Supreme National Defense University Quarterly Journal of Defense Logistics and Technology

https://amfad.sndu.ac.ir E-ISSN: 2980-8073

Vol. 8, No. 3, Issue. 27, Autumn 2025 **Received:** 2024/12/05 **Accepted:** 2025/01/21

Research paper

A Method for Cyber Identity Discovery of Users in the Islamic Republic of Iran

Mostafa Saeedi
PhD Student in Strategic Cyber Management (Security Orientation), Department of Cyber Management, Faculty of National Security, Supreme National Defense University, Tehran, Iran
Email: mostafa.saeedi@chmail.ir
Nasibollah Dousti Motlagh
Assistant Professor, Department of Cyber Management, Faculty of National Security, Supreme National Defense University, Tehran, Iran
Email: dousti@sndu.ac.ir
Hatef Rasouli
Postdoctoral Researcher, Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran
Email: rasouli@borhan.ir
Ebrahim Kolivand
Assistant Professor, Faculty of Engineering, University of Information and National Security, Tehran, Iran
Email: kolivand@gmail.com

Abstract
The increasing penetration of cyberspace usage in the country and the widespread use of foreign services have led to greater anonymity for users within cyberspace. In recent years, governmental requests for service providers, such as messaging apps and social networks, to provide identity information of Iranian users for cyberspace management have not yielded results. Consequently, pursuing legal action against cybercriminal activities in Iran has become extremely challenging. Identifying and uncovering the identities of users in cyberspace is therefore crucial. Blocking access to Iranian users during critical situations is either impossible or entails significant material and moral costs if the identities of individuals disrupting public order are unknown. Hence, the solution lies in discovering methods to reveal the cyber identities of Iranian users. Since users' traces exist across various layers of cyberspace, combining, integrating, and enriching these traces over time can lead to the desired outcome: cyber identity discovery. A review of existing research indicates that no study precisely matches the scope of this article, though related studies were utilized. This article, derived from the PhD dissertation titled "Providing an Integrated Cyber Identity Management Model for Users in the Islamic Republic of Iran", first presents a practical definition of the cyber border and then introduces a model offering a method for discovering users' cyber identities.

Keywords: Identity, Cyber Identity, Identity Discovery, Identity Management, Users' Cyber Identity

سال هشتم، شماره سوم (پیاپی ۲۷)، پاییز ۱۴۰۴، صص. ۲۱۵- ۲۵۰
تاریخ دریافت: ۱۴۰۳/۰۹/۱۵ ـ تاریخ پذیرش: ۱۴۰۳/۱۱/۰۲

مقاله پژوهشی

ارائه روشی برای کشف هویت سایبری کاربران جمهوری اسلامی ایران

مصطفی سعیدی
دانشجوی دکتری مدیریت راهبردی فضای سایبر (گرایش امنیت)، گروه مدیریت سایبر، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران
Email: mostafa.saeedi@chmail.ir

نصیب‌الله دوستی مطلق
استادیار گروه مدیریت سایبر، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران
Email: dousti@sndu.ac.ir

هاتف رسولی
پسادکتری دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران
Email: rasouli@borhan.ir

ابراهیم کولیوند
استادیار دانشکده فنی، دانشگاه اطلاعات و امنیت ملی، تهران، ایران
Email: kolivand@gmail.com

چکیده

افزایش ضریب نفوذ استفاده از فضای مجازی در کشور و استفاده از خدمات خارجی متنوع در این بستر باعث افزایش گمنامی کاربران در فضای سایبر شده است. طی سال‌های گذشته، درخواست مسئولان کشورمان از صاحبان ارائه خدمات نظیر پیام‌رسان‌ها و شبکه‌های اجتماعی برای ارائه اطلاعات هویتی کاربران ایرانی به‌منظور مدیریت فضای سایبر به نتیجه نرسیده است. به این سبب، پیگیری قضایی فعالیت‌های مجرمانه در فضای سایبر ج. ا. ایران بسیار دشوار شده است. شناسایی و کشف هویت کاربران در فضای سایبر از اهمیت زیادی برخوردار است و مسدودسازی دسترسی کاربران ایرانی، در مواقع بحرانی به دلیل عدم شناسایی هویت برهم‌زنندگان نظم عمومی یا امکان‌پذیر نیست و یا با هزینه‌های مادی و معنوی بسیاری همراه خواهد بود. بنابراین، چاره کار در یافتن راهی برای کشف هویت کاربران ایرانی در فضای سایبر است. با توجه به این‌که ردپای کاربران در لایه‌های مختلف فضای سایبر، در دسترس است، بنابراین می‌توان با کنار هم قرار دادن ردپاهای مختلف و یکپارچه کردن آن‌ها و غنی‌سازی آن در طول زمان، به نتیجه مطلوب که همان کشف هویت سایبری کاربران است، دست یافت. با کنکاش در پژوهش‌های صورت گرفته، تحقیقی با عنوان این مقاله یافت نشد؛ اما تحقیقاتی به موضوع این نوشتار نزدیک است که از آن‌ها استفاده شده است. در این مقاله، که برگرفته از رساله دکتری با عنوان: «ارائه الگوی مدیریت یکپارچه هویت سایبری کاربران برای جمهوری اسلامی ایران» است، ابتدا تعریف کاربردی برای مرز سایبری ارائه شده است و سپس با ارائه الگویی، روشی برای کشف هویت سایبری کاربران ارائه شده است.

کلیدواژه‌ها: هویت، هویت سایبری، کشف هویت، مدیریت هویت، هویت سایبری کاربران

20.1001.1.28212606.1404.8.3.7.6 https://amfad.sndu.ac.ir/ E-ISSN: 2980-8073

مقدمه

فضای سایبر از زمان ایجاد، با هدف کمک به ایجاد جامعه جهانی طراحی گردیده است. این نوع طراحی باعث شده حاکمیت کشورها به خطر افتاده و حکمرانی‌ها خدشه‌دار شوند. اداره کردن این جامعه جهانی بزرگ با توجه به ذائقه‌های متفاوت و تنوع فرهنگ‌ها، نیازمند شناسنامه‌دار کردن بهره‌برداران آن است. فضای سایبر دارای این قابلیت است که هویت‌های جدیدی علاوه بر هویت فیزیکی برای افراد قائل می‌شود. با گسترش فناوری اطلاعات و ارتباطات، هر روز بر ابعاد این هویت‌های جدید اضافه می‌شود. هویت سایبری می‌تواند هر چیزی مثل نام شناسه ایمیل، شماره کارت و یا وب‌سایت یک نفر باشد. این هویت چیزی است که تعریف و توصیف منحصربه‌فرد یک کاربر را تشکیل داده و در این خصوص ارتباط بین هویت واقعی و هویت سایبری لازم و ضروری است.

یکی از مظاهر مدیریت فضای سایبر، راه‌اندازی خدمات فضای سایبر توسط کشورهای غربی و بهره‌برداری سایرین از خدمات ارائه‌شده توسط ایشان است. گرچه در ابتدا مسئله هویت کاربران از چالش‌های به وجود آورندگان اینترنت بود؛ اما به‌مرور زمان با اتخاذ تدابیری توانستند به شناسایی کاربران خود دست پیدا کنند. این امر با وابسته کردن دریافت خدمات به سامانه‌های دارای هویت (مانند شبکه تلفن همراه) ممکن گردید.

روش پیش‌گرفته شده، برای کنترل و حکمرانی در فضای سایبر در طی چندساله گذشته باعث گردیده مرزهای کشورها درهم شکسته شود و احراز هویت و اعطای دسترسی توسط شرکت‌هایی نظیر گوگل و مایکروسافت انجام شود. هم‌اکنون بسیاری از سرویس‌دهنده‌های خدمات در فضای سایبر، نظیر فیس‌بوک، سامانه مستقل احراز هویت کاربران راه‌اندازی نمی‌کنند، بلکه از سیستم احراز هویت به‌واسطه ایمیل استفاده می‌کنند. با توجه به فراگیر بودن استفاده از ایمیل گوگل، اکثر کاربران از طریق گوگل اصالت‌سنجی می‌شوند؛ وقتی تعداد سرویس‌های بهره‌مند از خدمات احراز هویت، افزایش یابد در واقع این گوگل است که بر هویت کاربران و دسترسی‌های آنان مدیریت و نظارت می‌کند. با ظهور سیستم‌عامل اندروید و فراگیرشدن آن در اغلب تلفن‌های همراه هوشمند و وابستگی شدید این سیستم‌عامل به

سرویس‌ها و خدمات گوگل، اتصال گوشی تلفن همراه به اینترنت و احراز هویت آن توسط گوگل برای خدماتی نظیر گوگل پلی، دریایی از اطلاعات را که در حکمرانی استفاده می‌شود، در اختیار این شرکت قرار داده است. با راهبرد کشور آمریکا و فراگیر شدنِ فناوری‌هایی نظیر رایانش ابری و کنسول‌های دسترسی سبک (نظیر تین کلاینت)، در آینده‌ای نه‌چندان دور برای دسترسی به رایانه شخصی و دسترسی به داده‌های ذخیره شده، باید از شرکت‌هایی نظیر گوگل اجازه بگیریم.

با توجه به مطالب بیان شده، مدیریت فضای سایبر و فائق آمدن بر مشکلات آن، بدون کشف هویت کاربران، دور از دسترس است. اگر براساس تعریف مرکز ملی فضای مجازی، برای فضای سایبر ۴ لایه افقی فرض کنیم، کاربران فضای سایبر هنگام استفاده از این فضا، در این لایه‌ها ردپاهایی از خود ثبت می‌نمایند و به دلیل اینکه ردپای کاربران در لایه‌های مختلف فضای سایبر، در دسترس است، بنابراین می‌توان با کنار هم قرار دادن ردپاهای مختلف و یکپارچه کردن آن‌ها، به نتیجه مطلوب که همان کشف هویت کاربران است، دست یافت. ردپاهای کاربران در لایه‌های مختلف فضای سایبر، همانند قطعات پازل، باعث می‌شود که تصویری شفاف از هویت سایبری کاربران ترسیم شود.

اهمیت:

- شرایط حاکم بر فضای مجازی کشور و نبود بارقه امید برای بهبود شرایط، مدیریت فضای مجازی و در نتیجه حکمرانی را با چالش مواجه کرده است؛
- شرط لازم برای مدیریت، احراز و کشف هویت سایبری و جلوگیری از گمنامی است؛
- اعمال مدیریت چه با رویکرد سلبی و چه با رویکرد ایجابی نیازمند کشف و احراز هویت است؛
- با توجه به امکانات موجود، کشف هویت سایبری کاربران دور از دسترس نیست.

ضرورت:

- نبود امکان کشف و احراز هویت سایبری، باعث می‌گردد که اعمال مجرمانه در این فضا افزایش یابد و حکمرانی خدشه‌دار شود؛
- عدم یکپارچگی در کارهای انجام شده در حوزه هویت سایبری کاربران، باعث کاهش تأثیر زحمات کشیده شده و اثربخشی آن‌ها خواهد شد و انتخاب رویکرد سلبی در حل مسائل فضای سایبر را در پی خواهد داشت.

