربرمحور است. در سال ۲۰۰۵ نخستین نسخه از پروتکل OpenID گسترش یافت و مورد توجه زیاد جامعه توسعه اینترنت و شرکت‌های اینترنتی قرار گرفته است؛ که راه حل SSO را برای سرویس‌های وب در بستر اینترنت مهیا می‌کند [14] و امروزه به‌وسیله تعداد زیادی از مهیاکنندگان سرویس وب مانند AOL, BBC, Google, IBM, Yahoo و غیره استفاده می‌شود[16]، [17]. OpenID اجازه می‌دهد که کاربران اینترنت بتوانند به تعداد زیادی وب‌سایت اینترنت بر اساس یک هویت دیجیتال متصل شوند و نیاز به نام کاربری و گذرواژه‌های متفاوت را برای هر سایت حذف می‌کند. هدف اصلی آن حل مشکل single sign on برای خدمات وب است.

[1] attribute
[2] Identity Metasystem

OpenID یکی از گسترده‌ترین سامانه‌های مدیریت هویت است[18].

سامانه مدیریت هویت Shibboleth

Shibboleth یک سامانه مدیریت هویت فدرال (Federated) و متن باز است که به‌وسیله کنسرسیوم اینترنت۲ به‌وجود آمده است و اساس آن استاندارد SAML[3] است [19]. این استاندارد به سایت‌ها اجازه می‌دهد تا برای دسترسی افراد به منابع برخط محافظت شده و حفظ حریم خصوصی، برای authorization دادن تصمیمات آگاهانه بگیرند. این سامانه یکی از سامانه‌های مدیریت هویت فدرال است که به‌طور گسترده و به‌ویژه در محیط دانشگاهی پذیرفته شده است [20].

هدف این پروتکل آسان‌کردن ارتباط و دسترسی به منابع محافظت‌شده در میان مؤسسات، بدون استفاده از حساب‌های موقت یا خارجی است. برنامه‌هایی که از این راه‌حل سود می‌برند به اطلاعات پایگاه‌داده کتاب‌خانه‌ای دسترسی دارند. مانند دوره‌های آموزش از راه دور، برنامه‌های همکاری برای توسعه پروژه و ... .

در Shibboleth اطلاعات مربوط به شناسه‌های دیجیتال کاربران به‌وسیله مؤسسه که متعلق به آن است، مدیریت می‌شود. زمانی‌که یک کاربر نیازمند دسترسی به منابع موجود در مؤسسه دیگر است، صفات شناسه همراه با درخواست ارسال می‌شود؛ ولی فقط صفاتی که درقبل با اشتراک آنها موافقت شده است، فرستاده می‌شوند. این صفات سرانجام برای تصمیم‌گیری در مورد پذیرش یا عدم پذیرش درخواست دسترسی کاربر باتوجه به سیاست کنترل دسترسی محلی مورد استفاده قرار می‌گیرد. بنابراین نیاز به فرستادن شناسه اصلی کاربر نیست و بنابراین حریم خصوصی اطلاعات کاربران ممکن است در Shibboleth حفظ شود.

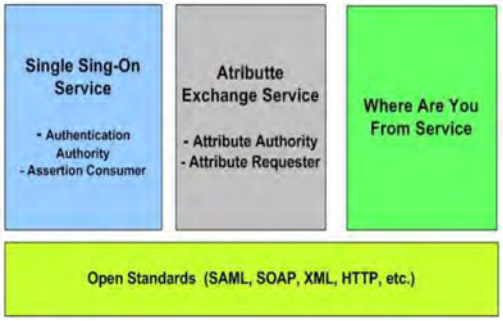
معماری

معماری این روش نیز بر پایه استانداردهای باز مانند Http، XML، SOAP و SAML ایجاد شده است. شکل (۵) خدمات تشکیل‌دهنده معماری را نشان می‌دهد.

Single sign-On: SSO شروع‌کننده فرآیند احراز شناسه است. این ماژول مشخص نمی‌کند که چطور احراز شناسه کاربر باید انجام شود؛ اما این کار با هماهنگی با سامانه احراز

[3] Security Assertion Markup Language

شـــنـاســـه محلی کار می‌کند. این ســـرویس از دو مؤلفه Assertion Consumer و Authentication Authority برای تبادل اظهارات احراز شـناسه به‌منظور تولید محتوای امن که در آن کاربران بتوانند به منابع محافظت‌شـده دسـترسی پیدا کنند، استفاده می‌کند.



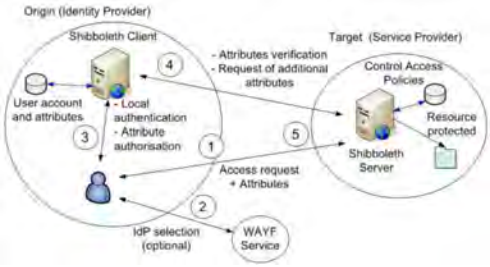
(شکل-۵): معماری Shibboleth [2]

Attribute Exchange Service: این سرویس صفات را به SP ارسال می‌کند، که سیاست کنترل دسترسی را به‌کار می‌گیرد که مشـخص کند آیا اجازهٔ دسـترسی به منابع محافظت‌شده داده شـده اسـت یا خیر. دو عملکرد برای انجام این سرویس تعریف شـده‌اند: Attribute Authority و Attribute Requet. صفات فقط درصورتی‌که سیاست محلی به‌وسیله IDP تعریف شده باشد و کاربر اجازه دسترسی دهد، افشا می‌شوند.

Where Are You From (WAYF): WAYF یک ســرویس دلخواه اسـت که SP را قادر می‌سـازد که IDP مشـترکان را محل‌یابی کند. WAYF مانند یک دایرکتوری اسـت که برای انتخاب IDP که عملیات احراز شـنـاســه را انجام می‌دهد، با کاربر تعامل می کند [2].

عناصر و عملکردها

Shibboleth شـامل سه عنصر است: origin (منبع، منشأ) که Identity Provider اســت؛ Target که Service Provider می‌باشـد و WAYF که دلخواه اسـت. Origin حسـاب‌های کـاربران مـانـنـد Credential و attribute را نگـه می‌دارد و عملیات احراز شـنـاســه را انجام می‌دهد. به‌علاوه، این مؤلفه احراز شـنـاسـه یا ادعای احراز شـنـاسـه را برای هدف، تولید می‌کند. Target منابع محافظت‌شـده را تولید و دسترسی آن را بر اسـاس ادعای شـناسه منتشرشده به‌وسیله هدف کنترل می‌کند. سرویس WAYF اگر پیاده‌سازی شود، به کاربر اجازه می‌دهد که Origin مسـئول فرآیند احراز شناسه را شناسایی کنـد. شـکـل (۶) ارتبـاط و عملکردهـای بین مؤلفـه‌هـای Shibboleth را نشان می‌دهد.



(شکل-۶): عناصر Shibboleth [2]

زمانی که کاربر نیاز دارد به منابع محافظت‌شـده که در خارج از سـازمان قرار دارد، دسـترسـی یابد (۱)، target از کاربر می‌خواهد خودش را احراز شناسه کند. به‌طورمعمول، Origin یا IDP سـازمانی است که کاربر متعلق به آن است، به‌صورت دلخواه خدمات WAYF می‌تواند اسـتفاده شـود که Origin انتخاب شـود (۲)، زمانی که کاربر احراز شـناسـه شـد (۳)، Origin صـفاتی را که به Target نمایش داده شـده اسـت، نشـان می‌دهد. این صـفات ازآنجایی که به‌وسـیله یک کانال ارتباطی امن تحویل داده می‌شـوند، اثبات شـده‌اند که معتبر هسـتند (۴). زمانی که به‌وسـیله سـیاسـت کنترل دسترسی Authorization با موفقیت انجام می‌شـود، اجازه دسترسی به منابع صـادر می‌شـود (۵). در برخی موارد، ممکن اسـت به‌منظور مهیاکردن خدمات صفات اضافی نیز مورد نیاز باشد. این صـفات فقط بعد از دریافت اجازه کاربر صادر می‌شود. در معماری Shibboleth، حریم خصوصی اطلاعات کاربران بسیار مهم است.

همان طور که مشـخص اسـت، اطلاعات شناسه کاربر فقط در origin ذخیره می‌شـود؛ اما بعضـی از صـفات ممکن اسـت به Target منتقل شود که به آنها برای اجرای سیاست کنترل دسترسی نیاز دارد. بنابراین، یک قرارداد شامل صفات و منابع به اشـتراک گذاشـته شده باید بین Origin و Target وجود داشته باشد [2].

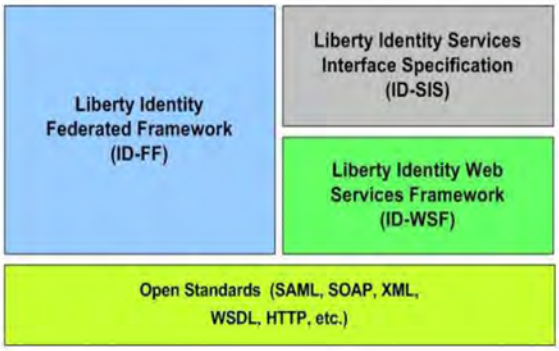
سامانهٔ مدیریت هویت Liberty Alliance (LA)

LA در سـال ۲۰۰۱ تأسـیس شـده اسـت و هم‌اکنون با نام ابتکار Kantara شناخته می‌شود، کنسرسیومی از سازمان‌های تجاری و غیر تجاری اسـت که هدف آن گسـترش و ایجاد اسـتانداردهای سـازگار و باز برای مدیریت هویت فدرال است [28]. Kantara سـیر تکاملی Liberty Alliance است، که در

سال ۲۰۰۸ به‌منظور ایجاد یک نقطه کانونی قدرتمند برای همکاری در جامعه هویت تأسیس شد. هدف این پروژه کار بر روی مسائل کلیدی مانند تضمین هویت، سیاست، حریم خصوصی، گسترش نرم‌افزار و قابلیت همکاری بود [22].

