Semiannual Journal of Iran Futures Studies
Volume 5, Number 2, Fall & Winter 2021:35-65

The Drivers of Sustainable Cyber Service Offer in the Government with an Emphasis on Maintaining Security Using Artificial Intelligence

Babak Mohammadhosseini
Assistant Professor of Physics, Imam Khomeini International University, Qazvin, Iran.
babak.mohammadhosseini@gmail.com
Morteza Hadizadeh*
M.A. in Organizational Entrepreneurship Management, Shahid Beheshti University, Tehran, Iran, (Corresponding Author) morteza.hadizadeh72@gmail.com
Sayed Fahim Ghafelebashi
M.A. Student in Information Technology Management, Shahid Beheshti University, Tehran, Iran, fahim.ghafelebashi@gmail.com

Abstract

Purpose: Due to the increasing development of information technology, researchers estimate that in the near future, organizational structures will act hastily for fear of backwardness. Without sufficient attention to the security dimensions, they ignore the need for intelligent security simply by emphasizing cyberization and allocating large costs for preparing the technical infrastructure. In this regard, by observing the security dimensions, our research tries to identify and prioritize the drivers that have the most ability to provide cyber services.

Method: Our research is descriptive-analytical. The data collection is done theoretically in accordance with library studies; its tool is analytically questionnaire and data analysis is conducted by SPSS and Mic-Mac software.

Findings: Considering the security dimensions according to experts, we identified 12 drivers with the highest potential to provide cyber services and prioritized them in 4 areas. Next, by considering the two parameters of action and reaction, we explored the relationships between the drivers. Finally, we tried to bring the system closer to stability by prescribing an appropriate procedure.

Conclusion: According to the results of the research, in order to provide cyber services, the government should consider the degree of the organization's action and reaction and avoid making sporadic decisions that do not have a specific priority. In the realization of its cyber services, it should also pay special attention to the security dimension.

Keywords: Futures Studies, Cyber Security, Artificial Intelligence, E-Government, Mic-Mac

*Received on 2020/August /23 Accepted on 2020 /December /21
DOI**:** 10.30479/jfs.2021.14002.1221

دو فصلنامه آینده‌پژوهی ایران
مقاله پژوهشی، سال پنجم، شماره دوم، پاییز و زمستان ۱۳۹۹ صفحه: ۳۵-۶۵

پیشران‌های ارائه‌ی خدمات سایبری پایدار در دولت با تأکید بر حفظ امنیت از طریق هوش مصنوعی

بابک محمدحسینی
استادیار، دانشگاه بین المللی امام خمینی(ره،) قزوین، ایران، babak.mohammadhosseini@gmail.com
مرتضی هادی زاده*
دانش‌آموخته کارشناسی‌ارشد مدیریت‌کارآفرینی سازمانی،دانشگاه شهید بهشتی تهران،ایران(نویسنده مسئول)
morteza.hadizadeh72@gmail.com
سیدفهیم قافله باشی
دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه شهید بهشتی تهران، ایران،
fahim.ghafelebashi@gmail.com

چکیده

هدف: با توجه به توسعه‌ی روزافزون فناوری اطلاعات، این خطر پیش‌بینی می‌شود که در آینده‌ی نزدیک ساختارهای سازمانی از ترس عقب‌ماندگی شتابزده عمل کرده و بدون توجه کافی به ابعاد امنیتی، صرفاً برای سایبری‌سازی و تخصیص هزینه‌های کلان جهت آماده‌سازی زیرساخت‌های فنی، از توجه به ضرورت برقراری امنیت هوشمند غفلت کنند. در این خصوص این پژوهش سعی دارد تا با رعایت ابعاد امنیتی، به شناسایی و اولویت‌بندی پیش‌ران‌هایی بپردازد که بیشترین قابلیت ارائه‌ی خدمت در حوزه‌ی سایبری را داشته باشند.
روش: روش پژوهش حاضر توصیفی– تحلیلی است و همچنین، روش گردآوری اطلاعات در بخش نظری، مطالعات کتابخانه‌ای و ابزار گردآوری اطلاعات در بخش تحلیلی، پرسشنامه و تحلیل داده‌ها با نرم افزارهای «اس. پی. اس. اس» و«میک مک» انجام شده است.
یافته‌ها: با درنظر گرفتن بُعد امنیت بر اساس نظر خبرگان، ۱۲ پیش‌ران که دارای بیشترین پتانسیل ارائه‌ی خدمت در حوزه‌ی سایبری هستند، شناسایی و در ۴ محور اولویت‌بندی شدند. در ادامه با در نظر گرفتن دو شاخص اثرگذاری و اثرپذیری، به کشف روابط بین پیش‌ران‌ها پرداخته و در نهایت سعی شد تا با تجویز رویه‌ی مناسب، سیستم به پایداری نزدیک شود.
نتیجه‌گیری: با توجه به نتایج تحقیق لازم است که دولت در راستای ارائه‌ی خدمات سایبری، میزان تأثیرپذیری و تأثیرگذاری سازمان از یکدیگر را در نظر گرفته و از اخذ تصمیمات پراکنده که اولویت‌بندی مشخصی ندارد، اجتناب کند، و همچنین در تحقق خدمات سایبری بر رعایت بعد امنیت اهتمام ویژه‌ای داشته باشد.

واژگان کلیدی: آینده‌پژوهی، امنیت سایبری، هوش مصنوعی، دولت الکترونیک، میک مک.

---

* تاریخ دریافت مقاله: ۱۳۹۹/۶/۲ تاریخ پذیرش نهایی: ۱۳۹۹/۱۰/۱

۱– مقدمه

امروزه رشد فناوری‌های اطلاعات و ارتباطات[1]، زمینه را برای ارائه‌ی خدمات الکترونیکی آنلاین از طریق اینترنت در سراسر جهان فراهم کرده است. علی‌رغم رشد به ظاهر غیرقابل کنترل در ارائه‌ی خدمات الکترونیکی، عوامل مرتبط با حفظ حریم خصوصی و سایر خطرات ذاتی در استفاده از اینترنت به‌عنوان تهدید، مانع از بهره‌مندی کاربران از تمام مزایای پیش‌بینی شده می‌شود. پس می‌توان مطرح کرد که حملات سایبری یکی از جدی‌ترین تهدیدها برای اقتصاد جهانی به حساب می‌آید (Kisekka & Abdelhamid, 2019). همچنین سازمان‌ها و شرکت‌ها به سرعت در حال انجام عملیات خود به‌صورت آنلاین هستند تا به محبوبیت روزافزون بازار خدمات الکترونیکی دامن بزنند (Statista, 2017). اگرچه با وجود رشد خدمات الکترونیکی، نگرانی‌های مربوط به امنیت سایبری همچنان مانع استفاده از خدمات الکترونیکی می‌شود (Deloitte, 2015: 8).

در ایران ارزیابی‌های صورت گرفته در حوزه‌ی دولت الکترونیک نشان دهنده‌ی وضعیت در حال توسعه‌ی کشور است (شجاعیان و همکاران، ۱۳۹۸: ۵۱). به استناد بندهای ۱۵ و ۲۵ سیاست‌های کلی نظام اداری ابلاغی رهبری در فروردین ماه ۱۳۸۹، سیاست‌های کلی توسعه‌ی دولت الکترونیک کشور ترسیم شده است، بند ۱۵ دربرگیرنده‌ی توسعه‌ی نظام اداری الکترونیک و فراهم آوردن الزامات آن به منظور ارائه‌ی مطلوب خدمات عمومی است و بند ۲۵ اشاره به کارآمدسازی و هماهنگی ساختارها و شیوه‌های نظارت و کنترل در نظام اداری و یکپارچه‌سازی اطلاعات دارد. همچنین طبق ماده‌ی ۶۷ و ۶۸ از قانون برنامه‌ی ششم توسعه (۱۳۹۰–۱۴۰۰)، در ۷ بند و ۱۳ محور به مشخص کردن وظیفه‌ی نهادهای اجرایی در راستای توسعه‌ی الکترونیک پرداخته شده است.

تحولات اخیر در هوش مصنوعی[2] نشان می‌دهد که این فناوری نوظهور، تأثیر تعیین کننده و بالقوه‌ای بر قدرت نظامی، رقابت استراتژیک و سیاست جهانی خواهد داشت (Johnson, 2019: 147). اخیراً برخی سازمان‌ها از جمله سازمان ملل متحد درزمینه‌ی «هوش مصنوعی برای زندگی بهتر»، طرح‌هایی را انجام داده‌اند. بنابراین، موضوعی که با آن روبه‌رو هستیم این است که، چگونه می‌توان در میان حملات سایبری و نقض حریم خصوصی، از هوش مصنوعی استفاده کرد؟ (Thuraisingham, 2020). امنیت، اشکال مختلفی از قبیل امنیت اطلاعات، امنیت اسناد و امنیت دارایی دارد. امنیت، در بسیاری از اشکال، دائماً با استفاده از تکنیک‌های مدرن بهبود می‌یابد. دنیای ما تحت تأثیر فناوری شبکه‌ای، از بانکداری اینترنتی تا زیرساخت‌های

1. ICT
2. Artificial Intelligence

دولتی قرار گرفته است. بنابراین، محافظت از داده‌ها بسیار مهم است. امنیت سایبری، خطر از دست دادن داده‌های ضروری را کاهش می‌دهد، اما حملات سایبری افزایش یافته و قدرتمندتر شده‌اند. در جرایم سایبری، عامل انسانی، مهم‌ترین عامل است و دلیل اصلی عدم امنیت نیز محسوب می‌شود. برای برطرف کردن این ضعف، از سیستم‌های خودکار مانند کاربردهای هوش مصنوعی در امنیت سایبر استفاده می‌شود و این رویکرد، تغییرات ساختاری در امنیت سایبری ایجاد کرده است (NaveedAbbas et al, 2019 :1189).

با توجه به ابلاغ استراتژی های کلان و تدوین قوانین جهت حرکت سازمان‌های حاکمیتی و دولتی به سمت تحقق دولت الکترونیک و بعد از آن دولت هوشمند، این خطر احصاء می‌شود که در آینده نزدیک ساختارهای سازمانی از ترس عقب ماندگی به شتاب‌زدگی رو آورده و بدون توجه کافی به ابعاد امنیتی، صرفا با تاکید بر سایبری‌سازی و تخصیص هزینه‌های کلان جهت آماده سازی زیرساخت‌های فنی و ایجاد رویه‌های جدید در سازمان، از توجه به ضرورت برقراری امنیت هوشمند غفلت کنند. همانطور که می‌توان آثار خسارت‌های مالی و نظامی که نتیجه غفلت از نحوه پیاده‌سازی اشتباه ساختارهای الکترونیکی را در سایر کشورها به تحقیق نظاره‌گر بود، در این خصوص این پژوهش سعی دارد تا با در نظر گرفتن پیشران‌های کلان جهت تصمیم‌گیری به نهادهای مسئول در راستای برنامه‌ریزی اصولی با تاکید بر حفظ امنیت کمک کند.

۲- مبانی نظری

۲-۱. امنیت سایبری

امنیت سایبری را می‌توان مجموعه‌ای از فناوری‌ها و فرآیندهای طراحی شده برای محافظت از رایانه‌ها، شبکه‌ها، برنامه‌ها و داده‌ها تعریف کرد که در برابر حملات، دسترسی‌های غیرمجاز، تغییر و یا تخریب، واکنش‌گر باشد (Aftergood, 2017: 30). تمرکز امنیت سایبری بر تکنیک‌هایی است که بتوانند بر مبنای آن تأمین کننده‌ی امنیت در حوزه‌های مذکور باشند (Bhatele, et al, 2019: 175). از این رو، توجه به تعریف سیستم‌های امنیتی اهمیت می‌یابد، این سیستم‌ها شامل یک سیستم امنیت شبکه و یک سیستم امنیتی رایانه است، و هر یک از این سیستم‌ها شامل فایروال‌ها[1]، نرم‌افزارهای ضدویروس[2] و سامانه‌های تشخیص نفوذها[3] هستند که «آی. دی. اس.» به تعیین و شناسایی رفتارهای غیرمجاز سیستم‌ها کمک می‌کنند (Milenkoski, 2015: 25).

1. Firewall
2. Antivirus
3. IDS

یکی از اصلی‌ترین خطرات سایبری این است که گمان شود چنین خطراتی وجود ندارند. مورد دیگر سعی در رفع همه خطرات احتمالی است. از این رو، ابتدا محافظت از آنچه حیاتی‌تر به‌نظر می‌رسد و آمادگی برای واکنش صحیح در برابر تهدیدات مربوطه نسبت به داده‌ها، اهمیت دارد؛ همچنین باید به یکپارچگی، آگاهی، تجربه‌ی مشتری، رعایت اعتبار و شهرت در مورد خدمات تجاری نیز پرداخته شود (Nappo, 2017: 175).