۱. پیشینه پژوهش

با کنکاش در پژوهش‌های صورت گرفته، تحقیقی با عنوان این مقاله یافت نشد؛ اما تحقیقاتی که به موضوع این نوشتار نزدیک است به شرح زیر است.

گودل (۲۰۱۹) یک معماری غیرمتمرکز برای هویت دیجیتال ارائه کرد. وی در مقاله خود با تمرکز بر مشکلات و محدودیت‌های روش احراز هویت متمرکز کاربران، معماری غیرمتمرکز برای احراز هویت کاربران ارائه کرد. معماری‌های فعلی برای مدیریت هویت براساس روش‌های متمرکز از بالا به پایین است که متکی به مراجع معتمد و اپراتورهای ارائه خدمات سایبری است. براساس این مقاله در فضای سایبر، باید به هر فرد اجازه داده شود تا اطلاعات شخصی خود را به روش‌های متفاوت در زمینه‌های مختلف مدیریت کند و برای این کار، هر فرد باید قادر به ایجاد چندین هویت حتی به‌صورت غیرمرتبط باشد. بنابراین، ابتدا مجموعه‌ای از محدودیت‌های اساسی تعریف می‌شود که سیستم‌های هویت دیجیتال برای حفظ و ارتقای حریم خصوصی، برآورده کنند. با در نظر گرفتن این محدودیت‌ها، یک روش غیرمتمرکز و مبتنی بر استاندارد پیشنهاد شده است. دغدغه اصلی این مقاله، ایجاد معماری غیرمتمرکز هویت دیجیتال با رعایت حفظ حریم خصوصی است (Goodell, 2019).

بندیاب و همکاران (۲۰۱۸) مدل قابل اعتماد مدیریت هویت کاربران در فضای ابری را ارائه کردند. با گسترش خدمات مبتنی بر ابر، فدراسیون مدیریت هویت (FIM) در سال‌های اخیر مورد توجه بسیاری قرار گرفته است. این یک روش امیدوارکننده برای تسهیل اشتراک

امن منابع بین شرکای همکاری در Cloud در نظر گرفته شده است. بااین‌حال، چهارچوب‌های FIM فعلی مانند OpenID, Liberty Alliance, SAML, Shibboleth و WS ـ Federation یک مدل اعتماد مناسب برای ایجاد فدراسیون پویا و چابک تعریف نمی‌کنند. ازاین‌رو، نمی‌توان آن‌ها را در محیط‌های پویا و باز مانند رایانش ابری مستقر کرد. این مقاله، با ارائه مدل اعتماد پویای جدید که نیازهای ابر را برآورده می‌کند، به این موضوع می‌پردازد. مدل پیشنهادی تئوری نقشه‌های شناختی فازی (FCM) را در مدل‌سازی و ارزیابی قابلیت اطمینان موجودیت‌های ناشناخته در سیستم‌های FIM معرفی می‌کند (Bendiab, Shiaeles & Boucherkha, 2018).

مایکل (۲۰۱۸) طی مقاله‌ای به بررسی ارتباط بین «ساماندهی هویت سایبری» و «کاهش جرائم سایبری» پرداخته است. این مقاله، ساماندهی موضوع هویت سایبری را کمک‌دهنده به حل جرائم سایبری می‌داند و ادعا دارد به دلیل این‌که موضوع هویت سایبری در خیلی از جاها، تعیین تکلیف نشده است، افزایش تعداد کاربران فضای سایبر، جرائم این حوزه را بیشتر کرده است. در این مقاله سعی شده است مبتنی بر مباحث حقوقی و جرائم سایبری، موضوع هویت سایبری هستی‌شناسی گردد و چهارچوبی محاسباتی برای کمک به حل جرائم سایبری ارائه گردد. داده‌های استفاده شده در موضوع تشخیص هویت سایبری؛ «داده‌های بیوگرافی» مانند نام، تاریخ تولد، آدرس‌ها، تحصیلات، شغل، ویژگی‌های جسمی (به‌عنوان مثال، نژاد یا رنگ مو و تاریخ مرگ)، داده‌های رفتاری (براساس فعالیت زمانی اعمال و تعاملات شخص با دیگران، محیط موجود در یک موقعیت یا سناریو، «داده‌های بیومتریک» (اثرانگشت، عنبیه چشم و ...) و «داده‌های فیزیولوژیکی» در نظر گرفته شده است (Michel, Carvalho, Crawford & Esterline, 2018).

کاراتی و همکارانش (۲۰۱۸) به موضوع احراز هویت در سامانه‌های سایبرفیزیکال پرداخته‌اند. از تلفیق فضای مجازی با فضای فیزیکی و واقعی، سامانه‌های سایبرفیزیکال پدید می‌آیند. این سامانه‌ها در «انقلاب صنعتی ۴»، بیشتر قابل لمس و احساس هستند و IoT یکی از نمونه‌های قابل تصور این‌گونه سیستم‌ها است. این مقاله احراز هویت را به‌عنوان یکی از پارامترهای اصلی تأمین امنیت در محیط‌های ابری سامانه‌های سایبرفیزیکال دیده است و

ازاین‌رو سعی دارد با پیشنهاد یک پروتکل سبک (به لحاظ مراحل کاری و زمان مورد نیاز) به بالا بردن امنیت این‌گونه محیط‌ها کمک کند (Karati, Amin, Islam & Choo, 2018).

۲. مفهوم شناسی

۲-۱. هویت

پرسش از «هویت»[1] یکی از مهم‌ترین و درعین‌حال چالش‌برانگیزترین پرسش‌ها است. این منازعه در عرصه‌های مختلف مباحث هویت مطرح است؛ این‌که، هویت چیست؟ چگونه شکل می‌گیرد؟ از چه عناصر و مؤلفه‌هایی تشکیل شده است؟ ذاتی (طبیعی) است یا عرضی (مصنوعی)؟ ثابت است یا متغیر؟ چه سطوحی دارد؟ نسبت این سطوح با یکدیگر چیست؟ و... (لطف‌آبادی، ۱۳۹۲).

کلمه «هویت» از نظر لغوی به معنی «هستی وجود، ماهیت و سرشت» و ریشه لغوی آن از واژه «هو» گرفته شده که اشاره به غایت، نهایت و کمال مطلق دارد (معین، ۱۳۷۹) و در حوزه انسانی موجب شناسایی فرد و اجتماع از دیگری می‌شود؛ یعنی مجموعه خصائل و خصوصیات که از روی آن فرد یا یک گروه اجتماعی شناخته می‌شود و از دیگران متمایز می‌گردد (تاجیک، ۱۳۸۳). این تعریف دو معنای اصلی و متناقض دارد: اولین معنای آن بیانگر تشابه مطلق است؛ این با آن مشابه است. معنای دوم آن به مفهوم تمایز است که با مرور زمان سازگاری و تداوم را فرض می‌گیرد. به‌این‌ترتیب، مفهوم هویت به‌طور هم‌زمان میان افراد و اشیا دو نسبت محتمل برقرار می‌سازد؛ از یک‌طرف شباهت و از طرف دیگر تمایز (جنکینز، ۱۳۸۱). انسان از زمانی که خود را شناخت، مسئله هویت برایش مطرح گردید (Mousavi, 2024).

«خصیصه»[2]، مشخصه متمایزکننده یک شیء است. خصیصه یک شیء به‌منظور توصیف آن استفاده می‌شود. خصیصه معمولاً به سه صورت است: «خصیصه ذاتی» که در قالب صفات فیزیکی مانند اندازه، شکل وزن و رنگ و ... برای اشیای جهان واقعی بیان می‌شود؛ «خصیصه اکتسابی» که فرد به‌واسطه شرایطی مشخص مانند اخذ مدرک مهندسی یا جایگاه شغلی دارای

1. Identity
2. Attribute

آن خصیصه می‌شود و «خصیصه انتسابی» مانند کد ملی که به فرد نسبت داده می‌شود. اشیا در فضای سایبری هم دارای خصیصه‌هایی هستند که اندازه، نوع کدگذاری، آدرس شبکه و نظایر آن را نشان می‌دهند. «خصیصه»، اسمی است که به یک موجودیت (شخص یا یک شیء) نسبت داده شده یا به‌صورت ذاتی در او وجود دارد. هر خصیصه نشان‌دهنده کلاسی از اطلاعات است که به یک موجودیت نسبت داده می‌شود و مقدار خصیصه، نمونه‌ای از کلاس اطلاعات ارائه‌شده توسط نوع خصیصه است (N, 2012) خصیصه‌ها معمولاً به‌صورت زوج «نام خصیصه» و «مقدار آن» مورد استفاده قرار می‌گیرند. خصیصه بیانگر تکه‌هایی از اطلاعات مانند نام، آدرس و تاریخ تولد است که به تأیید منحصربه‌فرد اطلاعات در مورد یک شخص یا یک شیء کمک می‌کند (Digital Transformation Agency, 2019).

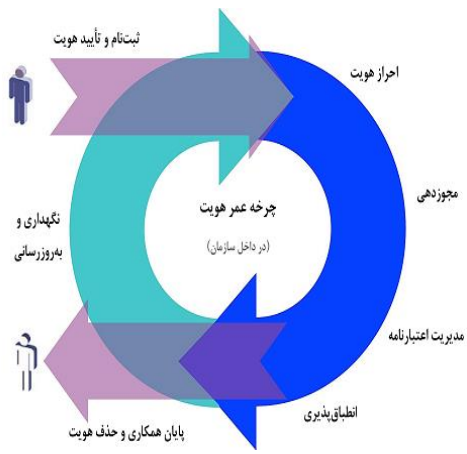
«خصیصه هویتی»[1]، یک عنصر داده قابل تشخیص (مانند نام، نام خانوادگی، تاریخ تولد و غیره) برای هر فرد یا شیء است که می‌تواند در ایجاد هویت به کار گرفته شود. خصیصه هویتی (فارغ از ذاتی یا اکتسابی یا انتسابی بودن) برای موجودیت‌های مختلف، متفاوت است. به‌عنوان مثال خصیصه هویتی یک انسان، کد ملی، اثرانگشت، تصویر عنبیه چشم است ولی در یک خودرو، شماره پلاک خودرو، شماره موتور و ... است. خصیصه‌های هویتی یا توسط تشخیص‌دهنده هویت تولید می‌شود یا براساس یک توافق به خصیصه‌های هویتی تولیدشده توسط سایرین اعتماد می‌گردد. به‌عنوان مثال هنگامی‌که ما بخواهیم شهروندان کشور خودمان را شناسایی کنیم از کد ملی که به آن‌ها ارائه‌شده است استفاده می‌کنیم و با اعتماد به سایر کشورها در تولید خصیصه هویتی گذرنامه، پذیرای اتباع سایر کشورها هستیم و آن‌ها را براساس خصیصه هویتی گذرنامه (با وجود صدور توسط سایرین) می‌شناسیم. خصیصه‌های هویتی دارای انواع مختلفی هستند و با ترکیب و در کنار هم قرار دادن آن‌ها می‌توان به احراز هویتی با اطمینان بالاتر رسید.

