ITRC ICT Research Institute (Iran Telecommunication Research Center)

Journal of Information and Communication Technology

Iranian Society of Information and Communication Technology

Volume 16, Issue 59-60, Spring and Summer 2024, pp. 167-178

Identifying the Key Drivers of Digital Signature Implementation in Iran (Using Fuzzy Delphi Method)

Ghorbanali Mehrabani[1]*, Fatemeh Zargaran Khouzani[2]

[1] Ph.D. in Strategic management, Faculty of Management, Supreme National Defense University, Tehran, Iran
[2] Ph.D. in Business Management, Faculty of Management, Allameh Tabataba'i University, Tehran, Iran

Received: 04 February 2023, Revised: 25 February 2023, Accepted: 02 June 2023
Paper type: Research

Abstract

Despite the emphasis of researchers and experts on the need to implement digital signatures and the progress of technology towards the digitization of all affairs and electronic governance, Iran is still facing the challenge of implementing digital signatures. The purpose of this article is to identify and analyze the key drivers of digital signature implementation in Iran with a fuzzy Delphi approach. In terms of practical purpose and in terms of information gathering, the research has benefited from a hybrid approach. The statistical community consists of all experts and specialists in the field of information technology and digital signature and articles in this field. The sample size of the statistical community of experts is 13 people who were selected by the purposeful sampling method. 31 articles were selected based on their availability and downloadable, non-technical nature, and relevance to the topic. The method of data analysis was done according to the fuzzy Delphi approach. Validity and reliability were calculated and confirmed using the CVR index and Cohen's kappa test with coefficients of 0.83 and 0.93, respectively. The results prove that the key drivers of digital signature implementation in Iran include 5 main dimensions and 30 concepts, which are 1) security (information confidentiality, information security, sender authentication, document authentication, privacy protection, trust between parties), 2) business (digital business models, communication needs, staff management, organization size, organizational structure, organization resources, organizational culture, top managers, competition ecosystem, e-governance), 3) user (perceived convenience, perceived benefit, consumer behavior, consumer literacy, consumer lifestyle), 4) technical (development of technical infrastructure, systems integration, system complexity, system tanks, design quality, technical speed of certificate production and verification, impermeability of hackers) and 5) Legal (legal licenses, penal laws, legislative body, e-commerce laws). It is suggested that in the field of digital signature implementation, special attention should be paid to rewriting rules, training users, creating a security culture, and digital signature policymakers should invite knowledge-based companies to cooperate in developing infrastructure and making relevant software competitive.

Keywords: Digital Signature, Digital Transformation, fuzzy Delphi, Information Security, Authentication, Key Drivers.

* Corresponding Author's email: a.mehrabanii54@gmail.com

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال شانزدهم، شماره های ۵۹ و ۶۰، بهار و تابستان ۱۴۰۳، صفحه ۱۶۷ الی ۱۷۸

شناسایی پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال در ایران (به روش دلفی فازی)

قربانعلی مهربانی [۱*]، فاطمه زرگران خوزانی [۲]

[۱] دکتری مدیریت راهبردی، دانشگاه عالی دفاع ملی، تهران، ایران

[۲] دکتری مدیریت بازرگانی، دانشگاه علامه طباطبائی، تهران، ایران

تاریخ دریافت: ۱۴۰۱/۱۱/۱۵ تاریخ بازبینی: ۱۴۰۱/۱۲/۰۶ تاریخ پذیرش: ۱۴۰۲/۰۳/۱۲

نوع مقاله: پژوهشی

چکیده

با وجود تأکید محققان و متخصصان بر لزوم پیاده‌سازی امضای دیجیتال و سیر و روند پیشروی تکنولوژی به سمت دیجیتالی شدن همه امور و حکمرانی الکترونیک، همچنان ایران با چالش پیاده‌سازی امضای دیجیتال در سازمان‌های خود روبرو است. هدف این مقاله، شناسایی و واکاوی پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال در ایران با رویکرد دلفی فازی است. پژوهش ازنظر هدف کاربردی و از لحاظ گردآوری اطلاعات، از رویکرد فراترکیب بهره برده است. جامعه آماری را خبرگان و متخصصان حوزه فناوری اطلاعات و امضای دیجیتال و مقالات این حوزه تشکیل می‌دهند. حجم نمونه جامعه آماری خبرگان ۱۳ نفر است که با روش نمونه‌گیری هدفمند انتخاب شدند. مقالات نیز براساس در دسترس و دانلود بودن، غیرفنی بودن و مرتبط بودن با موضوع تعداد ۳۱ مقاله انتخاب شد. روش تحلیل داده‌ها با توجه به رویکرد دلفی فازی انجام شد. روایی و پایایی به ترتیب با استفاده از شاخص CVR و آزمون کاپای کوهن با ضریب ۰/۸۳ و ۰/۹۳ محاسبه و تائید شد. نتایج گواه این است که پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال در ایران شامل ۵ بعد اصلی و ۳۰ مفهوم است که عبارت‌اند از ۱) امنیتی (محرمانگی اطلاعات، امنیت اطلاعات، احراز هویت فرستنده، احراز هویت سند، حفظ حریم خصوصی، اعتماد میان طرفین)، ۲) کسب‌وکاری (مدل‌های کسب‌وکار دیجیتال، نیازهای ارتباطی سریع، مدیریت کارکنان عملیاتی، اندازه سازمان، ساختار سازمانی، منابع سازمان، فرهنگ‌سازمانی، مدیران ارشد، اکوسیستم رقابت، حکمرانی الکترونیک)، ۳) کاربری (سهولت درک شده، منفعت درک شده، رفتار مصرف‌کننده، سواد مصرف‌کننده، سبک زندگی مصرف‌کننده)، ۴) فنی (توسعه زیرساخت‌های فنی، یکپارچگی سیستم‌ها، پیچیدگی سیستمی، اِشکال و خطاهای سیستمی، کیفیت طراحی، سرعت فنی تولید و تائید گواهی، نفوذناپذیری هکرها) و ۵) قانونی (مجوزهای قانونی، قوانین مجازاتی، نهاد قانون‌گذار، قوانین تجارت الکترونیک). پیشنهاد می‌گردد در زمینه پیاده‌سازی امضای دیجیتال به‌طور خاص به بازنویسی قوانین، آموزش کاربران، ایجاد فرهنگ امنیتی توجه ویژه داشت و سیاستگذاران امضای دیجیتال از شرکت‌های دانش‌بنیان برای توسعه زیرساخت‌ها و رقابتی کردن نرم‌افزارهای مربوطه، دعوت به همکاری کنند.

کلیدواژگان: امضای دیجیتال، تحول دیجیتال، دلفی فازی، امنیت اطلاعات، احراز هویت، پیشران‌های کلیدی.