امروزه به دلیل ماهیت تکاملی خطرات موجود در فضای مجازی، جمعیت بیشتری در معرض حملات سایبری قرار می‌گیرند. راه‌های نفوذ از طریق فعالیت‌های خطرناک و تهاجمی ساخته می‌شوند که دسترسی غیرمجاز به شکارچیان (هکرها و کراکرها) روی سیستم‌های رایانه‌ای یا شبکه‌ها را ممکن می‌سازند. این فعالیت‌ها تهدید سایبری نامیده می‌شوند. مهاجمان برای ایجاد این مسیرها، روی ایرادها و خطاهای موجود در سیستم یا شبکه کار می کنند. برای تهدیدهای سایبری مثال‌هایی مانند باج افزار، ویروس، کرم‌ها، تروجان[1]، جاسوس‌افزارها، نرم‌افزارهای تبلیغاتی مزاحم، مهندسی اجتماعی، حمله به واسطه‌ی یک فرد[2] و موارد دیگر وجود دارد. همه دارایی‌های ارزشمند و اطلاعات محرمانه‌ای دارند که تحت اختیار آن‌ها هستند و وقتی شخص خارجی به آن دارایی‌ها و داده‌ها دسترسی پیدا می کند، می‌تواند زیان‌های شدید ایجاد کند. با توجه به فضای مجازی، این دسترسی‌ها بدون رضایت مالک می‌تواند نتیجه یک یا چند تهدید سایبری باشد. در اینجا امنیت سایبری اهمیت پیدا می‌کند و در دسترس بودن، محرمانه بودن و یکپارچگی سیستم یا شبکه را تضمین می‌کند و به آن کمک می کند تا بدون هیچ‌گونه خطری با امنیت کامل و به‌صورت کارآمد عمل کند (Panimalar, 2018: 5).

۲-۲. هوش مصنوعی

هوش مصنوعی، یک اصطلاح کلی است که بر استفاده از رایانه برای مدل‌سازی رفتار هوشمند با حداقل دخالت انسان دلالت دارد. هوش مصنوعی معمولاً با اختراع روبات‌ها شناخته می‌شود. این اصطلاح از کلمه‌ای به زبان چک[3] با عنوان «روبوتا» گرفته شده است که به معنی کار اجباری است. هوش مصنوعی، که به‌عنوان علم و مهندسی ساخت ماشین‌های هوشمند توصیف شده است، در سال ۱۹۵۶ رسماً متولد شد (Hamet & Tremblay, 2017: 36).هوش مصنوعی، دانشی است که بیش از آن‌که مبتنی بر انسان و حیوان باشد، یک هوش بر پایه‌ی ماشین است. این بدین معنی است که فعالیت‌هایی مثل حل مسئله و یادگیری که معمولاً توسط افراد انجام می‌شود، به ماشین سپرده شود. امروزه هر شرکت و سازمانی می‌خواهد در این زمینه

1. Trojan
2. MITM
3. Czech language

پیشرفت کند و در تلاش برای ساختن محصول خود بر پایه‌ی هوش مصنوعی، به‌عنوان دستیار است. این امر سبب می‌شود از فناوری بهینه استفاده شود و با سازماندهی یکپارچه، اطلاعات مفیدی در اختیار کاربران قرار گیرد (Dasoriya et al., 2018: 1). همچنین، هوش مصنوعی به یکی از فناوری‌های مهم و اساسی که بر ایجاد ماشین‌های هوشمند متمرکز است و می‌تواند مانند انسان فکر کند، کار کند و واکنش نشان‌دهد، تبدیل شده است. از این فناوری پیشرفته می‌توان در توسعه‌ی یادگیری تطبیقی، بازی‌ها و برنامه‌های نرم‌افزاری برای اهداف آموزشی، استفاده کرد (Shanmugam et al., 2019).

هوش مصنوعی دامنه‌ی متنوعی دارد که این مزیت رقابتی می‌تواند برای دستیابی به بهترین نتایج، در زمینه‌های مختلف مورد استفاده قرار گیرد. برخی از مزایای سیستم‌های هوش مصنوعی در ادامه بیان شده است. مثلاً کار بدون وقفه و یکنواخت با جایگزین کردن روبات‌ها و ماشین‌های خودکار با انسان امکان‌پذیر می‌شود (Annon, 2017). هوش مصنوعی سبب شده است تا پزشکان راحت‌تر و سریع‌تر کار کنند؛ زیرا از گزارش‌های الکترونیکی بهداشت استفاده می‌شود. این امر در تشخیص زودرس بیماری کمک می‌کند که کاهش هزینه را نیز در پی دارد. حتی جراحی را می‌توان با کمک روبات‌ها انجام داد. چراکه جراحی با کمک ربات‌ها با دقت بیشتری انجام می‌شود و ماندن در بیمارستان‌ها کوتاه‌تر می‌شود (Kumar et al., 2016: 111). همچنین، هوش مصنوعی که با روباتیک، دستگاه‌های هوشمند، پردازش زبان طبیعی، عامل‌های مجازی، یادگیری ماشین و بسیاری دیگر از فناوری‌های مرتبط شناخته می‌شود، به‌عنوان دانشی تلقی می‌شود که بازی کسب و کار را از طریق بهبود تولید، کاهش قیمت‌ها، ایجاد شغل و فرصت‌های رشد جدید، تغییر خواهد داد (Dasoriya et al., 2018: 2)

۲-۳. نقش هوش مصنوعی در سرویس‌های دولت

کلمات کلیدی مانند اختلال دیجیتال و تحول دیجیتال عمدتاً در زمینه‌ی کسب و کارها استفاده می‌شود. اگرچه در مقیاس کمتر، دوره‌ی دیجیتالی نیز در حال دستیابی به حوزه‌های جدید مطالعاتی است، مانند مدیریت عمومی (Amorim et al, 2018: 411). قابل اشاره است که در مواردی که دولت‌ها برای معرفی خدمات آنلاین برای پیوند شبکه‌های دولتی با شهروندان سرمایه‌گذاری‌های کلانی انجام می‌دهند، نفوذ این سرویس‌ها به نظر رضایت بخش نبوده و به‌عنوان مثال بازده کافی را برای سرمایه‌گذاری فراهم نمی‌کند (Hung et al., 2006: 97). بنابراین، اصلِ سطح پایین پذیرش کاربر از خدمات دولت الکترونیکی، به‌عنوان یک مشکل بزرگ و جدی برای سیاست‌گذاران، مدیران اداری عمومی و جامعه شناخته شده است (Lamberti et al., 2014: 596). علاوه بر این، به گفته‌ی (Agarwal, 2018)، «مدیران دولتی

آمادگی لازم برای مقابله با این تغییرات روزافزون و نمایی را ندارند، زیرا بسیاری از ساختارها و فرآیندهای موجود دولت که طی چند قرن اخیر شکل گرفته‌اند، به سادگی در آینده‌ی نزدیک قابل تغییر نیستند». موجی از فناوری، مانند داده‌های بزرگ[1]، یادگیری‌ماشین[2]و هوش مصنوعی مدت‌هاست که مورد بحث قرار گرفته و در حال تغییر ساختار خدمات دولتی هستند. در بیشتر دموکراسی‌های غربی، خطر واقعی توسط محققان و دست‌اندرکاران در مدیریت عمومی نشان داده می‌شود که از دنیای مدیریت جدا شده‌اند و بدون درک پیامدهای حاکمیت دولت اداری، مشغول بحث و تصمیم گیری‌های فناوری هستند(Barth & Arnold, 1999: 332). با توجه به این پیش‌زمینه، نیاز به درک کاملی از دامنه و تأثیر برنامه‌های مبتنی بر هوش مصنوعی و چالش‌های مرتبط با این تکنولوژی در ابعاد مختلف وجود دارد (Witz et al., 2018: 10). دانشمندان نسبت به اهمیت آموزش و سرمایه‌گذاری‌های دولتی در پیشرفت‌های هوش مصنوعی تأکید دارند. به‌عنوان مثال، (Mikhaylov et al., 2018: 124)، استدلال می‌کند که «چالش بزرگ هوش مصنوعی نیاز به همکاری بین دانشگاه‌ها و بخش‌های دولتی و خصوصی دارد»، از طرف دیگر (Bughin et al., 2018: 224) بیان می‌کنند که برنامه‌های آموزش نیروی کار در سیستم‌های آموزش عمومی باید برای اطمینان از این‌که کارمندان مهارت‌های مکمل همچون همکاری با ماشین‌ها را دارند، مجدداً مورد بازنگری قرار گیرند.

۲-۴. نقش هوش مصنوعی در امنیت سایبری

طیف گسترده ای از هم‌پوشانی بین‌رشته‌ای بین امنیت سایبری و هوش مصنوعی وجود دارد. از یک سو، فناوری‌های هوش مصنوعی مانند یادگیری عمیق،[3]می‌توانند برای ایجاد مدل‌های هوشمند جهت اجرای طبقه‌بندی بدافزار و تشخیص نفوذ و تهدیدسنجی اطلاعات، در امنیت سایبری، وارد شوند. از سوی دیگر، مدل‌های هوش مصنوعی با تهدیدهای سایبری مختلف روبه‌رو خواهند شد که این امر باعث اختلال در نمونه، یادگیری و تصمیمات آن‌ها خواهد شد. بنابراین، مدل‌های هوش مصنوعی برای مبارزه با یادگیری ماشین‌های مخالف، حفظ حریم شخصی در یادگیری ماشین و ..... نیاز به فناوری‌های خاص دفاعی و حفاظتی امنیت سایبری دارد (JianHuaLI, 2018: 2). امروزه، فناوری‌های مختلف شبکه و محاسبات جدید، مانند شبکه‌های نرم افزاری[4] تعریف شده، داده‌های بزرگ و محاسبات «اف. او. جی.»[5]، پیشرفت

1. Big Data
2. Machine Learning
3. Deep Learning
4. SDN
5. FOG

سریع فضای مجازی را ارتقا داده‌اند (Li LZ et al., 2018: 14). در همین حال، امنیت سایبری به یکی از مهم‌ترین موضوعات در فضای مجازی تبدیل شده است (Guan et al., 2017: 1934). امنیت فضای مجازی تأثیر شگرفی بر زیرساخت‌های حیاتی مختلف تحمیل کرده است. امنیت سنتی برای کنترل امنیت شبکه مطابق با قوانین از پیش‌تعیین‌شده، متکی به کنترل استاتیک دستگاه‌های امنیتی، مانند فایروال‌ها،سیستم‌های تشخیص نفوذ[1] و سیستم‌های پیشگیری از نفوذ[2] است. با این حال، این روش پدافند غیرعامل نیست (Jian-Hua LI, 2018: 2).

هوش مصنوعی شاخه‌ای در حال رشد در علم کامپیوتر است که تئوری‌ها، روش‌ها، تکنیک‌ها و سیستم‌های کاربردی را برای شبیه‌سازی و گسترش هوش انسانی تحقیق و توسعه می‌دهد. به لطف توسعه‌ی فناوری محاسبات با اثربخشی زیاد و ظهور یادگیری عمیق، فناوری هوش مصنوعی در سال‌های اخیر پیشرفت بسیاری داشته است. به طور خاص، فناوری یادگیری عمیق به افراد این امکان را داده است تا از داده‌های بیشتری بهره‌مند شوند، نتایج بهتری کسب کنند و پتانسیل بیشتری را توسعه دهند. این فناوری به طرز چشمگیری زندگی مردم و فناوری سنتی هوش مصنوعی را تغییر داده است. هوش مصنوعی، طیف گسترده‌ای از برنامه‌ها مانند تشخیص چهره، تشخیص گفتار و روباتیک دارد، اما دامنه‌ی کاربرد آن فراتر از سه جنبه تصویر، صدا و رفتار است. همچنین بسیاری برنامه‌های برجسته‌ی دیگر در زمینه‌ی امنیت سایبر، مانند نظارت بر بدافزارها و تشخیص نفوذ، دارد. در توسعه‌ی اولیه فناوری هوش مصنوعی، فناوری یادگیری ماشینی، نقش مهمی در مقابله با تهدیدات فضای مجازی داشت. اگرچه یادگیری ماشین بسیار قدرتمند است، اما بیش از حد به استخراج ویژگی وابسته است. این نقص به ویژه وقتی در زمینه‌ی امنیت سایبر اعمال می‌شود، بسیار چشمگیر است. به‌عنوان مثال، برای فعال کردن یک راه حل یادگیری ماشین برای تشخیص بدافزار، باید ویژگی‌های مختلف مرتبط با بدافزار را به صورت دستی کامپایل کنیم، که بدون شک باعث کاهش کارایی و صحت تشخیص تهدید می‌شود. این امر به این دلیل است که الگوریتم‌های یادگیری ماشین مطابق ویژگی‌های خاص ازپیش‌تعریف‌شده کار می‌کنند، به این معنی که ویژگی‌هایی که از قبل تعریف نشده‌اند را نمی‌توانند کشف کنند. در نتیجه می‌توان نتیجه گرفت که عملکرد اکثر الگوریتم‌های یادگیری ماشین به صحت تشخیص ویژگی و استخراج آن بستگی دارد(Golovko, 2017: 9).

اگرچه فناوری‌های جدید هوش مصنوعی مانند یادگیری عمیق نقش مهمی در دفاع از فضای مجازی دارند، اما سیستم هوش مصنوعی نیز ممکن است مورد حمله یا فریب قرار بگیرد و

1. IDS
2. IPS

منجر به طبقه‌بندی نادرست یا نتایج پیش‌بینی نشده شود. به‌عنوان مثال، در محیط‌های حساس، دستکاری نمونه‌های تمرینی منجر به حملات می‌شود و دستکاری نمونه‌های آزمایش منجر به حملات فرار خواهد شد. هدف از حمله در محیط‌های حساس، تضعیف صداقت و قابلیت استفاده در برنامه‌های مختلف هوش مصنوعی و گمراه‌سازی شبکه‌ها با استفاده از نمونه‌های نادرست است و باعث می‌شود طبقه‌بندی‌های به دست آمده از طبقه‌بندی اشتباه استفاده کنند. البته اقدامات متداول دفاعی در برابر حملات خصمانه نیز وجود دارد (Akhtar & Mian, 2017: 15).