«احراز هویت»[2] فرایندی است که یکسان بودن هویت افراد یا موجودیت‌ها را با هویت مورد ادعای آن‌ها مورد بررسی قرار می‌دهد. احراز هویت به‌صورت متداول «ورود به حساب

1. Identity Attribute
2. Authentication

کاربری» خوانده می‌شود و با ترکیبی از نام کاربری و کلمه عبور انجام می‌شود. احراز هویت بیانگر مجوزهای کاربر در سامانه‌ها نیست. در فرایند احراز هویت، ممکن است هویت یک کاربر، اصالت یک محصول یا قابل اطمینان بودن یک برنامه تأیید شود (Harvard, 2014).

پایگاه داده هویت شامل مجموعه‌ای ساختاریافته از اطلاعات است (InCommon, 2017). برای ایجاد چنین پایگاه داده‌ای و بالا بردن دقت آن در احراز هویت، دسترسی به بانک‌های اطلاعاتی متعدد هویتی مورد نیاز است. «چرخه عمر هویت»[1]، بیانگر مجموعه‌ای از فرایندهایی است که از زمان ایجاد یک هویت تا زمان حذف، تعلیق یا غیرفعال‌سازی آن مورد استفاده قرار می‌گیرد. شکل (۱)، چرخه عمر هویت را نشان می‌دهد. چرخه عمر هویت یک فرایند مستمر و دارای دور است و توقفی برای آن تا زمان حذف هویت وجود ندارد.



شکل ۱: چرخه عمر هویت (برهان، ۱۴۰۲)

به مجموعه‌ای از قواعد تعریف شده که در هنگام رسیدگی خودکار به رویدادهای معمول مربوط به یک موجودیت، می‌تواند عملیات مناسب را مشخص کند، «قواعد چرخه عمر» می‌گویند. برای مثال می‌توان به تعلیق یک حساب کاربری اشاره کرد که برای مدت مشخصی بدون استفاده بوده است (Axel, Werner, & Andy, 2009).

1. Identity Lifecycle

«هویت هم‌پیمان شده»[1] توافق‌نامه‌ای است که بین چندین سازمان منعقد می‌شود و به مشترکین اجازه می‌دهد تا از داده‌های هویتی یکسانی، برای دسترسی به شبکه‌های تمام سازمان‌ها استفاده کنند (Rouse, 2017) . مدیریت هویت هم‌پیمان شده معرف ابزارها و استانداردهایی است که به کاربر اجازه می‌دهند تا از اطلاعات هویتی یکسان در چندین شرکت یا چند دامنه مختلف استفاده نماید (Janice, 2007) .

«هماهنگ‌سازی هویت»[2]، بیانگر ایجاد ارتباط مابین رکوردهای هویتی در بین سامانه‌های مختلف سازمان و یا گروه‌های هم‌پیمان است. سامانه‌های هماهنگ‌سازی هویت، خصیصه‌های هویتی را بین سیستم‌های مختلف شناسایی کرده و به‌طور خودکار تغییرات را از یک سیستم به سیستم دیگر اعمال می‌کنند. هماهنگ‌سازی هویت معمولاً بدون وجود یک رابط کاربری انجام می‌شود؛ بدین معنا که جریان داده از یک سیستم به یک یا چند سیستم دیگر، بدون دخالت کاربر صورت می‌گیرد (Hitachi ID System, 2020) .

به تحلیل متون ارائه‌شده در رسانه دیجیتال یا فیزیکی که به ارزیابی متون در بافتار تاریخی و فرهنگی و مشخص کردن ویژگی‌های معنایی و نحوی آن‌ها کمک می‌کند، «تحلیل بافتاری» می‌گویند. تحلیل بافتاری متون می‌تواند به شناسایی ساختارها، ویژگی‌ها و ارتباطات میان آن‌ها و تشخیص هویت نویسنده منجر شود. به‌عبارت‌دیگر، تحلیل بافتاری نوعی روش مطالعه متن و بافتار سیاسی، اجتماعی و فرهنگی آن است که معمولاً توسط باستان‌شناسان، منتقدان هنری یا جامعه‌شناسان مورد استفاده قرار می‌گیرد (Cookiebot, 2020) .

«مدیریت هویت آگاه به بافتار»[3]، رویکردی در مدیریت هویت است که از اطلاعات بافتاری بلادرنگ و پویای به دست آمده از داده‌های محیطی، مکان‌ها، حسگرها، ترجیحات کاربر، پروفایل، ویژگی‌های رفتاری برای توسعه روش‌های احراز هویت و مجوزدهی استفاده می‌کند. «مدیریت هویت آگاه به بافتار» به سازمان‌ها اجازه می‌دهد تا کاربران متقاضی دسترسی را با دقت بیشتری شناسایی کنند(Atis, 2018) .

1. Federated Identity
2. Identity Synchronization
3. Context-Aware Identity Management

۲-۲. فضای سایبر

«فضای سایبر» یک مفهوم بین‌المللی است که فناوری دیجیتال گسترده و به‌هم‌پیوسته را توصیف می‌کند. این اصطلاح از داستان‌های علمی و هنری وارد فرهنگ عامه شده است. این واژه در دهه ۱۹۹۰ میلادی، که استفاده از اینترنت، شبکه و ارتباطات دیجیتال همه به طرز چشمگیری در حال رشد بود، رواج پیدا کرد و اصطلاح «فضای سایبر» توانست بیانگر ایده‌ها و پدیده‌های جدیدی باشد که در حال ظهور بودند.

فضای سایبر، در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی.» البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص در آن، زنده و مستقیم روی می‌دهد.» قید «واقعی»، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیرواقعی بودن آن است؛ چراکه در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد. ضمن این‌که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال بر خط، نباشد ولی زنده و واقعی و مستقیم است (طارمی، ۱۳۸۸).

فضای سایبر، دارای مسائل مختلف و متنوعی است و تحلیلگران و متخصصین این حوزه، برای فائق آمدن بر چالش‌های آن سعی نموده‌اند فضای سایبر را به علت گستردگی و بزرگی و غیرقابل‌کنترل بودن هیبت یکپارچه آن، به بخش‌هایی افراز نمایند. به‌عنوان نمونه، برای قانون‌گذاری و نظم‌بخشی فضای سایبر، اتحادیه بین‌المللی ارتباطات راه دور(ITU) ، مدلی پنج‌لایه از فضای سایبر ارائه داده است. این مدل دارای ارکان و شاخص‌های همکاری، ظرفیت‌سازی، سازمانی، فنی و قانونی است. مدل امنیت سایبر ارائه‌شده توسط یوچای بنکلر، یک مدل سه‌لایه است که شامل بخش‌های فیزیکی، منطقی و اجتماعی است و نشان‌دهنده این است که اگر بخواهیم قانون‌گذاری در فضای سایبر برای ایجاد امنیت داشته باشیم، بایستی

از این سه منظر فضای سایبر را تقسیم‌بندی نماییم.

مدل‌های قانون‌گذاری فضای سایبر، با توجه به ماهیتشان و علت به وجود آمدنشان و تفاوت با هدف این پژوهش، مورد استفاده این تحقیق نیستند. مرکز ملی فضای مجازی، نیز مدلی برای فضای مجازی ارائه کرده است. بنابراین، محقق مدل مرکز ملی فضای مجازی را انتخاب و الگوی مدیریت یکپارچه را براساس آن طراحی کرده است.

این مدل که در شکل (۲)، نشان داده شده است، دارای چهار لایه افقی و دو لایه عمودی در کنار آن‌ها است.

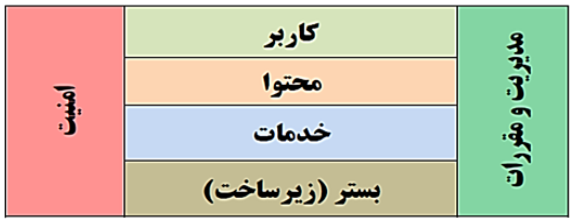
❖ لایه‌های افقی

۱. زیرساخت: در این لایه کلیه سخت‌افزارهای ارتباطی، ذخیره‌سازی و پردازشی که باعث می‌شود کاربر به‌وسیله آن به وارد فضای سایبر شود، اطلاق می‌گردد.
۲. خدمات: در این لایه، کلیه خدمات ارائه‌شده به کاربر قرار دارد. انواع برنامه‌های فضای مجازی شامل شبکه‌های اجتماعی، پیام‌رسان‌ها، بانکداری و ... در این لایه تعریف می‌شوند.
۳. داده: عبارت است از، اطلاعات مرتبط با کاربر که هم می‌تواند توسط خدمات ارائه‌شده در فضایی در سایبر ذخیره شود و هم می‌تواند به‌صورت مستقل در قالب خدماتی مانند خدمات ابری ذخیره گردد.
۴. کاربر: کاربر و ویژگی‌های آن به‌عنوان انسان، یکی از لایه‌های فضای سایبر در نظر گرفته شده است.

❖ لایه‌های عمودی

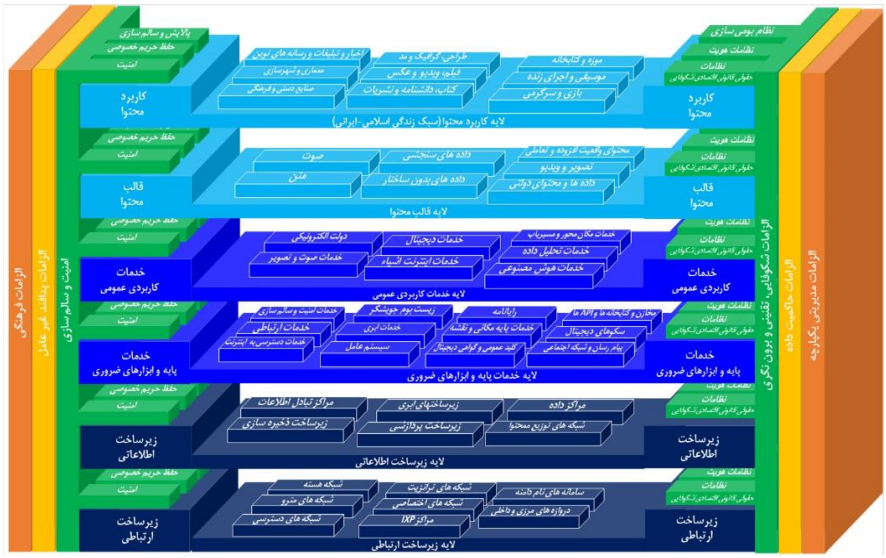
۱. مدیریت و مقررات: در این لایه مدیریت و مقررات، فضای مجازی قرار دارد. طبق این تعریف، مدیریت و مقررات، در تمامی لایه‌های فضای سایبر قرار دارد و عنوان این رساله، در این لایه قرار می‌گیرد.
۲. امنیت: لایه امنیت به‌صورت عمودی قرار دارد و در تمامی لایه‌های افقی مفهوم امنیت قرار دارد.

