فصلنامه پژوهش در مدیریت شماره۲- دوره۲-بهار ۱۴۰۵ صفحات۱۷۴-۱۶۶
Journal of Research in Management
Issn: 3060-6241

ارائه چارچوب معماری سازمانی با رویکرد هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری در پیاده‌سازی دولت الکترونیک

فاطمه خانی[۱] حمید رضا اکبرپناه[۲]

چکیده:

هدف این تحقیق بررسی نقش معماری سازمانی در هم‌راستاسازی حکمرانی داده‌محور و به کارگیری الزامات امنیت سایبری در پیاده‌سازی دولت الکترونیک است . این پژوهش با رویکرد تحلیلی و بر اساس مرور ادبیات علمی و تحلیل تطبیقی چارچوب‌های معماری سازمانی ، حکمرانی داده و استانداردهای امنیت سایبری انجام شده است . کمبود چارچوب‌های یکپارچه و هماهنگ، اغلب منجر به ناکارآمدی فرآیندها، افزایش ریسک‌های امنیتی و کاهش بهره‌وری در ارائه خدمات دیجیتال می‌شود. معماری سازمانی، به‌عنوان یک چارچوب ساختاری و مدیریتی، پتانسیل قابل توجهی در ایجاد انسجام میان سیاست‌ها، فرآیندها و فناوری‌ها دارد، اما نقش دقیق آن در هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری به صورت نظام‌مند مورد تحلیل قرار نگرفته است. تحلیل مفهومی و مرور نظام‌مند ادبیات علمی از ویژگی های این مقاله است و شامل گردآوری داده‌های تجربی از طریق پرسشنامه یا مصاحبه نمی‌باشد. نتایج پژوهش یک چارچوب مفهومی ارائه می‌دهد که روابط بین مؤلفه‌های کلیدی معماری سازمانی و سطح هم‌راستاسازی سیاست‌ها، فرآیندها و الزامات امنیت سایبری را تشریح می‌کند. این چارچوب علاوه بر تأمین پایه نظری برای پژوهش‌های آتی، می‌تواند به مدیران و سیاست‌گذاران دولت الکترونیک کمک کند تا تصمیمات راهبردی مبتنی بر معماری سازمانی اتخاذ کنند و انسجام و امنیت پروژه‌های دیجیتال را بهبود بخشند.

واژگان کلیدی : معماری سازمانی ،حکمرانی داده محور،امنیت سایبری ،دولت الکترونیک

[۱] کارشناسی ارشد مدیریت اجرایی دانشگاه آزاد تهران شمال – نویسنده اول

[۲] کارشناسی ارشد مهندسی صنایع دانشگاه خوارزمی تهران - نویسنده مسئول

مقدمه

در محیط پیچیده دولت الکترونیک، هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری به دلیل حجم بالای داده‌ها، تنوع منابع اطلاعاتی و تعدد فرآیندهای فناوری اطلاعات، یکی از چالش‌های کلیدی مدیریت فناوری اطلاعات در سازمان‌های دولتی است .معماری سازمانی [۳]به‌عنوان چارچوبی ساختاری و مدیریتی، ظرفیت بالقوه‌ای برای ایجاد انسجام بین مؤلفه‌های کلان سازمان، فناوری‌ها و جریان داده‌ها دارد و می‌تواند نقش اساسی در تسهیل هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری ایفا کند(Janssen et al., ۲۰۲۰؛ OECD, ۲۰۲۱). با این حال، شواهد تحلیلی سیستماتیک در خصوص نقش معماری سازمانی در مدیریت کلان داده و هم‌راستاسازی حکمرانی داده‌محور محدود است.مطالعات اخیر نشان می‌دهد که معماری سازمانی می‌تواند از طریق ساختاردهی جریان‌های داده، شفاف‌سازی مسئولیت‌ها و یکپارچه‌سازی سیاست‌ها، نقش تسهیل‌کننده‌ای در هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری ایفا کند.