۲-۵. جایگاه امنیت سایبری در دولت و نقشه‌ی راه مدیران

استفاده از فناوری اطلاعات به دلیل ماهیت خاص خود، خطرات قابل توجهی برای سیستم‌های اطلاعاتی و به ویژه منابع حساس دارد (Pereira & Santos, 2010: 17). بنابراین، امنیت اطلاعات باید به درستی مدیریت و کنترل شود. امنیت اطلاعات، محافظت از اطلاعات در برابر طیف گسترده‌ای از تهدیدات به منظور اطمینان از تداوم مشاغل، به حداقل رساندن ریسک در کسب و کار و به حداکثر رساندن بازده سرمایه گذاری‌هاو فرصت‌های شغلی است (Larrocha et al., 2010: 907). «آی. تی. آی. ال.»،[1] مجموعه‌ای از بهترین روش‌ها برای مدیریت خدمات فناوری اطلاعات است. «آی. تی. آی. ال.» به سازمان‌ها کمک می‌کند از ارزش تجاری که خدمات «آی. تی.»[2] در اختیار ذینفعان داخلی و خارجی قرار می‌دهد، آگاه شوند. فرایند مدیریت امنیت «آی. تی. آی. ال.»، توصیف ساختاریافته‌ی امنیت در سازمان مدیریت است (Wegmann et al., 2010: 2). «آی. تی. آی. ال.»، چارچوبی از بهترین روش‌ها است که باعث ارتقاء خدمات محاسبات با کیفیت در بخش فناوری اطلاعات می‌شود. مبحث «آی. تی. آی. ال.»، برای اولین بار توسط آژانس مرکزی رایانه و ارتباطات مرکزی انگلیس توسعه داده شد، که در سال ۲۰۰۱ با دفتر بازرگانی دولت انگلستان «اُ. جی. اس.»[3] ادغام شد (Zegers, 2006). در سال‌های اخیر، امنیت سایبری مورد توجه بسیار زیاد در جامعه‌ی تحقیقاتی قرارگرفته است. امنیت سایبری باعث می‌شود از سیستم‌های اطلاعاتی مانند سخت‌افزار، نرم‌افزار و زیرساخت‌های مربوطه، داده‌های مربوط به این سیستم‌ها و خدمات ارائه شده توسط این سیستم‌ها، محافظت شود که با این روش به مقابله با دستیابی غیرقانونی از طرف عوامل خرابکار (مزاحمان یا مهاجمان) می‌توان پرداخت و همچنین در برخی موارد، می‌تواند عمداً صدمه‌ای توسط یک اپراتور به سیستم وارد شود. بنابراین، هر دو آسیب عمدی یا تصادفی

1. ITIL
2. IT
3. OGS

می‌تواند منجر به عدم پیروی از مراحل امنیتی شود (Deibert et al., 2010: 16). با توجه به بررسی انجام شده از طیف گسترده ای از منابع در سال ۲۰۱۶، این نکته آشکار شد که اعمال مقررات جدید برای مدیریت ریسک سایبری، در بین خدمات اساسی مختلف از جمله زیر ساخت‌های ملی امری ضروری است (Wazid et al., 2017).

۳- پیشینه‌ی پژوهش

برای جستجوی سوابق پژوهش، کلید واژه‌های امنیت سایبری، هوش مصنوعی، خدمات دولت و امنیت سایبری مبنای جستجو قرار گرفت. مهم‌ترین تحقیقات پیشین صورت گرفته، در رابطه با امنیت سایبری در دولت با تأکید بر هوش مصنوعی به شرح جدول (۱) است.

جدول ۱. مهم‌ترین تحقیقات پیشین صورت گرفته، دررابطه با امنیت سایبری در دولت با تأکید بر هوش مصنوعی

ردیف	نام اثر	هسته بحث
۱	آینده‌ی امنیت سایبری: تأثیر عمده‌ی هوش مصنوعی، یادگیری ماشین و یادگیری عمیق در فضای سایبری (Geluvaraj et al., 2019)	در این مقاله ذکر شد که هوش مصنوعی بیشتر برای شناسایی تهدیدها و حملات استفاده می‌شود و سیستم‌ها باید به گونه‌ای توسعه بیابند که بتوانند به تنهایی و سرعت به شرایط واکنش نشان دهند. و همچنین بیان شده که سیستم‌های هوش مصنوعی در انجام وظایف خود اشتباه نمی کنند. بنابراین، هر تهدید به روش مؤثر و مناسب پاسخ داده می‌شود و درآینده شاهد افزایش سریع درگیری‌های بین‌المللی در فضای مجازی خواهیم بود. این امر ممکن است شامل حمله به زیرساخت ها و تأسیسات و همچنین آسیب رساندن به عملکردهای عادی دستگاه‌های دولتی و مالی، مؤسسات جامعه‌ی سنتی مانند بانک ها، مطبوعات، اجرای قانون و قضایی شد. از این رو، در نظر گرفتن امنیت سایبری به‌عنوان موضوعی اساسی برای این مقاله، به ما اجازه می‌دهد چالش‌ها را ببینیم و بدانیم نقش «ای. آی»[1]، «ام. ال.»[2]و «دی. ال.»[3]در جلوگیری از جرایم سایبری در آینده چیست.
۲	هوش مصنوعی در خدمات دولتی: بررسی سیستماتیک ادبیات (Reis et al., 2018)	هدف پژوهش در این مقاله، ارائه‌ی یک مرور کلی در مورد چگونگی نقش هوش مصنوعی در شکل گیری دوره‌ی دیجیتال، در سیاست‌گذاری‌ها و دولت است. این تحقیق، فرصت‌های جدید را یافته و سیاست‌گذاران را متوجه پیامدهای آن می‌کند. در این تحقیق از یک بررسی متون ادبی استفاده شده است که شامل بیش از یک تکنیک تجزیه و تحلیل داده‌ها به منظور تولید جامع و دانش غنی است،
۳	نقش هوش مصنوعی در امنیت سایبری (Bhatele et al, 2019	در این مقاله بیان شده که در دوران دیجیتال، امنیت سایبری به یک نگرانی اساسی تبدیل شده است. این چالش‌ها همیشه در حال ابداع کنترل‌ها و رویه‌های درست و اجرای آن‌ها با حساسیت تمام، جهت مقابله با حملات سایبری و جرایم بی‌پایان بوده است. نویسندگان، فنون خاصی را در هوش مصنوعی مطرح می‌کنند که امیدوار کننده است.آن‌ها کاربردهای این فنون را در امنیت سایبری پوشش می‌دهند. بحث را با گفتگو در مورد حوزه‌ی آینده‌ی هوش مصنوعی و امنیت سایبر پایان می دهند.
۴	بررسی کاربردهای هوش مصنوعی در امنیت سایبری (Abbas et al., 2019)	این پژوهش بر کاربرد هوش مصنوعی در امنیت سایبری متمرکز است. در مقاله یاد شده که از زمان ظهور «ای. آی»، تغییرات ساختاری در امنیت سایبری مشاهده شده است. این مطالعه به توسعه‌ی نظریه در مورد هوش مصنوعی در امنیت سایبری می‌پردازد، به محققان کمک می‌کند تا مسیرهای تحقیق را تعیین کنند و مرجعی را ارائه می‌دهند که سازمان‌ها و دولت‌ها می‌توانند برای برنامه‌ریزی برنامه‌های هوش مصنوعی در صنعت امنیت سایبری از آن‌ها استفاده کنند. این مطالعه تجسم تغییرات ساختاری، نقاط مهم و روندهای نوظهور در مطالعات هوش مصنوعی را تجسم می‌کند. همچنین، به ارائه‌ی دیدگاه کلی از نقاط مهم و روند تحقیقات در زمینه‌ی هوش مصنوعی در

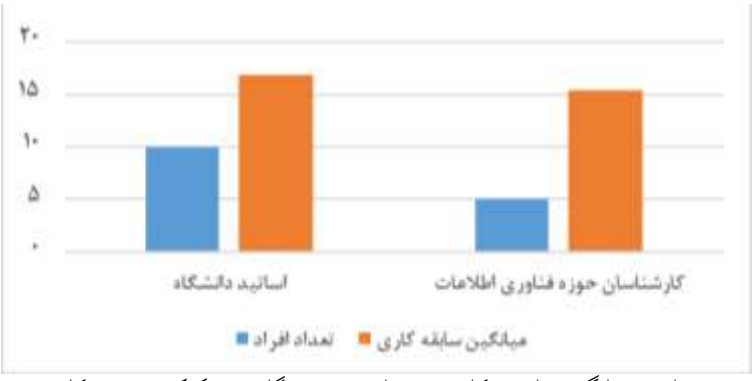
1. AI
2. ML
3. DL

		حوزه‌ی امنیت سایبری می‌پردازد.
۵	امنیت سایبری با هوش مصنوعی ملاقات می‌کند: یک بررسی (Li te al., 2018)	بررسی انجام شده در این مقاله نشان می‌دهد که طیف گسترده‌ای از همپوشانی‌های بین‌رشته‌ای بین امنیت سایبری و هوش مصنوعی وجود دارد. همچنین ذکر شده است که فناوری‌های هوش مصنوعی مانند یادگیری عمیق می‌توانند برای ایجاد مدل های هوشمند و اجرای طبقه‌بندی بدافزارها و تشخیص نفوذ و تهدید سنجی اطلاعات، در امنیت سایبری وارد شوند. پژوهشگر در این مقاله، تلاش‌های تحقیقاتی موجود را از نظر مبارزه با حملات سایبری با استفاده از هوش مصنوعی، از جمله اتخاذ روش‌های یادگیری ماشین و راه حل‌های یادگیری عمیق موجود، خلاصه کرده است. سپس، ضد حمله‌هایی را که ممکن است «ای. آی» به آن دچار شود، تجزیه و تحلیل می‌کند، ویژگی‌های آن‌ها را جدا کرده و روش‌های دفاعی مربوطه را طبقه‌بندی می‌کند. سرانجام چگونگی ساختن یک سیستم هوش مصنوعی ایمن را جستجو می‌کند.

با مطالعه‌ی ادبیات تحقیق می‌توان به این نتیجه رسید که پژوهش‌های صورت پذیرفته در حوزه‌ی آینده‌ی امنیت سایبری در دولت با تأکید بر هوش مصنوعی، بسیار ضعیف و ناقص است. فقدان پژوهشی بنیادی در این حوزه می‌تواند آسیب‌های جبران‌ناپذیری، به دلیل نداشتن شناخت و همچنین از دست دادن فرصت‌ها، داشته باشد. با بررسی‌های انجام شده، پژوهشی که دقیقاً به بررسی آینده‌ی امنیت سایبری در دولت با تأکید بر هوش مصنوعی بپردازد چه در پژوهش های داخل کشور چه در خارج از کشور، یافت نشد. بنابراین، با توجه به اهمیت حیاتی این موضوع، این پژوهش از این لحاظ که به تحلیل و بررسی مهم‌ترین شاخص‌های تأثیرگذار بر آینده‌ی امنیت سایبری در دولت می‌پردازد، بی بدیل است.

۴- اطلاعات توصیفی خبرگان

نمونه‌ی آماری این پژوهش شامل ۱۵ نفر از اساتید دانشگاه و کارشناسان حوزه‌ی امنیت سایبری است. ۱۰ نفر از (۶۶,۷ درصد) از پاسخگویان از اعضای هیأت علمی دانشگاه با مدرک دکتری و ۵ نفر (۳۳,۳) از پاسخگویان از کارشناسان حوزه‌ی امنیت سایبری با مدرک کارشناسی ارشد هستند. از اعضای هیأت علمی، ۶ نفر (۶۰ درصد) در کارشناس حوزه‌ی آینده‌پژوهی و۴ نفر (۴۰ درصد) کارشناس حوزه‌ی فناوری اطلاعات هستند. از نظر جنسیت ۱۲ نفر از پاسخگویان مرد (۸۰ درصد) و ۳ نفر (۲۰ درصد) از پاسخگویان زن هستند. در این قسمت به نمایش نمونه‌ی آماری با توجه به فراوانی خبرگان پرداخته می‌شود. در نمودار شماره‌ی (۱)، میانگین سابقه‌ی کاری و تعداد دقیق خبرگان به تفکیک حوزه‌ی کاری نمایش داده شده است.



نمودار ۱: میانگین سابقه‌ی کاری و تعداد دقیق خبرگان به تفکیک حوزه‌ی کاری

۵– روش‌شناسی پژوهش

این پژوهش در ابتدا با مطالعات کتابخانه‌ای به منظور شناسایی پیش‌ران‌ها و همچنین عوامل مؤثر، فعالیت خود را آغاز نموده و در گام بعد با بررسی به روش پرسشنامه‌ای و تحلیل آن با استفاده از روش دلفی و بهره‌مندی از نرم‌افزار «اس. پی. اس. اس. ۱»، به تخصیص اولویت در عوامل مؤثر، پرداخته شد. همچنین، در ادامه‌ی پژوهش با کمک گرفتن از اطلاعات حاصل از روش دلفی و نظر خبرگان، با تشکیل ماتریس متقابل، به تحلیل ساختاری ارتباط عوامل در حال و آینده، جهت تدوین استراتژی پرداخته شد که در انجام این مورد نرم افزار «میک مک۲» به کار گرفته شد. در مجموع می‌توان اعلام داشت روش پژوهش حاضر توصیفی – تحلیلی است و همچنین روش گردآوری اطلاعات در بخش نظری، کتابخانه‌ای و در بخش تحلیلی، پرسش‌نامه ای است و با توجه به امکان به کار گیری نتایج حاصل از این تحقیق در حل مسئله اجرایی و عملیاتی، می‌تواند به‌عنوان یک تحقیق کاربردی نیز درنظر گرفته شود.