Liberty Alliance گروهی متشکل از دویست شرکت از قسمت‌های مختلف است که در سال ۲۰۰۱ با هدف ایجاد چارچوب فنی، کسب و کار و سیاست برای پیاده‌سازی معماری شناسهٔ یکپارچه راه‌اندازی شده است.

Alliance راهنمای تجاری را برای کمک به شرکت‌ها در جهت هم‌گراشدن به سمت قرارداد تجاری گسترش داده است و از یک معماری یکپارچه که تمرکز آن بر روی امکان‌پذیر بودن، ریسک و اعتماد متقابل است، پیروی می‌کند. معماری Liberty Alliance چارچوبی است که شامل مجموعه‌ای از ویژگی‌های فنی و تجاری برای ایجاد یک معماری مدیریت شناسهٔ یکپارچه است. این معماری در شکل (۷) نشان داده شده که شامل سه ماژول است که بر روی استانداردهای باز فنی توسعه‌داده‌شده به‌وسیله OASIS، W3C و IETF عمل می‌کند.



(شکل-۷): معماری Liberty Alliance [3]

ID-FF (Identity – Federation Framework): این ماژول بخش اساسی و اصلی معماری را تشکیل می‌دهد، تعریف مجموعه ای از عملکردها مانند: اتصال حساب‌ها (Identity federation)، مدیریت جلسه (Single sign on and Single sign out)، وابستگی (ظرفیت انتخاب IdP برای شناسه یکپارچه).

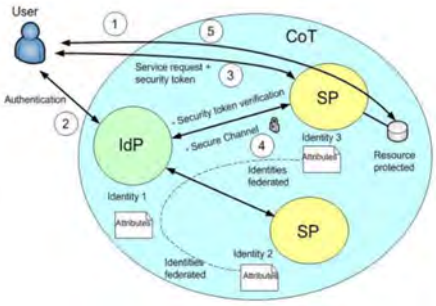
ID-WSF (Identity – Web Services Framework): چارچوبی را برای خدمات وب به‌منظور ایجاد، یافتن و درخواست سرویس‌های خدمات مشخص می‌کند. ID-WSF همچنین بر روی استانداردهای پروتکل باز عمل می‌کند و از عملکردهای زیر پشتیبانی می‌کند: به‌اشتراک‌گذاری صفات، کشف خدمات، سازوکارهای امنیتی برای انتقال پیام و ...

ID-SIS (Identity – Services Interface Specification): برای ایجاد خدمات امنیتی سطح بالا (خدمات عملی) براساس چارچوب ID-WSF ایجاد می‌شود. مثالی از خدمات ID-SIS شامل: درخواست اطلاعات شخصی، خدمات مکان جغرافیایی (geo-location)، خدمات دایرکتوری و ...

عناصر و عملکردها

Liberty Alliance یک دایره اعتماد (CoT[1]) تعریف می‌کند؛ به‌طوری‌که SPها و IDPها به‌منظور حمایت از تعاملات امن در میان اعضای CoT پایبند به امضای یک قرارداد تجاری هستند.

همان‌طور که در شکل (۸) نشان داده شده است، هر عضو CoT ممکن است با شناسه‌های مجزا شناخته شود. همه شناسه‌ها به روشی یکپارچه شده‌اند که فرآیند احراز شناسه بتواند به‌وسیله هر عضو CoT انجام شود. بدین صورت گفته می‌شود Liberty Alliance توزیع شده است؛ زیرا هر IDP در CoT ممکن است یک کاربر را احراز شناسه کند.



(شکل-۸): دایره اعتماد معماری Liberty Alliance [2]

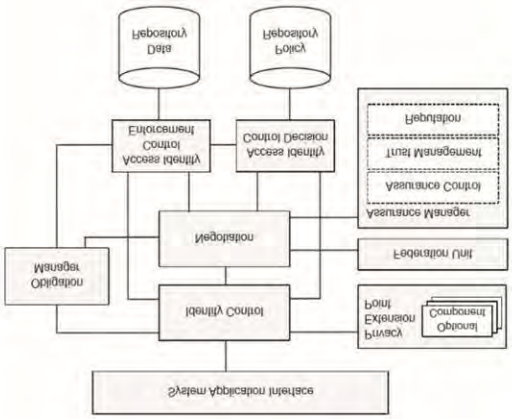
برای کاربری که می‌خواهد به خدماتی در CoT دسترسی پیدا کند(۱)، SP از کاربر می‌خواهد تا یک IDP را انتخاب کند، و کاربر به این IDP برای احراز شناسه‌شدن نیازمند است (۲)، IDP کاربر را احراز شناسه می‌کند و یک توکن امنیتی را به همراه اطلاعات شناسه برایش اختصاص می‌دهد که در گام (۳) برای SP فرستاده می‌شود. توکن امنیتی بین SP و IDP در یک کانال ارتباطی امن بررسی می‌شود(۴)، و در صورت تأیید اعتبار اجازه دسترسی به خدمات داده می‌شود. اگر مهیاکننده خدمات صفات اضافی را درخواست

[1] Circle of Trust

کند، آنها به‌وسیله یک کانال امن از IDP درخواست داده می‌شوند. مدل CoT نیازمند به این است که SP به IDP اعتماد کند. بنابراین، به یک زیرساخت ارتباطی امن نیازمند است که جامعیت، محرمانگی و عدم‌انکار پیام ارسالی را تضمین کند. سازوکار امنیتی شرکت‌کننده در مشخصات Liberty Alliance شامل امنیت کانال ارتباطی و همچنین امنیت پیام تبادلی است. ارتباط امن می‌تواند به‌وسیله پروتکل های رایج کنونی مانند TLS، SSL و IPSec پیاده‌سازی شود. این پروتکل‌ها سازوکارهای احراز شناسه را بین SP، IDP و کاربران قبل از تبادل پیام شروع می‌کند[2].

معماری PRIME[1]

پروژه PRIME با حمایت مالی اتحادیه اروپا و دولت سویس در مارس سال ۲۰۰۴ ایجاد شد و هدف آن انجام پژوهش‌هایی در این زمینه بود که چطور مسائل مختلف فنی و غیر فنی از فناوری‌های حریم خصوصی را با سناریوهای مدیریت هویت یکپارچه سازد و سپس نمونه‌هایی از سامانه‌های مدیریت هویت که باعث افزایش حریم خصوصی می‌شود، طراحی کند و گسترش دهد و نتیجه آن ایجاد معماری PRIME بود که تمرکز اصلی آن بر حفظ حریم خصوصی است [23]. هدف این پروژه گسترش یک نمونهٔ کاری برای بهبود حریم خصوصی سامانه Idm به‌وسیله استفاده از هویت‌های جزئی است. ایده اصلی PRIME سازگاری با فناوری‌های پیش رو در شبکه‌های آینده[2] است [25]. معماری PRIME در شکل (۹) آورده شده است.



(شکل-۹): معماری PRIME[۲۴]

شکل (۹) مرور کلی مؤلفه‌ها در معماری PRIMEرا نشان می‌دهد. در مجموعه‌ای از مخازن داده[3] هر یک از داده و ابرداده‌های ذخیره‌شده توسط بخشی(که این داده‌ها در آن است) یا هربخش دیگر نگه‌داری می‌شود. یک سامانه کاربرمحور[4] یک مخزن داده واحد برای ذخیرهٔ داده‌های خودش به‌صورت رمزنگاری‌شده و یک enterprise که تعدادی مخازن داده که برای مدیریت داده مورد نیاز هست، خواهد داشت. مخازن داده می‌توانند توسط دیگر اجزای درون سامانه PRIME و همچنین درخواست‌کنندگان بیرونی، از جمله کاربر و یا یک سرویس، دردسترس باشند.

یکی از اجزای کلیدی در معماری PRIMEجزء تصمیم‌گیرندهٔ کنترل دسترسی[5] (ACD) است و برای اینکه نفوذ کند، در پیاده‌سازی یک پروتکل مذاکره بین دو طرف طراحی شده است. مؤلفهٔ ACD مؤلفهٔ مرکزی است که باعث دسترسی و انتشار تصمیم روی واحد منفرد داده می‌شود. اجرای کنترل دسترسی[6] (ACE) مؤلفهٔ میانیهٔ همه دسترسی‌ها به اطلاعات است. روی ACD، برای دسترسی و خواندن داده از مخزن داده اگر دسترسی مفروض باشد ، فراخوانده می‌شود. این مؤلفه شبیه به یک تابع اجرای سنتی در معماری کنترل دسترسی است، با یک تفاوت کلیدی که ACD بسیار پیشرفته شده است؛ زیرا برای تصمیم‌گیری استفاده می‌شود. هر گونه دسترسی به مخازن از طریق مؤلفهٔ ACEانجام می‌شود. مؤلفهٔ اجرا روی مؤلفهٔ ACD برای محاسبه یک تصمیم دسترسی مساوی است. سیاست‌ها در یکی از مخازن سیاست که به‌احتمال متعدد است و توسط ACDدر دسترس است، ذخیره شده‌اند.

مؤلفهٔ مذاکره[7] ، عملکرد مذاکره را که هدف اصلی آن بردن تبادل داده‌ها بین بخش‌ها ، به‌ویژه به‌منظور ایجاد اعتماد و تبادل داده‌هایی که به طریقی دیگر مورد نیاز است، پیاده‌سازی می‌کند. مؤلفهٔ مذاکره روی درخواست‌های ترکیب[8] و پاسخ‌های ترکیب اجرا می‌شود؛ به این معنی که در سرتاسر ویژگی‌ها می‌تواند شامل چندین ویژگی و اظهارات شود؛ و مؤلفهٔ ACD را برای به‌دست‌آوردن سیاست تصمیم‌ها برای واحدهای داده اتمی(اطلاعات جزئی) درگیر در مذاکره، استنطاق می‌کند. این مؤلفه نتایج دریافت‌شده از مؤلفهٔ ACDرا جمع‌آوری می‌کند. دسترسی به داده از طریق مؤلفهٔ ACE انجام می‌شود.