با این حال، اثربخشی این نقش به عواملی نظیر سطح بلوغ مدیریت داده و کلان‌داده، آمادگی سازمانی و الزامات قانونی و مقرراتی وابسته است (Abraham et. al, ۲۰۱۹; OECD, ۲۰۲۱). تحول دیجیتال در بخش عمومی موجب شده است که دولت‌ها به طور فزاینده‌ای بر داده‌ها و کلان‌داده‌ها به‌عنوان مبنای تصمیم‌گیری، سیاست‌گذاری و ارائه خدمات عمومی تکیه کنند. در این راستا، مفهوم حکمرانی داده‌محور[۴]به‌عنوان رویکردی کلیدی برای مدیریت نظام‌مند داده‌ها، تعیین مسئولیت‌ها، تضمین کیفیت، قابلیت استفاده و ارزش‌آفرینی داده‌ها مطرح شده است (OECD, ۲۰۱۹; Janssen et. al, ۲۰۲۰)حکمرانی داده‌محور در دولت الکترونیک نه‌تنها به مدیریت فنی داده‌ها، بلکه به هم‌راستاسازی سیاست‌ها، فرآیندها و سازوکارهای نهادی مرتبط با استفاده از داده‌ها توجه دارد.با افزایش حجم، تنوع و حساسیت داده‌ها در محیط‌های دیجیتال دولتی، الزامات امنیت سایبری به یکی از ارکان اساسی حکمرانی داده‌محور تبدیل شده است.

چارچوب‌های نوین امنیت سایبری، امنیت را به‌عنوان بخشی جدایی‌ناپذیر از حکمرانی داده و مدیریت ریسک سازمانی در نظر می‌گیرند [۵].مطالعات اخیر نشان می‌دهد که عدم هم‌راستاسازی حکمرانی داده با الزامات امنیت سایبری می‌تواند منجر به افزایش ریسک‌های سایبری، کاهش اعتماد عمومی و تضعیف اثربخشی دولت الکترونیک شود(Janssen & Van den Hoven, ۲۰۱۵; Zuiderwijk et .al., ۲۰۲۱).

در این زمینه، معماری سازمانی به‌عنوان یک رویکرد کلان‌نگر برای طراحی و مدیریت ساختارهای سازمانی، داده‌ای و فناوری اطلاعات، نقش مهمی در مواجهه با پیچیدگی‌های داده‌محور ایفا می‌کند. معماری سازمانی با هدف ایجاد انسجام و هم‌راستاسازی میان لایه‌های کسب‌وکار، داده، کاربرد و فناوری توسعه یافته است و به‌عنوان ابزاری برای تحقق حکمرانی مؤثر در سازمان‌های پیچیده، از جمله سازمان‌های دولتی، شناخته می‌شود (Ross et. al, ۲۰۱۹; Lankhorst, ۲۰۲۲).چارچوب‌های مرجع معماری سازمانی نظیرTOGAF ، بر یکپارچگی لایه داده و لحاظ الزامات امنیتی در طراحی معماری تأکید دارند. معماری سازمانی، به‌عنوان یک چارچوب ساختاری و مدیریتی، پتانسیل قابل توجهی در ایجاد انسجام میان سیاست‌ها، فرآیندها و فناوری‌ها دارد، اما نقش دقیق آن در هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری به صورت نظام‌مند مورد تحلیل قرار نگرفته است. این پژوهش با رویکرد تحلیلی و بر اساس مرور نظام‌مند ادبیات علمی و تحلیل تطبیقی چارچوب‌های معماری سازمانی[۶] ، حکمرانی داده و استانداردهای امنیت سایبری[۷] انجام شده است.

چارچوب نظری و مدل مفهومی پژوهش

[۳] Enterprise Architecture (EA)
[۴] Data-Driven Governance
[۵] ISO/IEC ۲۷۰۰۱:۲۰۲۲; NIST Cybersecurity Framework ۲.۰, ۲۰۲۴
[۶] TOGAF - ArchiMate
[۷] NIST CSF - ISO/IEC ۲۷۰۰۱

بر این اساس، در این پژوهش یک چارچوب مفهومی تحلیلی ارائه می‌شود که در آن معماری سازمانی به‌عنوان متغیر مستقل، هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری به‌عنوان متغیر وابسته و بلوغ داده و فناوری، فرهنگ سازمانی و الزامات قانونی به‌عنوان متغیرهای تعدیل‌کننده در نظر گرفته شده‌اند. همچنین، انسجام سیاست‌ها، فرآیندها و جریان‌های داده‌ای به‌عنوان متغیر واسطه‌ای در این رابطه لحاظ می‌شود. این چارچوب، مبنایی نظری برای تحلیل نقش معماری سازمانی در پیاده‌سازی دولت الکترونیک مبتنی بر داده و امن فراهم می‌کند(Aier et .al, ۲۰۲۱; Hinkelmann & et .al,۲۰۲۲) .