همان‌طور که بیان شد، در این پژوهش پرسشنامه به‌عنوان ابزار گردآوری اطلاعات، گزینش شد. پرسشنامه‌ی مورد نظر از ۱۴ پیش‌ران که داری بیشترین قابلیت ارائه‌ی خدمت در قالب سایبری بود، تشکیل شده است. این پیش‌ران‌ها در۴ محور بررسی شده‌اند که احتمال ارائه‌ی خدمات در قالب سایبری، با در نظر گرفتن نحوه‌ی برقراری امنیت، در آن‌ها سنجیده شده است. با تحلیل یافته‌های حاصل از مطالعه‌ی کتابخانه‌ای و مصاحبه‌ی خبرگان، عوامل را در قالب یک پرسشنامه برخط تنظیم کردیم و آن را در اختیار خبرگان قرار دادیم. پرسشنامه‌ی ارسالی، احتمال وقوع عوامل مؤثر در پیدایش پیش‌ران‌ها را از یک طرف و میزان ضرورت حفظ امنیت و فرآیند تحقق آن را از طرف دیگر مـورد پرسش و بررسی قرار داده است. پاسخ‌ها با تبعیت

1. SPSS
2. MicMac

از طیف ۵ درجه‌ای لیکرت مورد سنجش قرار گرفته است، که در آن گزینه‌ی ۱ معرف اهمیت خیلی کم، گزینه‌ی ۲ معرف اهمیت کم، گزینه‌ی ۳ معرف اهمیت متوسط، گزینه‌ی ۴ معرف اهمیت زیاد و گزینه‌ی ۵، معرف اهمیت خیلی زیاد است. در تحلیل پرسشنامه‌های گردآورده شده، از روش دلفی[1] با استفاده از نرم‌افزار «*اس. پی. اس. اس.*» استفاده شد. همچنین در بررسی ماتریس متقابل از اعداد و حروف، ۰ و ۱ و ۲ و ۳ و P جهت نسبت دادن مقادیر تأثیرپذیری و تأثیرگذاری استفاده شد. امتیازهایی مابین ۰ تا ۳ میزان شدت در اثرگذاری متقابل و نماد پی، برای در نظر گرفتن اثرات بالقوه به‌کار می‌رود. نهایتاً تحلیل این ماتریس و بررسی نحوه‌ی گذار به وضعیت پایدار، در نرم‌افزار «میک مک» صورت گرفته است.

۵– ۱. دلفی

تکنیک دلفی، توسط هرمان کان و همکارانش (Kahn et al., 1967: 705)، به‌منظور کسب دیدگاه متخصصان درباره‌ی یک موضوع مشخص ابداع شد. این تکنیک با استفاده از توزیع پرسشنامه در بین جمعی از خبرگان و طی چند مرحله انجام می‌شود. نظرات ارائه شده در هر مرحله، بر اساس نتایج مرحله‌ی قبلی توسط شرکت کنندگان، اصلاح می‌شود. این تکنیک یک دیدگاه اجتماعی، در مورد توسعه‌ها و تحولات احتمالی آینده تولید می‌کند. هرچند، گاهی اوقات این روش به جهت فشار آوردن به دیدگاه‌های واگرا برای نیل به وفاق و همگرایی، مورد انتقاد هم قرار می‌گیرد، اما در کل یک روش بسیار مفید در حوزه‌ی آینده‌پژوهی است (طبائیان، ۱۳۸۸: ۱۲۷).

۵–۲. نرم افزار «میک مک»

نسخه کلاسیک آنالیز «میک مک»، توسط (Duperrin & Godet, 1973: 45)، به منظور تجزیه و تحلیل قدرت تأثیرگذاری و قدرت وابستگی متغیرها تهیه شده است که علاوه بر در نظرگرفتن تأثیرات مستقیم، تأثیرات غیرمستقیم را نیز در نظر می‌گیرد. بر این اساس متغیرها در چهار دسته طبقه‌بندی می‌شوند. دسته‌ی اول، حاوی متغیرهای خودمختار است، که دارای قدرت تأثیرگذاری ضعیف و قدرت وابستگی ضعیف هستند. دسته‌ی دوم، شامل متغیرهای وابسته است که قدرت تأثیرگذاری ضعیفی دارند، اما قدرت وابستگی قوی‌ای دارند. دسته‌ی سوم، شامل متغیرهای پیوندی است، که دارای قدرت محرک قوی و همچنین قدرت وابستگی قوی هستند. سرانجام دسته‌ی چهارم، از متغیرهای مستقل تشکیل شده است که دارای قدرت محرک قوی، اما قدرت وابستگی ضعیف هستند(Dubey & Ali, 2014:131). استفاده از آنالیز «میک مک» در زمینه‌ی تحقیقات مدیریت پروژه و مهندسی نیز گسترش یافته است. به‌عنوان مثال

1. Delphi

(Bredillet et al., 2018)، از تجزیه و تحلیل «میک مک» برای کشف روابط متقابل که در تغییرات دفاتر مدیریت پروژه شیوع داشتند، استفاده کردند. تجزیه و تحلیل با رویکرد «میک مک»شامل مراحل زیر خواهد بود:

شناسایی عوامل مؤثر و پیشران؛

شناسایی روابط متقابل بین عوامل؛

تشکیل ماتریس؛

تجسم شبکه؛

شناسایی مهم‌ترین عوامل، تجزیه و تحلیل کمی از روابط متقابل.

۶- یافته‌های پژوهش

۶-۱. یافته‌های کتابخانه‌ای

این پژوهش در ابتدا با مطالعات کتابخانه‌ای به منظور شناسایی پیش‌ران‌ها و همچنین عوامل مؤثر، به ۱۴ پیش‌ران که قابلیت بیشترین ارائه‌ی خدمات در بستر سایبری را دارند، رسیده است که می‌توان آن‌ها را در ۴ حوزه که شامل امکان وقوع خدمات سایبری، اهمیت برقراری امنیت، امکان حفظ امنیت توسط انسان و یا امکان حفظ امنیت توسط هوش مصنوعی می باشد، طبقه‌بندی کرد. ۱۴ پیش‌ران یاد شده به شرح زیر است:

جدول ۲. پیش‌ران‌های ارائه‌ی خدمت‌های سایبری در دولت

پیش‌ران	چرایی پیش‌ران	منابع
آموزشی	برای سنجش ادراک شهروندان در استفاده از دولت الکترونیک نیاز به ابزارهای عملی‌تری در زمینه‌ی آموزش وجود دارد، و توجه به به‌کارگیری و توسعه‌ی ابزارهای سایبری در آموزش را به عنوان یک مسئولیت برای دولت ایجاد می‌کند.	(Wong & Jackson, 2017)
	در مبارزه با شیوع بیماری کرونا، کشورها آموزش از راه دور سنتی را با آموزش از راه دور به‌عنوان یک ابزار دفاعی جایگزین کرده اند. اگرچه بسیاری از کشورها قبلاً در معرض بلایای طبیعی و انسانی بوده‌اند، اما آموزش از راه دور به همان روشی که در پی بحران ویروس کرونا اعمال شده است، به‌عنوان راه حلی برای آن بحران ها استفاده نمی‌شده است. آموزش از راه دور بحران، در فلسفه و رویه‌های خود بی‌نظیر است و از چند جهت با آموزش معمول از راه دور تفاوت اساسی دارد.	(Essa Al Lily et al., 2020)
پزشکی	استفاده از «آی. سی. تی.»[1]در زندگی روزمره شهروندان، فشاری بر دولت‌ها ایجاد می‌کند تا خدمات عمومی را با کارآیی، شفافیت بیشتر و از طریق اینترنت ارائه دهند. یک مثال عملی، اجرای پروژه‌ی بهداشت الکترونیکی است که روند ارائه‌ی خدمات بهداشتی را ساده می کند.	(Gasova & Stofkova, 2017)

1. ICT

بانکداری	توسعه‌ی بانکداری اینترنتی توسط بخش خصوصی در توانایی دولت برای راه‌اندازی خدمات آنلاین تعاملی بسیار اساسی است.	(Kitsing, 2017)
دموکراسی	استفاده از تکنولوژی دیجیتال، نه تنها در بخش دولتی، بلکه در تحقق دموکراسی، درجوامع، محل بحث جدی قرار گرفته‌است. نتایج در بین گروه‌های مختلف ذینفعان مورد مناقشه قرار می‌گیرد و فواید و مضرات این رویکرد مبهم است. در این میان برخی از مقالات تأکید بر اهمیت برقراری دموکراسی بر مبنای زیرساخت‌های سایبری را مطرح می‌کنند.	(Sundberg, 2019)
ورزشی تفریحی	از خدمات دولت الکترونیک در بخش ورزشی و تفریحی می‌توان به ایجاد مراکز اوقات فراغت، خدمات اجتماعی و ترویج ورود اجتماعی افراد دارای معلولیت جسمی به جامعه اشاره کرد.	(Gasova & Stofkova, 2017)
ارتباط جمعی	لازم است تأثیری که برنامه‌های شبکه‌های اجتماعی و رسانه‌های اجتماعی بر دولت الکترونیکی گذاشته‌اند بررسی شود و نقشی که این فناوری‌های جدید بازی کرده‌اند و همچنین پیامدهای آن‌ها برای آینده، بررسی شود. این امر به ویژه با توجه به این واقعیت که رؤسای بسیاری از دولت‌های اروپایی معتقدند خدمات عمومی مجهز به «آی. سی. تی.» تأثیر بسزایی در رشد اقتصادی، شمول و کیفیت زندگی خواهد داشت، موجب گسترش استفاده از رسانه‌های اجتماعی برای مباحثات و مبارزات ریاست جمهوری در ایالات متحده به صورت امری عادی شده است. اگرچه استفاده از برنامه‌های شبکه‌های اجتماعی و رسانه‌های اجتماعی ساده است، اما به ابزاری برای برقراری ارتباط، اوقات فراغت و تغییر تبدیل شده‌اند و انتظار می‌رود که در آینده‌ای قابل پیش‌بینی جهان ما را تحت تأثیر قرار دهد.	(Magro, 2012)
معاملاتی	در بخش مالی و معاملاتی، دولت الکترونیکی می‌تواند خدماتی چون مدیریت مالیات‌ها، یارانه‌ها، هزینه‌ی محلی برای پسماند شهری و ضایعات ساختمانی و هزینه‌ی خدمات عمومی را ارائه دهد.	(Gasova & Stofkova, 2017)
قضاوت	مدیریت سوابق، عامل اصلی موفقیت در سیستم قضایی است. سیستم مدیریت سوابق سیستماتیک، کارآمد و سازمان یافته، اطلاعات کاملی برای دادگاه‌ها جهت تضمین تصمیم بی‌طرف فراهم می‌کند. سیستم اطلاعاتی شفاف و مدیریت سوابق خوب به طور غیرمستقیم مانع سوءاستفاده از قدرت یا فساد، به تعویق انداختن پرونده و تأخیر در تصمیم‌گیری می‌شود.	(Saman & Haider, 2012)
حمل و نقل	لجستیک عامل اصلی برای مزیت رقابتی است. حمل و نقل، یک فرآیند فرعی از تدارکات، نقش مهمی در تجارت و تجارت بین‌المللی دارد. با افزایش تعداد ذینفعان و پیچیدگی عملیات، نیاز به برنامه‌های سیستم اطلاعاتی برای مدیریت حمل و نقل، اهمیت بیشتری پیدا می کند. از آنجا که نهادهای دولتی ذینفعان مهمی در برنامه‌های حمل و نقل هستند، برنامه‌های دولت الکترونیکی و حمل و نقل الکترونیکی نیز نقش مهمی در مدیریت حمل و نقل مؤثر و کارآمد دارند.	(Saatcioglu et al., 2009)
کشاورزی	استفاده کنندگان از خدمات دولت الکترونیکی کشاورزی، اهمیت زیادی به معیارهای تعامل و دسترسی می‌دهند. از این جهت توسعه‌ی زیرساخت‌های فناوری نوین به عنوان خواست در صنعت کشاورزی مطرح می‌شود.	(Bournaris, 2020)
گردشگری	«آی. سی. تی.»، شیوه‌ی تعامل و همزیستی شهروندان، شرکت ها و دولت‌ها را تغییر داده است. تحولات فناوری اطلاعات و ارتباطات شیوه‌های عملیاتی و استراتژیک سازمان ها را در سطح جهانی تغییر داده و رقابت شرکت‌ها و مناطق را در سطح جهانی تغییر داده است. حوزه‌ی گردشگری نیز از این قاعده مستثنی نیست. فناوری اطلاعات و ارتباطات تغییرات	(Kalbaska et al., 2016)

	مثبتی ایجاد می‌کند و تجربه بازدیدکنندگان گردشگری راتسهیل می‌کند.	
خدمات شهری و شهرسازی	با استفاده از بسترهای جدید، می‌توان مجموعه‌ای از خدمات دولت الکترونیکی را برای مدیریت سازندگان و ناظران عملیات در دستگاه‌های دولتی و سایر صنایع شهر هوشمند مانند شهرسازی، حفاظت از محیط زیست، حمل و نقل هوشمند، نظارت و ارزیابی منابع شهری انجام داد.	(Zhihan Lv et., 2017)
ثبت	خدمات دولت الکترونیک، در ایجاد اشتغال شخصی از طریق وب سایت و یا بر طرف کردن نیازهای ثبتی در عرض یک ساعت، مؤثر است. بدین ترتیب ایجاد یک شرکت ساده با مسئولیت محدود بسیار آسان شده است. برخلاف گذشته، برای تأسیس یک شرکت نیازی به مراجعه به دفاتر مختلف و دریافت مجوزهای مختلف یا پرداخت مبالغ بالا در دفاتر اسناد رسمی نیست.	(Janevski et al.,2014)
روانشناسی	خدمات قابل ارائه دولت الکترونیکی در زمینه‌ی روانشناسی می‌تواند شامل مراقبت‌های اولیه با استفاده از داده، مراقبت‌های دارویی و پزشکی و همچنین خدمات اضطراری باشد.	(Gasova & Stofkova, 2017)

۶-۲- محاسبه دلفی در دو مرحله

روش دلفی، پیمایشی است که به وسیله‌ی یک گروه پایش هدایت شده و شامل چندین مرحله نظرخواهی از گروه خبرگان می‌شود که برای یکدیگر ناشناس هستند، به‌طوری که دستیابی به وفاق و اجماع در خصوص پیش‌بینی قضاوتی-شهودی این خبرگان مدنظر است. پس از هر مرحله پیمایش، یک بازخورد آماری استاندارد از نتایج، به خبرگان ارائه می‌شود و توافق و امکان مخالفت در مورد جواب‌ها، بررسی می‌شود. در روش دلفی از صاحب‌نظران هر حوزه خواسته می‌شود تا به صورت مستقل، پیش‌بینی خود را از روند تحولات آتی در حوزه‌ی تخصصشان بیان کنند. (woudenberg, 1991). به عبارت دیگر، در روش دلفی ارسال پرسشنامه، جمع‌آوری و تحلیل آن در چند مرحله انجام می‌شود تا جایی که گروه مجری به این نتیجه برسد که همگرایی در پاسخ‌ها ایجاد شده و کفایت پویش را می‌تواند اعلام نماید (Young, 2009).