[1] Privacy and Identity Management for Europe
[2] Future Network
[3] Data Repositories
[4] user-side system

[5] Access Control Decision
[6] Access Control Enforcement
[7] Negotiation
[8] compound requests

واحد فدرال [1] (FU) مسئول گواهی‌دادن و تبادل داده است که می‌تواند پروتکل‌های مختلف را اجرا کند. پروتکل ارائه‌شده توسط پروژه PRIME روی سامانه‌های گواهی‌دهی خصوصی (سامانهٔ اعتباردهی ناشناس)[2] با توجه به مزایای متعدد آنها از نظر حفظ حریم خصوصی، متمرکز است. FU تنها مؤلفه‌ای است که تبادل داده را به‌طوری‌که توسط قواعد مؤلفهٔ مذاکره و مداخلات کاربر دیکته‌شده (امرشده)، انجام می‌دهد. دیگر پروتکل‌های موجود می‌توانند با این مؤلفه به‌منظور ایجاد معماری PRIME که با پروتکل‌های مناسب سازگار شده، یکپارچه شده باشد.

یک کاربر می‌تواند خواص مختلف ارائه‌دهندهٔ خدمات را به‌منظور تشخیص بهتر قابل اعتماد بودن ارائه‌دهنده خدمات ارزیابی کنند. ارزیابی بیش‌تر بر پایه تضمین (تضمین مدیر) است، که ارائه‌دهندهٔ خدمات می‌تواند با کاربر که درخواست خدمات داده است، ارتباط برقرارکند. این تضمین، خواص سازمان، فرایندهای آن، سامانهٔ حفاظت از داده در محل و پلت فرم‌های منحصربه‌فرد آن را پوشش می‌دهد. به‌خصوص، در دسترس‌بودن سازوکارهای حفاظت خاص می‌تواند برای کاربران آزاد شده باشد (asserted). مؤلفهٔ مدیر تضمین[3] توسط سه زیرمؤلفهٔ تضمین کنترل[4]، مدیریت اعتماد و اعتبار، تشکیل شده است.

مؤلفهٔ تضمین کنترل مسئول بررسی تضمین‌ها یا برای استفاده محلی و یا در تعامل با بخش‌های دیگر است. یکی از ویژگی‌های آن این است که اطلاعات به‌دست‌آمده از مؤلفه‌های مدیریت اعتماد یک یا پلت‌فرم‌های مختلف که شامل خدمات سامانه می‌شود، جمع‌آوری می‌کند. مؤلفهٔ تضمین کنترل، تضمین‌ها را تولید و تضمین را ارزیابی می‌کند و به بخش‌ها اجازه می‌دهد بر اساس آن (ارزیابی اطمینان) برای اعتماد به خدمات تصمیم‌گیری کنند. منابع داده، اختصاصی‌کردن ایجاد اعتماد، می‌تواند در یک سامانهٔ IDM اجرا شده باشد. معماری PRIME یک مؤلفهٔ مدیریت اعتماد تعریف می‌شود که می‌تواند گواهی داده را به دیگر اجزای به‌دست‌آمده از یک ارزیابی پلت‌فرم محلی ارائه دهد. یک قابلیت کلیدی مؤلفهٔ مدیریت اعتماد برای ایجاد و تأیید گواهی روی قابل اعتماد بودن پلت‌فرم است. مؤلفهٔ اعتبار می‌تواند به‌عنوان یک منبع داده مفید برای ارزیابی اعتمادبخش ناشناختهٔ دیگری به کار رود.

[1] Federation Unit
[2] anonymous credential systems
[3] Assurance Manager

کنترل هویت [5] (IDCtrl) مؤلفهٔ کنترل جریان داده از طریق معماری و امکانات برای ثبت مؤلفه‌ها، برای یک معماری توسعه‌پذیر و قابل‌انعطاف را فراهم می‌کند. مؤلفه‌های IDCtrl دو بخش با یکدیگر برای تبادل اطلاعات و توافق روی سیاست‌ها ارتباط برقرار می‌کنند. IdCtrl و مؤلفه‌های مذاکره هر دو می‌توانند با دیگر مؤلفه‌ها در معماری به دلیل نقش آنها از کنترل‌کنندهٔ کلی و کنترل‌کنندهٔ مذاکره تداخل کنند.

رابط برنامهٔ سامانه[6]، مؤلفهٔ رابط کاربر مرکزی PRIME است. که ارتباط بین PRIME و کاربر فراهم می‌کند. به سامانه اجازه می‌دهد که یک کاربر را از لحاظ آنچه از فعل و انفعالات مربوط به هویت اتفاق می‌افتد آگاه کند و نیز به‌عنوان یک رابط اجرا وظایف اجرای داده و سیاست را عمل می‌کند. از لحاظ معماری، مهم است که این کنسول باید به بخش‌های دیگر PRIME متصل شود؛ چنانچه فرآیندهای خصمانه نتوانند سامانهٔ PRIME را بدون شناخت کاربر آن کنترل کنند.

پروتکل OAuth

یک پروتکل امنیتی است که به کاربران توانایی دسترسی به منابع وب‌شان را بدون نیاز به واردکردن passwords می‌دهد.

OAuth یکی از سریع‌ترین مشخصات در حال رشد مبتنی بر جامعه است و با هدف از بین‌بردن محدودیت‌های وکالت موجود در مدل خدمات سنتی طراحی شده است [26] . مشخصات اصلی، که با عنوان OAuth ۱,۰ شناخته می‌شود در آوریل ۲۰۱۰ نهایی شد و در RFC ۵۸۴۹ مشخص شده است[۲۷] . اگرچه نسخه جدید و اصلاح‌شدهٔ این مدل با عنوان OAuth ۲,۰ در حال انتشار است [28].

۴- نیازمندی‌های حریم خصوصی و امنیت در سامانه‌های مدیریت هویت

در این بخش نیازمندی‌های مورد نیاز در سامانهٔ مدیریت هویت را در دو حوزهٔ حریم خصوصی و امنیت به‌طور خلاصه توضیح می‌دهیم. از این نیازمندی‌ها می‌توان به‌عنوان معیارهای مقایسه‌ای برای مقایسه سامانه‌های مختلف مدیریت هویت که در بالا ذکر شد استفاده کنیم [15]،[12]،[13]،[14].

[4] Assurance Control
[5] Identity Control
[6] System Application Interface

۴-۱- حریم خصوصی (PRIV)

در همین اواخر، حفظ حریم خصوصی کاربران، هویت کاربران و اطلاعات هویتی بسیار مهم شده است. تفناوری‌های افزایش حریم خصوصی(PETs[1]) به‌عنوان سازوکار پایه‌ای برای تضمین حریم خصوصی است. پیکربندی یک IDM با قوانین PET باید سازوکار حفاظت از حریم خصوصی را تضمین کند. در زیر نیازمندی‌هایی را که برای تضمین حریم خصوصی کاربر در سامانهٔ مدیریت هویت استفاده می‌شود، بیان می‌کنیم:

۴-۱-۱- حمایت از گمنامی (ANON[2]) و نام مستعار (SAP[3])

یک سامانهٔ مدیریت هویت مبتنی بر حفظ حریم خصوصی باید به‌صورت قوی از گمنامی پشتیبانی کند. همچنین، باید از نام مستعار نیز برای تضمین اینکه کاربران در SPها به هم پیوند نیستند، استفاده کرد.

از روش‌های حفاظت از حریم خصوصی با استفاده از روش‌های رمزنگاری متنوع برای دستیابی به این نیازمندی‌ها می‌توان استفاده کرد.

۴-۱-۲- توانمندسازی کاربر با شفافیت (TR[4]) و کنترل کنترل داه (DC[5])

تمام نیازمندی‌های حریم خصوصی ذکرشده در بالا درصورتی‌که کاربر هیچ کنترلی بر روی داده‌هایش نداشته باشد و نداند که چه داده‌هایی برای چه نهادی ارسال شده است، بیهوده خواهد بود. با ایجاد شفافیت (به کاربران اجازه بدهیم که بدانند چه داده‌های خصوصی به چه نهادی انتقال داده شده است و چطور داده‌ها در بخش‌های مختلف ذخیره و پردازش می‌شوند) و کنترل‌کردن جریان داده می‌توان به کاربران در قوی ساختن مدیریت هویتشان کمک کرد.

۴-۱-۳- Data Minimisation (DM)

Data Minimisation می‌تواند تضمین کند که فقط داده‌های موردنیاز در ارائه‌دهندگان سرویس، ذخیره و پردازش می‌شوند و از انتشار داده‌های حساس و غیرضروری اشخاص به طرف‌های غیرقابل مجاز محافظت می‌کند که درنهایت خطر نقض حریم خصوصی را کاهش می‌دهد.

۴-۱-۴- مدیریت از راه دور سیاست‌های کاربر (RAP[6]) (RAP[6])

در سامانه‌های مدیریت هویت سنتی، زمانی‌که داده‌ها برای سایر بخش‌ها منتشر می‌شود، کاربران هیچ کنترلی بر روی داده‌هایشان ندارند. یک روش برای اجرای کنترل بر روی داده‌های منتشرشده این است که به کاربران اجازه دهیم داده‌های خود را از راه دور مدیریت کنند.

۴-۱-۵- استفاده از استانداردهای حریم خصوصی (UPS[7])

چارچوب اجرایی برای پروژه Privacy Preferences (P3P[8]) یک استاندارد W3C است که به وب‌سایت‌ها اجازه می‌دهد مجموعه داده‌ها و سیاست‌های مدیریتی خود را در یک فرمت قابل خواندن توسط دستگاه به بازدیدکنندگان نشان دهند. استفاده از استاندارد حریم خصوصی مانند P3P می‌تواند به کاربران اجازه دهد نا نیازمندی‌های حریم خصوصی خود را در روشی استاندارد بیان کنند.