* رایانامهٔ نویسنده مسؤول: a.mehrabanii54@gmail.com

۱- مقدمه

ایران مانند بسیاری از کشورها در سراسر جهان به انقلاب اینترنتی و تحول دیجیتال واکنش نشان داده و برای برقراری دولت الکترونیک، در تلاش است تا از این انقلاب فناوری بهره ببرد. از اثرات مستقیم دولت الکترونیک می‌توان به صرفه‌جویی در هزینه‌ها، کارایی، بهبود و تعاملات و ارتباطات مستمر با شهروندان، امکانات و خدمات‌رسانی عمومی بهتر و بهبود وصول مالیات اشاره کرد. دیجیتالی شدن امور، باعث می‌شود تا نحوه ارائه خدمات دولت‌به‌شهروندان و کسانی که در داخل مرزهای این کشور زندگی می‌کنند، بهبود یابد. در میان عناصر تحول موفقیت‌آمیز دولت الکترونیک، اصلاح فرآیندها در اولویت فهرست قرار دارد. دولت الکترونیک فقط به معنای خودکارسازی فرآیندها و ناکارآمدی‌های کنونی نیست. بلکه طراحی فرآیندها و روابط جدید بین تمامی ذینفعان است. در ایران، فقدان فرآیندهای بهینه، خودکار و دیجیتالی شده در بخش‌های مختلف دولتی مانع از اثربخشی و کارایی فرآیندهای معاملاتی شده است. برای مثال هنوز هم مداخلات دستی در معاملات به‌منظور مطابقت با الزام قانونی در اخذ امضای دستی اسناد، یک چالش اساسی در تجارت و معاملات به‌حساب می‌آید. این امر مشکلاتی را در یکپارچه‌سازی فرآیندها در ادارات دولتی و عقد قراردادها با شهروندان و سایر بنگاه‌های اقتصادی ایجاد کرده است. حال‌آنکه در سال ۱۹۹۴، دولت ایالات‌متحده به‌طور رسمی DDS یا استاندارد امضای دیجیتال را صادر کرده و در سال ۱۹۹۵، استاندارد امضای دیجیتال چین (GB15851-1995) تدوین شده است[۱]، به این معنا که نزدیک به ۳۰ سال از پذیرش امضای دیجیتال در کشورهای توسعه‌یافته می‌گذرد بنابراین به‌منظور برخورداری از مراودات اقتصادی بایستی که اجرایی شدن امضای دیجیتال هرچه سریع‌تر اتفاق افتد. در ایران نیز بیش از دو دهه از صحبت کردن راجع به پیاده‌سازی امضای دیجیتال و الکترونیکی گذشته اما هنوز در هیچ سازمانی، این فناوری مفید، موردپذیرش قطعی قرار نگرفته است. درنتیجه، این پژوهش به دنبال پاسخ به این سؤال است که چه عواملی باید وجود داشته باشد تا امکان بهره‌برداری از امضای دیجیتال در خودکارسازی خدمات دولت الکترونیک برای معاملات یکپارچه افراد حقیقی و حقوقی فراهم شود. چارچوب امضای دیجیتال می‌تواند راهنمایی برای خط‌مشی‌گذاران تحول دیجیتال به‌ویژه در ادارات دولتی برای پیاده‌سازی امضا دیجیتال باشد.

به‌منظور پاسخ به سؤال تحقیق، در ادامه مبانی نظری و پیشینه پژوهش بررسی و نتایج آن‌ها به‌عنوان ورودی کار تحلیلی استفاده شده است. به این صورت که از مطالعات پیشین، عواملی که تأثیر آن‌ها بر پیاده‌سازی امضای دیجیتال مورد تائید قرارگرفته است، به‌عنوان مؤلفه‌هایی فهرست شده در اختیار خبرگان قرارگرفته (بخش روش پژوهش) و پس از نظرخواهی از بزرگان این حوزه در ایران، دسته‌بندی عوامل اثرگذار در بخش یافته‌های پژوهش به‌عنوان پاسخ نهایی آورده می‌شود. ازآنجایی‌که یافته‌ها باید به نتایجی بیانجامد، در قسمت نهایی، پیشنهادهایی مبتنی بر نتایج آورده شده است.

۲- مبانی نظری

۲-۱- حاکمیت الکترونیک

ظهور اینترنت نوآوری‌های جدید، روش‌های جدید کسب‌وکار، روش‌های جدید کار، روش‌های جدید تعامل، و اشکال جدیدی از مدل‌های کسب‌وکار را به همراه داشته است[۲]. روش‌های اساسی کسب‌وکار شرکت‌ها و دولت‌ها به دلیل افزایش نوآوری و کارایی هزینه‌ای که این دوره به همراه داشته است، در حال تغییر است [۳].

حاکمیت الکترونیکی بستر فناوری اطلاعات و ارتباطات است که در آن کلیه خدمات دولتی به‌صورت آنلاین ارائه‌شده، تبادل اطلاعات به‌صورت الکترونیکی، ارتباطات از طریق شبکه و به‌جای سیستم سنتی، معاملات به‌صورت الکترونیکی انجام می‌شود. بازیگران بسیاری مانند کلیه شهروندان، بنگاه‌های اقتصادی و دولت در این سیستم حکمرانی الکترونیکی مشارکت دارند [۴] و مدل‌های معاملاتی متنوعی وجود دارد که دربرگیرنده تمامی این بازیگران می‌شود. روابطی همچون دولت‌به‌شهروندان (G2C)، دولت به بنگاه اقتصادی (G2B) یا دولت‌به‌دولت (G2G) یا بالعکس تقویت می‌شود [۵] و ازآنجایی‌که اطلاعات محرمانه و ایمن زیادی از طریق معاملات الکترونیکی و درون‌شبکه‌ای منتقل می‌شود، تأکید شده است که امنیت آن تأمین شود [۲].

۲-۲- امضای دیجیتال

امضای دیجیتال یک تکنیک ریاضی است و کمک می‌کند بدانیم آیا یک سند یا اطلاعات احراز هویت شده است یا خیر. امضای دیجیتال در این تکنیک به‌عنوان دلیل معتبری برای دریافت‌کننده است تا یقین داشته باشد که این سند یا اطلاعات فقط توسط فرستنده مجاز ارسال‌شده است و همچنین اطمینان داشته باشد که پیام در حین انتقال از طریق شبکه تغییر نمی‌کند [۶]. امضای دیجیتال روشی است که برای اعتبارسنجی و مجوز دادن به محتوا و کاربرانی که در سیستم حکمرانی الکترونیکی مشارکت می‌کنند،

استفاده می‌شود. امضای دیجیتال هویت فرستنده را که غیرقابل‌انکار است، تضمین می‌کند، بدین معنی که فرستنده نمی‌تواند نفی کند که پیام یا سندی با محتوای خاصی را ارسال نکرده است [۴]. در استاندارد IS07498-2، امضای دیجیتال به این صورت تعریف شده است: «برخی از داده‌های الصاق شده روی سلول‌های داده یا تبدیل رمزنگاری سلول‌های داده، این داده‌ها به گیرنده سلول‌های داده اجازه می‌دهد منبع سلول داده و یکپارچگی سلول داده را تائید کند، به‌منظور محافظت از داده‌ها از جعل شدن توسط شخصی (به‌عنوان‌مثال، گیرنده)» [۱].