با توجه این‌که این پژوهش با هدف ارائه الگویی برای مدیریت یکپارچه هویت سایبری کاربران در جمهوری اسلامی ایران انجام شده است، بنابراین مدل و الگوی ارائه‌شده توسط مرکز ملی فضای مجازی مورد استناد و تعریف آن است.



شکل ۲: مدل مرکز ملی فضای مجازی برای فضای سایبر

معماری دیگری نیز توسط وزارت ارتباطات در سال ۹۸، تحت عنوان معماری شبکه ملی اطلاعات، به شورای عالی فضای مجازی ارائه گردیده است و در اواخر سال ۱۳۹۸، به تصویب این شورا رسیده است. شاید در وهله اول این گمانه به ذهن برسد که معماری مصوب سال ۱۳۹۸، به‌روزتر است و بایستی در این پژوهش مورد استناد قرار می‌گرفت. در پاسخ به این سؤال باید بیان شود که شبکه ملی اطلاعات، بخشی از فضای سایبر جمهوری اسلامی ایران است و در اصطلاح یک تخصیص از یک عام کلی است. اگر بخواهیم دقیق‌تر موضوع را بررسی نماییم، همان‌گونه که در شکل (۳)، نشان داده شده است، شبکه ملی اطلاعات، در واقع نمایانگر، سه لایه «زیرساخت»، «خدمات» و «داده» (به‌جز کاربر)، مدل مرجع شورای عالی فضای مجازی، در داخل کشور است. مدل مرجع شورای عالی فضای مجازی، اشاره‌ای به داخلی یا خارجی بودن لایه‌ها ندارد.



شکل ۳: لایه‌های شبکه ملی اطلاعات

با توجه به این‌که بعد از آخرین تعریف ارائه‌شده برای فضای سایبر کشور در چهار لایه افقی و دولایه عمودی (شکل ۲)، تاکنون تعریف جدیدی ارائه نشده است و به دلیل این‌که الگوی ارائه‌شده در این پژوهش قرار است برای فضای سایبری کشور عزیزمان ایران باشد، بنابراین تعریف پایه برای ارائه «الگوی مدیریت یکپارچه هویت سایبری کاربران برای جمهوری اسلامی ایران»، تعریف ارائه‌شده توسط مرکز ملی فضای ملی جمهوری اسلامی ایران است و برای ارائه الگوی مدیریت، شرایط فعلی حاکم بر فضای سایبری کشور به‌عنوان مبنا در نظر گرفته شده است و پیش‌فرضی بر الگوی ارائه‌شده مترتب نیست.

۲-۳. هویت سایبری

از نظر معنایی در تعاریف ارائه شده، «هویت سایبری» معادل «هویت دیجیتال» در نظر گرفته می‌شود. هویت دیجیتال، مجموعه‌ای از خصیصه‌های الکترونیکی مرتبط با یک موجودیت است که می‌تواند آن را به‌صورت منحصربه‌فرد در یک تراکنش برخط نمایش دهد (White House, 2010). هویت دیجیتال ترکیبی از گواهی‌ها و خصیصه‌های توسعه داده شده و ثبت‌شده

به شکل الکترونیکی از یک شخصیت قابل شناسایی به‌صورت منحصربه‌فرد است که قابل اتصال به یک فرد در جهان واقعی است (IIF, 2019). هویت دیجیتال معرف یک موجودیت در فضای مجازی است که به‌صورت آنلاین و با استفاده از ثبت الکترونیکی خصیصه‌های موجود در اسناد هویتی ایجاد می‌شود، بدون این‌که نیازی به دفاتر دولتی باشد. هویت دیجیتال می‌تواند به دفعات برای دسترسی امن به طیف گسترده‌ای از خدمات دولتی و غیردولتی مورد استفاده قرار گیرد (Digital Transformation Agency, 2019).

همه کاربران می‌دانند که چه کسی هستند؛ اما وقتی صحبت از دیگران می‌شود، آن‌ها به‌نوعی از پارامترها نیاز دارند تا همدیگر را شناسایی کنند. این می‌تواند، شامل نام یا چهره یا هر نوع اطلاعات دیگر باشد. در حقیقت، این اطلاعات توسط منابع دیگری در اختیار آن‌ها قرار می‌گیرد. بنابراین وقتی صحبت از هویت دیجیتالی می‌شود، هر نوع اطلاعات گسسته‌ای که به کاربران متصل می‌شود، از خصیصه‌های هویت است. هیچ محدودیتی در تعداد خصیصه‌های قابل تعریف وجود ندارد. به‌عنوان‌مثال، بسیاری از خصیصه‌های هویت دیجیتالی بیومتریک مانند چهره، جنسیت، اثرانگشت یا الگوهای صوتی وجود دارد. همچنین خصیصه‌های هویت دیجیتالی دیگر مانند نام، تاریخ تولد وضعیت تأهل یا آدرس فعلی نیز می‌تواند کاربران را از نظر اجتماعی تعریف کند. بنابراین، هویت دیجیتالی نوعی قالب هویت است که در آن هویت فرد از طریق ابزارهای دیجیتال نشان داده می‌شود. علاوه بر این، هویت می‌تواند تجزیه‌ناپذیر یا تجمعی نیز باشد. سطوح مختلفی از هویت دیجیتالی وجود دارد و هرکدام دیدگاه متفاوتی را ارائه می‌دهند.

هویت دیجیتال، صرفاً از لایه‌های زیرساخت و خدمات بهره می‌برد؛ اما در تعریف عملیاتی ارائه‌شده در این پژوهش، هویت سایبری، نه‌تنها تمامی لایه‌های چهارگانه فضای سایبر (زیرساخت، خدمات، داده و کاربر) را در برمی‌گیرد، بلکه از داده‌های موجود در فضای واقعی نیز استفاده می‌کند. به‌عنوان نمونه، هویت سایبری یک دانش‌آموز که در ایام کرونا، از فضای سایبر برای تحصیل استفاده می‌نماید، شامل اطلاعات سیم‌کارت و کنسول دسترسی در لایه زیرساخت، اطلاعات هویتی در لایه خدمات (سامانه شاد)، داده‌های انتقال داده شده

به‌عنوان تکلیف از طریق سامانه شاد، پیام‌رسان‌های خارجی یا حتی خدمت ایمیل در لایه داده و اطلاعات مربوط به بیومتریک در لایه کاربر است. سایر اطلاعات تحصیلی، مکانی، هویت پدر و مادر، دوستان و رفیقان و اطلاعات مهارتی در فضای واقعی، منجر به شکل‌گیری هویت سایبری خواهد شد. هویت سایبری در مثال بیان شده در مورد کاربران بیان شده است، درصورتی‌که هویت سایبری شامل هر آنچه در فضای سایبر است (اعم از انسان و غیر انسان) می‌شود.

۳. تجربیات کشف و احراز هویت کاربران

۳-۱. تجربه جهانی

روسیه: روسیه در فضای سایبری به دنبال تضعیف هژمونی ایالات متحده آمریکا است و نظام هویت سایبری، یکی از الزامات تحقق آن است. این کشور، برای سامان دادن هویت دیجیتال خود، قصد دارد تا پایان سال ۲۰۲۴، از سامانه هویت دیجیتال خود بهره‌برداری کند. در این سامانه قرار است، بهره‌مندی از خدمات شهروندی از بستر و زیرساخت سامانه احراز هویت انجام شود. این پروژه قرار است، ۱۲ پروژه ملی روسیه در موضوعات جمعیت‌شناسی، فرهنگ، بهداشت و درمان، آموزش، مسکن و محیط شهری، زیرساخت‌های جاده‌ای، بهره‌وری نیروی کار و حمایت از اشتغال، علم، اقتصاد دیجیتال، تجارت کوچک و متوسط، همکاری بین‌المللی و صادرات را در قالب اقتصاد دیجیتال سامان دهد (tass, 2021).

چین: در چین سامانه متمرکز و جامع برای احراز هویت کاربران در فضای مجازی وجود ندارد و از سامانه احراز هویت مبتنی بر اطلاعات بیومتریک که توسط یکی از شرکت‌های وابسته به گروه علی‌بابا تولید شده است و مورد تأیید وزارت امنیت دولت است استفاده می‌شود. این سامانه در خدمات مالی و عمومی کشور چین به کار می‌رود ولی دولت این کشور قرار است کارت شناسایی دیجیتال را برای بهره‌برداری در سراسر چین معرفی ارائه نماید. نخست‌وزیر چین، اعلام کرده است که قرار است شناسه سراسری دیجیتال براساس کارت شناسایی ملی، امکانی را فراهم آورد تا شهروندان کشور چین به‌راحتی به خدمات مهم

آنلاین دسترسی داشته باشند. این امکان برای شهروندانی که دور از شهرهای بزرگ و در روستاها و مناطق کم برخوردار زندگی می‌کنند از اهمیت ویژه‌ای برخوردار است. استفاده از سامانه جامع احراز هویت، برای برقراری عدالت در توزیع منابع، در کشور چین به‌عنوان پرجمعیت‌ترین کشور دنیا از اهمیت خاصی برخوردار است.

کانادا: وجود ساختار هویت سایبری و دیجیتال برای کشور کانادا، به‌عنوان یک الزام، توسط شورای تعیین هویت و احراز هویت دیجیتال کانادا در سال ۲۰۱۵ اعلام گردید. خطر عقب افتادن کانادا در عرصه اقتصاد دیجیتال، به‌واسطه فقدان یک نظام تعیین هویت و احراز هویت دیجیتالی قابل اتکا، یکی از دلایل الزام کشور کانادا در موضوع هویت دیجیتال بیان شده است. در این سند بر راهکار کانادایی تأکید شده است؛ منظور از راهکار کانادایی راهکاری است که در درون کانادا و برای کانادا تدوین شده است.

همچنین مزیت‌های راهکار بومی در احراز هویت سایبری، در کشور کانادا، مورد توجه قرار گرفته است. روش پیش گرفته شده توسط دولت کانادا برای ساماندهی وضعیت هویت دیجیتال، ایجاد زیرساخت فدرال برای مشارکت، بازیگران دولتی و خصوصی به‌منظور احراز هویت دیجیتال است. در این حالت به‌منظور دسترسی به خدمات عمومی از مدل «اعتبار خود را بیاورید» استفاده شده که کاربران را قادر می‌سازد از اعتبارهای هویتی خود که قبلاً احراز کرده‌اند، استفاده نمایند(DIACC, 2015) .