۴-۲- امنیت (SEC)

یک سامانهٔ مدیریت هویت برای دسترسی به خدمات مختلفی اعم از شرکت در فعالیت‌های شبکه‌های اجتماعی، وبلاگ نویسی و ارسال ایمیل برای دسترسی به خدمات دولت، بانک‌داری برخط، فعالیت‌های تجارت الکترونیک و غیره می‌تواند استفاده شود. سطوح مختلفی از امنیت برای هر کدام از این خدمات وجود دارد. هر فعالیت به حداقل ضمانت امنیتی نیاز دارد تا تضمین کند فقط کاربر تصدیق هویت‌شده می‌تواند به صورت امن به خدمات درخواستی دسترسی پیدا کند.

۴-۲-۱- سازوکارهای امنیتی پایه: احراز هویت (AUTH) ، محرمانگی(CONF) ، یکپارچگی (INTG) و انکارناپذیری(NR)

سازوکار اصلی یک سامانه مدیریت هویت این است که صحت یک کاربر را تضمین کند. برای مثال در مورد خدمات وب می‌توان با استفاده از شناسه کاربری و کلمه عبور این کار را انجام داد. برای خدماتی که به امنیت بیشتری نیاز دارند، مانند خدمات مالی یا دولتی باید از روش‌هایی مانند

[1] Privacy Enhancing Technologies
[2] Anonymity
[3] Pseudonym
[4] Transparency
[5] Data Control
[6] Remote Administration of User Policies
[7] Usage of Privacy Standard
[8] Platform for Privacy Preferences Project

بیومتریک، گذرواژه بلادرنگ، توکن‌های سخت‌افزاری و غیره استفاده کرد. محرمانگی برای تضمین این است که داده‌های منتقل‌شده بین طرفین برای هیچ نهاد غیرمجازی فاش نشود. یکپارچگی تضمین می‌کند که داده انتقالی در حین انتقال، دست‌خوش تغییر نشود. انکارناپذیری تضمین می‌کند یک کاربر، که وارد یک تراکنش شده است، نتواند آن را انکار کند. از سازوکارهای رمزنگاری برای تضمین محرمانگی، یکپارچگی و انکارناپذیری استفاده می‌شود.

۴-۲-۲- امنیت چندجانبه[1](MS)

وقتی که در یک عمل بیش از یک طرف حضور داشته باشد، تضمین امنیت همه آنها موضوع امنیت چندجانبه می‌شود. یک سامانه مدیریت هویت به‌طوراساسی بیش از یک بخش را درگیر می‌سازد و به همین دلیل بسیار مهم است که مسألهٔ امنیت چندجانبه را در سامانهٔ مدیریت هویت در نظر بگیریم. در امنیت چندجانبه فرض می‌شود که هر یک از طرفین دست‌کم اعتماد را به طرف دیگر دارد و هر کدام از طرفین می‌تواند اهداف امنیتی خود را اجرا کند.

۵- مروری بر کارهای پیشین

سامانهٔ مدیریت هویت به‌عنوان یک پلت‌فرم مناسب برای گسترش برنامه‌های کاربردی در حوزه‌های مختلف به‌دلیل ارائه خدمات مقرون‌به‌صرفهٔ خود، از جمله (مدیریت داده‌ها، ذخیره‌سازی و منابع محاسباتی) و ویژگی‌هایی مانند (هویت یکتا در حوزه‌های مختلف، قابلیت اطمینان و انعطاف‌پذیری) که توسط اجزای سامانه فراهم می‌شود، به‌عنوان یک پلت‌فرم مناسب برای گسترش برنامه‌های کاربردی در حوزه‌های مختلف مورد استفاده قرار می‌گیرد [18]. با وجود این جاذبه‌ها در سامانه‌های مدیریت هویت، فقدان کنترل و آگاهی کاربر از انتشار ویژگی و صفات خود، خطر افشای اطلاعات حریم خصوصی کاربر را افزایش می‌دهد؛ حتی زمانی که از مدل‌های کنترل دسترسی سنتی در محل [18] استفاده می‌شود، به‌دلیل این که اطلاعات ذخیره‌شده رمزگذاری نشده بر روی ابر قرار دارد، در برابر افشای غیرمجاز یا تغییر آسیب‌پذیر است. بنابراین رمزگذاری پایان‌به‌پایان اطلاعات شامل (ذخیره‌سازی و انتقال) در سامانه‌های مبتنی بر ابر امری لازم است. در این بخش به مطالعهٔ کارهای گذشته می‌پردازیم:

[1] Multi-lateral securit

۵-۱- امنیت و حریم خصوصی در سامانه‌های مدیریت هویت

قبل از معرفی سامانه‌های مدیریت هویت، بسیاری معتقدند که شیوه‌های مربوط به هویت برخط به‌دلایل زیر با مشکل روبه‌روست:

- هر SP مجموعه‌ای از هویت‌های کاربران را حفظ و نگهداری می‌کند؛ بنابراین کاربران باید هویت‌های زیادی داشته باشند؛ (حداقل برای هر SP یک هویت که با این هویت با SP در تعامل است) که این خود باعث بار مسئولیت وایجاد یک نقطه‌ای از خطر برای هویت کاربر می‌شود.
- کاربران کنترلی بر روی انتشار ویژگی‌های خود ندارند؛ این امر منجر به نقض حریم خصوصی و سرقت هویت کاربر می‌شود.

در طول سالیان گذشته سامانه‌های مدیریت هویت با هدف پرداختن به این مشکلات تکامل یافته‌اند، سامانهٔ مدیریت هویت در جهت کاهش نگرانی‌های امنیتی و راحتی بیشتر کاربران توسعه یافته است. سامانهٔ مدیریت هویت در جهت امنیت و راحتی بیشتر، بستری را برای تعاملات فراهم‌کنندگان خدمات و کاربران فراهم کرده است. این بستر امن به‌کمک جزء فراهم‌کننده هویت صورت می‌پذیرد. همان‌طور که در بخش پیش اشاره کردیم، انواع مدل‌ها و نیازمندی‌های مرتبط با سامانه بررسی و تجزیه و تحلیل شده است. حال با توجه به اهمیت دو موضوع امنیت و حریم خصوصی، در این بخش بر روی این الزامات تمرکز شده و طرح‌های ارائه‌شده در این زمینه طی سالیان اخیر مرور و بررسی شده است.

۵-۱-۱- بررسی استاندارد های موجود در سامانه‌های مدیریت هویت

در این بخش به توضیح برخی از مفاهیم و ویژگی‌های پایه‌ای مورد نیاز برای توصیف حریم خصوصی سامانه‌های مدیریت هویت می‌پردازیم. ویژگی‌های حریم خصوصی در چند پروتکل شناخته‌شده در جدول (۲) بررسی می‌شود [16].

در این مقاله شناسایی ویژگی‌های حریم خصوصی مرتبط با فناوری احراز هویت و تعین و تخمین اینکه چه ویژگی‌های حریم خصوصی توسط هر کدام از فناوری‌های احراز هویت فراهم شده، ارائه شده است.

(جدول-۲): ویژگی‌های حریم خصوصی مدل‌های مدیریت هویت [16].

	Unobservability by identity or attribute provider	Free choice of identity or attribute provider	Anonymity	Selective disclosure	Issue-show unlinkability	Multishow unlinkability by different parties	Multishow unlinkability by same party
5. Microsoft Passport				✔			
6. SAML browser SSO profile		✔		✔			
7. Shibboleth		✔	✔	✔		✔	✔
8. OpenID (without PPID)		✔		✔			
9. ICAM OpenID profile		✔	✔	✔		✔	
10. OAuth		✔		✔			
11. OpenID Connect		✔		✔			

همان‌طورکه در جدول (۲) آورده شده است به جنبه‌های محتلف حریم خصوصی پرداخته است؛ در این کار مسأله مرتبط با نگرانی از نفوذ و آگاهی افراد یا قسمت‌هایی که با تولید و یا ثبت اعتبار کاربر اقدام می‌کنند، در روند و چگونگی استفاده کاربر، بررسی شده است.

در ادامهٔ راهکاراها و فناوری‌های مختلف سامانه از جمله مسائل مرتبط با فناوری احراز هویت که به کاربر اجازه می‌دهد تا IDP مورد نظر خودش را که در آن احراز هویت می شود، انتخاب کند. در ادامه ویژگی گمنامی در بررسی پروتکل‌ها بررسی شده است؛ این ویژگی اجازه می‌دهد تا کاربر درحالی‌که احراز هویت به SP شده است، اما به‌طور ناشناس برای SP باقی بماند و اطلاعات هویتی خود را برای SP ارسال نمی‌کند.

مسألهٔ مرتبط با انتشار ویژگی‌ها، یکی دیگر از ویژگی‌های بررسی شده است، به‌طوری‌که برخی از ویژگی‌ها توسط کاربر اجازه افشا و انتشار پیدا کند. در آخر هم سه ویژگی بررسی‌شده، مرتبط با مخفی‌نگه‌داشتن ارتباط بین فعالیت‌ها و هویت‌ها در سامانه‌های مدیریت هویت است.

ویژگی‌های حریم خصوصی ذکرشده [16]، برخی از ویژگی‌های حریم خصوصی را مطرح و چندین پروتکل مطرح را در استفاده از این ویژگی‌ها بررسی کرد.

در این مقاله شناسایی ویژگی‌های حریم خصوصی مرتبط با فناوری احراز هویت و تعین و تخمین اینکه چه ویژگی‌های حریم خصوصی توسط هر کدام از فناوری‌های احراز هویت فراهم شده مورد بررسی قرار گرفته است.

در همین زمینه کار دیگری انجام شده است؛ در این کار ویژگی‌های ذاتی سامانه‌های موجود را شناسایی کرده است و آنها را به سه دسته تقسیم‌بندی کرده است [16].

ما بر روی ارتباطات بین انتخاب‌های شناسایی‌شده در سامانه‌های جاری و بحث بر روی این انتخاب‌ها بر روی فعالیت سامانه توجه کردیم. هم‌چنین رویکرد حریم خصوصی را اتخاد کردیم که متمرکز بر سه ویژگی حریم خصوصی است .