این مطالعه یک چارچوب تحلیلی مفهومی ارائه می‌دهد که روابط بین معماری سازمانی، حکمرانی داده‌محور و الزامات امنیت سایبری را مشخص می‌کند. در این چارچوب:

متغیر مستقل:معماری سازمانی شامل چارچوب‌ها و استانداردهای[۸] انسجام سازمانی و فناوری، قابلیت یکپارچه‌سازی سیاست‌ها و فرآیندها و هماهنگی با مدیریت داده‌ها و کلان‌داده‌ها.

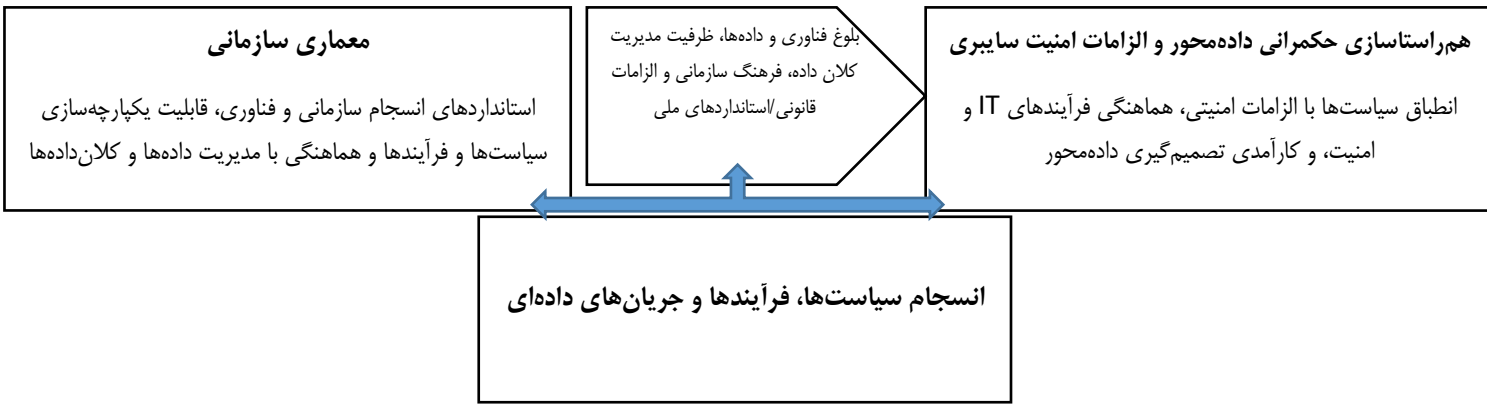
متغیر وابسته :هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری، سنجیده با شاخص‌هایی شامل انطباق سیاست‌ها با الزامات امنیتی، هماهنگی فرآیندهای IT و امنیت، و کارآمدی تصمیم‌گیری داده‌محور.

متغیرهای تعدیل‌کننده:بلوغ فناوری و داده‌ها، ظرفیت مدیریت کلان داده، فرهنگ سازمانی و الزامات قانونی/استانداردهای ملی.

متغیر واسطه‌ای : انسجام سیاست‌ها، فرآیندها و جریان‌های داده‌ای، که نقش اصلی در اثر معماری سازمانی بر هم‌راستاسازی دارد.

این چارچوب، امکان تحلیل سیستماتیک روابط بین معماری سازمانی، حکمرانی داده‌محور و الزامات امنیت سایبری را فراهم می‌کند و پایه‌ای برای مطالعات نظری آینده و ارائه توصیه‌های راهبردی به مدیران و سیاست‌گذاران دولت الکترونیک ایجاد می‌کند.

شکل ۱-۱:مدل مفهومی تحقیق



روش تحقیق

پژوهش حاضر از نظر هدف، کاربردی و از نظر ماهیت و روش، تحلیلی-توصیفی با رویکرد مفهومی است. با توجه به ماهیت موضوع پژوهش که ناظر بر تحلیل نقش معماری سازمانی در هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری در بستر دولت الکترونیک است، این مطالعه بر تحلیل مفهومی و مرور نظام‌مند ادبیات علمی استوار بوده و شامل گردآوری داده‌های تجربی از طریق پرسشنامه یا

[۸] EA (TOGAF ،ArchiMate)