در تعریفی دیگر گفته‌شده است که امضای دیجیتال یک مکانیسم احراز هویت[1] است و فرستنده پیام را قادر می‌سازد تا کد منحصربه‌فردی را که به‌عنوان امضا عمل می‌کند، ضمیمه کند، معمولاً امضا با گرفتن هش[2] پیام و رمزگذاری پیام با کلید خصوصی فرستنده[3] تشکیل می‌شود. امضای دیجیتال، منبع و صحت پیام را تضمین می‌کند. استاندارد امضای دیجیتال یک استاندارد NIST است که از الگوریتم هش ایمن استفاده می‌کند. پیام ساده، امضای پیام و کلید عمومی فرستنده باهم بسته‌بندی می‌شوند که با استفاده از کلید عمومی گیرنده به پیام امضاشده و رمزگذاری‌شده تبدیل می‌شود. گیرنده، پیام دریافتی را باز می‌کند که پیام امضاشده و رمزگذاری‌شده است و پس از آن از همان تابع هش برای محاسبه خلاصه پیام دریافتی استفاده می‌شود که با امضای رمزگشایی‌شده مقایسه می‌شود [۷]. امضای دیجیتال به اشکال مختلفی مانند امضای دیجیتال معمولی، امضای دیجیتال داوری، امضای غیرقابل‌انکار، امضای کور، امضای گروهی، امضای آستانه و غیره ارائه می‌شود. نسخه تصویر دیجیتال امضای دست‌نویس چیزی شبیه امضا یا مهر دست‌نویس است و می‌توان آن را مهر الکترونیکی نامید. پس از امضای برخی از اسناد مهم، ممکن است اعتبار آن‌ها را تائید کنیم. بدیهی است که جعل امضای سنتی کار دشواری نیست، بنابراین تفاوت مهم بین امضای دیجیتال و امضای سنتی مشخص می‌شود: بدون کلید خصوصی که امضا را تولید می‌کند، جعل امضای دیجیتال، ازنظر فنی غیرممکن است [۱]. سه موضوع اساسی در فرآیند امضای دیجیتال، بررسی احراز هویت امضاکننده، احراز هویت سند و تائید امضای دیجیتال است[۸-۹] قدرت امضای دیجیتال به روش رمزنگاری مورداستفاده و طول کلید بستگی دارد [۱۰] بااین‌حال، فناوری امضای دیجیتال هنوز نیاز به توسعه بیشتری دارد [۲].

۲-۳- پیشینه پژوهش

تحقیقات متعددی در حوزه برنامه‌نویسی و مهندسی نرم‌افزار در مورد مشکلات امنیتی و ارائه مدل‌های جدید امضای دیجیتال با ویژگی‌های جدید، انجام‌شده است، برای مثال در پژوهشی محققان تأکید کردند که لازم است در سطح قانون‌گذاری به‌وضوح مشخص شود که امضای دیجیتال بیومتریک چیست؟ به معنای نمایش دیجیتالی از ویژگی‌های بیومتریک شخص (اثرانگشت)، مجموعه‌ای از داده‌های شخصی جمع‌آوری‌شده براساس تثبیت ویژگی‌های آن، که از ثبات کافی برخوردار بوده و با پارامترهای مشابه افراد دیگر تفاوت اساسی دارند[۱۱]. دیگران دریافتند که ازآنجایی‌که سیستم حکمرانی الکترونیکی بسیار گسترده است و با شهروندان، بنگاه‌ها یا دولت‌های دیگر در ارتباط است، باید دغدغه‌های امنیتی در هر معامله الکترونیکی در نظر گرفته شود [۴]. همچنین یافته‌های پژوهشی نشان داد ایجاد تغییرات، باعث بی‌اعتباری امضای دیجیتال می‌شود و این نشان‌دهنده ایجاد تمهیداتی برای کاهش احتمال جعل اسناد است [۱۲]. در مطالعه‌ای نیز کلیه تحقیقاتی را که در یک دهه گذشته در مورد امضای دیجیتال انجام شده بود، مرور و مزایا و معایب امضای دیجیتال را با استفاده از رمزنگاری کلید عمومی شناسایی کرد. درنهایت تمام تکنیک‌های مرتبط با امضای دیجیتال و بر اساس رمزنگاری کلید عمومی هستند، مورد تجدیدنظر قرار گرفتند[۶]. محققان دیگری به این نتیجه رسیده‌اند که در حال حاضر نمی‌توان سیستم رمزنگاری کنونی را به‌طور کامل ایمن در برابر تلاش‌های هکرها، در نظر گرفت، باید برای پیشرفت‌های بیشتر در زمینه تولید گواهی و سیستم مدیریت پایگاه داده تلاش بیشتری کرد[۱۳]. مطالعه‌ای دریافت در پیاده‌سازی امضای دیجیتال، حریم خصوصی، احراز هویت، یکپارچگی و عدم انکار چهار عامل کلیدی برای دستیابی به امنیت اطلاعات هستند[۷]. در پژوهشی محققان با بیان اینکه امنیت دیجیتال در ابتکارات دولت الکترونیک اهمیت دارد، بر ضرورت حفظ حریم خصوصی هر معامله یا اطلاعات موجود در شبکه و محافظت از مطالب مهم، داده‌ها یا اطلاعات محرمانه در مقابل کاربران غیرمجاز در پروژه‌های دولت الکترونیک تأکید کردند زیرا ازنظر آن‌ها امنیت برای اجرای موفقیت‌آمیز چنین پروژه‌هایی حیاتی است [۱۴]. سال‌ها پیش نیز طرحی توسط محققان ارائه شد که شامل راهکارهایی برای حل برخی از چالش‌های ایمنی در اسناد الکترونیکی مانند عدم اعتماد کافی بین فرستنده و گیرنده و غیره بود. در این طرح بر ترکیب امنیت با کارایی در دولت الکترونیک

[1] Authentication Mechanism

[2] Hash

[3] Senders Private Key

تأکید شد. در این طرح نتیجه گرفتند که علاوه بر مشکلات امنیتی که می‌توانند به‌طور کامل حل شوند، باید عوامل دیگری مانند امنیت و اعتبار شبکه و سخت‌افزار مربوطه نیز در نظر گرفته‌شده و کارکنان فعال در این زمینه، به‌خوبی مدیریت شوند[۱۵]. عده‌ای نیز در پژوهش خود با بیان اینکه چندین مؤسسه بایگانی براساس رمزنگاری کلید عمومی (ازجمله آرشیو ملی کانادا، استرالیا و ایالات‌متحده)، در مورد چشم‌انداز حفظ سوابق با امضای دیجیتال ابراز تردید کرده‌اند، استدلال کردند که اختلاف بین پاسخ‌های فنی، حقوقی و آرشیوی در مورد چالش حفظ طولانی‌مدت اسناد امضاشده دیجیتالی براساس درک متفاوت آن‌ها از اصالت الکترونیکی است[۱۶]. بااین‌حال، از ابتدا تأکید شده است امضای دیجیتال به توسعه اعتماد بیشتری برای پیاده‌سازی نیاز دارد [۱۷].