۱- Undetectability: پنهان‌کردن و مخفی‌نگه‌داشتن فعالیت کاربران

۲- Unlinkability: مخفی‌نگه‌داشتن ارتباط بین فعالیت‌ها و هویت‌ها

۳- Confidentiality: قادرساختن کنترل کاربر بر روی انتشار ویژگی‌های خود

Undetectability, unlinkability, and confidentiality با همه نگرانی‌هایی که در دسترسی داشتن قسمت‌های مختلف سامانه به داده‌های خاص است، مرتبط است.

ممکن است این خواص در انتخاب طراحی به هم عمود باشند و بنابراین بهتر است که به‌طور مستقل در نظر گرفته شوند. این سه ویژگی تعریف‌شده مبتنی بر فضای طراحی حریم خصوصی شکل گرفته است.

(جدول-۳): بررسه سه قسمت اصلی حریم خصوصی درسیستم‌های مدیریت هویت [17]

			Passport	Liberty	Idemix	Shibboleth	Higgins	PRIME	OpenID	CardSpace	U-Prove	CS-Federation	P-IMS	Facebook SSO
Undetectability		Interactive	■	■		■			■					■
		Active client		■			■			■		■		
		Credential			■			■			■		■	
Unlinkability	Identities	Centralized	■											■
		Federated		■								■		
		Decentralized			■	■	■	■	■	■	■		■	
	Identity/ action	Pseudonymous	■	■		■	?	■	■	?		■		?
		Anonymous			■	■	?	■	■	?	■		■	
	Actions	Authorization request	■	■		?	?		?	?	■	■	■	■
		Issue/use	■	■		■	?		■	?			■	■
Confidentiality	Intentional	Instance		?	■	■	■		?	■	■	■	■	■
		Policy	■	?		■		■	?					
	Forwarding	Deniable	■	■	■	■	?	■	■	?	■			
		Obligations					?	■		?				
	Inference	Actions	■	■		■	?		■	?	■	■	■	■
		Attributes	■	■	■	■	?		■	?	■	■	■	■

در جدول (۳) بر روی تأثیر ویژگی‌های حریم خصوصی در طراحی سامانه مدیریت هویت متمرکز شده است؛ با این حال عوامل تأثیرگذاری مؤثر دیگری هم برای پیاده‌سازی و موفقیت

سامانه مدیریت هویت وجود دارد؛ از قبیل مسائل اقتصادی، و طراحی رابط کاربری که می‌تواند برخی از نگرانی‌های حریم خصوصی را برطرف کند.

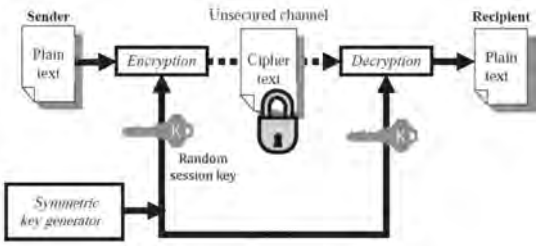
۵-۲- بررسی روش‌های کنترل کاربر

در کارهای پیشین بررسی معماری‌های موجود، ویژگی‌های حریم خصوصی، راهکارهایی جهت کنترل و آگاهی کاربر در جهت حفظ حریم خصوصی، بیان شده است؛ لذا سعی شده است در این بخش به‌طور مشخص این ویژگی‌ها و پیشنهادها را مورد بررسی و تجزیه و تحلیل قرار دهیم.

۵-۲-۱- بررسی روش‌های رمزنگاری

۵-۲-۱-۱- رمزنگاری با کلید متقارن (SKE)

این روش‌ها به‌عنوان مثال AES (استاندارد رمزگذاری پیشرفته)، به‌طور معمول یک مقدار محرمانه را بین دو طرف به اشتراک می‌گذارند. در رمزنگاری متقارن با استفاده از کلید K که به اشتراک گذاشته می‌شود، رمزگذاری و رمزگشایی صورت می‌گیرد. شکل (۵) الگوریتم رمزنگاری متقارن را نشان می‌دهد.



(شکل-۵): الگوریتم رمزنگاری متقارن [19]

$$M=D_k(E_k(M)) \qquad (۱)$$

در تابع بالا، E تابع رمزنگاری است و با استفاده از کلید K که به اشتراک گذاشته شده است، پیام M رمزگذاری می‌شود. از سوی دیگر D تابع رمزگشایی است و با استفاده از کلید K به اشتراک گذاشته‌شده، پیام رمزشده را رمزگشایی می‌کند. دو شرکت‌کننده مانند آلیس و باب برای استفاده از SKE نخست باید بر روی کلید K به اشتراک گذاشته‌شده به توافق برسند. پس از آن آلیس M را با استفاده از الگوریتم رمزنگاری E و K کلید برای به‌دست‌آوردن متن رمزی $C = E_k(M)$ رمزگذاری می‌کند. آلیس پس از آن C را به باب می‌فرستد. باب با استفاده از الگوریتم رمزگشایی D و همان کلید K پیام $M = D_k(C)$ را بازیابی می‌کند [38].

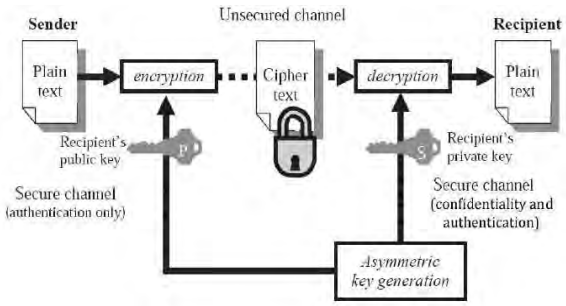
روش‌های SKE به‌طورمعمول کارآمد هستند؛ اما به‌دلیل سازوکارهای اضافی مورد نیاز برای اعمال کنترل دسترسی، موجب پیچیدگی در سامانه می‌شوند. همچنین، طرفین که مایل به استفاده از SKE هستند، برای نخستین‌بار باید روی کلید مشترک از طریق روش تبادل کلید به توافق برسند، به‌عنوان مثال از رمزنگاری کلید عمومی مانند پروتکل تبادل کلید دیفی-هلمن استفاده می‌شود. از آنجا که SKE با استفاده از یک کلید مشترک در میان طرفین عمل می‌کند، اگر کلید به اشتراک گذاشته‌شده به خطر بیفتد، تمام اطلاعات رمز شده نیز به خطر می‌افتد.

۵-۲-۱-۲- رمزنگاری کلید عمومی (PKE)

روش‌هایی مانند RSA ارائه‌شده توسط (ریوست، شامیر و آدلمن)، روشی را برای توزیع کلید به اشتراک گذاشته‌شده، احراز هویت و عدم انکار فراهم می‌کنند. در PKE، هر فرد یک جفت کلید دارد: PK کلید عمومی است که برای همه شناخته شده است و SK کلید مخفی است که تنها فرد از آن اطلاع دارد.PKE از کلید عمومی PK برای رمزنگاری و SK کلید برای رمزگشایی استفاده می‌کند:

$$M = D_{sk}(E_{pk}(M)) \qquad (۲-۳)$$

در تابع بالا، E، تابع رمزنگاری است و از کلید عمومی PK برای رمزگذاری پیام M استفاده می‌کند. D، تابع رمزگشایی از SK کلید برای رمزگشایی پیام رمزشده استفاده می‌کند. شکل (۶) الگوریتم رمزنگاری نامتقارن را نشان می‌دهد.



(شکل-۶): الگوریتم رمزنگاری نامتقارن [19]

برای آلیس و باب که از PKE استفاده می‌کنند، فرض کنید باب یک جفت کلید: PK و SK دارد و آلیس می‌خواهد پیام M را برای باب رمزگذاری کند. آلیس رمزگذاری M را با استفاده از الگوریتم رمزنگاری E و کلید عمومی باب PK برای

به‌دست‌آوردن متن رمزشده $C = E_{pk}(M)$ انجام می‌دهد. آلیس متن رمز شده C را به باب می‌فرستد و او با استفاده از تابع رمزگشایی و کلید SK مخفی خود برای محاسبه $M = D_{sk}(C)$ استفاده می‌کند و پیام M را بازیابی می‌کند. PKE به‌علت نیاز به زیرساخت کلید عمومی (PKI) گران‌قیمت که برای توزیع و مدیریت کلیدهای عمومی و گواهینامه‌های دیجیتال برای افراد مورد نیاز است، یک راه‌حل عملی مناسب برای ذخیره‌سازی امن داده‌ها نیست [38].

نارسایی و ناکارآمدی روش‌های استاندارد کنترل دسترسی و رمزگذاری بالا در حمایت از سامانه‌های مبتنی بر ابر انگیزه‌ای را برای بررسی روش‌های دیگر ایجاد می‌کند. در این پژوهش به‌دنبال بهره‌گیری از ویژگی‌ها برای کنترل دسترسی و مدیریت داده‌های امن با استفاده از شیوه رمزنگاری مبتنی بر ویژگی با سیاست متن رمزشده هستیم. هدف ما در این بخش نشان‌دادن این امر است که چگونه می‌توان ویژگی‌ها و سیاست‌های به‌طور مؤثر در طراحی سامانه‌های کنترل دسترسی به کار برد، به‌نحوی‌که موجب بهبود فرآیند تصمیم‌گیری کنترل دسترسی و کم‌کردن بار محاسباتی شود.