کانادا برای تدوین اکوسیستم هویت خود از دو دسته اصول و الزامات بنیادین تبعیت می‌کند:

- ❖ هفت الزام جهانی برای اکوسیستم هویت دیجیتال:

۱. قابل اتکا، امن و گسترش‌پذیر باشد؛
۲. تقویت‌کننده و حفاظت‌کننده حریم خصوصی باشد؛
۳. جامع و شفاف باشد؛
۴. نیازهای گسترده ذی‌نفعان را برآورده سازد؛
۵. میزان جمع‌آوری داده‌ها را به حداقل برساند؛

۶. بر مبنای آگاهی و رضایت باشد؛
۷. راحت و آسان باشد؛

❖ چهار الزام مضاعف کانادا برای اکوسیستم هویت دیجیتال:

۱. بر مبنای پروتکل‌های مبتنی بر استانداردها بازساخته شود؛
۲. با استانداردهای بین‌المللی تعامل‌پذیر باشد؛
۳. از نظر هزینه مقرون‌به‌صرفه باشد و نسبت به نیروهای رقابتی بازار ممانعتی نداشته باشد؛
۴. به‌صورت مستقل ارزیابی و ممیزی گردد و مشمول اعمال قوانین گردد.

استونی: شهروندان و ساکنین کشور استونی، ملزم به داشتن کارت هویت الکترونیک هستند. این کارت هویت به‌عنوان مدرک شناسایی در محیط فیزیکی و دیجیتال است. سامانه هویت دیجیتال معرفی شده در سال ۲۰۰۲، نزدیک به ۹۴ درصد شهروندان کشور استونی را پوشش می‌دهد و با سطح پذیرش ۹۰ درصدی، بیش از ۹۴۰ موسسه و بخش خصوصی و دولتی به آن متصل هستند (White, et al., 2019).

براساس اطلاعات (ITU, Digital Identity Roadmap Guide, 2018)، کشور استونی، پیشرفته‌ترین سامانه هویت دیجیتال در جهان را داراست. مجموعه‌ای از احرازهای هویت از طریق، کارت، موبایل و سامانه هویت هوشمند در این کشور استفاده می‌شوند. از هویت دیجیتال در احراز هویت برای دسترسی به حساب‌های بانکی، امضای دیجیتال، دسترسی به خدمات دولتی، نظیر پزشکی و امور مالیاتی استفاده می‌گردد (ISA2, Digital Public Administration factsheet Estonia, 2020). در استونی طرح متمرکز تحت نظارت دولت (از سال ۲۰۰۲) با نام طرح e-Estonia با مشارکت بخش خصوصی راه‌اندازی شد و چندین اعتبارنامه و روش‌های احراز هویت را به شهروندان و مشاغل مختلف ارائه می‌دهد، از کارت هوشمند ملی هویت استاندارد گرفته تا برنامه هویت تلفن همراه مبتنی بر SIM و هویت هوشمند مبتنی بر PKI. در سال ۲۰۲۰ حدود ۹۹ درصد خدمات دولتی آن آنلاین بوده که حتی رأی‌گیری الکترونیکی را هم شامل می‌شده است. ابزارهای استفاده شده در این طرح کارت هوشمند، شناسه موبایل مبتنی بر سیم‌کارت،

شناسه موبایل مبتنی بر موبایل e-Identity APP است (Onepoint & AIS, 2021)

استرالیا: دولت استرالیا، به‌منظور حمایت از رشد اقتصادی و توسعه تجارت الکترونیک در سال ۲۰۱۴، ساختار هویت دیجیتال قابل اعتماد را ارائه کرد. این چهارچوب با همکاری سازمان‌های دولتی و خصوصی درحال‌توسعه است و در حال حاضر ۸/۱ میلیون استرالیایی برای دسترسی به ۷۰ خدمت دولتی از آن استفاده می‌نمایند. استفاده از سامانه ملی هویت دیجیتال در استرالیا، اختیاری است و داده‌های حداقلی از کاربران در خود نگهداری می‌نماید. استفاده از این سامانه ارزش‌افزوده‌ای را برای کاربران در استفاده از خدمات دولتی فراهم می‌آورد (Branson, 2020).

در کشور استرالیا، ایجاد یک هویت دیجیتال و استفاده از آن در صورت ظاهر، اختیاری است؛ ولی برای استفاده از خدمات دولتی بایستی از هویت دیجیتال بهره برد. مدیریت هویت به‌صورت فدرالی است و عملیات زیر در آن انجام می‌شود:

- ارائه‌دهندگان سرویس هویت: مسئولیت ثبت، جمع‌آوری، تأیید، افشا، اصلاح و حذف اطلاعات هویت و ویژگی‌های مرتبط و ادعاشده را بر عهده دارند؛
- ارائه‌دهندگان سرویس اعتبارنامه: عملیات ثبت، ایجاد، برقراری ارتباط بین یک هویت ادعایی و یک عامل احراز هویت خاص، پذیرش، تمدید، اصلاح، تعلیق، لغو و حذف اعتبارنامه احراز هویت را انجام می‌دهند؛
- ارائه‌دهندگان ویژگی: ویژگی‌های مربوط به عناوین، صلاحیت‌ها، روابط یا ویژگی‌های خاص افراد و نهادها را اعمال، جمع‌آوری، تأیید، افشا، اصلاح و حذف می‌نمایند؛
- تبادل هویت: تأیید اطلاعات هویت ویژگی‌ها، ادعاها و اعتبارنامه‌های احراز هویت را درخواست و نتایج تأیید را فراهم می‌کند.

انگلستان: راهبرد کشور انگلستان در حوزه ارائه خدمات حکمرانی و حکومتی، تحت عنوان «دیجیتال به‌صورت پیش‌فرض» در سال ۲۰۱۲، با تأکید بر ارائه خدمات برخط و دسترسی گسترده معرفی گردید. پیش‌نیاز تحقق چنین راهبردی، یک راه‌حل قوی برای احراز هویت

کاربران در فضای سایبر به‌صورت برخط و قابل اعتماد است. برای این منظور، پروژه GOV.UK Verify، برای احراز هویت کاربران کشور انگلستان اجرایی گردید. ارائه‌دهندگان خدمات می‌توانند خدمات خود را براساس این پروژه ارائه دهند و این امکان نیز وجود دارد که ارائه‌دهندگان سرویس احراز هویت در این پروژه به‌منظور شناسایی هویت‌ها با یکدیگر تعامل داشته باشند (ITU, Digital Identity Roadmap Guide, 2018). این پروژه شبیه یک پلتفرم است که می‌تواند در یک بستر میان ارائه‌دهندگان خدمات سایبری و مشتریان خدمات سایبری و همچنین ارائه‌دهندگان خدمات احراز هویت، تعامل برقرار نماید. معماری احراز هویت در صورت ظاهر به‌صورت فدرالی است که اجازه حضور شرکت‌های خصوصی را هم فراهم می‌نماید.

کره جنوبی: کشور کره جنوبی، در موضوعات مربوط به حکمرانی فضای مجازی، از «الگوی توسعه‌ای دولت راهبر؛ الگوی همکاری آزادانه» استفاده می‌کند، اگرچه یعنی این الگو وجود یک نظام فکری دموکراتیک را نشان می‌دهد، بااین‌حال برخی نمونه‌ها حاکی از تلاش حاکمیت برای کنترل بوده است که با اعتراضاتی از سوی جامعه مدنی همراه شده است به‌عنوان مثال، در سال ۲۰۰۸، ذی‌نفعان مجبور به اعتراض به دادگاه قانون اساسی شدند تا علیه یک سیاست دولتی یک‌جانبه برای محدود کردن ناشناس بودنِ فعالیت‌های آنلاین افراد اقدام کنند. این روش موسوم به «تأیید نام واقعی» است. تأیید نام واقعی، نیاز به ارائه اطلاعات شخصی کاربران پیش از قرار دادن اطلاعات در فضای مجازی به‌صورت آنلاین دارد. دولت کره جنوبی اعلام کرده است که مردم کره جنوبی حق دارند انتقادات خود از سیاست‌های دولت یا رهبران سیاسی را در فضای مجازی ابراز کنند مشروط به آن‌که پیش از قرار دادن نظرات «تأیید نام واقعی» (احراز هویت حقیقی) شوند و اظهارات ایشان موجب تهدید امنیت ملی و تهمت نباشد (مجدی‌زاده، ۱۳۹۸).

ایجاد سامانه ثبت هویت کاربران و الزام ایجادکنندگان خدمات دسترسی برای احراز هویت کاربران، ازجمله اقدامات کره برای مدیریت اینترنت بوده است. همچنین الزام به ثبت و احراز هویت ایجادکنندگان محتوای داخلی شامل وبگاه‌ها و میزبانی و الزام به ثبت هویت

تمامی اظهارنظر کنندگان مطالب در وبگاه‌های با تعداد مراجعه‌کنندگان بیش از ۱۰۰ هزار نفر از دیگر اقدامات برای مدیریت اینترنت در این کشور است. سیستم پالایش محتوای اینترنتی هم در کره جنوبی وجود دارد. سیستم ثبت هویت واقعی و قوانین بازدارنده در مرحله تولید و ارسال محتوا و وجود سازمان‌های تعیین‌کننده مصادیق استاندارد اطلاعات، ازجمله سازوکارهای کره برای مدیریت محتوای اینترنتی در این کشور است. به این صورت که مصادیق توسط کمیسیون استاندارد ارتباطات و کمیسیون انتخابات احصا شده و در صورت بروز مواردی مغایر قانون، به خدمات‌دهندگان اینترنتی میزبان‌ها وبلاگ‌ها برای رفع تخلف اخطار داده می‌شود و در صورت عدم توجه به اخطار اقدام لازم انجام خواهد شد.

کره جنوبی نسبت به فناوری‌های نوظهور، نظیر بلاک‌چین، متاورس و هوش مصنوعی روی خوش نشان داده است و سعی دارد با ایجاد یک زیست‌بوم هویت در بسترهای نوظهور، هویت سایبری کاربران خود را مدیریت نماید.

ایتالیا: طرح هم‌پیمانی تحت نظارت دولت ایتالیا، از سال ۲۰۱۶، اجرایی شده است در این طرح، سیستم عمومی هویت دیجیتال ایتالیا (SPID) توسط سازمان دیجیتال‌سازی ایتالیا (AgID) مدیریت می‌شود و توسط ارائه‌دهندگان هویت خصوصی معتبر تأمین مالی می‌گردد. SPID به کلیه شهروندان و مشاغل ایتالیا یک هویت دیجیتال بدون نیاز به دستگاه الکترونیکی برای دسترسی آسان به خدمات الکترونیکی خصوصی و دولتی به‌صورت رایگان ارائه می‌دهد. ابزار استفاده شده در این طرح، عدد/ نام کاربری/ گذرواژه SPID است (Onepoint & AIS, 2021).

در ایران، کارهای مختلفی برای شناسایی هویت کاربران، انجام شده است. این کارها به دو بخش «اسناد بالادستی» (هم شامل فضای واقعی و هم فضای سایبر می‌شود) و «اجرایی» تقسیم می‌گردد که به شرح ذیل معرفی می‌گردد.