مصاحبه نمی‌باشد. چنین رویکردی برای تبیین روابط مفهومی و توسعه چارچوب‌های نظری در حوزه‌های نوظهور و بین‌رشته‌ای توصیه شده است. این پژوهش در زمره مطالعات غیرتجربی قرار می‌گیرد و از روش مرور نظام‌مند و تحلیل محتوای کیفی برای استخراج، مقایسه و تلفیق مفاهیم کلیدی استفاده می‌کند. مطالعات تحلیلی–مفهومی با هدف شناسایی الگوها، شکاف‌های پژوهشی و تبیین روابط نظری میان مفاهیم به‌کار می‌روند و در حوزه‌هایی مانند حکمرانی داده، امنیت سایبری و معماری سازمانی کاربرد گسترده‌ای دارند.گردآوری داده‌ها از طریق مطالعه کتابخانه‌ای و مرور نظام‌مند منابع علمی انجام شده است. بدین منظور، کلیدواژه‌های مرتبط با موضوع پژوهش استخراج و جستجوی هدفمند در پایگاه‌های علمی بین‌المللی انجام شده و سپس منابع منتخب مورد بررسی عمیق قرار گرفته‌اند. در کنار منابع بین‌المللی، پژوهش‌های فارسی مرتبط با حکمرانی داده و دولت الکترونیک نیز به‌منظور تقویت بعد بومی تحلیل استفاده شده است (سجادی‌نژاد و همکاران، ۱۴۰۱).تحلیل داده‌ها با استفاده از تحلیل محتوای کیفی و سنتز مفهومی انجام شده است.همچنین، مفاهیم کلیدی، رویکردها و الگوهای مطرح‌شده در منابع استخراج، مقایسه و طبقه‌بندی شده و روابط میان آن‌ها مورد تحلیل قرار گرفته است. تحلیل محتوای کیفی امکان تبیین ساختارمند روابط میان مفاهیم نظری و توسعه چارچوب مفهومی پژوهش را فراهم می‌سازد.

تجزیه و تحلیل تحلیل یافته های تحقیق

یافته‌های این پژوهش بر اساس تحلیل نظام‌مند و تلفیقی ادبیات علمی داخلی و خارجی در حوزه معماری سازمانی، حکمرانی داده‌محور، امنیت سایبری و دولت الکترونیک استخراج شده است. از آنجا که پژوهش حاضر ماهیتی تحلیلی-مفهومی دارد، یافته‌ها نه بر مبنای داده‌های تجربی، بلکه بر پایه شناسایی الگوهای مفهومی، روابط علی و مؤلفه‌های کلیدی مطرح‌شده در پژوهش‌های معتبر پیشین ارائه می‌شود.

یافته‌های تحلیل مفهومی نشان می‌دهد که:

- وجود معماری سازمانی منسجم، امکان یکپارچه‌سازی جریان‌های داده، فرآیندهای سازمانی و سیاست‌های امنیت سایبری را فراهم می‌کند (سجادی‌نژاد و همکاران، ۱۴۰۱)
- نبود انسجام در معماری سازمانی، موجب پراکندگی داده‌ها، افزایش مخاطرات امنیتی و کاهش کارایی تصمیم‌گیری داده‌محور می‌شود(محمدی و همکاران، ۱۴۰۰؛۲۰۱۹ ,Abraham et .al)
- اثربخشی معماری سازمانی تحت تأثیر عواملی مانند بلوغ داده، حمایت مدیریتی، فرهنگ سازمانی و چارچوب‌های قانونی قرار دارد (عباسی و همکاران، ۱۴۰۰؛۲۰۲۱ ,OECD)

این یافته‌ها با مطالعات بین‌المللی نیز همخوانی دارد که معماری سازمانی را به‌عنوان ابزاری برای **هم‌راستاسازی سیاست‌های داده و الزامات امنیت سایبری** معرفی کرده‌اند.(Lankhorst, ۲۰۲۲; Ross et. al, ۲۰۲۱)

معماری سازمانی به‌عنوان زیرساخت حکمرانی داده‌محور در دولت الکترونیک

تحلیل منابع نشان می‌دهد که معماری سازمانی نقش اساسی در سامان‌دهی ساختارهای حکمرانی داده‌محور، تعیین سطوح مسئولیت‌پذیری داده و یکپارچه‌سازی جریان‌های داده‌ای در سازمان‌های دولتی ایفا می‌کند. پژوهش‌های داخلی تأکید دارند که نبود معماری سازمانی منسجم در نهادهای دولتی ایران، منجر به شکل‌گیری سیلوهای اطلاعاتی، تکرار پایگاه‌های داده و ضعف در بهره‌گیری از کلان‌داده‌ها در فرآیند سیاست‌گذاری عمومی شده است (احمدی و رضایی، ۱۴۰۰؛ سجادی‌نژاد و همکاران، ۱۴۰۱).