۵-۳- بررسی روش‌های سیاست حریم خصوصی

در طرح‌های ارائه‌شده قبلی، از سیاست‌های حریم خصوصی برای حفظ و کنترل بر روی انتشار داده‌های کاربر استفاده شده است. آنچه که در این طرح‌ها به‌عنوان سیاست حریم خصوصی بیان شده، سیاست و تنظیماتی است که کاربر برای دسترسی به ویژگی‌های خود اعلام می‌کند. تعریف سیاست دسترسی فقط توسط کاربر تعریف نمی‌شوند و فراهم‌کنندگان خدمات هم برای خود سیاست دسترسی دارند. با توجه به تعریف سیاست توسط چندین قسمت داخل سیستم در این کار از یک سری وب‌سرویس‌هایی استفاده شده که وظیفه آنها بررسی و تطبیق این سیاست‌ها، قبل از به‌اجرادرآمدن هر درخواست است؛ بنابراین یک‌بار یک برنامه درخواست را برای پردازش برخی داده‌ها دریافت می‌کند و آن باید از وب‌سرویس پیشنهادشده مشورت بگیرد که که می‌تواند با عمل درخواست‌شده ادامه دهد [20].

در کار دیگری یک پروتکل اعتبار را ارائه می‌کند که در این پروتکل وزن اعتبار موجودیت‌های فدرال به‌منظور حمایت داده‌های افشاشده بررسی می‌شود. با این راه کاربران می‌توانند قبل از اینکه هر گونه اطلاعاتی را به آن ارسال کنند، اعتبار SPها را در سامانه فدرال بررسی کنند. با توجه به سطح‌های اعتماد sp، کاربر تصمیم می‌گیرد که با کدام یک از ویژگی‌ها و داده‌های خود با sp تعامل و ارتباط برقرار کند. بدیهی است که چگونگی ارتباط کاربر با sp مبتنی بر اعتماد کم یا زیاد کاربران به sp است [40].

در طرح ارائه‌شده دیگری، یک معماری جدید را برای مدیریت هویت مبتنی بر پویایی فضای سایبر پیشنهاد می‌کند. بنابراین کاربر می‌تواند انتخاب کند که داده‌ها را بدون رمز یا با رمزنگاری به IDP بفرستد. کنترل دسترسی استفاده‌شده در این مدل برای اعطای مجوز دسترسی، از طریق مدل (PMP)– نقطه مدیریت سیاست- صورت می‌گیرد؛ اما چگونگی پیاده‌سازی آن در این پیشنهاد مشخص شده است.

مدل‌های مختلفی برای کنترل دسترسی مانند ABAC (Attribute based Access Control), RBAC (Role-based Access Control), PBAC (Purpose-based Access Control), . و ... می‌تواند ارائه شود. معماری پیشنهادشده در این مدل مطابق شکل زیر است [22].

(شکل-۷): مرکز تصمیم‌گیری سیاست‌ها [22]

شکل (۷) جزئی اضافی را در جهت حفظ سامانه‌های مدیریت هویت توصیف می‌کند. در جریان درخواست مدیریت، سیاست‌های متصل به صفات را بر عهده دارد که این جزء با نام سیاست مدیریت نقطه (PMP) در سامانه قرار داده شده است. در اصل عنصر PMP نقطه‌ای متمرکز است که مسئول ارزیابی قوانین سیاست‌های حریم خصوصی است.

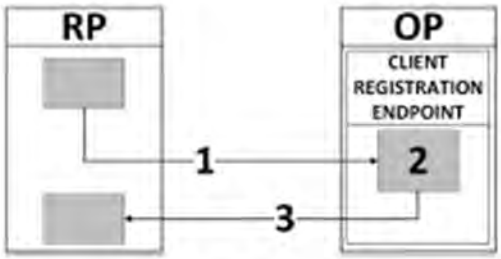
در طرح ارائه‌شدهٔ دیگری ویژگی‌های مرتبط با حفاظت از حریم خصوصی در سامانه‌های مدیریت، گردآوری و تعریف شده است. چهار حوزه حریم خصوصی پیشنهاد شده است. SP باید دست‌کم این چهار حوزه را پشتیبانی کند که با توجه به پروفایل مشخصات و نقش دسترسی برای هر کاربر تقسیم شده است [23] .

- Anonymous Access: کاربر بدون هیچ‌گونه قابلیت شناسایی که سبب به‌خطرافتادن حریم خصوصی‌اش شود به SP دسترسی پیدا می‌کند. در این حوزه، کاربر پس از احراز هویت از طریق IDP به منابع محافظت‌شده دسترسی پیدا خواهد کرد. همچنین SP، اطلاعات مرتبط

با احراز هویت کاربر را دریافت می‌کند؛ اما اطلاعات دریافت‌شده توسط SP، بدون شناسه کاربر و اطلاعات شخصی هویتی وی است.

- Access with Pseudonym: در این حوزه SP نام مستعاری را از کاربر دریافت می‌کند. ممکن است ویژگی‌هایی را از کاربر که به ویژگی‌های شخصی هویتی کاربر مرتبط نشود، نیز دریافت کند. استفاده از نام مستعار جهت حفظ حریم خصوصی کاربران است و کاربر در SP با نام مستعار خود شناخته می‌شود.
- Partial Attributes Access: کاربر ویژگی‌هایی را که می‌خواهد به SP ارسال شود، انتخاب می‌کند؛ بدین صورت که IDP فهرستی از ویژگی‌های کاربر را نمایش می‌دهد و کاربر از بین ویژگی‌های این فهرست، ویژگی‌های مد نظر خود را انتخاب و برای SP ارسال می‌کند. علاوه‌براین کاربر می‌تواند ویژگی‌های انتخاب‌شده را رمز کند.
- Access with Total Attributes: ارسال مجموع ویژگی‌ها و صفات کاربر برای SP است. زمانی که SP درخواست دریافت ویژگی‌ها و صفات کاربر را می‌دهد کاربر اجازه ارسال تمامی صفات و ویژگی‌های خود را می‌دهد.

در طرح ارائه‌شده دیگری با استفاده از حوزه‌های حریم خصوصی و در محیط پویا، ابتدا RP که همان SP است در OP که همان IDP است، به‌صورت برخط ثبت می‌شود و سپس حوزه‌های حریم خصوصی از کاربر مورد سؤال قرار می‌گیرد.



(شکل-۸): روال ثبت نام پویای SP در IDP [24]

در این طرح، سامانه‌های مدیریت هویت در محیط‌های پویا و برخط مورد بحث و بررسی است، همان‌طورکه در شکل (۸) مشخص است، SP خود را به‌طور برخط در IDP ثبت می‌کند. مراحل ثبت نام مطابق عملکرد زیر بیان شده است [44]:

۱- درخواست ثبت نام SP

SP یک پیام HTTP را با نوع محتوای نرم‌افزار Json در جهت جهت ثبت بر روی IDP با پارامترهایی خود می‌فرستد. SP پارامترهای خود را بر طبق فهرست اعلام‌شده که توسط IDP حمایت می‌شود، می‌فرستد. در فضای مجازی و برخط بودن، هدف فقط هدایت URLها هستند که مورد نیاز است. بقیه پارامترها اختیاری‌اند.

۲- ثبت نام SP

IDP به SPیک شماره هویت منحصربه‌فرد خاصی را اختصاص می‌دهد. SP کلید عمومی و پارامترهای مرتبط خود را در درخواست صدور شناسه به IDP ارسال می‌کند. IDP با توجه به فهرست مورد پشتیبانی و حمایت خودش ممکن است برخی از ویژگی‌های SP را بپذیرد و یا رد کند.

۳- پاسخ ثبت نام RP

پس از آنکه ثبت نام SP در IDP صورت پذیرفت، IDP کد HTTP201 ایجادشده را به‌همراه ابرداده‌های ثبت‌شده در یک سند JSON (نرم‌افزار JSON برای پشتیبانی نوعی محتواست) برای IDP این سند شامل فیلدهای ثبت‌شده و احیاناً تغییریافته توسط IDP است که به‌همراه شناسهٔ معین‌کنندهٔ هویت SP، به SP ارسال می‌کند.

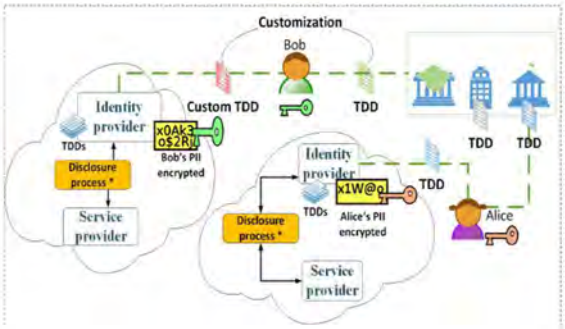
(شکل-۹): صفحه انتخاب حوزه حریم خصوصی توسط کاربر [24]

با توجه به آنچه که در شکل (۹) آمده است، کاربر در هنگام انتشار اطلاعات به IDP، حوزه‌های حریم خصوصی خود را برای ارتباط و تعامل با SP اعلام می‌کند. بدین منظور از صفحه‌ای استفاده شده است که در آن کاربر می‌تواند یکی از چهار حوزهٔ گمنامی، نام مستعار، ویژگی‌های جزئی و ویژگی‌های حقیقی را انتخاب و به IDP اعلام کند؛ IDP نیز با توجه به حوزه‌های اعلام‌شده، صفات و ویژگی‌های کاربر را برای SP ارسال می‌کند.

۵-۳-۱- بررسی روش‌های تلفیقی رمزنگاری و سیاست حریم خصوصی

در این طرح‌ها به‌طور ترکیبی از رمزنگاری، مدیریت سیاست و آگاهی درباره سطح اعتماد SP استفاده شده است؛ همچنین کمبود کنترل کاربر بر روی داده‌های هویتی‌اش را زمانی که

ثبت نام بر روی IDP مورد بررسی قرار گرفته است، کاربران می‌توانند سیاست‌های انتشاری خود را تعریف کنند و مشخص کنند که کدام یک از داده‌های شخصی هویتی خود را منتشر کنند [25].