اسناد بالادستی عبارتند از:

۱. قانون تجارت الکترونیکی مصوب سال ۱۳۸۲
۲. دستورالعمل شناسایی مشتریان مؤسسات مالی و اعتباری مصوب ۱۳۸۷
۳. دستورالعمل شناسایی مشتریان در بازار سرمایه مصوب ۹۰/۰۷/۱۹ که در مصوبه

ششصدوشصتمین جلسه، شناسایی مشتریان به‌صورت غیرحضوری از طریق سامانه سجام الزامی شده است.

۴. دستورالعمل رعایت مبارزه با پول‌شویی در خدمات الکترونیک بازار سرمایه مصوب ۹۰/۰۷/۱۹

۵. مصوبه جلسه سی‌وپنجم شورای عالی فضای مجازی در تاریخ ۹۵/۰۹/۲۰ که برالزام مدیریت و شناسایی هویت قابل اعتماد به‌صورت نظام یکپارچه تأکید شده است.

۶. قانون مبارزه با پول‌شویی مصوب ۹۷/۰۷/۰۳، مجلس شورای اسلامی

۷. مصوبه جلسه پنجاه‌ونهم در تاریخ ۹۸/۰۶/۰۹ با موضوع نظام هویت معتبر در فضای مجازی

۸. آیین‌نامه اجرایی ماده ۱۴ قانون مبارزه با پول‌شویی مصوب ۹۸/۰۷/۲۱، هیئت‌وزیران

۹. مصوبه کمیسیون عالی امنیت فضای مجازی کشور تاریخ ۹۹/۰۵/۲۰ با موضوع نگاشت نهادی تأمین‌کنندگان شناسه هویت معتبر

۱۰. سند الزام احراز هویت قوی مشتریان در خدمات بانکداری الکترونیکی از راه دور، مصوب ۹۹/۰۹/۱۲

اقدامات اجرایی نیز شامل موارد زیر است:

۱. سامانه احراز هویت الکترونیکی موسوم به سجام (سامانه جامع ثبت‌احوال اطلاعات مشتریان) ایجاد شد.

۲. سامانه هویت و دسترسی ایرانیان (هدا) در سال ۱۳۹۳، توسط سازمان ثبت‌احوال برای استعلام بر خط هویت ایرانیان راه‌اندازی گردید.

۳. سامانه نظام هویت‌سنجی الکترونیکی بانکی (نهاب) ـ که تخصیص شماره شناسایی منحصربه‌فرد را برای هریک از افراد جامعه میسر می‌نماید ـ تولید شد.

۴. پلتفرم برنا توسط شرکت خدمات انفورماتیک زیر نظر بانک مرکزی توسعه داده شد.

۵. سامانه احراز مشتریان تجارت الکترونیک (امتا) توسط مرکز توسعه تجارت

الکترونیکی ایجاد شد.

۶. مرکز دولتی صدور گواهی الکترونیکی ریشه

۷. سامانه شاهکار (شبکه احراز هویت کاربران ایران)، سامانه‌ای است که زیر نظر سازمان تنظیم مقررات و ارتباطات رادیویی فعالیت می‌کند.

۸. سامانه احراز هویت وزارت ارتباطات و فناوری اطلاعات (سماوا) این سامانه به‌نوعی درگاه واحد هویت معتبر در فضا مجازی است.

۹. سامانه ثنا، قوه قضاییه به‌موجب ماده ۱۷۵ قانون آیین دادرسی کیفری مصوب سال ۱۳۹۲ قوه قضائیه؛ موظف است اوراق قضایی را با استفاده از سامانه‌های الکترونیکی یا مخابراتی ابلاغ نماید. مراجعان به قوه قضاییه موظف‌اند جهت دریافت الکترونیکی اوراق قضایی به سامانه‌ای که به این منظور ایجاد گردیده مراجعه کنند.

۱۰.سامانه سخا، نیروی انتظامی؛ یکی از سامانه‌های بسیار کاربردی و مهم در زمینه ارائه خدمات گوناگون اینترنتی و متعلق به نیروی انتظامی است.

با توجه به مطالب بیان شده و توصیف اقدامات کشور در حوزه اسناد بالادستی و اجرایی، شاید این سؤال مطرح شود که مگر کارهای انجام شده در این حوزه، کفایت نمی‌کند و ضرورت انجام این پژوهش چیست؟ در پاسخ به این سؤال باید بیان داشت که وضعیت فعلی فضای سایبر در کشور با وجود اقدامات انجام‌شده به‌صورت قطعات پازل تکه‌تکه و جدا از هم قرار گرفته و نمی‌تواند تصویر یکپارچه و قابل استفاده‌ای را فراهم آورد. بر این اساس، کارهای متنوع و متعددی برای ساماندهی هویت در فضای سایبر در کشور عزیزمان ایران انجام شده است، ولی به دلیل عدم یکپارچگی، دارای اثربخشی و بهره‌وری لازم نیستند.

۳-۲. قلمروِ سایبری

یکی از مفاهیم پایه در فضای سایبر، مفهوم «قلمروِ سایبری» و «مرز سایبری» است. انسان‌ها، برای مشخص کردن محدوده فعالیت خود، به‌طوری که با محدوده همسایگان تداخل پیدا نکند، ناچار به تعیین حدود پیرامونی خود و متمایز کردن آن هستند. نمونه گسترش‌یافته این

تعریف، تعیین محدوده یک کشور است که جنبه سیاسی پیدا کرده است و خطی که محدوده جغرافیایی دو کشور را از هم جدا می‌نماید به‌عنوان مرز شناخته می‌شود (مجتهد زاده، ۱۳۸۱) و محدوده‌های مجاز فعالیت در داخل مرزها به‌عنوان قلمروِ حکومتی و حکمرانی شناخته می‌شود. تعریف عام لغوی مرز، عبارت است از هر چیز مشخص‌کننده حد و دامنه چیزی. مرز عامل تشخیص و جدایی یک واحد متشکل سیاسی یا کشور، از دیگر واحدهای مجاور و در واقع جداساز قلمروِ حاکمیتی دو نظام سیاسی است (غمامی و خلیلی‌نژاد، ۱۴۰۰).

مرزها یکی از الزامات و مقدمات دولت‌های مدرن به‌حساب می‌آید که مشخص‌کننده حدود سرزمینی و حدود صلاحیت حکمرانی است. مرزهای جغرافیایی مهم‌ترین عامل تشخیص و جدایی یک کشور از کشورهای دیگر است. در حقیقت مرزها خطوطی هستند که حدود بیرونی قلمروِ سرزمین تحت حاکمیت یک دولت ملی را مشخص می‌کند (حافظ‌نیا، ۱۳۸۵). بنابراین تحقق حکمرانی و مدیریت فضای سایبر مستلزم تشخیص مرز سایبری است (غمامی و خلیلی‌نژاد، ۱۴۰۰).

احترام گذاشتن به قلمروِ حکمرانی کشورها و مرز آن‌ها، یکی از اصول روابط بین‌الملل است و هر کشوری که این اصل را زیرپا بگذارد با قواعد تنبیهی مواجه خواهد شد. این امر در فضای واقعی به‌راحتی قابل فهم و تبیین است ولی در فضای سایبر، موضوع خیلی شفاف نیست و تفاوت در تعریف باعث شده است که نظریات مختلفی در این رابطه ارائه گردد.

در عصر حاضر، با گسترش فضای سایبر، حیات اجتماعی و سیاسی ما دچار تغییر و تحولات زیادی شده است. مرزهای جغرافیایی کشورها به‌وسیله اینترنت و فضای سایبر، متداخل شده و فواصل دور بسیار نزدیک و در جوار یکدیگر قرار گرفته است. در حقیقت جهان به دوران جدیدی از نظام فرهنگی، اجتماعی و سیاسی وارد شده است (بدیعی ازنداهی و همکاران، ۱۳۹۲). با توجه به از بین رفتن مفهوم مرزهای جغرافیایی در فضای سایبر، دولت‌ها و ملت‌ها با تهدیدات ناشناخته‌ای مواجه شده‌اند که مقابله با این تهدیدات، مستلزم شناخت مرز و تعیین قلمروِ سایبری برای کشورها است. بنابراین تعریف مرز و قلمروِ سایبری، یکی از شروط لازم برای مدیریت آن است و مدیریت یکپارچه هویت سایبری کاربران برای

جمهوری اسلامی ایران، از این قاعده مستثنا نیست. با توجه به خصوصیات فضای سایبری و تفاوت آن با فضای واقعی، اساساً این سؤال مطرح است که آیا تعریف مرز در فضای سایبر امکان‌پذیر است؟ پژوهش‌های متعددی در موضوع تبیین مفهوم مرز و قلمروِ سایبری انجام شده است و هرکدام سعی کرده‌اند از جنبه‌های مختلفی (سیاسی، اجتماعی، حقوقی، حاکمیتی و ...) به این موضوع بپردازند. تحولات دوران معاصر در حوزه فناوری اطلاعات و ارتباطات، تعریف و کارکرد مفهوم مرز و قلمرو را دستخوش تغییرات اساسی و بنیادین کرده است ولی نتوانسته است که ماهیت آن را تغییر دهد. در تعریف مرز سایبری، معمولاً اشتباهی که رخ می‌دهد این است که فضای سایبر را در سطح فنی و ابزارآلات آن تقلیل می‌دهند.

برای تعریف مرز و قلمرو در فضای سایبر، می‌توان همان تعریف مرز در فضای واقعی را تعمیم داد منتهی در تعاریف بیان شده از چهار لایه فضای سایبر، بیشتر معطوف به لایه زیرساخت بوده است و لایه‌های خدمات، داده و کاربر مورد غفلت قرار گرفته است. فضای سایبری از هر حیث بر فضای واقعی تکیه دارد، بنابراین با توجه به اصالت فضای واقعی نمی‌توان از خصوصیات فضای واقعی برای تعریف ویژگی‌ها و تعاریف فضای سایبر صرف‌نظر کرد (حافظ‌نیا، ۱۳۹۰).