در ادبیات خارجی نیز، معماری سازمانی به‌عنوان یک سازوکار کلیدی برای تحقق حکمرانی داده‌محور و پشتیبانی از تصمیم‌گیری مبتنی بر داده در دولت‌های دیجیتال معرفی شده است (Janssen et .al, ۲۰۲۰; Abraham et .al, ۲۰۱۹). این مطالعات نشان می‌دهند که معماری سازمانی می‌تواند پیوند میان اهداف راهبردی، سیاست‌های داده‌ای و قابلیت‌های فناورانه را برقرار سازد.

نقش معماری سازمانی در نهادینه‌سازی الزامات امنیت سایبری

یافته‌های پژوهش نشان می‌دهد که معماری سازمانی، بستر لازم برای ادغام الزامات امنیت سایبری در لایه‌های کسب‌وکار، داده و فناوری را فراهم می‌سازد. مطالعات داخلی بیان می‌کنند که رویکردهای جزیره‌ای به امنیت سایبری در پروژه‌های دولت الکترونیک، اغلب موجب افزایش آسیب‌پذیری‌های امنیتی و ناهماهنگی میان سیاست‌های امنیتی و عملیاتی شده است (صادقی و همکاران، ۱۳۹۹؛ حسینی و کریمی، ۱۴۰۱).

در پژوهش‌های انجام شده پیشین نیز بر این نکته تأکید شده است که بدون اتکا به معماری سازمانی، پیاده‌سازی چارچوب‌های امنیت سایبری در محیط‌های داده‌محور با چالش‌های جدی مواجه خواهد شد (ISO/IEC ۲۷۰۰۱, ۲۰۲۲; Ross et al., ۲۰۲۱). این یافته‌ها نشان می‌دهد که معماری سازمانی می‌تواند به‌عنوان ابزار هم‌راستاسازی الزامات امنیتی با جریان‌های داده‌ای و فرآیندهای سازمانی عمل کند.

هم‌راستاسازی حکمرانی داده‌محور و امنیت سایبری از منظر معماری سازمانی

یکی از یافته‌های محوری پژوهش حاضر آن است که هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری در دولت الکترونیک، بدون بهره‌گیری از معماری سازمانی اثربخش، امکان‌پذیر نخواهد بود .مطالعات داخلی نشان می‌دهد که در بسیاری از پروژه‌های دولت الکترونیک، تمرکز صرف بر توسعه سامانه‌های دیجیتال بدون توجه به انسجام معماری داده و امنیت، موجب بروز ریسک‌های سایبری و کاهش اعتماد شهروندان شده است (محمدی و همکاران، ۱۴۰۰؛ زارعی و همکاران، ۱۴۰۱).

در ادبیات بین‌المللی نیز معماری سازمانی به‌عنوان سازوکاری کلیدی برای ایجاد تعادل میان استفاده گسترده از داده‌ها و حفظ امنیت و حریم خصوصی معرفی شده است .(Lankhorst, ۲۰۲۲; Tangi et. al, ۲۰۲۱) این پژوهش‌ها هم‌راستا با یافته‌های داخلی نشان می‌دهند که معماری سازمانی نقش **واسطه‌ای و هماهنگ‌کننده** میان حکمرانی داده‌محور و امنیت سایبری ایفا می‌کند.

عوامل زمینه‌ای و محدودکننده نقش معماری سازمانی

یافته‌ها نشان می‌دهد که اثربخشی معماری سازمانی در هم‌راستاسازی حکمرانی داده‌محور و امنیت سایبری، تحت تأثیر عواملی نظیر سطح بلوغ مدیریت داده، فرهنگ سازمانی، حمایت مدیران ارشد، چارچوب‌های قانونی و سیاست‌های ملی داده قرار دارد. پژوهش‌های داخلی تأکید دارند که ضعف در این مؤلفه‌ها می‌تواند منجر به ناکارآمدی معماری سازمانی و تحقق ناقص اهداف دولت الکترونیک شود (عباسی و همکاران، ۱۴۰۰؛ نادری و همکاران، ۱۴۰۲).این یافته‌ها با نتایج مطالعات پیشین هم‌خوانی دارد که بر اهمیت بلوغ سازمانی و حکمرانی کلان داده در موفقیت دولت‌های دیجیتال تأکید می‌کنند.(OECD, ۲۰۲۱; World Bank, ۲۰۲۰)