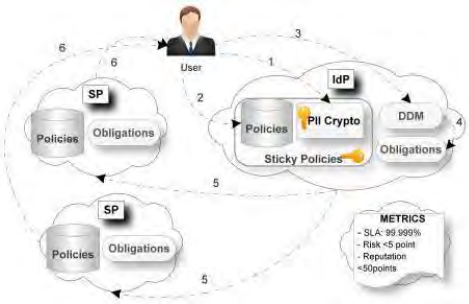


(شکل-۱۰): نمای رمزنگاری اطلاعات کاربر توسط خودش در سامانه مدیریت هویت [25]

با توجه به موجودیت‌های کنجکاو و مخرب داخلی در داخل فراهم‌کنندگان (SP و IDP) با دسترسی و امتیاز و امکانات فنی برای آسیب‌رساندن به حریم خصوصی کاربر، از رمزنگاری داده‌ها قبل از ثبت اطلاعات در IDP استفاده شده است. بنابراین پیشنهاد شده است، داده‌های شخصی هویتی کاربران در داخل IDPها به‌صورت رمزشده ذخیره شوند و فقط راهی باشد که فقط کاربر آن را رمزگشایی و از آن استفاده کند. هیچ راهی برای مقابله با عدم حفظ حریم خصوصی در طرف SP در این طرح پیشنهاد نشده است. روشی که برای رمزنگاری استفاده شده رمزنگاری متقارن است که در آن کاربر با کلید عمومی خودش اطلاعات خود را رمز می‌کند و بدیهی است، رمزگشایی با کلید خصوصی کاربر صورت می‌گیرد. رمزگشایی سمت کاربر انجام می شود و به‌هیچ‌عنوان کلید خصوصی کاربر به IDP فرستاده نمی‌شود. با توجه به رمزگشایی از طرف کاربر، انتخاب اینکه کدام داده ها توسط کاربر رمز گشایی و به SP فرستاده شود، توسط کاربر صورت می‌پذیرد[25] .

در طرح ارائه‌شدهٔ دیگری سعی شده است با استفاده از رمزنگاری و مدیریت سیاست و مرکزی در جهت تصمیم‌گیری و تطبیق سیاست‌های دسترسی، مدلی را برای بهبود حریم خصویصی نمایش دهد.

شکل (۱۱)، تعاملات حریم خصوصی را بررسی می‌کند. این جریان، شامل محیط‌های پویایی است که در آن هزاران نفر از کاربران در حوزه‌های مختلف از طریق IDM با هم ارتباط برقرار می‌کنند؛ با این حال، کنترل دسترسی باید در یک سامانه IDM فدرال طوری برقرار شود که اولویت کاربر در نظر گرفته شده باشد؛ بنابراین لازم و ضروری است IDM به کاربران اجازه دهد تا اطلاعات شخصی هویتی خودشان را بر روی IDP خودشان ثبت کنند و معیارهای استفاده و انتشار داده‌های خودشان را انتخاب کنند. در گام شماره یک؛ کاربر اطلاعات و ویژگی حود را به‌صورت رمزگذاری‌شده یا نشده بر روی IDP ارسال می‌کند. در گام دو؛ IDP به کاربر اجازه می‌دهد تا سیاست‌های حریم خصوصی خود را در جهت چگونگی استفاده و انتشار داده‌ها، ثبت کند.



(شکل-۱۱): مدل تعامل ارائه‌شده برای اطلاعات کاربر [26]

در گام سه؛ مدل‌های پویای انتشار دادهٔ توافق‌شده بین SP و IDP به کاربر ارائه می‌شود و کاربر با توجه از آگاهی و اطلاع درباره معیارهای اعتبار یا خطرات احتمالی مدل‌ها، انتخاب می‌کند که از کدام استفاده می‌کند. IDP مدل‌های ممکن دسترسی موجود را برای تعاملات به کاربر نمایان می‌کند. دسترسی گمنام، دسترسی نام مستعار، دسترسی با کمینه ویژگی‌های انتخاب‌شده، در گام چهار؛ بعد از همه تعاریف، سامانه قوانینی را که SPها باید ملاقات کنند و به آن متعهد شوند جمع‌آوری و به بسته اضافه می‌کند. در گام پنج؛ IDP بسته‌ای را شامل سیاست‌های چسبنده و تعهدات به SP انتقال می‌دهد. در انجام تعهدات، فراهم کننده تضمین می‌کند که سیاست‌ها و اولویت‌های کاربر انجام خواهد شد. سرانجام، در گام شش، کاربر به نرم‌افزار دسترسی پیدا می‌کند.

بسیاری از سیاست‌های در گیر در فرایند مجوز IDM به‌طوراساسی به برنامه‌های کاربردی، قوانین و کاربران مبتنی هستند. سیاست‌های حریم خصوصی، اسنادی هستند که جزئیات چگونگی به‌کارگیری داده‌های کاربر را بیان می کند؛ مجموعه‌ای از تنظیمات حریم خصوصی تعریف‌شده به‌وسیلهٔ کاربر بر روی مجموعه وجود دارد، هدف، حفظ و انتشار داده است. سیاست کنترل دسترسی مشخص می‌کند که افراد در چه حالتی می‌توانند به اشیا دسترسی داشته باشند. همان‌طور که در بحث [8]، مدل شامل جزء مدیریت PDP(نقطه

تصمیم‌گیری سیاست) است. این مرکز بایستی بین PDPهای متعدد موجود در SPهای گوناگون مدیریت کند. مدل‌های مختلف کنترل دسترسی، در حال حاضر مانند ABAC (Attributebased کنترل دسترسی)، RBAC (کنترل دسترسی مبتنی بر نقش)، PBAC (کنترل دسترسی مبتنی بر هدف)، وجود دارد.

در ادامه طرح پیشنهادی، بحث رمز نگاری مطرح شده است. رمزنگاری اطلاعات شخصی هویتی، تهدیدات حریم خصوصی را کاهش می‌دهد و اجازه کنترل ویژگی‌هایی را که باید منتشر شود، می‌دهد. پیشنهاد ارائه‌شده رمز نگاری ویژگی‌ها قبل از ارسال آنها به IDP است و قادر است کاربر تا برخی ویژگی‌های خود را رمز کند. اطلاعات شخصی قابل شناسایی، مجموعه‌ای از ویژگی‌های اساسی (نام، رایانامه، اسناد هویت، شماره کارت اعتباری، شماره تلفن و نشانی) تعریف شده است. کاربر در تمامی مراحل از جمله در زمان رمزگشایی ویژگی‌های فرستاده‌شده به ارائه‌دهندهٔ خدمات، شرکت دارد. بنابراین، در طول فرآیند ثبت نام، کاربر داده‌های شخصی هویتی خود را رمز می کند. رمزنگاری ابتدایی مورد استفاده در معادله (۱) آمده است.

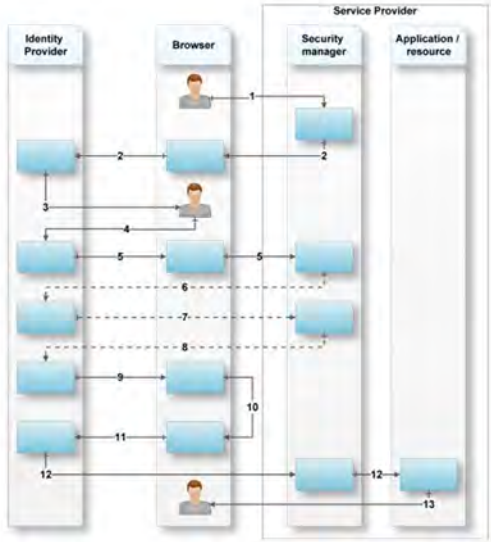
$$E(K1, ps) = ps' \qquad (1)$$

در این حال کاربر ویژگی را مثل PS را با کلید K رمز می‌کند و سپس 'PS را به‌عنوان ویژگی رمزشده به IDP می‌فرستد. شکل (۱۲) تعامل میان اجزای مسئول تجزیه و تحلیل و تصمیم‌گیری در سیاست‌های چسبنده را نشان می‌دهد. کاربر، اطلاع‌رسانی سیاست حفظ حریم خصوصی مرتبط با داده‌های خود را انجام می‌دهد. همان زمان، SP سیاست‌های کنترل دسترسی در جهت دستیابی کاربران به نرم‌افزار اعلام می‌کند. پس از آن، تجزیه و تحلیل این سیاست‌ها توسط قسمت متمرکزی صورت می‌گیرد و همچنین مؤلفه‌ای در IDP مسئول نظارت بر حرکت داده‌های کاربر و گزارش در مورد رعایت تعهدات و سیاست‌های چسبنده کاربر است.

تصمیم‌گیرنده جزء SP است که داده‌های شخصی هویتی، سیاست حفظ حریم خصوصی، و سیاست‌های کنترل دسترسی را دریافت می‌کند. تصمیم‌گیرنده مسئول تصمیم‌گیری است و انطباق و یا عدم انطباق مرتبط با سیاست‌های کنترل دسترسی کاربر را اعلام می‌کند. درضمن جزء نظارتی در IDP، حفظ و یا نقض حریم خصوصی کاربر را با توجه به داده‌های منتشرشده به کاربر اطلاع می‌دهد.

(شکل-۱۲): مرکز تصمیمی‌گیری جهت دسترسی با توجه به سیاست اجزا [26]

مدلی که برای حفظ حریم خصوصی بیان شده مطابق شکل (۱۳) است.



(شکل-۱۳): مدل ارائه‌شده حفظ حریم خصوص کاربر [26]

در شکل (۱۳) مدلی از سیستم‌های مدیریت هویت با تکیه بر حریم خصوصی ارائه شده است. گام‌های مدل ارائه‌شده در زیر آمده است[26].

۱- در گام نخست کاربر جهت دستیابی به منابع محافظت‌شده در SP درخواست می‌دهد.
۲- قسمت مدیریت امنیتی DP درخواست کاربر را دریافت می‌کند و احراز هویت کاربر را از او می‌پرسد.
۳- کاربر IDPخود را با توجه به اعتبار خود انتخاب می‌کند.
۴- کاربر اعتبار خود را برای IDP فراهم می‌کند.
۵- IDP اعتبار کاربر را برایش و تأیید می‌کند و گواهی آن را به کاربر بر می‌گرداند و کاربر نیز آن را به SP می‌دهد.
۶- SP گواهی احراز هویت ارسال به IDP می‌کند تا سؤال کند این گواهی مورد تأیید است یا نه.
۷- IDP اعتبار گواهی را بررسی و تأیید یا عدم تأییدبودن گواهی را به SP اعلام می‌کند.