در موردپذیرش امضای الکترونیکی و چالش‌های آن نیز تحقیقات به‌ویژه در حوزه مدیریت رو به افزایش است. در جدیدترین پژوهش‌ها، محققی به عوامل مؤثر بر پذیرش کاربران از فناوری‌های امضای دیجیتال دست‌یافت که عبارت‌اند از: که کارایی، امنیت اطلاعات، راحتی، عملکرد مقایسه‌ای، توابع مقیاس‌پذیر، تجربه کاربر، در دسترس بودن اطلاعات و سایر عوامل زمینه‌ای[۱۸]. همچنین در پژوهشی که در همه‌گیری کوید ۱۹ انجام شد، مشخص گردید درصورتی‌که عملکرد برنامه الکترونیکی امضای دیجیتالی به‌خوبی اجرا شود، یعنی هیچ باگی نداشته باشد (ازجمله مشکلات دسترسی، فرایندها و منوهای موجود در سیستم، پردازش، تراکنش، بارگذاری، دانلود اسناد، فرایند تائید و دسترسی به داده‌های موجود در منوی راهنما) سطح پذیرش امضای دیجیتال به بیش از ۸۲ درصد می‌رسد[۱۹]. پژوهشگری نیز اذعان داشت توسعه الکترونیکی، پیشرفت بانکداری الکترونیکی را به همراه دارد. تجارت الکترونیکی از طریق بانکداری الکترونیکی و امضای الکترونیکی یکی از مشخصه‌های مهم اقتصاد جهانی معاصر است[۲۰]. همچنین محققان نتیجه گرفتند که فناوری جدید تلفن‌های هوشمند و مدرن، مانند عناصر سخت‌افزاری ایمن و روش‌های احراز هویت بیومتریک می‌توانند احراز هویت ایمن را فراهم کنند [۲۱]. در بررسی کاربردهای دیجیتال در بایگانی اسناد نتیجه گرفته شد که امنیت بایگانی‌ها ضرورتی است که علاوه بر ثبت کلیدهای عمومی و خصوصی پرسنلی که قدرت قانونی برای امضای آن‌ها دارد، استفاده از فناوری زیرساخت‌های کلیدی عمومی (PKI) برای تولید یک سند دیجیتال نیز ضروری است[۲۲]. محققان دیگری نیز دریافتند که نگرش (منفعت درک‌شده و سهولت استفاده) و کنترل رفتاری درک‌شده (خودکارآمدی و شرایط تسهیل‌کننده) بر قصد استفاده از امضای دیجیتال اثرگذار است[۲۳]. در تحقیقی نیز شش عامل در بررسی متغیرهای مؤثر بر عدم پذیرش امضاهای الکترونیکی شناسایی شد که عبارت‌اند از فرهنگ و آداب‌ورسوم غالب مرتبط با امضاهای دستی، ناآگاهی در مورد فناوری امضای الکترونیکی، نگرانی‌های حقوقی و مسائل امنیتی، هزینه استفاده از فناوری و پیچیدگی مربوط به راه‌اندازی و استفاده از آن [۲۴]. عوامل مؤثر بر پذیرش امضای الکترونیکی در میان مدیران بیمارستانی در پژوهشی موردبررسی قرار گرفت. محققان در ویژگی‌های سازمانی به بررسی عواملی مثل درگیری کاربر، منابع کافی، اندازه بیمارستان و نیاز داخلی پرداختند. در مورد ویژگی‌های محیطی نیز مواردی همچون پشتیبانی شرکت‌های تأمین‌کننده محصول و سیاست‌های دولت اهمیت داشت. در مورد ویژگی‌های امضای الکترونیکی نیز موضوعاتی مثل حفاظت از امنیت، پیچیدگی سیستمی در نظر گرفته شد[۲۵]. در مدلی برای پذیرش و پیاده‌سازی فناوری امنیتی (از طریق بررسی عوامل مؤثر بر پذیرش و اجرای فناوری زیرساخت‌های کلید عمومی (PKI)) مؤلفه‌هایی مانند ویژگی‌های سازمانی، ویژگی‌های تکنولوژی امنیتی، قابلیت‌های سازمانی، پیچیدگی فناوری شناسایی شد [۲۶]. محققان همچنین ماهیت ناامنی اینترنت را عاملی جهت عدم اعتماد و عدم تمایل افراد و کسب‌وکارها به استفاده از امضای الکترونیکی و دیجیتال می‌داند و بر این باورند که هنگام وضع قوانین یا دستورالعمل‌ها باید مسائل حریم خصوصی و سایر حساسیت‌های امنیتی را با دقت بیشتری در نظر گرفت [۲۷]. محققی نیز در سال ۲۰۰۰، امضای دیجیتال الکترونیکی را مقوله‌ای قانونی می‌دانست و معتقد بود استفاده ازاین‌گونه عبارات در اسناد هنجاری به‌عنوان آنالوگ امضای شخصی و معادل امضای شخصی یک شخص نامطلوب است، زیرا مشارکت‌کنندگان را درگیر مسائل حقوقی کرده و می‌تواند به مشکلاتی در فرایندها و شناسایی افرادی که از امضای دیجیتال الکترونیکی برای تائید اسناد رایانه‌ای استفاده می‌کنند، منجر شود[۲۸]. به‌زعم برخی محققان، فناوری‌های دیجیتال ازجمله امضای دیجیتال با مشروعیت یافتن، می‌تواند در بازار گسترش‌یافته و به کار گرفته شوند [۲۹]. دیگران با تأکید بر اهمیت و لزوم پیاده‌سازی امضای دیجیتال در خرید الکترونیکی، مشکلاتی نظیر هزینه و پیچیدگی را مطرح کردند [۳۰]. محققانی نیز بر این باورند که چارچوب‌های نظارتی و قوانین حاکم بر به‌کارگیری امضای دیجیتال باعث ایجاد محدودیت‌هایی برای برخی از شرکت‌های کوچک و متوسط و تأمین‌کنندگان در مناقصات دولتی و معاملات خواهد شد [۳۱]. مسائل امنیتی و سرعت محاسباتی نیز از سایر چالش‌های به‌کارگیری امضای دیجیتال است[۳۲]. در پژوهشی نیز ضمن بیان مزایای اصلی امضای دیجیتال ازجمله افزایش کارایی، کاهش هزینه‌ها و افزایش رضایت مشتری، تأکید کرده است که

امضای دیجیتال باید به‌وضوح از فرایندهای متداول احراز هویت فاصله گرفته و این یکی از چالش‌های اصلی پیاده‌سازی آن است [۳۳].