در پژوهش حاصل، برای تحلیل اطلاعات گردآوری شده‌ی مستخرج از نظر خبرگان، با اعمال حدآستانه‌ی ۳، به غربال عوامل مؤثر بر پیش‌ران‌ها پرداخته شد و با احتساب حدآستانه، مؤلفه‌های ورزشی‌تفریحی و کشاورزی حذف شدند. با اعلام نتایج آماری حاصل از مرحله‌ی اول دلفی به خبرگان، مجدداً نظر آن‌ها را جویا شدیم، در مرحله‌ی دوم، شاهد همگرایی میان نظرات خبرگان بودیم، به‌گونه‌ای که در تمام پیش‌ران‌ها حدآستانه رعایت شده است. همچنین در مرحله‌ی اول، مشخص شد که شاخص بانکداری و عوامل مؤثر در ترویج ارتباط اجتماعی، امتیاز قابل توجهی را به خود اختصاص داده است.

جدول۳. اطلاعات محاسبات آماری انجام شده از نظر خبرگان در مرحله‌ی اول دلفی در ۱۴ پیش‌ران و ۴ محور

ردیف	موضوع		میانگین نظرات خبرگان	درصد اجماع	مقدار وزن	رتبه		میانگین نظرات خبرگان	درصد اجماع	مقدار وزن	رتبه
۱	آموزشی	امکان وقوع سایبری	۳,۵۳۳۳۳	۶۰	۰۶۹۵۵.۰	۱۱	اهمیت برقراری امنیت	۴,۲	۴۰	۰۷۱۲۷.۰	۹
۲	پزشکی		۳,۶۶۶۶۷	۳۳۳۳.۵۳	۰۷۲۱۸.۰	۶		۴,۴۶۶۶۷	۶۰	۰۷۵۷۹.۰	۴
۳	بانکداری		۴,۴۶۶۶۷	۳۳۳۳.۵۳	۰۸۷۹۳.۰	۱		۴,۸	۸۰	۰۸۱۴۵.۰	۱
۴	دموکراسی		۳,۸	۳۳۳۳.۳۳	۰۷۴۸.۰	۵		۴,۵۳۳۳۳	۶۰	۰۷۶۹۲.۰	۳
۵	ورزشی‌تفریحی		۲,۹۳۳۳۳	۶۶۶۷.۴۶	۰۵۷۷۴.۰	۱۳		۳,۳۳۳۳۳	۳۳۳۳.۳۳	۰۵۶۵۶.۰	۱۴
۶	ارتباط جمعی		۴,۰۶۶۶۷	۶۶۶۷.۴۶	۰۸۰۰۵.۰	۲		۴,۱۳۳۳۳	۳۳۳۳.۵۳	۰۷۰۱۴.۰	۱۰
۷	معاملاتی		۳,۶۶۶۶۷	۶۶۶۷.۴۶	۰۷۲۱۸.۰	۶		۴,۶	۶۰	۰۷۸۰۵.۰	۲
۸	قضاوت		۳,۲	۳۳۳۳.۳۳	۰۶۲۹۹.۰	۱۲		۴,۲۶۶۶۷	۳۳۳۳.۵۳	۰۷۲۴.۰	۷
۹	حمل و نقل		۳,۶	۴۰	۰۷۰۸۷.۰	۹		۴,۲۶۶۶۷	۳۳۳۳.۵۳	۰۷۲۴.۰	۷
۱۰	کشاورزی		۲,۷۳۳۳۳	۶۶۶۷.۴۶	۰۵۳۸۱.۰	۱۴		۳,۴	۳۳۳۳.۵۳	۰۵۷۶۹.۰	۱۳
۱۱	گردشگری		۴	۴۰	۰۷۸۷۴.۰	۳		۴,۱۳۳۳۳	۴۰	۰۷۰۱۴.۰	۱۰
۱۲	خدمات شهری و شهرسازی		۳,۶۶۶۶۷	۴۰	۰۷۲۱۸.۰	۶		۴	۴۰	۰۶۷۸۷.۰	۱۲
۱۳	ثبت		۳,۸۶۶۶۷	۶۶۶۷.۴۶	۰۷۶۱۲.۰	۴		۴,۴۶۶۶۷	۶۶۶۷.۶۶	۰۷۵۷۹.۰	۴
۱۴	روانشناسی		۳,۶	۴۰	۰۷۰۸۷.۰	۹		۴,۳۳۳۳۳	۳۳۳۳.۵۳	۰۷۳۵۳.۰	۶
۱	آموزشی	برقراری امنیت توسط انسان	۲,۶	۶۶۶۷.۴۶	۰۶۴۱۶.۰	۱۳	برقراری امنیت توسط هوش مصنوعی	۴,۶۶۶۶۷	۶۶۶۷.۶۶	۰۷۷۰۹.۰	۱
۲	پزشکی		۲,۹۳۳۳۳	۶۶۶۷.۴۶	۰۷۲۳۹.۰	۶		۴,۴۶۶۶۷	۳۳۳۳.۵۳	۰۷۳۷۹.۰	۵
۳	بانکداری		۳	۳۳۳۳.۳۳	۰۷۴۰۴.۰	۴		۴,۶	۶۶۶۷.۶۶	۰۷۵۹۹.۰	۳
۴	دموکراسی		۳	۳۳۳۳.۵۳	۰۷۴۰۴.۰	۴		۴,۶۶۶۶۷	۶۶۶۷.۶۶	۰۷۷۰۹.۰	۱
۵	ورزشی تفریحی		۳,۴۵۴۵۵	۵۴۵۵.۵۴	۰۸۵۲۵.۰	۱		۳,۷۳۳۳۳	۴۰	۰۶۱۶۷.۰	۱۴
۶	ارتباط جمعی		۲,۶۶۶۶۷	۶۶۶۷.۴۶	۰۶۵۸۱.۰	۱۲		۴,۴	۶۰	۰۷۲۶۹.۰	۷
۷	معاملاتی		۲,۷۳۳۳۳	۶۶۶۷.۴۶	۰۶۷۴۵.۰	۱۱		۴,۴۶۶۶۷	۶۰	۰۷۳۷۹.۰	۵
۸	قضاوت		۲,۶	۶۶۶۷.۴۶	۰۶۴۱۶.۰	۱۳		۴,۱۳۳۳۳	۶۶۶۷.۴۶	۰۶۸۲۸.۰	۱۱
۹	حمل و نقل		۳,۰۶۶۶۷	۶۶۶۷.۴۶	۰۷۵۶۸.۰	۲		۴,۲	۳۳۳۳.۵۳	۰۶۹۳۸.۰	۱۰
۱۰	کشاورزی		۲,۸	۴۰	۰۶۹۱.۰	۹		۳,۹۳۳۳۳	۴۰	۰۶۴۹۸.۰	۱۳
۱۱	گردشگری		۲,۹۳۳۳۳	۳۳۳۳.۳۳	۰۷۲۳۹.۰	۶		۴,۲۶۶۶۷	۳۳۳۳.۵۳	۰۷۰۴۸.۰	۸
۱۲	خدمات شهری و شهرسازی		۲,۸۶۶۶۷	۳۳۳۳.۵۳	۰۷۰۷۴.۰	۸		۴,۲۶۶۶۷	۶۶۶۷.۴۶	۰۷۰۴۸.۰	۸
۱۳	ثبت		۲,۸	۳۳۳۳.۵۳	۰۶۹۱.۰	۹		۴,۶	۶۶۶۷.۶۶	۰۷۵۹۹.۰	۳
۱۴	روانشناسی		۳,۰۶۶۶۷	۳۳۳۳.۳۳	۰۷۵۶۸.۰	۲		۴,۱۳۳۳۳	۳۳۳۳.۵۳	۰۶۸۲۸.۰	۱۱

در مرحله‌ی دوم با حذف مؤلفه‌های ورزشی تفریحی و کشاورزی و همچنین اعلام نتایج پرسشنامه‌ی اولیه، از خبرگان درخواست شد تا به سؤالات در پرسشنامه دوم پاسخ دهند. تحلیل پاسخ‌های حاصل از پرسشنامه‌ی دوم به شرح زیر است.

جدول۴. اطلاعات محاسبات آماری انجام شده از نظر خبرگان در مرحله‌ی دوم دلفی در ۱۲پیش‌ران و ۴ محور

ردیف	موضوع		میانگین نظرات خبرگان	درصد اجماع	مقدار وزن	رتبه		میانگین نظرات خبرگان	درصد اجماع	مقدار وزن	رتبه
۱	آموزشی	امکان وقوع سایبری	۴,۰۹۰۹۱	۷۲۷۳.۷۲	۰۸۹۲۹.۰	۴	اهمیت برقراری امنیت	۴,۳۶۳۶۴	۴۵۴۵.۴۵	۰۸۳۷۷.۰	۶
۲	پزشکی		۳,۵۴۵۴۵	۵۴۵۵.۵۴	۰۷۷۳۸.۰	۱۰		۴,۲۷۲۷۳	۵۴۵۵.۵۴	۰۸۲۰۲.۰	۸
۳	بانکداری		۴,۶۳۶۳۶	۶۳۶۴.۶۳	۱۰۱۱۹.۰	۱		۴,۹۰۹۰۹	۹۰۹۱.۹۰	۰۹۴۲۴.۰	۱
۴	دموکراسی		۳,۷۲۷۲۷	۷۲۷۳.۷۲	۰۸۱۳۵.۰	۷		۴,۸۱۸۱۸	۸۱۸۲.۸۱	۰۹۲۵.۰	۲
۵	ارتباط جمعی		۴,۲۷۲۷۳	۷۲۷۳.۷۲	۰۹۳۲۵.۰	۲		۴,۲۷۲۷۳	۷۲۷۳.۷۲	۰۸۲۰۲.۰	۸
۶	معاملاتی		۴,۱۸۱۸۲	۶۳۶۴.۶۳	۰۹۱۲۷.۰	۳		۴,۵۴۵۴۵	۵۴۵۵.۵۴	۰۸۷۲۶.۰	۴
۷	قضاوت		۳,۰۹۰۹۱	۷۲۷۳.۷۲	۰۶۷۴۶.۰	۱۱		۴,۳۶۳۶۴	۶۳۶۴.۶۳	۰۸۳۷۷.۰	۶
۸	حمل و نقل		۳,۹۰۹۰۹	۳۶۳۶.۳۶	۰۸۵۳۲.۰	۵		۴,۴۵۴۵۵	۵۴۵۵.۵۴	۰۸۵۵۱.۰	۵
۹	گردشگری		۳,۹۰۹۰۹	۶۳۶۴.۶۳	۰۸۵۳۲.۰	۵		۳,۵۴۵۴۵	۵۴۵۵.۵۴	۰۶۸۰۶.۰	۱۲
۱۰	خدمات شهری و شهرسازی		۳,۷۲۷۲۷	۴۵۴۵.۴۵	۰۸۱۳۵.۰	۷		۴	۶۳۶۴.۶۳	۰۷۶۷۹.۰	۱۰
۱۱	ثبت		۳,۷۲۷۲۷	۴۵۴۵.۴۵	۰۸۱۳۵.۰	۷		۴,۶۳۶۳۶	۶۳۶۴.۶۳	۰۸۹۰۱.۰	۳
۱۲	روانشناسی		۳	۴۵۴۵.۴۵	۰۶۵۴۸.۰	۱۲		۳,۹۰۹۰۹	۶۳۶۴.۶۳	۰۷۵۰۴.۰	۱۱
۱	آموزشی	برقراری امنیت توسط انسان	۲,۶۳۶۳۶	۵۴۵۵.۵۴	۰۷۲۳۲.۰	۱۱	برقراری امنیت توسط هوش مصنوعی	۴	۴۵۴۵.۴۵	۰۸.۰	۹
۲	پزشکی		۲,۵۴۵۴۵	۶۳۶۴.۶۳	۰۶۹۸۳.۰	۱۲		۴,۰۹۰۹۱	۵۴۵۵.۵۴	۰۸۱۸۲.۰	۸
۳	بانکداری		۳,۲۷۲۷۳	۴۵۴۵.۴۵	۰۸۹۷۸.۰	۱		۴,۱۸۱۸۲	۴۵۴۵.۴۵	۰۸۳۶۴.۰	۵
۴	دموکراسی		۳	۶۳۶۴.۶۳	۰۸۲۲۹.۰	۹		۴,۵۴۵۴۵	۵۴۵۵.۵۴	۰۹۰۹۱.۰	۱
۵	ارتباط جمعی		۳,۱۸۱۸۲	۴۵۴۵.۴۵	۰۸۷۲۸.۰	۳		۴,۱۸۱۸۲	۸۱۸۲.۸۱	۰۸۳۶۴.۰	۵
۶	معاملاتی		۳,۱۸۱۸۲	۳۶۳۶.۳۶	۰۸۷۲۸.۰	۳		۴,۴۵۴۵۵	۵۴۵۵.۵۴	۰۸۹۰۹.۰	۲
۷	قضاوت		۲,۸۱۸۱۸	۴۵۴۵.۴۵	۰۷۷۳۱.۰	۱۰		۴	۳۶۳۶.۳۶	۰۸.۰	۹
۸	حمل و نقل		۳,۱۸۱۸۲	۶۳۶۴.۶۳	۰۸۷۲۸.۰	۳		۴,۲۷۲۷۳	۵۴۵۵.۵۴	۰۸۵۴۵.۰	۴
۹	گردشگری		۳,۲۷۲۷۳	۴۵۴۵.۴۵	۰۸۹۷۸.۰	۱		۴,۱۸۱۸۲	۶۳۶۴.۶۳	۰۸۳۶۴.۰	۵
۱۰	خدمات شهری و		۳,۰۹۰۹۱	۵۴۵۵.۵۴	۰۸۴۷۹.۰	۷		۴	۶۳۶۴.۶۳	۰۸.۰	۹