نتیجه‌گیری

پژوهش حاضر نشان داد که معماری سازمانی به‌عنوان سازوکاری کلیدی می‌تواند نقش واسطه‌ای و هماهنگ‌کننده در هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری در بستر دولت الکترونیک ایفا کند. نتایج این پژوهش نشان می‌دهد که معماری سازمانی می‌تواند به‌عنوان زیربنایی راهبردی برای هم‌راستاسازی حکمرانی داده‌محور و الزامات امنیت سایبری در دولت الکترونیک ایفای نقش کند. تحلیل تطبیقی چارچوب‌های مختلف معماری سازمانی و استانداردهای امنیت اطلاعات حاکی از آن است که مدل‌های معماری مبتنی بر یکپارچگی لایه‌های کسب‌وکار، داده، کاربرد و فناوری، بیش از سایر رویکردها توانایی ایجاد هم‌راستایی بین اهداف حکمرانی داده و دستورالعمل‌های امنیتی را دارند.

از دیدگاه نظری، یافته‌ها بیانگر آن‌اند که ایجاد چارچوب مفهومی مشترک میان معماری سازمانی، سیاست‌های داده‌محور و ضوابط امنیتی می‌تواند شکاف‌های مفهومی موجود میان این حوزه‌ها را کاهش داده و یک زبان مشترک برای تصمیم‌گیران و مدیران فناوری فراهم آورد. به‌ویژه در ساختار دولت الکترونیک که تمرکز اصلی بر ارزش‌افزایی داده‌ها و امنیت خدمات دیجیتال است، وجود چنین معماری منسجمی زمینه‌ساز ارتقای هماهنگی در سیاست‌گذاری، طراحی فرآیندها و مدیریت ریسک‌های امنیتی خواهد بود.

از منظر کاربردی، چارچوب مفهومی ارائه‌شده در این پژوهش می‌تواند به عنوان راهنمایی برای سیاست‌گذاران، معماران نظام‌های اطلاعاتی و مدیران فناوری دولت الکترونیک به کار رود تا تصمیمات خود را بر اساس رویکردی منظم، مبتنی بر معماری سازمانی و با تمرکز بر حکمرانی داده و امنیت سایبری اتخاذ کنند. این رویکرد نه تنها انسجام و کارایی پروژه‌های دیجیتال را افزایش می‌دهد، بلکه موجب کاهش آسیب‌پذیری‌ها و ارتقای اعتماد عمومی به دولت الکترونیک خواهد شد(سجادی‌نژاد،۱۴۰۱).

در نهایت، پژوهش حاضر با ارائه چارچوبی مفهومی، بیش از هر چیز بر اهمیت یکپارچه‌سازی سه رویکرد کلیدی معماری سازمانی، حکمرانی داده و امنیت سایبری در تحقق دولت الکترونیک پایدار و امن تأکید کرده است. پیشنهاد می‌شود در مطالعات آتی، این چارچوب از طریق مدل‌سازی تجربی و تحلیل کمی در محیط‌های اجرایی دولت الکترونیک مورد ارزیابی قرار گیرد تا میزان تأثیر هر یک از مؤلفه‌ها بر هم‌راستاسازی راهبردی مشخص شود.

پیشنهادات کاربردی تحقیق

- تدوین و بومی‌سازی چارچوب‌های معماری سازمانی مطابق استانداردهای جهانی[۹] برای سازمان‌های دولتی ایران (سجادی‌نژاد و همکاران، ۱۴۰۱).
- ادغام الزامات امنیت سایبری با جریان‌های داده‌ای و فرآیندهای سازمانی به‌عنوان بخشی از برنامه‌های تحول دیجیتال(حسینی و کریمی، ۱۴۰۱)