در ایران نیز تحقیقاتی در زمینه پذیرش و اجرای امضای دیجیتال انجام‌شده است، زیرا اولین گام در شکستن مقاومت در برابر تغییر فناوری و به‌کارگیری فناوری جدید، پذیرش آن فناوری است [۳۴]. فرهنگ دیجیتال (پذیرای تحول، سرعت و دقت و توجه به مالکیت معنوی)، فرایندسازی دیجیتال (خودکارسازی، تحلیل دیجیتالی، سازمان‌دهی تکنولوژی‌های دیجیتال، ساختار منعطف و مناسب، همسوسازی فرایندها و ارتباطات سازمانی)، فناوری‌های دیجیتال (کلان داده، فین تک، بلاکچین، اینترنت اشیاء، رایانش ابری و 5G)، فضای کار دیجیتال (کارکنان دانشی، مهارت دیجیتال، آموزش دیجیتال، اتاق فکر دیجیتال) و درنهایت فعالیت دیجیتال (توسعه محصولات دیجیتال، توسعه نوآوری، مشتری مداری دیجیتال، کانال توزیع دیجیتال، تعامل دیجیتال، پشتیبانی دیجیتال، ایجاد و نگهداری پلتفرم‌های دیجیتال و برقراری امنیت دیجیتال) از عوامل مؤثر بر موفقیت تحول دیجیتال شناسایی‌شده است [۲]. محققان با بررسی قوانین و مقررات ایران نتیجه‌گیری کردند که قرارداد الکترونیکی رویکرد بسیار مطلوبی نسبت به جهانی‌سازی یا دیجیتالی شدن دارد، زیرا هرروز شاهد این هستیم که به سمت دنیای فناوری اطلاعات در حال حرکت هستیم. محقق اشاره کرد عوامل سازمانی (دغدغه‌های امنیت داده، وابستگی به سیستم‌های فناوری اطلاعات، پشتیبانی مدیر ارشد، زیرساخت فنی، نیروی انسانی)، عوامل محیطی (فشار اجبار، پشتیبانی قانونی، فشار تقلیدی، پشتیبانی ارائه‌دهنده خدمات امضاء)، اعتماد (اعتماد به فناوری، اعتماد به ارائه‌دهنده فناوری) و ویژگی‌های فناوری (سازگاری، پیچیدگی و مزیت نسبی) از عوامل اشاعه امضای دیجیتال هستند [۳۵]. همچنین در پژوهشی، عوامل مؤثر بر استقرار سیستم امضای الکترونیکی به هفت‌طبقه عوامل مربوط به ساختار، عوامل قانونی، عوامل مدیریتی، عوامل فردی-شخصی، عوامل سازمانی، عوامل فرهنگی، عوامل تکنولوژیکی تقسیم‌بندی شد [۳۶]. در مقاله‌ای دیگر، با عنوان احراز هویت در اینترنت اشیاء با استفاده از امضای الکترونیکی تأکید شد یکی از چالش‌های عمده‌ای که باید به‌منظور نفوذ اینترنت اشیاء به جهان واقعی حل شود، مسئله امنیت است [۳۷]. محققی به این نتیجه رسید که قابلیت دسترسی، سودمندی ادراک‌شده، سهولت استفاده ادراک‌شده، تطابق تکنولوژی با سبک زندگی فردی بر اعتماد به امضای الکترونیکی مراجعه‌کنندگان به خدمات عمومی، تأثیر مثبت معنی‌داری دارد [۳۸]. در بررسی عوامل مؤثر بر آمادگی سازمان‌ها به‌منظور استفاده از امضای الکترونیکی نیز نشان داده شد که اثرات متغیرهای تائید شده در قالب بعد ساختاری (فنی، مالی، امنیتی)، بعد رفتاری (مدیریت، فرهنگ سازمانی، دانش و آموزش) و بعد زمینه‌ای (مشتریان، رقبا، قانونی-سیاسی، اشخاص ثالث) قابل دسته‌بندی هستند [۳۹]. درنهایت، محققی نتیجه‌گیری کرد که ایجاد تعامل میان فلسفه گسترش تجارت الکترونیکی و ایمنی و اطمینان به آن، بهترین گزینه است که با ثبت الکترونیکی امضا و مدارک به‌راحتی می‌توان به آن دست پیدا کرد [۴۰].

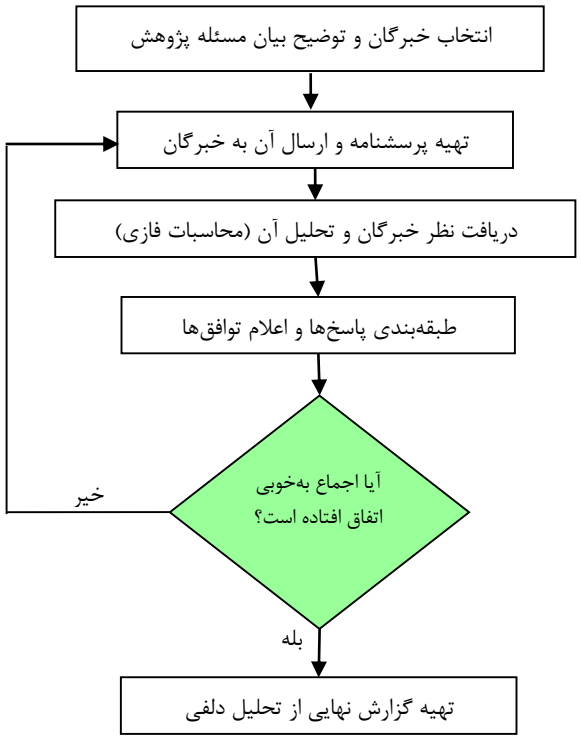
با توجه به پیشینه پژوهش، با وجود تحقیقات متعدد در پیاده‌سازی امضای دیجیتال، حتی در کشورهایی که مدت زیادی از اجرای آن می‌گذرد، برخی چالش‌ها همچنان باقی‌مانده یا به شکلی دیگری ظاهر شده‌اند. بنابراین، انجام تحقیقات کیفی و بنیادی در مورد عوامل مؤثر بر پیاده‌سازی امضای دیجیتال در هر کشور می‌تواند به اجرای بهتر آن کمک کند و تا حد زیادی چالش‌ها را پیش‌بینی کرده و گام‌های بهتری در جهت رفع آن بردارد.

۳- روش پژوهش

با توجه به سؤال اصلی پژوهش که الگوی پیاده‌سازی امضای دیجیتال در ایران کدام است؟ این پژوهش به دنبال شناسایی عوامل مؤثر بر اجرای امضای دیجیتال در سازمان‌های ایرانی می‌باشد. با در نظر گرفتن اینکه قرار است از نتایج و دستاوردهای پژوهش کنونی در تدوین سیاست‌های کلان حوزه فناوری می‌توان بهره برد، پژوهش از نوع کاربردی است. جامعه آماری این پژوهش، خبرگان و متخصصان مدیریت فناوری و اطلاعات و مطالعات منتشرشده و قابل‌دسترس در بازه زمانی سال‌های ۱۹۹۰ تا ۲۰۲۳ داخلی و خارجی می‌باشد که از دیدگاه مدیریتی (نه فنی، برنامه‌نویسی و حقوقی) به موضوع امضای دیجیتال پرداخته باشند. با توجه به زمینه مقالات، زبان فارسی و انگلیسی و محدودیت‌های جستجو در پایگاه‌های بین‌المللی و دانلود آن، نهایتاً ۳۱ مقاله انتخاب شدند. جامعه آماری را خبرگان و متخصصان حوزه فناوری اطلاعات و امضای دیجیتال تشکیل می‌دهند. ۱۳ خبره به‌عنوان مشارکت‌کننده با روش نمونه‌گیری هدفمند انتخاب شدند و عوامل استخراج‌شده از مطالعه مبانی نظری پژوهش را بررسی کردند. ۵ نفر عضو هیئت‌علمی یا پژوهشگر و ۸ نفر از مدیران این حوزه در سازمان‌ها و نهادهای سیاست‌گذار فناوری اطلاعات و ارتباطات در ایران بودند. پژوهش به روش فراترکیب به جمع‌آوری داده پرداخته و تحلیل آن با رویکرد دلفی فازی انجام‌شده است. با استفاده از شاخص CVR و آزمون کاپای کوهن، به ترتیب روایی ۰/۸۳ و پایایی ۰/۹۳ به‌دست‌آمده و روایی محتوا نیز توسط خبرگان تائید شد.