	شهرسازی										
۱۱	ثبت		۳,۰۹۰۹۱	۳۶۳۶.۳۶	۰۸۴۷۹.۰	۷		۴,۴۵۴۵۵	۵۴۵۵.۵۴	۰۸۹۰۹.۰	۲
۱۲	روانشناسی		۳,۱۸۱۸۲	۴۵۴۵.۴۵	۰۸۷۲۸.۰	۳		۳,۶۳۶۳۶	۶۳۶۴.۶۳	۰۷۲۷۳.۰	۱۲

۶-۲- ۱. بررسی روایی (اعتبار) و پایایی پرسشنامه

این پژوهش با شیوه‌های متداول به بررسی روایی و پایایی پرسشنامه پرداخته است. پس از طراحی اولیه‌ی پرسشنامه، آن را در اختیار خبرگان قرار دادیم تا سنجش اولیه‌ی پرسشنامه صورت پذیرد. نتایج حاصل گویای آن بود که خبرگان درک مشترکی از موضوع و سؤالات پرسشنامه دارند که این موضوع نشان از وجود روایی سازه در پرسشنامه بود. همچنین هنگام طراحی سؤالات پرسشنامه، سعی شد با مطالعه‌ی ادبیات پژوهش و مقالات مرتبط، به شناسایی شاخص‌های مؤثر و مرتبط در ارزیابی پرداخته شود. در ادامه بر اساس نظرات خبرگان غربال اولیه شکل گرفت و سپس سؤالات بر اساس شاخص‌های تأیید شده طراحی شد، بنابراین، می‌توان اذعان کرد که سوالات به روایی یا اعتبار محتوایی پرسشنامه دلالت دارد. برای بررسی پایایی پرسشنامه نیز از آلفای کرونباخ استفاده شد، که نتایج حاصل از آلفای کرونباخ به شرح زیر است:

جدول ۵. محاسبه‌ی آلفای کرونباخ در پرسشنامه‌ی دلفی

موضوع	نتیجه حاصل	
	تعداد موارد	آلفای کرونباخ
آلفای کرونباخ در سؤالات مرتبط با امکان تحقق خدمات مطرح شده در قالب سایبری.	۱۴	۰,۹۱۱
آلفای کرونباخ در سؤالات مرتبط با اهمیت برقراری امنیت در خدمات مطرح شده.	۱۴	۰,۹۱۸
آلفای کرونباخ در سؤالات مرتبط با امکان برقراری امنیت سایبری در خدمات مطرح شده به‌وسیله‌ی انسان.	۱۴	۰,۹۱۰
آلفای کرونباخ در سؤالات مرتبط با امکان برقراری امنیت‌سایبری در خدمات مطرح شده به‌وسیله‌ی هوش‌مصنوعی.	۱۴	۰,۹۳۲
آلفای کرونباخ در تمامی سؤالات پژوهش.	۱۴	۰,۹۱۱

۶-۳- بررسی ماتریس متقاطع در «میک مک»

۶-۳-۱. شناسایی عوامل مؤثر، پیش‌ران و اقسام ماتریس

مرحله‌ی اول به شناسایی عوامل مؤثر در پژوهش اختصاص دارد. عوامل مؤثری که باید آن را منتج از ادبیات تحقیقی دانست که به تأیید پنل متخصصان مورد نظر ما رسیده است. از مجموع این عوامل، ۱۴ مورد حاصل شد که با اجماع نظر خبرگان ۱۲ مورد از آن به تأیید نهایی رسید و معیار این تأیید توجه به وجه ارائه‌ی خدمت در قالب سایبری است که حفظ امنیت آن وام‌دار هوش مصنوعی است.

شناسایی پنل خبرگان بر روابط متقابل بین عوامل مؤثر در پروژه متمرکز است، این روابط متقابل در یک ماتریس$n \times n$ به نمایش درآمده است، n معرف تعداد عوامل مؤثر در ماتریس

است. به میزان تأثیری که فاکتور i از فاکتور j می‌پذیرد، مقادیری از ۰ و ۱ و ۲ و ۳ و p، نسبت می‌دهیم.

اقسام ماتریس: نرم‌افزار «میک مک» دارای چهار تعریف از ماتریس به نام‌های زیر است که موارد یک و دو، عناصر ورودی مطالعه در «میک مک» را تشخیص می‌دهند و موارد ۳ و ۴ نتایج به‌دست آمده از مطالعه و نتایجی که باید تفسیر شوند را، ارائه می‌دهند.

«ام. دی. آی.»[1]: ماتریس تأثیرات مستقیم.

«ام. پی. دی. آی.»[2]: ماتریس تأثیرات مستقیم بالقوه.

«ام. آی. آی.»[3]: ماتریس تأثیرات غیرمستقیم.

«ام. پی. آی. آی.»[4]: ماتریس تأثیرات بالقوه غیرمستقیم.

۶-۳-۲. تجسم شبکه و شناسایی مهم‌ترین عوامل، تجزیه و تحلیل کمی از روابط متقابل

این مرحله در روش پیشنهادی شامل تجسم است. تجسم در درجه‌ی اول، شامل بازنمایی داده‌ها و اطلاعات در قالب یک تصویر است. یکی از مزیت‌های مهم تجسم این است که از طریق تصاویر ذهنی قادر به تسهیل در ایجاد درک بیشتر و بسیار پیچیده‌تر است (Lengler & Eppler, 2007: 83). اهمیت ویژه‌ای که این مطالعه دارد آن است که ادبیات پژوهش به مزایای بی‌شمار تجسم اشاره می‌کند. به‌عنوان مثال: تجسم یادگیری را افزایش می‌دهد (Meyer, 1997: 275). در واقع، نمایشگرهای گرافیکی عملکرد تصمیم‌گیری در کارهایی مانند تشخیص و مقایسه روندها یا کشف الگوهای روابط بین متغیرها را بهبود می‌بخشند (Liu et al., 2014: 1373).

در ادامه رویکرد توسعه یافته، شامل تجزیه و تحلیل کمی از روابط متقابل برای شناسایی مهم‌ترین عوامل است. برای تحلیل روابط متقابل بین عوامل، از دو وجه قدرت محرکه و قدرت وابستگی استفاده خواهیم کرد. چگالی شبکه می‌تواند برای ارزیابی پیچیدگی روابط متقابل در یک شبکه استفاده شود. از ادبیات پژوهش می‌توان تصور کرد که با افزایش پیچیدگی پژوهش، پتانسیل تأثیر در عوامل مؤثر نیز افزایش یابد (Mirza & Ehsan, 2017: 108).

به منظور شناسایی بهتر روابط آینده، اطلاعات حاصل از ماتریس «ام. دی. آی.» جهت تشکیل ماتریس «ام. پی. دی. آی.» در نظر گرفته شد و به دنبال آن ماتریس «ام. پی. آی. آی» با تکرار ۵ مرحله پی‌درپی تشکیل شد. خروجی کار شاخص پرشدگی ۹۱,۶۶ است که شاخص قابل قبولی برای صحت عملکرد حساب می‌آید.

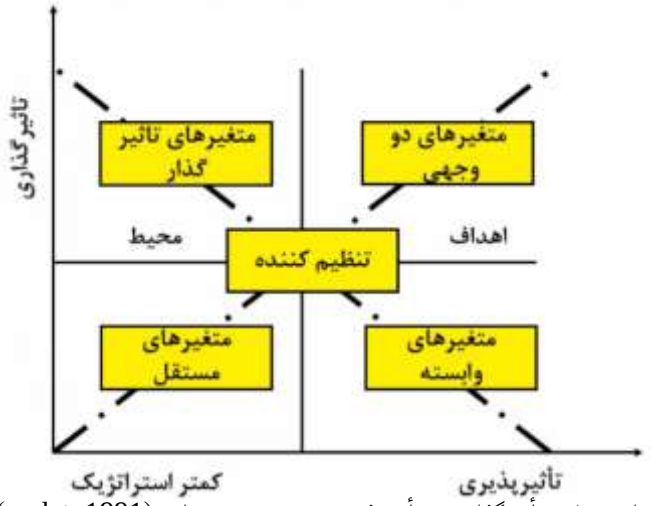
1.MDI
2. MPDI
3. MII
4. MPII

جدول۶. اطلاعات کمی دادهای وارد شده در نرم‌افزار «میک مک»

پارامتر	سایز	تعداد تکرار	تعداد صفر	تعداد یک	تعداد دو	تعداد۳	تعداد p	مجموع	پرشدگی
مقدار	۱۲	۵	۱۲	۵	۶۱	۴۹	۱۴	۱۸	%۶۷.۹۱

۶-۴. وضعیت متغیرها روی نواحی پلن اثرگذار و اثربخش

متغیرها بر اساس موقعیت قرارگیری به چهارنوع تقسیم می‌شوند که هرکدام در یکی از نواحی چهارگانه ی اثرگذاری-اثرپذیری قرار می‌گیرند. متغیرهای نواحی یک (دووجهی یا راهبردی) دارای دو ویژگی مشترک تأثیرگذاری و تأثیرپذیری زیاد می‌باشند که هرتغییری روی این متغییرها در سایر متغیرها نیز واکنش و تغییر ایجاد خواهد کرد. متغیرهای ناحیه‌ی ۲، بیش از آن‌که از سیستم تأثیر بپذیرند، برآن اثر می‌گذارند. متغیرهای ناحیه‌ی ۳، به‌طور میانگین أثرگذاری و أثرپذیری کمتری دارند؛ به این معنی که نه زیاد از سیستم تأثیر می‌پذیرند و نه زیاد بر آن تأثیر می‌گذارند. و در نهایت متغیرهای ناحیه‌ی چهار تأثیرگذاری کمی بر سیستم دارند و خود تابع تغییرات در سایر متغیر ها هستند (Godet et al., 2003).

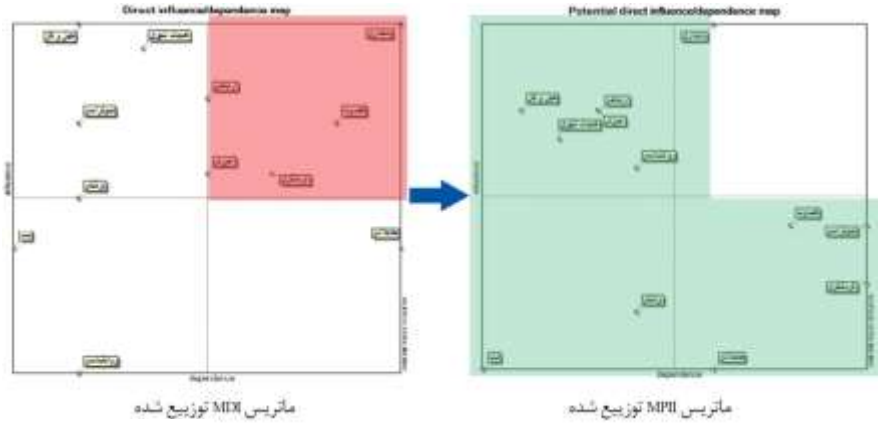


نمودار ۲. پلان تأثیرگذاری و تأثیرپذیری در محور مختصات (godet, 1991).

۶-۵. بررسی سیستم‌های پایدار و ناپایدار در خروجی «میک مک»

در تحلیل اثرات متقابل با نرم‌افزار «میک مک»، شیوه‌ی توزیع متغیرها در صفحه‌ی پرا کندگی، نشان دهنده‌ی میزان پایداری و یا ناپایداری سیستم است که شاهد دو نوع توزیع تعریف شده به نام سیستم‌های پایدار و سیستم‌های ناپایدار هستیم. در سیستم‌های پایدار توزیع متغیرها به صورت L انگلیسی است؛ یعنی برخی متغیرها دارای تأثیرگذاری بالا و برخی دارای تأثیرپذیری بالا هستند. در این سیستم، جایگاه و نقش هریک از عوامل مشخص است. وضعیت در سیستم‌های ناپایدار پیچیده‌تر از سیستم‌های پایدار است. در این سیستم‌ها، متغیرها حول

محور قطری صفحه پراکنده هستند و در بیشتر مواقع حالت بینابینی از تأثیرگذاری و تأثیرپذیری را نشان می‌دهند. در این سیستم نیز راه‌هایی ترسیم شده است که می‌تواند راهنمای گزینش و شناسایی عوامل کلیدی باشد (Godet et al., 2003).