۸- SP از IDP ویژگی‌های اضافی از کاربر را دریافت می‌کند.
۹- IDP کاربر را از حوزه‌های انتشار داده‌ای که SP حمایت می‌کند با خبر می‌سازد.
۱۰- کاربر یک حوزه را انتخاب و اگر لازم باشد برخی از داده‌های خود را رمز می‌کند.
۱۱- کاربر IDP را از حوزه‌های انتخاب‌شده آگاه می‌کند.
۱۲- IDP با توجه به حوزهٔ حریم خصوصی انتخاب‌شده توسط کاربر، داده و اطلاعات را به SP ارسال می‌کند.

SP دسترسی به منابع را با توجه به ویژگی‌های منتشرشده می‌دهد.

۶- نتیجه

برای دستیابی به اهداف بالا سامانه کنترل حریم خصوصی با به‌کارگیری رمزنگاری و اعمال سیاست حریم خصوصی در سال‌های اخیر با درنظرگیری سناریوی رمزنگاری پرونده در IDP ارائه شد. با استفاده از رمزنگاری متقارن و نامتقارن داده را قبل از ارسال به IDP رمز می‌کردند و پروندهٔ رمزشده در حالت نخست برای SP فرستاده می‌شود و کاربر با SP وارد ارتباط می‌شود و فقط برخی از ویژگی‌هایی را که می‌خواهد رمزگشایی و یا IDP با کاربر وارد ارتباط می شود و کاربر برخی از ویژگی‌ها را رمزگشایی می‌کند و به SP می‌فرستد. پیشنهادهای بالا داری مشکلات کاربر محوری بودند و سربار زمانی و درگیری زمانی SP یا IDP با کاربر بسیار زیاد تلقی می‌شود. برخی از پیشنهادها هم در حوزه‌های حریم خصوصی صورت گرفته بود. بدین شکل که یا سیاست‌ها را به داده‌ها می‌چسباندند و این سیاست‌ها را که توسط هر قسمت مجموعه ممکن است تعریف شود در مرکزی جمع می‌شود و آن نقطه به‌عنوان نقطه متمرکز و تصمیم‌گیر و انطباق این اعمال دسترسی عمل می‌کند. مشکل این روش‌ها اضافه‌کردن مرکز یا قسمتی برای مدیریت سیاست‌ها تلقی می‌شود که وظیفه بررسی کردن سیاست‌ها را دارد؛ در ضمن سربار ارتباطی و محاسباتی این روش‌ها به‌دلیل نگهدار و ارسال سیاست حریم خصوصی به یک مرکز تصمیم‌گیری مستقل و سپس استعلام از انطباق سیاست‌ها یا عدم آنها و درضمن احتمال نفوذ در این سامانه توسط SP و ... باعث افزایش خطرات این روش شده است. برخی از طرح‌های پیشنهادشده هم، به معرفی چهار حوزه در حریم خصوصی پرداخته‌اند و با استفاده از این چهار حوزه مدل خود را پیشنهاد داده‌اند. آخرین این کارها در سال ۲۰۱۶ ارائه شده است. در این پیشنهاد IDP پس از تأیید کاربر و اعلام آن به SP، و در زمانی که SP ویژگی‌های کاربر را از IDP درخواست می‌کند، IDP وارد ارتباط مجدد با کاربر می‌شود و از کاربر می‌خواهد تا یکی از چهار حوزه حریم خصوصی را در ارتباط با این SP انتخاب کند و سپس IDP بر مبنای انتخاب کاربر، ویژگی‌ها را به SP ارسال میکند. مشکل این روش عدم آگاهی کاربر از سطح اعتماد SP است که به هیچ طریقی برای کاربر روشن نشده است و همچنین ارتباط IDP به‌عنوان مرکز شلوغ در سامانه (که شاید در ثانیه بایستی چندین ملیارد درخواست را پاسخ‌گو باشد) با کاربر که باعث کارایی پایین سامانه می شود؛ لذا روش‌های بالا هم خیلی نمی‌تواند جامع تلقی شود و نیاز به یک روش جدید در جهت حفظ امنیت و حریم خصوصی احساس می‌شود.

۷- مراجع

[1]Y. Cao and L. Yang, “A survey of identity management technology,” in Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on, December 2010, pp. 287 –293.

[2] maryline Laurent, uciel fragoso, jose incera “Federated Identity Management” International Conference on Availability, Reliability and Security (ARES 09.), Fukuoka, Japan, 2006 Marc Andreas Barisch

[3] 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.

[4] T. 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.

[5] G. Ahn, and M. Ko,, "User-centric Privacy Management for Federated Identity Management," in Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2007), pp. 187-195, New York, November 2007.

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

[7] A. A. 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 75–82, Dec 2015.

[8] Future of Identity in the Information Society (FIDIS) Project WP3, "Study on Mobile Identity Management," May 2005.

[9] Eran Hammer-Lahav, "Introducing OAuth 2.0," 15May2010.http://hueniverse.com/2010/05/introducing-oauth-2-0

[10] Marit Hansen, "Privacy-enhancing technologies," Alexander Rossnagel (Ed.): Handbuch Datenschutzrecht; Verlag C.H. Beck, pages 291–324, Munchen 2003.

[11] The Platform for Privacy Preferences (P3P) Project. http://www.ws3.org/P3P/

[12] Stefanie Potzsch, Martin Meints, Bart Priem, Ronald Leenes and Rani Husseiki, "D3.12: Federated Identity Management – what's in it for the citizen/customer?" 10 June 2009.

[13] Stefanie Potzsch, Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann and Sandra Steinbrecher, "Requirements for Identity Management from the Perspective of Multilateral Interactions." in Jan Camenisch, Ronald Leenes, and Dieter Sommer, editors, Digital Privacy, volume 6545 of Lecture Notes in Computer Science, pages 609–626. Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642-19050-6 22

[14] Tobias Kolsch, Jan Zibuschka, and Kai Rannenberg, "Digital privacy. Chapter: Privacy and Identity Management Requirements: An Application Prototype Perspective," pages 735–749. Springer-Verlag, Berlin, Heidelberg, 2011

[15] M. S. Ferdous and R. Poet, "A comparative analysis of identity management systems," in Proc. 2012 International Conference on High Performance Computing and Simulation , 2012, pp. 454-461.

[16] F. Corella and K. Lewison, "Privacy postures of authentication technologies," in The Internet Identity Workshop, ser. IIW 2013, Mountain View, CA, 2013, [retrieved: September, 2015].

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

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

[19] A. Kahate, "Cryptography and network security," Tata McGraw-Hill Education, ISBN:0-07-049483-5, 2013.

[20] D. W. Chadwick and K. Fatema, "A privacy preserving authorization system for the cloud," Journal of Computer and System Sciences, vol. 78, no. 5, 2012, pp. 1359–1373.

[21] R. S´anchez, F. Almenares, P. Arias, D. D´ıaz-S´anchez, and A. Mar´ın, "Enhancing privacy and dynamic federation in idm for consumer cloud computing," Consumer Electronics, IEEE Transactions on, vol. 58, no. 1, 2012, pp. 95–103.

[22] S. Betg´e-Brezetz, G.-B. Kamga, M. Ghorbel, and M.-P. Dupont, "Privacy control in the cloud based on multilevel policy enforcement," in Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on. IEEE, 2012, pp. 167–169.

[23] J. Werner, C. M. Westphall, R. Weingartner, G. A. Geronimo, and C. B. Westphall, "An approach to idm with privacy in the cloud," in Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, Oct 2015, pp. 168–175.

[24] L. M. Bodnar, C. M. Westphall, J. Werner, and C. B. Westphall, "Towards privacy in identity management dynamic federations," in Networks (ICN), The Fourteenth International Conference on. Lisbon, Portugal: IARIA, February 2016, pp. 40–45.

[25] R. Weing¨artner and C. M. Westphall, "Enhancing privacy on identity providers," in SECURWARE 2014, Portugal, Nov 2014, pp. 82–88.

[26] Jorge Werner_, Carla Merkle Westphall, A Model for Identity Management with Privacy in the Cloud, 2016 IEEE Symposium on Computers and Communication (ISCC), 978-1-5090-0679-3/16/$31.00 ©2016 IEEE

محمد علی دوستاری در سال ۱۳۵۴ وارد دانشکده مهندسی دانشگاه شیراز شد و در رشته مهندسی کامپیوتر به تحصیل پرداخت. از سال ۱۳۶۶ الی ۱۳۷۲ با اخذ بورسیه دولتی ژاپن جهت گذراندن یک دوره پژوهشی، دوره کارشناسی ارشد و دکترا به کشور ژاپن عزیمت کرد و در دانشگاه صنعتی کیوتو در زمینه الکترونیک و اطلاعات به تحصیل پرداخت. ایشان پس از بازگشت از تحصیل، در گروه مهندسی کامپیوتر دانشکده فنی و مهندسی دانشگاه شاهد همکاری خود را با آن دانشگاه آغاز کرد. در حال حاضر تمرکز

پژوهش‌های ایشان در زمینه امنیت اطلاعات، کارت هوشمند، زیرساخت کلید عمومی، شناسایی هویت و بیومتریک است.

محمد خدیوی کاشانی مدرک کارشناسی خود را در رشته مهندسی کامپیوتر-نرم‌افزار از دانشگاه صنعتی قم در سال ۱۳۹۳ و مقطع کارشناسی ارشد را در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات در دانشگاه شاهد تهران در سال ۱۳۹۵ اخذ کرده است. از جمله زمینه‌های پژوهشی مورد علاقهٔ وی رمزنگاری، دولت الکترونیک، امنیت و حریم خصوصی است.