جدول ۱. مشخصات خبرگان مشارکت‌کننده (جمع‌آوری محقق)

تحصیلات			
دکتری	۳	کارشناسی ارشد	۱۰
رشته تحصیلی			
مدیریت فناوری اطلاعات و ارتباطات	۷	مدیریت	۲
مهندسی فناوری اطلاعات	۳	حقوق	۱
پست/شغل سازمانی			
معاونت	۲	مدیریت	۶
هیئت‌علمی	۴	پژوهشگر	۱
سابقه/تجربه فعالیت در زمینه امضای دیجیتال و حکمرانی الکترونیک			
بیش از ۱۵ سال	۶	بین ۱۰-۱۵ سال	۵
بین ۵-۱۰ سال	۲	کمتر از ۵ سال	۱



شکل ۱. فرایند اجرای دلفی فازی

پژوهشگر درروش فراترکیب، با مطالعه پژوهش‌های پیشین و تفسیر آن‌ها، یافته‌های جامع‌تری را کشف می‌کند. در این پژوهش از روش هفت مرحله‌ای سندلوسکی و باروسو (۲۰۰۷) استفاده شد که مراحل آن عبارت‌اند از: تنظیم سؤال، مرور ادبیات، جستجو و انتخاب متون، استخراج اطلاعات، تحلیل و ترکیب، کنترل کیفیت و درنهایت ارائه نتایج [۴۱]. درنهایت ۳۲ مؤلفه تأثیرگذار بر پیاده‌سازی امضای دیجیتال شناسایی شد که در ۵ مؤلفه قرار گرفتند. به‌منظور پالایش و گزینش مؤلفه‌های اثرگذار بر پیاده‌سازی امضای دیجیتال از روش دلفی فازی بهره گرفته شد. دلفی فازی شامل اجرای روش دلفی و تحلیل اطلاعات با در نظر گرفتن نظریه‌ها و پیشینه پژوهش است.

جدول ۲. مؤلفه‌ها و ابعاد پیاده‌سازی امضای دیجیتال در پیشینه (جمع‌آوری محقق)

بعد	مؤلفه	منابع و پیشینه
امنیتی	محرمانگی اطلاعات	۳۲-۲۵ -۲۴-۱۴
	امنیت اطلاعات	۴۰-۳۹-۳۵-۳۲ -۲۵ -۲۴-۱۸-۱۲-۴
	احراز هویت فرستنده	۳۷-۳۳-۲۸ -۲۱-۷
	احراز هویت سند	۳۷-۷
	حفظ حریم خصوصی	۲۷-۲۵-۱۴-۷
	اعتماد میان طرفین	۳۵-۲۷ -۱۷-۱۵
کسب‌وکاری	مدل‌های کسب‌وکار دیجیتال	۳۱-۲۵ -۲۰
	نیازهای ارتباطاتی سریع	۲ -۲۱
	مدیریت کارکنان عملیاتی	۳۵-۱۵
	اندازه سازمان	۳۱-۲۵
	ساختار سازمانی	۳۶-۲ -۲۶
	منابع سازمانی	۳۰-۲۵ -۲۴
	فرهنگ‌سازمانی	۳۹-۳۶-۲
	مدیران ارشد	۳۶-۳۵
	اکوسیستم رقابت	۳۹
	حکمرانی الکترونیک	۲۵ -۱۴-۴
کاربری	سهولت درک شده	۳۸-۲۳-۱۹-۱۸
	منفعت درک شده	۳۸-۲۳
	رفتار مصرف‌کننده	۲۵-۲۴
	سواد مصرف‌کننده	۳۹-۲۴
	سبک زندگی	۳۸-۲۴
فنی	توسعه زیرساخت‌های فنی	۳۹ -۳۶-۳۵-۲۶ -۲۲-۱۲
	یکپارچگی سیستم‌ها	۷
	پیچیدگی سیستمی	۳۵-۳۰-۲۶ -۲۵ -۲۴
	اِشکال و خطاهای سیستمی	۱۹ -۱۲
	کیفیت طراحی	تحقیقات متعدد مرتبط با برنامه‌نویسی
	سرعت فنی تولید و تائید گواهی	۳۲
	نفوذناپذیری هکرها	۱۳
حقوقی	مجوزهای قانونی	۳۹-۲۷ -۲۹-۲۴-۱۷
	قوانین مجازاتی	۲۴-۱۱
	نهاد قانون‌گذار	۳۹ -۳۶-۳۵-۲۹-۲۸ -۲۷
	قوانین تجارت الکترونیک	۱۱

همان‌طور که مشاهده می‌شود، مؤلفه‌های شناسایی‌شده در برخی از ابعاد بیشتر از سایر ابعاد مورد تأکید پیشینه تحقیقات بوده است. برای مثال موضوعات کاربری به‌تازگی در ادبیات امضای دیجیتال و با توجه به مبانی پذیرش فناوری گسترش یافته‌اند و برخی از مؤلفه‌های مرتبط با تجارت و حقوقی، از فناوری کمتری برخوردارند. مؤلفه‌های امنیتی همچنان بیشترین تأکیدات را در تحقیقات پیشین داشته‌اند. در ادامه، فرایند این دسته‌بندی توضیح داده خواهد شد.

۴- یافته‌ها پژوهش

به‌منظور شناسایی عوامل مؤثر بر پیاده‌سازی امضای دیجیتال با بهره‌مندی از مرور کتابخانه‌ای و مطالعه پژوهش‌های پیشین، ۳۲ مؤلفه در ۵ بعد امنیتی، کسب‌وکاری، کاربری، فنی و حقوقی شناسایی شد که در جدول ۲ نشان داده‌شده است.

در ادامه از تکنیک دلفی فازی برای تحلیل و تائید بهره برده شد که به ترتیب فرایندهای زیر انجام شد. شایان‌ذکر است که مؤلفه‌ها با توجه به نظر خبرگان، مفهوم‌سازی شدند و در تحقیقات محدودی، این متغیرها به این صورت و به‌عنوان چالش پیاده‌سازی مطرح‌شده و به‌طور مستقیم آورده نشده‌اند. به‌عنوان‌مثال چالش هزینه و تأمین نیروی انسانی به‌طورکلی در بحث منابع سازمانی آورده شده است و همچنین مواردی مانند استفاده شرکت‌ها با توجه به صنعت و بزرگ و کوچکی در مؤلفه اندازه سازمانی در نظر گرفته‌شده است.

۴-۱- تعریف متغیرهای کلامی

پرسشنامه پژوهش کنونی با هدف کسب نظر خبرگان درخصوص میزان موافقت ایشان با مؤلفه‌ها و معیارهای مدل طراحی‌شده است. به همین منظور، خبرگان از طریق متغیرهای کلامی نظیر خیلی زیاد، زیاد، متوسط، کم و خیلی کم نظر خود را اعلام کردند. به دلیل تأثیر خطاهای ادراکی افراد مشارکت‌کننده و شخصیت‌های متفاوت ایشان نسبت به متغیرهای کیفی، دامنه‌ای از متغیرهای کیفی ارائه شد و پاسخ‌دهندگان با دیدگاه و ذهنیت یکسانی و بدون از عارضه شخصی به سؤالات پاسخ دادند. این متغیرها به شکل اعداد فازی مثلثی تعریف شده‌اند.