نمودار ۳. بررسی پایداری پیش‌ران‌های مورد بررسی در نرم‌افزار «میک مک»

در ترسیم شکل از حالت «ام. دی. آی.» به حالت «ام. پی. آی.»، با کاسته شدن از مؤلفه‌های ریسک که پخش شده در انتهای محور نمودارند، گذار سیستم از حالت ناپایدار به حالت پایدار مشاهده شد، این امر گویای ثبات متغیرهای تأثیرگذار و تداوم تأثیر آن‌ها بر سایر متغیرها است. از جمله متغیرهای تأثیرگذار را می‌توان متغیرهای محیطی و زیربنایی از جمله حمل و نقل، خدمات شهری، حوزه‌ی ارتباطات، آموزش و روانشانسی دانست که توانایی اثربخشی بالقوه بر سایر متغیرها داشته باشند.

۶-۶. بررسی متغیرهای استراتژیک

متغیرهایی قابلیت تأثیرگذاری استراتژیک را دارند که اولاً قابل دستکاری و کنترل باشند، و ثانیاً روی پویایی و تغییر سیستم مؤثر واقع شوند. تأثیر این مورد را می‌توان در متغییرهایی دید که در حوالی خط قطری ناحیه‌ی اول و سوم قرار گیرند. به‌طور کلی می‌توان اعلام داشت هرچه از انتهای ناحیه‌ی سوم به سمت انتهای ناحیه‌ی اول شبکه‌ی مختصات نزدیک شویم، به‌میزان اهمیت و استراتژیک بودن متغیر، افزوده می‌شود.

در ادامه‌ی شناسایی متغییرهای استراتژیک می‌توان با تقسیم آن به دو نوع متغیر ریسک و هدف به تحلیل دقیق‌تری از عوامل پرداخت. متغیرهای ریسک پیرامون خط قطری شمال شرقی قرار گرفته‌اند و ظرفیت بالایی جهت تبدیل شدن به بازیگران کلیدی سیستم دارند و به علت دارا بودن حالت ناپایدار، پتانسیل تبدیل به نقطه‌ی انفصال سیستم را نیز دارا هستند. از متغییرهای

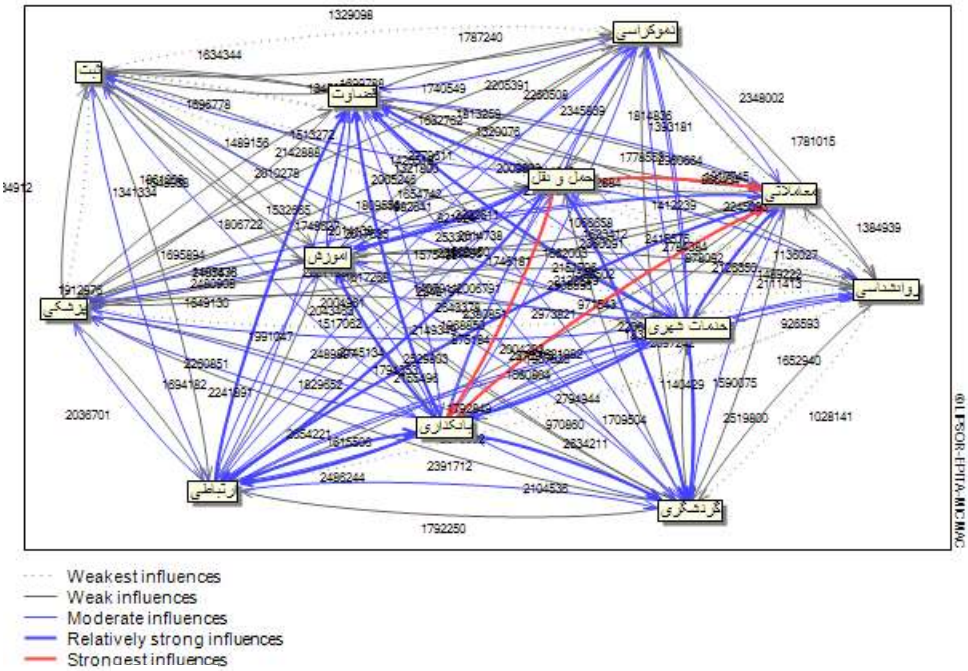
ریسک در این پژوهش می‌توان به حوزه‌ی آموزش و خدمات ارتباطی اشاره داشت. متغیرهای هدف در جنوب خط قطری شمال شرق قرار می‌گیرند و بیشتر از آن‌که تأثیرگذار باشند تأثیرپذیر هستند، با دستکاری این عوامل می‌توان به تکامل سیستم دست یافت، این متغیرها بیشتر از آن‌که نتیجه‌ی سیستم باشند، در اهداف سیستم جای خواهند گرفت. گردشگری و قضاوت از جمله متغیرهای هدف هستند. حوزه‌ی بانکداری هم قابلیت ریسک و هم قابلیت هدف را دارا است.

نمودار ۴. بررسی متغییرهای ریسک و هدف در نرم‌افزار «میک مک»

۶-۷. تحلیل گراف أثرگذاری

گراف اثرگذاری گرافی است منتج از ماتریس روابط که در برگیرنده‌ی اثرگذاری عوامل بر یکدیگر است و می‌تواند نمایانگر روابط متغیرها و چگونگی اثرگذاری آن‌ها بر یک‌دیگر باشد. در ترسیم این گراف از خطوط قرمز و آبی کمک گرفته شده است و ترسیم آن به‌گونه‌ای است که از گراف جهت‌دار بهره گرفته شده است. این جهت بیانگر جهت أثرگذاری متغیر است. خطوط قرمز نشان دهنده‌ی أثرگذای شدید عوامل بر یکدیگر و خطوط آبی با تفاوت در ضخامت، روابط متوسط تا ضعیف را نشان می‌دهند (علی اکبری و همکاران، ۱۳۹۷). نمودار ۵، نمایی کلی از توزیع متغیرها را در ۱۴ بعد از ابعاد بروز اجرایی حاکمیت، به منظور توسعه‌ی خدمات سایبری نشان می‌دهد.

همان‌گونه که مشخص شد، سه ضلعی بانک-حمل و نقل- معاملاتی، دارای بیشترین اثرگذاری متقابل است. در نظر گرفتن این سه ضلع و برنامه‌ریزی در جهت ارتقای این چرخه، می‌تواند تأثیرات مهمی در جهت ارتقای سایر عوامل داشته باشد. این موضوع نشان دهنده‌ی اهمیت بالای این سه شاخص در تصمیمات استراتژیک است.



نمودار ۵. گراف تأثیرپذیری و تأثیرگذاری پیش‌ران‌ها از یکدیگر در نرم‌افزار «میک مک»

۶-۸. سهم اثرگذاری و اثرپذیری غیرمستقیم به‌صورت مقایسه‌ای

لازمه‌ی محاسبه‌ی اثرات غیرمستقیم در ماتریس اثرات متقابل، ضرب متوالی ماتریسی است، این موضوع مؤیدی است بر بروز اعداد چندرقمی، که تحلیل و مقایسه‌ی نسبت آن به اثرمستقیم، دستخوش پیچیدگی و دشواری قرار می‌گیرد. در راستای سهولت تحلیل، نرم افزار «میک مک» جدول سهم عوامل را بر اساس اثرهای مستقیم و غیرمستقیم، در مقیاس ده‌هزار ارائه می‌دهد، نتیجه آن است که، أثرپذیری و أثرگذاری‌ها در مقیاس ده هزار محاسبه می‌شود و عدد نسبت داده شده به هرکدام، بیانگر سهم آن عامل از کل سیستم است. سهم هرکدام از عوامل مؤثر از کل را می‌توان در جدول (۸) ملاحظه و بررسی کرد. همان‌طور که در این جدول مشخص است، أثرگذاری مستقیم و اثرگذاری غیرمستقیم تنها در عوامل اول و دوم تفاوت دارند و سایر عوامل یکسان‌اند. این امر گویای حفظ میزان نسبت فعلی متغیرها در آینده خواهد بود.

جدول۷. بررسی مقایسه‌ای انواع أثرگذاری و أثرپذیری در نرم‌افزار «میک مک»

تأثیرپذیری غیرمستقیم	عنوان	تأثیرگذاری غیرمستقیم	عنوان	تأثیرپذیری مستقیم	عنوان	تأثیرگذاری مستقیم	عنوان	امتیاز
۹۸۸	بانکداری	۱۱۰۰	حمل و نقل	۹۹۵	بانکداری	۱۰۹۴	بانکداری	۱
۹۸۴	معاملاتی	۱۰۸۱	بانکداری	۹۹۵	معاملاتی	۱۰۹۴	حمل و نقل	۲
۹۲۳	قضاوت	۱۰۳۴	خدمات شهری	۹۴۵	قضاوت	۱۰۴۴	خدمات شهری	۳
۸۹۰	گردشگری	۹۸۲	ارتباطی	۸۹۵	گردشگری	۹۴۵	ارتباطی	۴
۸۴۱	آموزش	۸۷۲	دموکراسی	۸۴۵	آموزش	۸۹۵	دموکراسی	۵
۸۴۰	ارتباطی	۸۷۱	قضاوت	۸۴۵	ارتباطی	۸۹۵	قضاوت	۶
۸۰۲	خدمات شهری	۷۹۵	آموزش	۷۹۶	خدمات شهری	۷۹۶	آموزش	۷
۷۶۰	حمل و نقل	۷۷۸	گردشگری	۷۴۶	پزشکی	۷۹۶	گردشگری	۸
۷۵۸	پزشکی	۷۳۶	پزشکی	۷۴۶	دموکراسی	۷۴۶	پزشکی	۹
۷۵۰	دموکراسی	۶۷۸	معاملاتی	۷۴۶	حمل و نقل	۶۴۶	معاملاتی	۱۰
۷۴۶	روانشناسی	۶۴۶	ثبت	۷۴۶	روانشناسی	۶۴۶	ثبت	۱۱
۷۱۲	ثبت	۴۲۲	روانشناسی	۶۹۶	ثبت	۳۹۸	روانشناسی	۱۲

۷– نتیجه‌گیری و پیشنهادات آینده

توسعه‌ی فناوری اطلاعات همراه با ظهور ابزارهای جدید، می‌تواند پدیدآورنده‌ی ماهیتی نو و تغییر در سبک زندگی فردی و جمعی شود، تغییراتی که اقتضائات جدید را در جامعه ایجاد خواهد کرد، تا جایی که می‌توان گسترش این اقتضائات را در تغییر مطالبات مردم از دولت‌ها نیز شاهد بود. در این راستا ارائه‌ی خدمات در قالب سایبری را می‌توان به‌عنوان یکی از این تغییرسازها بررسی کرد. در این بررسی، تحلیل نقش دولت حائز اهمیت خواهد بود. وضع قوانین و نقشه‌ی راه برای توسعه دولت در جهت گذار به سطح دولت الکترونیک پیش‌روی گسترش ارائه خدمات سایبری در سطح جهانی است. باید تدوین قوانین برای خدماتی که توانسته اقبال عمومی را تا حدی به خود جلب کند و تبدیل به یک مطالبه‌ی عمومی از سمت مردم به دولت‌هایشان شود و همچنین دغدغه‌ی فراهم‌سازی بسترهای این امر به‌عنوان یک خواست عمومی، لحاظ شود. عموم دولت‌ها خواسته یا ناخواسته در مسیری هدایت می‌شوند که نه تنها توان مقابله برای عدم پذیرش این قبیل فناوری‌های نوظهور را نخواهند داشت، بلکه این احتمال نیز وجود دارد تا از ترس عقب ماندگی، بدون شناسایی صحیح اقتضائات این تکنولوژی، شتاب‌زده عمل کرده و پذیرای خطراتی از جمله نقض امنیت شوند. در دوران دیجیتال، امنیت سایبری به یک نگرانی اساسی تبدیل شده است. نقض داده‌ها، سرقت «آی.

دی.»[1]، شکستن رمز کپچا[2] و سایر خطرات از این دست بسیار زیاد است. این خطرات میلیون‌ها نفر از افراد و سازمان‌ها را نیز تحت تأثیر قرار داده است. این چالش‌ها همیشه در حال ابداع کنترل‌ها و رویه‌های درست و اجرای آن‌ها با حساسیت تمام برای مقابله با حملات سایبری و جرایم بی‌پایان بوده است. اما باید پذیرفت با توجه به پیشرفت‌های اخیر در هوش مصنوعی، خطر حملات و جنایات سایبری به‌صورت نمایی افزایش یافته است. این توپ آتش را نمی‌توان دور از مجرمان سایبری نگه داشت. با این تفاسیر می‌توان اعلام داشت حملات سایبری «عادی» اکنون به حملات سایبری «هوشمندانه» تبدیل شده‌اند. این پژوهش با در نظر گرفتن اهمیت تسریع در اجرای برنامه‌ی عملیاتی دولت، جهت ارائه‌ی خدمات سایبری و پیشروی به سمت تحقق دولت الکترونیک به رتبه‌بندی پیش‌ران‌های لازم برای تحقق ارائه‌ی خدمات سایبری در دولت پرداخته است و با توجه به اهمیت برقراری امنیت و نحوه‌ی اجرای آن و همچنین در نظر گرفتن تأثیرپذیری عوامل بر یکدیگر، زمینه را جهت تحلیل مناسب برای رسیدن به یک ساختار پایدار، فراهم می‌کند. خدماتی که می‌تواند به‌عنوان پیش‌ران دراین حوزه شناخته شده و مورد ارزیابی و رتبه‌بندی اولیه قرار گیرند. برای انجام این امور از روش دلفی و ماتریس متقابل استفاده شد که خروجی اطلاعات در نرم افزارهای «*اس. پی. اس. اس.*» و «میک مک» تولید و بررسی شده است. با توجه به مطالبی که اشاره شد به توصیه سه گام در تدوین برنامه‌ی عملیاتی دولت، جهت تحقق پایداری در ارائه‌ی خدمات الکترونیکی رسیده‌ایم که به شرح زیر می‌باشد.