شیوه مرز گذاری در فضای سایبر می‌تواند به دو صورت زیر باشد:

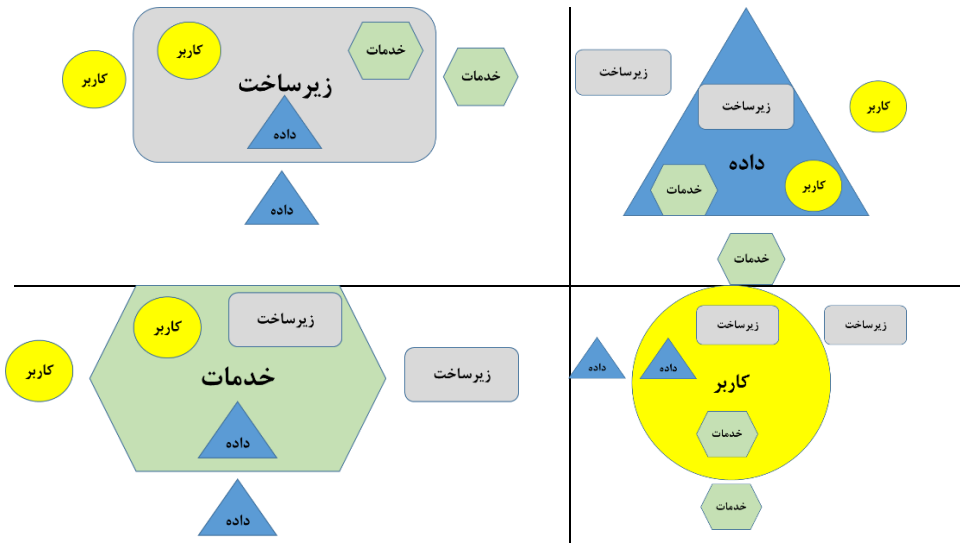
۱. مرز گذاری در فناوری ارتباطات: از طریق کنترل سیستم مسیریابی، نام دامنه، کنترل دروازه مرزی اینترنت و پروتکل‌های مرزی، کنترل ترافیک داده‌های داخلی و خارجی، کنترل پهنای باند، ایجاد دیواره آتش، ذخیره‌سازی داده‌ها در سرورهای ملی، ایجاد شبکه ملی اطلاعات و ... قابل انجام است.
۲. مرز گذاری در فناوری اطلاعات: به‌وسیله، فیلترینگ محتوا، مرز گذاری در سکوها، ایجاد قواعد مرز گذاری محتوایی، ابزارهای امنیت اطلاعات، مرز گذاری با قواعد حریم خصوصی و حفاظت از داده‌ها انجام می‌شود (غمامی و خلیلی‌نژاد، ۱۴۰۰).

امروزه، ظرفیت فضای مجازی به‌عنوان قدرتی نوظهور و مهم جلوه پیدا کرده است و روابط سنتی قدرت را برهم زده است. این امر باعث شده است که «حاکمیت مطلق دولت‌ها»

تبدیل به ادبیات «حکمرانی دولت‌ها» شود، چراکه حکمرانی زمانی مطرح می‌شود که دیگر دولت‌ها تنها بازیگر عرصه قدرت نباشند و بازیگران مختلف، قدرت و اثرگذاری داشته باشند (غمامی و خلیلی‌نژاد، ۱۴۰۰). حکمرانی در فضای مجازی نرم است. قلمرو در فضای مجازی خاکستری است؛ مثل قلمروِ جغرافیایی در فضای فیزیکی نیست؛ به عبارتی، هم «قلمرو» سیال است و هم «هویت»؛ منطق فازی دارد (مصاحبه با فیروزآبادی، ۱۴۰۲/۱۱/۰۱).

برای انجام این پژوهش، بیان تعریف عملیاتی مرز و قلمروِ سایبری، شرط لازم است و تا این موضوع مشخص نگردد، نمی‌توان الگوی مدیریت یکپارچه هویت سایبری کاربران برای جمهوری اسلامی ایران را ارائه داد. اگر تعریف فضای مجازی (سایبری) توسط مرکز ملی فضای مجازی کشور به‌عنوان مبنا قرار گیرد، مرز سایبری کشور در چهار لایه تعریف می‌گردد به‌طوری‌که، اگر کاربر فضای سایبر در هنگام فعالیت سایبری خود در یک یا چندلایه (زیرساخت، خدمات، داده و کاربر) که در مرزهای جغرافیایی جمهوری اسلامی ایران است، قرار گیرد، در قلمروِ حاکمیت و حکمرانی قرار گرفته است. به‌عنوان نمونه، اگر کاربری از زیرساخت داخل کشور برای اتصال به فضای سایبر استفاده نماید، ممکن است از خدمات داخلی یا خارجی استفاده نماید و همچنین داده‌هایش در داخل یا خارج از کشور ذخیره گردد و همچنین خود فرد و اطلاعات جانبی آن می‌تواند داخلی یا خارجی باشد. در نمونه‌ای دیگر، اگر کاربر خارجی، زیرساخت هم در خارج از کشور و از خدمات خارج از کشور استفاده شود در صورت ذخیره‌سازی داده‌ها در داخل کشور، فعالیت کاربر در قلمرو سایبری کشور به‌حساب می‌آید. همان‌طور که در شکل (۴)، نشان داده شده است، دو حالت (داخلی و خارجی)، برای لایه‌های چهارگانه افقی (زیرساخت، خدمات، داده و کاربر) مفروض است به‌عنوان نمونه اگر لایه زیرساخت را داخلی در نظر بگیریم، خدمات، داده و کاربر می‌تواند از نوع داخلی و خارجی باشد که در مجموع ۸ حالت در هر وضعیت می‌تواند رخ دهد که با کسر حالت‌های مشترک در مجموع ۱۶ حالت برای حضور در مرز و قلمروِ سایبری جمهوری اسلامی ایران می‌توان توصیف کرد. در هر ۱۶ حالت حضور در مرزهای سایبری جمهوری اسلامی ایران، ردپایی از حضور کاربر ثبت می‌گردد و با در کنار هم قرار دادن

ردپاهای مختلف امکان مدیریت یکپارچه هویت سایبری کاربران در جمهوری اسلامی ایران فراهم خواهد آمد.



شکل۴: حالت‌های مختلف لایه‌های فضای سایبر در مرز سایبری جمهوری اسلامی ایران

۴. روش‌شناسی

مرحله اصلی یک پژوهش ثمربخش و قابل دفاع به لحاظ علمی، روش‌شناسی آن است. در روش‌شناسی، محقق مشخص می‌کند که از چه راه و روشی می‌خواهد فرضیات خود را اثبات کند. به بیانی دیگر، روش پژوهش پلی است میان سطح نظری و عملی یک تحقیق. روش‌شناسی پژوهش، بیان فرایندی است که از طریق آن می‌توان در مورد ناشناخته‌ها به جستجو پرداخت و نسبت به آن‌ها شناخت لازم را کسب کرد. در این فرایند از چگونگی گردآوری داده‌ها و تبدیل آن‌ها به یافته‌ها تحت عنوان روش‌شناسی یاد می‌شود (سرمد، بازرگان و حجازی، ۱۳۷۹). در روش‌شناسی پژوهش، این امر بیان خواهد شد که اگر فرد دیگری بخواهد این پژوهش را انجام دهد با توجه به روش‌شناسی صورت گرفته، اگر از شیوه استفاده شده

توسط پژوهشگر استفاده نماید به احتمال بسیار زیاد به نتایج مشابه خواهد رسید.

نوع پژوهش پیش‌رو، توسعه‌ای-کاربردی است؛ تحقیق کاربردی با هدف توسعه دانش کاربردی و حل مشکل خاص علمی و یا اجتماعی انجام می‌گیرد و این تحقیق شیوه جدیدی را پدید می‌آورد که در جهت زندگی بهتر و به‌صورت مشخص و واضح در جامعه مورد استفاده قرار می‌گیرد. تحقیق توسعه‌ای به‌منظور گسترش دانش عمومی انجام می‌گیرد. بنابراین تحقیق و پژوهش روی تمامی موضوعاتی که بتواند به گسترش این علوم کمک کرده و مسائل ناشناخته آن را آشکار سازد جزو تحقیقات توسعه‌ای محسوب می‌گردد بدین‌صورت که قرار است توسعه دانش در یک زمینه خاص، رخ دهد (سرمد، بازرگان و حجازی، ۱۳۷۹). زمینه خاص این پژوهش هویت سایبری کاربران در فضای سایبری است و قرار است با مطالعه تحقیقات انجام شده، گزارشات فنی و تجربیات مفید (که بیشتر جنبه اقتصادی و مسائل پولی و مالی دارد) در زمینه هویت سایبری و دیجیتال و استفاده از خِرَد و دانش نخبگانی، روشی برای شناسایی هویت سایبری کاربران برای جمهوری اسلامی ایران ارائه شود.

با توجه به این‌که موضوع هویت سایبری، بعد از سال ۲۰۰۱ مورد توجه جدی قرار گرفته و پژوهش‌های مربوط به آن هم به همین سال‌ها برمی‌گردد، قلمرو زمانی این پژوهش از سال ۲۰۰۱ به بعد خواهد بود. قلمرو مکانی شامل قلمرو سایبری جمهوری اسلامی ایران است. قلمرو موضوعی پژوهش، عناوینی مرتبط با هویت دیجیتال و هویت سایبری است.

پژوهشگر، به گردآوری داده‌ها از طریق منابع، اسناد و مدارک در فضاهای واقعی (شامل کتابخانه‌ها، مراکز بایگانی و نگهداری اسناد و مدارک و ...) و همچنین فضای مجازی (شامل سایت‌های اینترنتی و مقالات و کتب و گزارشات منتشر شده در اینترنت و ...) است. مهم‌ترین مسئله، شناسایی منابع مناسب برای تحقیق و اسناد و مدارک است.

۵. تجزیه‌وتحلیل یافته‌ها

کاربران فضای سایبر، ریشه در فضای واقعی دارند و بخش قابل اعتنایی از اطلاعات هویتی آن‌ها در فضای سایبر، منبعث از اطلاعات آن‌ها در فضای واقعی است. توجه به این اطلاعات،

داده‌های هویتی را غنی می‌کند و باعث دقیق‌تر شدن اطلاعات هویتی می‌گردد. جدول (۱)، نمونه‌ای از این اطلاعات را نشان می‌دهد.

جدول ۱: اطلاعات کاربران در فضای واقعی

توجه: این جدول با ۲۶ بند بدلیل طبقه بندی محرمانه در بایگانی دبیرخانه فصلنامه محفوظ و قابل بهره برداری است.

همان‌گونه که در جدول فوق مشاهده می‌شود، اطلاعات فضای واقعی با مسئولیت یک نهاد حقوقی، صحت‌سنجی و اعتبارسنجی شده است.

اطلاعات موجود در فضای سایبر و فضای واقعی از کاربران فضای سایبر، این امکان را به ما می‌دهد تا بتوان با یکپارچه‌سازی این اطلاعات و اقدامات انجام‌شده در موضوع هویت سایبری در کشور، احراز و کشف هویت دقیق‌تری انجام دهیم. کارهای متعددی در کشور چه در زمینه تقنینی و چه در زمینه اجرایی، صورت گرفته است ولی عدم یکپارچگی آن‌ها باعث شده تا کارهای انجام شده اثربخشی لازم را نداشته باشد. بنابراین، «شناسایی هویت کاربران سایبری» عبارت است از: «استفاده هم‌زمان از دادگان هویتی فضای سایبر و فضای واقعی در لایه‌های چهارگانه فضای سایبر و تطبیق آن‌ها با شواهد ثبت‌شده از عملکرد کاربران در آن لایه‌ها به‌منظور دقیق‌تر شدن هویت کاربران.»