جدول ۳. تعریف متغیرهای کلامی- زبانی (مطابق با روش پژوهش)

متغیرهای زبانی	عدد فازی مثلثی	عدد فازی قطعی شده
خیلی زیاد	(۱ ،۰/۲۶ ،۰)	۰/۹۴۸۱
زیاد	(۰/۷۷ ،۰/۱۵ ،۰/۱۶)	۰/۷۶
متوسط	(۰/۶ ،۰/۲۶ ،۰/۲۷)	۰/۶
کم	(۰/۲ ،۰/۱۵ ،۰/۱۶)	۰/۲۴
خیلی کم	(۰ ،۰ ،۰/۲۶)	۰/۰۷۱۱

در جدول ۳، اعداد فازی قطعی شده با فرمول Minkowski محاسبه شدند.

$$x = m + \frac{\beta - \alpha}{4}$$

همچنین میانگین فازی هرکدام از مؤلفه‌های با توجه به روابط زیر محاسبه می‌شود:

$$A_i = \left(a_1^{(i)}, a_2^{(i)}, a_3^{(i)}\right), \quad i = 1,2,3,\dots,n$$

$$A_{ave} = (m_1, m_2, m_3) = \left(\frac{1}{n}\sum_{i=1}^{n} a_1^{(i)}, \frac{1}{n}\sum_{i=1}^{n} a_2^{(i)}, \frac{1}{n}\sum_{i=1}^{n} a_3^{(i)}\right)$$

در این رابطه a_i بیانگر دیدگاه خبره iام و A_{ave} بیانگر دیدگاه‌های خبرگان است.

۴-۲- مرحله اول دلفی

در این مرحله طرح کلی با ابعاد و مؤلفه‌های تعیین‌شده به اعضای گروه خبرگان ارسال شد و میزان اتفاق‌نظر آن‌ها با یکدیگر در رابطه با مؤلفه‌های کنونی و موجود سنجیده شد. به این صورت، با توجه به نظرات خبرگان، نتایج استخراج‌شده از بررسی و پیشنهادهای مطرح‌شده در جدول ۴، ۵ ، ۶ ، ۷ و ۸ آورده شده است. همچنین میانگین فازی مثلثی محاسبه‌شده و فازی زدایی شده است میانگین قطعی به‌دست‌آمده نشان‌دهنده موافقت خبرگان با هر یک از مؤلفه‌های پژوهش است.

۴-۳- مرحله دوم دلفی

در این مرحله، تغییرات ضروری در معیارها و مؤلفه‌ها انجام شد. پرسشنامه مرحله دوم تهیه و برای خبرگان ارسال شد. خبرگان مجدداً به سؤالات ارائه‌شده پاسخ دادند. نتایج شمارش پاسخ‌های ارائه‌شده در مرحله دوم، با استفاده از فرمول‌های مذکور مجدداً تحلیل شد.

۴-۴- مرحله سوم دلفی

در این مرحله، تغییرات دوباره‌ای انجام شد و پرسشنامه جدید به خبرگان ارسال شد. با توجه به اینکه اختلاف دیدگاه نظر خبرگان در مرحله دوم و سوم ناچیز بود، تکنیک دلفی در این مرحله به اتمام رسید. ضعف نظری در زمینه پیاده‌سازی امضای دیجیتال موجب شد به بررسی دقیق‌تر و جامع‌تری نسبت به این موضوع بپردازیم.

جدول ۴. نتایج موافقت خبرگان با پیشران‌های امنیتی (یافته‌های پژوهش)

ردیف	مؤلفه	مرحله اول	مرحله دوم	مرحله سوم
۱	محرمانگی اطلاعات	۰/۳۷	۰/۴۳	۰/۴۵
۲	امنیت اطلاعات	۰/۴۵	۰/۴۰	۰/۳۹
۳	احراز هویت فرستنده	۰/۵۳	۰/۵۷	۰/۵۵
۴	احراز هویت سند	۰/۳۱	۰/۳۴	۰/۳۴
۵	حفظ حریم خصوصی	۰/۳۲	۰/۴۶	۰/۴۶
۶	اعتماد میان طرفین	۰/۲۲	۰/۲۰	۰/۲۱

جدول ۵. نتایج موافقت خبرگان با پیشران‌های کسب‌وکاری (یافته‌های پژوهش)

ردیف	مؤلفه	مرحله اول	مرحله دوم	مرحله سوم
۱	مدل‌های کسب‌وکار دیجیتال	۰/۳۷	۰/۵۱	۰/۵۰
۲	نیازهای ارتباطاتی	۰/۱۵	۰/۲۴	۰/۲۳
۳	مدیریت کارکنان عملیاتی	۰/۲۱	۰/۲۷	۰/۲۶
۴	اندازه سازمان	۰/۳۲	۰/۲۷	۰/۲۵
۵	ساختار سازمانی	۰/۲۴	۰/۲۲	۰/۲۲
۶	منابع سازمانی	۰/۲۷	۰/۲۵	۰/۲۵
۷	فرهنگ‌سازمانی	۰/۴۵	۰/۲۷	۰/۲۸
۸	مدیران ارشد	۰/۲۷	۰/۲۵	۰/۲۴
۹	اکوسیستم رقابت	۰/۳۷	۰/۳۵	۰/۳۵
۱۰	حکمرانی الکترونیک	۰/۲۵	۰/۳۷	۰/۳۸

جدول ۶. نتایج موافقت خبرگان با پیشران‌های کاربری (یافته‌های پژوهش)

ردیف	مؤلفه	مرحله اول	مرحله دوم	مرحله سوم
۱	سهولت درک شده	۰/۲۸	۰/۳۳	۰/۳۳
۲	منفعت درک شده	۰/۲۹	۰/۴۱	۰/۴۰
۳	رفتار مصرف‌کننده	۰/۱۱	۰/۱۵	۰/۱۶
۴	سواد مصرف‌کننده	۰/۱۶	۰/۱۸	۰/۱۷
۵	سبک زندگی	۰/۳۷	۰/۳۱	۰/۳۰

جدول ۷. نتایج موافقت خبرگان با پیشران‌های فنی (یافته‌های پژوهش)

ردیف	مؤلفه	مرحله اول	مرحله دوم	مرحله سوم
۱	توسعه زیرساخت‌های فنی	۰/۳۶	۰/۲۷	۰/۲۷
۲	یکپارچگی سیستم‌ها	۰/۲۵	۰/۲۲	۰/۲۳
۳	پیچیدگی سیستمی	۰/۳۹	۰/۳۸	۰/۳۹
۴	اِشکال و خطاهای سی‌ستمی	۰/۲۵	۰/۲۸	۰/۲۸
۵	کیفیت طراحی	۰/۰۸	۰/۱۳	۰/۱۲
۶	سرعت فنی تولید و تائید گواهی	۰/۱۸	۰/۲۱	۰/۲۱
۷	نفوذناپذیری هکرها	۰/۳۷	۰/۳۴	۰/۳۵

جدول ۸. نتایج موافقت خبرگان با پیشران‌های حقوقی (یافته‌های پژوهش)

ردیف	مؤلفه	مرحله اول	مرحله دوم	مرحله سوم
۱	مجوزهای قانونی	۰/۴۱	۰/۴۲	۰/۴۱
۲	قوانین مجازاتی	۰/۳۸	۰/۴۳	۰/۴۳
۳	نهاد قانون‌گذار	۰/۳۷	۰/۳۶	۰/۳۷
۴	قوانین تجارت الکترونیک	۰/۲۵	۰/۲۲	۰/۲۲

لذا پژوهش کنونی در تلاش بود به این پرسش پاسخ دهد که عوامل مؤثر بر الگوی پیاده‌سازی امضای دیجیتال در ایران (در قالب یک الگو) کدام است؟ ازجمله مزیت‌های پژوهش کنونی و تفاوت قابل‌ذکر آن با سایر پژوهش‌های این حوزه این است که در این پژوهش، ابعاد به‌صورت یک الگو ترسیم شدند.