گام اول: پرداختن به متغیرهای ریسک و هدف. توجه به عواملی در اولویت قرار دارد که بیشترین تأثیرپذیری و تأثیرگذاری بر سایر عوامل دارند و انتظار می رود با توجه به این مؤلفه‌ها، آینده‌ی دولت الکترونیک در حوزه‌ی اجرا و امنیت با پایداری روبه‌رو باشد. این عوامل شامل پیش‌ران‌های: بانکی- آموزش- بستر سازی ارتباطات اجتماعی-قضاوت- معاملاتی وگردشگری است.

گام دوم: پرداختن به متغییرها با تأثیرگذاری بالا. این گام به اموری اختصاص می‌یابد که از میزان تأثیرپذیری کمتری نسبت به موارد گام اول برخوردار هستند. این عوامل شامل خدمات شهری و شهرسازی-دموکراسی- حمل و نقل و پزشکی است.

گام سوم: پرداختن به سایر عوامل موجود در پژوهش. در گام سوم از عواملی می‌توان یاد کرد که تأثیرپذیری و تأثیرگذاری پایین‌تری نسبت به سایر پیش‌ران‌هایی که در دو گام بالا مطرح شد، دارند، دو پیش‌ران، ثبت و روانشناسی در این دسته قرار می‌گیرند.

1. ID
2. Captcha

در این پژوهش با در نظر گرفتن فاکتور برقراری امنیت هوشمند به شناسایی و اولویت‌بندی پیش‌ران‌هایی پرداختیم که بیشترین قابلیت ارائه‌ی خدمات در بستر سایبری را دارند. بر این اساس پیشنهاد می‌شود افرادی که علاقه‌مند به پژوهش و تکمیل این موضوع در آینده هستند به بررسی پیش‌ران‌های هر حوزه در قالب مقالات جداگانه بپردازند.

کتابنامه

۱.شجاعان، امیر و همکاران. (۱۳۹۸). تحقق حاکمیت الکترونیک ایران: گامی به سوی دولت هوشمند. ***دو فصلنامه‌ی علمی پژوهشی مدیریت بحران***.۸(۱): ۴۹-۵۹.

۲.طبائیان، کمال. (۱۳۸۸). دلفی یکی از فنون مورد استفاده در آینده‌پژوهی. فصلنامه‌ی آینده‌پژوهی، مفاهیم و روش‌ها، شماره‌ی ۴: ۱۲۷-۱۴۰.

۳.علی اکبری، اسماعیل و همکاران. (۱۳۹۷). شناسایی پیش‌ران‌های مؤثر بر وضعیت آینده‌ی گردشگری پایدار شهر کرمان با رویکرد آینده‌پژوهی. ***فصلنامه‌ی علمی‌پژوهشی گردشگری و توسعه‌ی***. ۷(۱): ۱۵۶-۱۷۸.

References

1. Abbas, N., Tanveer A., Ullah Shah, S. H., Omar, M., & Woo Park, H. (2019). Investigating the applications of artificial intelligence in cyber security. Scientometrics*volume*, 121(2):1189–1211.

2. Aftergood, S. (2017). Cybersecurity: The cold war online," *Nature*, 547(2):30-31.

3. Akhtar, N. & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: a survey. ***IEEE*** *Access*, 6:14410 - 14430.

4. Al Lily, A., Fathy Ismail, A., Abunasser, F., & Alqahtani, R. (2020). Distance Education as a Response to Pandemics: Coronavirus and Arab Culture. ***Technology in Society***,63(2): 105-120.

5. AliAkbar, I., Ahmadpour, A., & Jalalabadi, L. (1397). Identifying drivers for the future of sustainable tourism in Kerman with a futures research approach. ***Journal of Tourism and Development***. 7: 156-175. (In Persian)

6. Anon, N. (2020). [online] Pros and Cons of Artificial Intelligence*:* https://www.linkedin.com/pulse/pros-cons-artificial-intelligence-mikefekety.

7. Barth, T., Arnold, E. .(1999). Artificial intelligence and administrative discretion: implications forpublic administration.***Am. Rev. Public Adm,***29(4): 332–351.

8. Bhatele, K., Sharivastava, H., & Kumari, N. (2017) The Role of ArtificialIntelligence in Cyber Security. ***Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems,*** 2017: 175-176.

9. Bournaris, T. (2020). Evaluation of e-GovernmentWeb Portals: The Case of Agricultural e-Government Services in Greece. ***Agronomy***, 10(7):932.

10. Bredillet, C., Tywoniak, S., & Tootoonchy, M. (2018). Why and how do project management offices change? A structural analysis approach. ***International Journal of Project Management***, 36(5), 744–761.
11. Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., Henke, N., & Trench, M. (2018). Artificial intelligence–the next digital frontier. ***McKinsey Glob Institute***, 17: 224-226.
12. Dasoriya R., Rajpopat J., Jamar R., & Maurya, M. (2018). The Uncertain Future of Artificial Intelligence,***2018 8th International Conference on Cloud Computing, Data Science & Engineering***,: 458-461.
13. Deibert, R. & Rohozinski, R. (2010).risking security: Policies and paradoxes of cyberspace security. ***International Political Sociology***, 4 (1): 15– 32.
14. Duperrin, J., & Godet, M. (1973). Methode de hierarchisation des elements d'un Systeme, ***Rapport Economique du CEA***, 5: 45-51.
15. Dubey, R. & Ali, S. (2014). Identification of flexible manufacturing system dimensions and their interrelationship using total interpretive structural modelling and fuzzy MICMAC analysis. ***Global Journal of Flexible Systems Management***, 15 (2), 131–143.
16. Gasova, K. & Stofkova, K. (2017). E-Government as a quality improvement tool for citizens' services. *TRANSCOM 2017:* ***International scientific conference on sustainable, modern and safe transport***,192(1): 225 – 230.
17. Geluvaraj, B., Satwik, P., & Ashok Kumar, T. (2019). The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. ***Conference: International Conference on SecurityAt: Garden City University,*** Bangalore.
18. Godet, A. J., Meunier, M. F., & Roubelat, F.,(2003). Structural analysis with the MICMAC,***method & actors' strategy with MACTOR method, FuturesResearch Methodology,*** 2:135-140.
19. Godet, M. (1991). From anticipation to action, ***UNESCO publishing***. Paris.
20. Golovko, V. (2017). Deep learning: an overview and main paradigms. *Opt Memory Neur Netw*, 26(1):1-17.
21. Guan, ZT., Li J., & Wu L. F. (2017). Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid.***IEEE Internet Things***, 4(6): 1934-1944.
22. Hamet, P. & Tremblay, J. (2017) Artificial intelligence in medicine. ***Metabolism journal***, 2017: 89-12.
23. Hung, S., Chang, C., & Yu, T. (2006). Determinants of user acceptance of the e-government services:the case of online tax filing and payment system. ***Gov. Inf. Q***, *23(1)*: 97–122.
24. Iqbal, S. & Pippon-Young, L. (2009). The Delphi method. ***Nursing Research***, 46(2), 116–118.
25. Janevski, Z et al. (2014). Business benefits from e-government services: case of Slovenia and Macedonia. ***Economic Development***, 12(3): 13-27.

26. Jian-Hua, L. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19: 1462-1474.
27. Johnson, J. (2019). Artificial intelligence & future warfare:implications for international security ***Defense & Security Analysis***,35: 1-23.
28. Kalbaska, N., Janowski, T., Estevez, E,. & Cantoni, L. (2016). E-Government Relationships Framework in the Tourism Domain. A First Map. ***Information and Communication Technologies in Tourism - Proceedings of the International Conference in Bilbao (Spain)***. *New York*, pp: 73-87.
29. Kahn, H. & Wiener, A. (1967). The Next Thirty-Three Years: A Framework for Speculation. ***Dœdalus****:* 705-732.
30. Kitsing, M. (2017). Internet Banking as a Platform for E-Government. ***Annual International Conference on Innovation and Entrepreneurship***,30: 99-107
31. Kumar, N., Kharkwal, N., Kohli, R., & Choudhary, S. (2016). Ethical aspects and future of artificial intelligence.***2016 International Conference on Innovation and Challenges in Cyber Security*** *(ICICCS-INBUSH*: 111-114
32. Lamberti, L., Benedetti, M., & Chen, S.(2014). Benefits sought by citizens and channel attitudes formultichannel payment services: evidence from Italy. ***Gov. Inf. Q.*** 31(4): 596-609.
33. Larrocha, E., Minguet, J., Díaz, G., Castro, M., & Vara, A. (2010). Filling the gap of Information Security Management inside ITIL: proposals for postgraduate students. ***IEEE EDUCON Edu.*** Engg, pp: 907-912.
34. Lengler, R. & Eppler, M. (2007). Towards a periodic table of visualization methods for management. ***InProceedings of the IASTED International Conference on Graphics and Visualization in Engineering***, pp: 83–88.
35. Li, L., Ota, K., & Dong, M. X. (2018). Deep learning for smart industry. ***efficient manufacture inspection system with fog computing. IEEE Trans Ind Inform***, 14(10): 4665- 4673.
36. Liu, S., Cui, W., Wu, Y., & Liu, M. (2014). A survey on information visualization: ***Recent advances and challenges. The Visual Computer***, 30(12): 1373–1393
37. Lv, Z,. Li, X,. Wang, W,. Zhang, B,. Hu, J,. & Feng, S. (2017).Government affairs service platform for smart city. ***Future Generation Computer Systems***: 81.
38. Magro, M. (2012). A Review of Social Media Use in E-Government. Administrative Sciences, 2(2):148-161.
39. Meyer, J. A. (1997). The acceptance of visual information in management. ***Information & Management***, 32(6): 275–287.
40. Mikhaylov, S., Esteve, M., & Campion, A. (2018). Artificial intelligence for the public sector:opportunities and challenges of cross-sector collaboration. Philos. ***Trans. R. Soc***, 37(5): 124-140.

41. Milenkoski A., Vieira M., Kounev S., Avritzer A., & Payne, B. D. (2015). Evaluating computer intrusion detection systems: A survey of commonpractices, ***ACM Comput. Surv***.,48(2):1-41.
42. Mirza, E. & Ehsan, N. (2017). Quantification of project execution complexity and its effect on performance of infrastructure development projects. ***Engineering Management Journal***, 29(2), 108–123.
43. Mohd Saman, W. & Haider, A. (2012). Electronic court records management in Malaysia: A case study. ***Journal of e-Government Studies and Best Practices***. 2: 1122-1133.
44. Nappo, S. (2017). The Role of Artificial Intelligencein Cyber Security. ***Goodreads***.75(2): 112-138.
45. Pereira, T. & Santos, H. (2010). A security audit framework to manage Information. ***Global Security, Safety and Sustainability***: 9-18.
46. Reis, J., Amorim, M., Melão, N., & Matos, P. (2018). Digital transformation: a literature review andguidelines for future research. In: ***Trends and Advances in Information Systems andTechnologies, WorldCIST***, Springer, 2018: 411-421.
47. Saatcioglu, O., Deveci, D., & Cerit, G. (2009). Logistics and transportation information systems in Turkey: E-government perspectives. Transforming Government People Process and Policy. 3(2):144-162.
48. Shanmugam K., Khairunnisha Zainal, N., & Gnanasekaren, Ch.(2019). Technology Foresight In The Virtual Learning Environment in Malaysia. ***Journal of Physics: Conference Series.*** 1228.
49. Shojaan, A., Taghavifard, T,. Elyasi, M., & Mohammadi, M. (2018). The Realization of Electronic Governance in Iran: A Step to the Intelligent Government. ***Journal of Emergency Management (JOEM).*** 8: 49-59. (In Persian).
50. Sundberg, L. (2019). Electronic government: Towards e-democracy or democracy at risk?.***Safety Science***,118:22:23.
51. Tabaeyan, K. (1388). Delphi is one of the techniques used in Futurology, Concepts and Methods), ***Defense Educational and Research Institute,*** 1388:127-1.(In Persian)
52. Thuraisingham, B. M. (2020). Can AI be for Good in the Midst of Security Attacks and Privacy Violations?.***Proceedings*** *ACM CODASPY*, 2020: 1-10.
53. Wazid M., Zeadally S., & Das A. K. (2019). Mobile banking: Malware threats and security solutions, ***IEEE ConsumerElectronics Magazine***, 8: 56-60.
54. Wegmann, A., Regev, G., Garret, G., & Maréchal, F. (2008). Specifying Services for ITIL Service Management. *Proc.* ***Int. Workshop Service-Oriented Computing Consequences for Engineering Requirements***, 2008:1-8.
55. Wirtz, B., Weyerer, J., & Geyer, C. (2018). Artificial intelligence and the public sector–applicationsand challenges. ***Int. J. Public Adm***, 13(7): 1–20

56. Wong, M. & Jackson, S. (2017). User Satisfaction Evaluation of Malaysian E-Government Education Services. ***2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)***: 27-29.
57. Woudenberg, f.(1991). an evaluation of Delphi . ***Technological forecasting and social change***, 40: 131-150.
58. Zegers, N. (2006). A methodology for improving information security incident identification and response. ***Master Thesis Inform.& Econom, Erasmus Univ. Rotterdam,*** 18: 57-60.