[۹] TOGAF, ISO/IEC ۲۷۰۰۱

- آموزش و ترویج فرهنگ داده‌محور در سازمان‌های دولتی برای افزایش پذیرش معماری سازمانی و بهبود تصمیم‌گیری مبتنی بر داده (محمدی و همکاران، ۱۴۰۰).
- توسعه و پیاده‌سازی چارچوب معماری سازمانی یکپارچه
- پیشنهاد می شود سازمان‌های دولتی باید با بهره‌گیری از چارچوب‌های معاصر معماری سازمانی، یک مدل جامع و منسجم طراحی و اجرا کنند که تمامی ابعاد فرآیندها، داده‌ها، فناوری و سیاست‌ها را در بر گیرد. این مدل باید به‌گونه‌ای طراحی شود که هم‌راستایی سیاست‌های حکمرانی داده و الزامات امنیت سایبری را تضمین نماید.
- ترغیب به فرهنگ سیاست‌گذاری داده‌محور و امنیت سایبری هم‌زمان
- سازمان‌ها باید سیاست‌های داخلی خود را بر اساس چارچوب‌های حکمرانی داده و استانداردهای امنیت سایبری تدوین و اجرا کنند. این سیاست‌ها باید در فرآیندهای عملیاتی، آموزش‌ها و ساختارهای سازمانی لحاظ شده و پی‌گیری مستمر شود.
- ایجاد تیم‌های تخصصی چندرشته‌ای
- تشکیل تیم‌های کارآمد متشکل از معماران سازمانی، متخصصان امنیت سایبری، سیاست‌مداران و مدیران داده، موجب بهبود فرآیند هم‌راستاسازی و ارتقاء سطح امنیت و کارایی پروژه‌های دیجیتال می‌شود.
- توسعه استانداردهای داخلی بر مبنای چارچوب‌های موجود
- سازمان‌ها باید بر اساس استانداردهای بین‌المللی و چارچوب‌های معاصر، استانداردهای داخلی خاص خود را برای حکمرانی داده و امنیت سایبری تدوین و پیاده‌سازی کنند تا انسجام و تطابق با سیاست‌های ملی و بین‌المللی حفظ شود.
- ارزیابی مستمر و اصلاح پیوسته معماری سازمانی
- ایجاد فرآیندهای ارزیابی دوره‌ای برای سنجش میزان هم‌راستاسازی استراتژیک، امنیت و کارایی فرآیندهای سازمانی و اصلاح ساختار بر اساس تغییر نیازها و فناوری‌های نوین.
- آموزش و توانمندسازی نیروی انسانی
- توسعه برنامه‌های آموزشی برای ارتقاء سطح دانش فنی و مدیریتی در حوزه معماری سازمانی، امنیت سایبری و حکمرانی داده در بین مدیران و کارمندان سازمان‌های دولتی(سجادی‌نژاد و همکاران، ۱۴۰۱).

پیشنهادات پژوهش های آتی

- انجام پژوهش‌های تجربی و پیمایشی برای سنجش میزان اثر معماری سازمانی در سازمان‌های دولتی ایران و تحلیل تطبیقی آن با تجارب بین‌المللی (عباسی و همکاران، ۱۴۰۰)
- بررسی اثر فناوری‌های نوین مانند هوش مصنوعی و کلان‌داده بر نقش معماری سازمانی در هم‌راستاسازی حکمرانی داده و امنیت سایبری.(Lankhorst, ۲۰۲۲; Tangi et al., ۲۰۲۱)

- تحلیل تطبیقی میان کشورهای مختلف برای شناسایی عوامل موفقیت در پیاده‌سازی معماری سازمانی و حکمرانی داده‌محور (زارعی و همکاران، ۱۴۰۱)