همان‌گونه که در بخش مرکزی شکل (۵)، نشان داده شده است، کاربران فضای سایبر در گذر زمان، ردپاهایی از حضور خود در فضای سایبر، ثبت می‌نمایند، این ردپاها هرچقدر غنی‌تر باشد، امکان وجود دادگان هویتی منحصربه‌فرد در آن زیادتر است و در صورت تطبیق هویتی با لایه‌های دیگر فضای سایبر یا سایر اطلاعات موجود در فضای سایبر و فضای واقعی، یک هم‌بندی میان این لایه‌ها و سایر اطلاعات ایجاد می‌نماید. هرچقدر این هم‌بندی و اتصال بیشتر باشد نشان‌دهنده این است که ضریب خطا در احراز هویت سایبری کاربر، کمتر است و کشف و احراز هویت دقیق‌تر است. بعد از احراز هویت از طریق ردپاهای هویتی در لایه‌های چهارگانه افقی فضای سایبر و سایر اطلاعات موجود، بانک‌های اطلاعاتی در لایه

مدیریت هویت سایبری کاربران ایجاد می‌گردد و این بانک‌ها در گذر زمان، غنی‌تر خواهند شد. با توجه به این‌که روش پیشنهادی برای شناسایی یکپارچه هویت سایبری به‌صورت فرابخشی و فراسازمانی قابلیت تحقق دارد، بنابراین بایستی تمام بخش‌ها با مرکز مدیریت هویت سایبری کاربران همکاری کنند.

شکل (۵)، نمایی از روش کشف هویت کاربران سایبری جمهوری اسلامی ایران را نشان می‌دهد.

شکل ۵: شناسایی هویت کاربران با استفاده از داده‌های فضای واقعی و سایبر

توجه: این شکل بدلیل طبقه بندی محرمانه در بایگانی دبیرخانه فصلنامه محفوظ و قابل بهره برداری است.

نتیجه‌گیری و پیشنهاد

با توجه به این‌که جمهوری اسلامی ایران، همواره در معرض تحریم‌های ظالمانه دشمن قرار داشته و در آینده هم بر همین منوال خواهد گذشت؛ ازهمین‌رو انتظار همکاری کشورهای غربی و بسترهای بین‌المللی و چندملیتی برای در اختیار قرار دادن اطلاعات هویتی ایرانیانی که از خدمات آن‌ها استفاده می‌کنند، عبث و بیهوده است. بر این اساس، هرگونه عوامل مجرمانه آن دسته از ایرانیانی که از چنین پلتفرم‌هایی برای اقدامات مجرمانه از قبیل جرائم فردی (مانند کلاهبرداری، تهدید، باج‌گیری و ...)، جرائم سازمان‌یافته (مانند قاچاق مواد مخدر، قاچاق اعضای انسان، خروج غیرقانونی از کشور و ...)، جرائم امنیتی (مانند اقدام به براندازی نظام، همکاری با سرویس‌های اطلاعاتی متخاصم، جاسوسی و ...) بهره‌برداری می‌کنند و حتی غیرایرانی‌هایی که به‌نوعی با هر یک از اقدامات مجرمانه مذکور در ارتباط هستند، از دید حاکمیت جمهوری اسلامی ایران پنهان بوده و در صورت رصد اعضای جامعه اطلاعاتی، هویت مرتکبین جرائم مذکور ناشناخته خواهد ماند و این به معنی به خطر افتادن امنیت فردی و اجتماعی و امنیت ملی ایران عزیز است.

بنابراین، باید چاره‌ای برای این مشکل اندیشید و پیشنهاد این مقاله ایجاد و راه‌اندازی بانک‌های اطلاعاتی هویتی کاربران ایرانی و غیرایرانی است که در قلمروِ سایبری جمهوری اسلامی ایران فعالیت می‌کنند و پر کردن خلأ اطلاعاتی بانک‌های مذکور با استفاده از اطلاعات به دست آمده از فضای واقعی و مجازی به کمک تکنیک‌های تلفیق اطلاعات، داده‌کاوی، عبور بانک‌ها از یکدیگر و ... است.

پیشنهادهای پژوهش

با توجه به گستردگی بحث هویت، هر یک از اجزا و عناصر روش ارائه شده در این مقاله قابلیت تبدیل شدن به یک پژوهش مستقل یا چند پژوهش مرتبط با هم را دارا هستند. پژوهش‌هایی از قبیل:

۱. استخراج و ارائه استاندارد بانک‌های اطلاعاتی خدمات شهروندی بخش خصوصی و دولتی به‌منظور اعلام به ارائه‌دهندگان خدمات شهروندی برای در اختیار قرار دادن اطلاعات درخواستی براساس استاندارد تدوین‌شده؛
۲. تدوین فرایندهای ارائه اطلاعات از سوی بخش‌های خصوصی و دولتی ارائه‌دهنده خدمات شهروندی به ایرانی‌ها و غیرایرانی‌ها به سامانه هویتی کشور؛
۳. طراحی و تدوین الزامات فنی شبکه دریافت اطلاعات از سامانه‌های بخش‌های خصوصی و دولتی ارائه‌دهنده خدمات شهروندی به ایرانی‌ها و غیرایرانی‌ها و همچنین ذخیره و پردازش اطلاعات مذکور؛
۴. طراحی سامانه‌های کشف هویت با استفاده از تلفیق اطلاعات، عبور بانک‌ها از یکدیگر و داده‌کاوی به‌منظور به‌کارگیری در بانک اطلاعات هویتی شهروندان ایرانی و غیرایرانی مرتبط با خدمات شهروندی یا فعال در فضای مجازی؛
۵. تدوین الزامات امنیتی سامانه کشف هویت کاربران سایبری جمهوری اسلامی ایران.

فهرست منابع

- اکبری، تورج (بی‌تا)، ***ساخت هویتی دیجیتال برای آینده کانادا***، سایت اینترنتی برهان.
- بدیعی ازنداهی، مرجان؛ احمدی فیروزجانی، میثم؛ انصاری‌زاده، سامان (۱۳۹۲)، ***تبیین مفهوم مرز در فضای سیاسی-مجازی ایران***، ***جغرافیا***، فصلنامه انجمن جغرافیایی ایران، دوره ۵.
- تاجیک، محمدرضا (۱۳۸۳)، ***جهانی‌شدن و هویت***، تهران: موسسه تحقیقات و توسعه علوم انسانی دانشگاه تهران.
- جنکینز (۱۳۸۱)، ***هویت اجتماعی***، مترجم: یاراحمدی، تهران: شیرازه.
- حافظ‌نیا، محمدرضا (۱۳۹۰)، ***جغرافیای سیاسی فضای مجازی***، تهران: سمت.
- خسروی، آرش (۱۳۸۹)، ***مفهوم‌شناسی هویت مجازی در فضای سایبر***، ره‌آورد نور.
- سرمد، زهره؛ بازرگان، عباس؛ حجازی، الهه (۱۳۷۹)، ***کتاب روش‌های تحقیق در علوم رفتاری***، نشر آگه.
- غمامی، سید محمد مهدی؛ خلیلی نژاد، سجاد (۱۴۰۰،). ***امکان‌سنجی و الزامات تعمیم‌پذیری پدیده مرز به فضای مجازی***. فصلنامه راهبرد اجتماعی- فرهنگی، ۶۵-۹۸
- مجتهدزاده، پیروز (۱۳۸۱). ***جغرافیای سیاسی و سیاست جغرافیایی***. تهران.
- مجدی‌زاده، زهرا (۱۳۹۸)، ***حکمرانی فضای مجازی در کره جنوبی***، تهران: پژوهشگاه فضای مجازی ـ گروه مطالعات فرهنگی و اجتماعی.
- معین، محمد (۱۳۷۹)، فرهنگ فارسی، تهران: امیرکبیر.

References

- Atis. (2018). Context-Aware Identity Management Framework.
- Axel, B., Werner, F. D., & Andy, C. J. (2009). Identity Management Design Guide with IBM Tivoli Identity Manager. IBM Corporation, International Technical Support Organization.
- Bendiab, K., Shiaeles, S., & Boucherkha, S. (2018). A New Dynamic Trust Model for "On Cloud" Federated Identity Management. IEEE.
- Binxing, F. (2018), Cyberspace Sovereignty. Retrived from: Cyberspace Sovereignty. springer.
- Cookiebot. (2020). What is consent managemenet Retrived from: Cookiebot: https://www.Cookiebot.com
- Digital Transformation Agency. (2019, october). Digital Identity glossary. Retrived from:https://www.dta.gov.au/our-projects/digital-identity/digital-identity-glossary
- Fang, b. (2018), Cyberspace Sovereignty: reflections on building a community of common future in cyberspace. Beijing: Springer.
- FATF. (2020), GUIDANCE ON DIGITAL IDENTITY. Paris: FATF.
- Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. Frontiers in Blockchain, 1-19.
- Harvard (2014), Identity and Access Management, Harvard University, PROGRAM PLAN, Harvard University Information Technology.
- Hitachi ID System, I. (2020), IAM Terminology. Hitachi Retrived from: https://hitachi-id.com/documents/identity-management-terminology.php
- IIF. (2019), Digital Identities in Financial Services - Responsible Digital Identities, The Key to Creating More Inclusive Economies. Paris: Institute of International Finanance (IIF),
- InCommon (2017), Incommon Glossary. Retrived from:Incommon: http://www.incommon.org/glossary.html
- isa2. (2020), Digital Public Administration factsheet 2020 Estonia. European Commission.
- ITU. (2016), Review of National Identity Programs. ITU-T Focus Group Digital Financial Services.
- ITU. (2018), Digital identity in The ICT ecosystem: An overview. ITU.
- Janice, M. (2007). Identity and Access Management Technologies.
- Karati, A., Amin, R., Islam, S., & Choo, K.-K. R. (2018). Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment. IEEE.
- Macdonald, A. (2022, 03 14), Mobile Biometrics. Retrived from: Biometrics Updates: https://www.biometricupdate.com/202203/china-to-introduce-digital-id-cards-nationwide
- Michel, M., Carvalho, M., Crawford, H., & Esterline, A. (2018), Cyber Identity: Salient Trait Ontology and Computational Framework to Aid in Solving Cybercrime. 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications. IEEE Computer Society.
- Mousawi, S. R. (2024). Social Media; Cyber Identity and Religious Identity. Al-daleel, 6(4).

- PWC. (2017), Feasibility Study of a Common Identity Repository (CIR). Pwc, EUROPEAN COMMISSION.
- Rouse, M. (2017). Defenition. Retrived from: Techtarget: http://whatis.techtarget.com
- tass. (2021), Russia to roll out digital IDs in 2024. Retrived from:RUSSIAN NEWS AGENCY: https://tass.com/science/1044074
- White House. (2010), National Strategy for Trusted Identities in Cyberspace. Washangton: Withe House.