منابع

- عباسی، ع.، حسینی، م.، و رضایی، س. (۱۴۰۰). روش‌شناسی پژوهش‌های مفهومی در علوم مدیریت .*فصلنامه روش‌های پژوهش در مدیریت*.
- سجادی‌نژاد، م.، حیدری، ع.، و موسوی، ف. (۱۴۰۱). حکمرانی داده‌محور در بخش عمومی: الزامات و چالش‌ها .*فصلنامه دولت‌پژوهی*
- عباسی، ع.، حسینی، م.، و رضایی، س. (۱۴۰۰). پژوهش‌های مفهومی در علوم مدیریت و فناوری اطلاعات .*فصلنامه روش‌های پژوهش در مدیریت*.
- احمدی، ح.، و رضایی، م. (۱۴۰۰). حکمرانی داده‌محور در دولت الکترونیک ایران .*فصلنامه مدیریت دولتی*.
- حسینی، ف.، و کریمی، ن. (۱۴۰۱). الزامات امنیت سایبری در دولت الکترونیک .*فصلنامه فناوری اطلاعات*.
- سجادی‌نژاد، م.، حیدری، ع.، و موسوی، ف. (۱۴۰۱). کلان‌داده و حکمرانی داده در بخش عمومی .*فصلنامه دولت‌پژوهی*.
- محمدی، س.، رضوانی، ع.، و شریفی، م. (۱۴۰۰). ریسک‌های سایبری دولت الکترونیک .*پژوهشنامه مدیریت فناوری*.
- نادری، ک.، رفیعی، س.، و زمانی، م. (۱۴۰۲). بلوغ دیجیتال در سازمان‌های دولتی .*فصلنامه مدیریت تحول دیجیتال*.
- زارعی، م.، لطیفی، ح.، و اکبری، ف. (۱۴۰۱). امنیت داده و اعتماد عمومی .*فصلنامه سیاست‌گذاری عمومی*.
- عباسی، ع.، حسینی، م.، و رضایی، س. (۱۴۰۰). پژوهش‌های مفهومی در علوم مدیریت و فناوری اطلاعات .فصلنامه روش‌های پژوهش در مدیریت.
- سجادی‌نژاد، م.، حیدری، ع.، و موسوی، ف. (۱۴۰۱). کلان‌داده و حکمرانی داده در بخش عمومی .فصلنامه دولت‌پژوهی.
- محمدی، س.، رضوانی، ع.، و شریفی، م. (۱۴۰۰). ریسک‌های سایبری دولت الکترونیک .پژوهشنامه مدیریت فناوری.
- حسینی، ف.، و کریمی، ن. (۱۴۰۱). الزامات امنیت سایبری در دولت الکترونیک .فصلنامه فناوری اطلاعات.
- زارعی، م.، لطیفی، ح.، و اکبری، ف. (۱۴۰۱). امنیت داده و اعتماد عمومی .فصلنامه سیاست‌گذاری عمومی.
- *Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework. International Journal of Information Management, 49, 424–438.*
- *Aier, S., Gleichauf, B., Saat, J., & Winter, R. (2021). Understanding the role of enterprise architecture in digital transformation. Enterprise Information Systems, 15(6), 1–25.*
- *Hinkelmann, K., Gerber, A., Karagiannis, D., & Thoenssen, B. (2022). Enterprise architecture management for data-driven organizations. Journal of Enterprise Architecture, 18(1), 21–34.*
- *ISO/IEC 27001. (2022). Information security, cybersecurity and privacy protection — ISMS requirements.*
- *Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2020). Benefits, adoption barriers and myths of open data and open government. Information Systems Management, 37(4), 1–13.*
- *Lankhorst, M. (2022). Enterprise Architecture at Work (4th ed.). Springer.*
- *OECD. (2019). The Path to Becoming a Data-Driven Public Sector.*
- *OECD. (2021). Data Governance in the Public Sector.*
- *Ross, J. W., Beath, C. M., & Mocker, M. (2019). Designed for Digital. MIT Press.*
- *The Open Group. (2022). TOGAF® Standard, 10th Edition.*
- *NIST. (2024). Cybersecurity Framework (CSF) 2.0.*
- *Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of open data for public sector governance. Government Information Quarterly, 38(1).*

- *Aier, S., Gleichauf, B., Saat, J., & Winter, R. (2021). Understanding the role of enterprise architecture in digital transformation. Enterprise Information Systems, 15(6), 1–25.*
- *Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2020). Data governance challenges in the public sector. Government Information Quarterly, 37(1).*
- *Krippendorff, K. (2019). Content Analysis: An Introduction to Its Methodology (4th ed.). Sage.*
- *OECD. (2019). The Path to Becoming a Data-Driven Public Sector.*
- *OECD. (2021). Data Governance in the Public Sector.*
- *Vom Brocke, J., et al. (2020). Standing on the shoulders of giants: Challenges and recommendations of literature search in IS research. Communications of the AIS, 37(1).*
- *Janssen, M., et al. (2020). Data governance in the public sector. Government Information Quarterly.*
- *Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework. International Journal of Information Management.*
- *Lankhorst, M. (2022). Enterprise Architecture at Work. Springer.*
- *Ross, J. W., Weill, P., & Robertson, D. (2021). Enterprise Architecture as Strategy. Harvard Business Review Press.*
- *OECD. (2021). The Path to Becoming a Data-Driven Public Sector.*
- *Tangi, L., et al. (2021). Digital government transformation. Information Polity*