۵- نتیجه‌گیری

تحول دیجیتال ازجمله روندهایی است که در چند سال اخیر موردتوجه کلیه صنایع قرارگرفته است و پیشران قوی برای ایجاد تغییرات اساسی در سازمان‌های امروزی و قرار گرفتنشان در مسیر دیجیتالی شدن است. یکی از موضوعاتی که از تقریباً ۲ دهه پیش در ایران موردبحث و بررسی قرارگرفته و همچنان بدون نتیجه و کار اجرایی، باقی‌مانده است، پیاده‌سازی امضای دیجیتال است. این مسئله به‌قدری به فراموشی سپرده‌شده است که مطالعه قابل‌توجهی در این زمینه نیز صورت نگرفته است. ازاین‌رو، پژوهش کنونی با هدف واکاوی پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال انجام شد که نتایج آن در جدول ۹ و شکل ۲ نشان داده شده است.

شکل ۲. پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال (یافته‌های پژوهش)

با مطالعه و بررسی ۳۱ مقاله داخلی و خارجی در دسترس و قابل دانلود، به بیش از ۳۰ مؤلفه در قالب ۵ بعدی امنیتی، کسب‌وکاری، کاربری، فنی و حقوقی دست یافتیم و در ادامه به‌منظور غربال‌گری و انتخاب مؤلفه‌های تأثیرگذار بر پیاده‌سازی امضای دیجیتال، از روش دلفی فازی استفاده شد. درنتیجه، از بین ۶ مؤلفه استخراج‌شده در بعد امنیتی، مهم‌ترین به ترتیب اولویت ازنظر خبرگان می‌توان به مؤلفه‌های احراز هویت فرستنده، محرمانگی اطلاعات و حفظ حریم خصوصی اشاره کرد.

در بعد کسب‌وکاری و از بین ۱۰ مؤلفه تائید شده به ترتیب اولویت‌بندی به ۳ مؤلفه مدل‌های کسب‌وکار دیجیتال، حکمرانی الکترونیک و اکوسیستم رقابت اشاره کرد. ۲ مؤلفه منفعت درک شده و سهولت درک شده نیز در بعد کاربری از اولویت بالاتری برخوردار بودند. در بعدی فنی، خبرگان بر اهمیت ۲ مؤلفه پیچیدگی سیستمی و (الزاماتی برای) نفوذناپذیری هکرها تأکید کردند و درنهایت می‌توان گفت که در بحث حقوقی، مؤلفه‌های قوانین مجازات و مجوزهای قانونی مهم‌ترین مؤلفه‌های تأثیرگذار شناخته شدند. در این راستا، نتایج پژوهش حاضر لاوری (۲۰۲۱)، آیدین و همکاران (۲۰۱۸) و پاسالار (۱۳۹۴) که به عوامل پذیرش امضای دیجیتال توسط کاربران پرداخته بود همسو می‌باشد[سازگار با ۱۸، ۲۳، ۳۳] که نتایج آن‌ها به بعد کاربری اشاره‌کرده بودند. موضوع سهولت کاربرد یک مؤلفه در بحث آموزش کاربران جهت استفاده صحیح از این ابزار است. همچنین سبک زندگی مورد اشاره در سیرواستا (۲۰۱۱) نیز در این تحقیق تائید شد [سازگار با ۱۱]. همچنین پژوهش‌های انجام‌شده توسط آفریانتو و همکاران (۲۰۲۱) که به مؤلفه اِشکال و خطاهای سیستمی اشاره‌کرده بود و پرداخته بود نشان داد که نفوذناپذیری هکرها از مؤلفه‌های فنی تأثیرگذار بر پیاده‌سازی امضای دیجیتال است[سازگار با ۱۹]. سیرواستا (۲۰۱۱) و کارایانیس و ترنر (۲۰۰۶) نیز به مسئله پیچیدگی سیستمی در به‌کارگیری اشاره کردند که در دسته فنی قرار می‌گیرد [سازگار با ۲۴، ۲۶]. در پژوهشی دیگر که توسط تونرمن و همکاران (۲۰۱۹) در رابطه با احراز هویت پرداختند نشان داد که از پیشران‌های امنیتی تأثیرگذار است [۲۱]. سایر پیشران‌های امنیتی همچون حریم خصوصی نیز در یافته‌های تحقیق کنونی و سیرواستا (۲۰۰۵) مشترک است [۲۷]. در پژوهشی که توسط توکلی‌راد و زرگران خوزانی (۱۴۰۱) و سپاشویلی (۲۰۲۰) در خصوص الزامات بانکداری الکترونیک و امثالهم صورت گرفت، نتایج آن با نتایج پژوهش کنونی سازگار می‌باشد [۲، ۲۰] و آن را از بعد کسب‌وکاری تائید می‌کند. اندازه و منابع سازمانی نیز در تحقیق چانگ و همکاران (۲۰۰۷) مشابه با بعد کسب‌وکاری مورداشاره قرار گرفت [۲۵]. همچنین نتایج پژوهش حاضر با تحقیقاتی ازجمله سیرواستا (۲۰۱۱) مبنی بر مسائل حقوقی هم‌راستا می‌باشند [سازگار با ۲۴].

جدول ۹. پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال (یافته‌های پژوهش)

امنیتی	کسب‌وکاری	کاربری	فنی	حقوقی
محرمانگی اطلاعات	مدل‌های کسب‌وکار دیجیتال	سهولت درک شده	توسعه زیرساخت‌های فنی	مجوزهای قانونی
امنیت اطلاعات	نیازهای ارتباطاتی سریع	منفعت درک شده	یکپارچگی سیستم‌ها	قوانین مجازاتی
احراز هویت فرستنده	مدیریت کارکنان عملیاتی	رفتار مصرف‌کننده	پیچیدگی سیستمی	نهاد قانون‌گذار
احراز هویت سند	اندازه سازمان	سواد مصرف‌کننده	اِشکال و خطاهای سیستمی	قوانین تجارت الکترونیک
حفظ حریم خصوصی	ساختار سازمانی	سبک زندگی	کیفیت طراحی	
اعتماد میان طرفین	منابع سازمانی		سرعت فنی تولید و تائید گواهی	
	فرهنگ‌سازمانی		نفوذناپذیری هکرها	
	مدیران ارشد			
	اکوسیستم رقابت			
	حکمرانی الکترونیک			

لذا به‌طورکلی نتایج پژوهش‌های پیشین، تائید کننده نتایج تحقیق کنونی است. با توجه به یافته‌های به‌دست‌آمده می‌توان گفت که در مقایسه با پژوهش‌های پیشین، چنین دسته‌بندی و الگویی برای شناسایی پیشران‌های کلیدی پیاده‌سازی امضای دیجیتال ارائه نشده است.

بدین منظور، هدف کاربردی پژوهش از ارائه مدل این است که مدیران سازمان‌های مرتبط با خط‌مشی‌گذاری کلان و پیاده‌سازی فرایندهای دیجیتال ازجمله امضای دیجیتال، به‌صورت یکپارچه از موارد تأثیرگذار استخراج‌شده در این مطالعه بهره گرفته و در تصمیم‌گیری، تدوین استراتژی، نگارش آیین‌نامه‌های اجرایی و دستورالعمل‌های ارسالی به آن توجه کنند و در تلاش باشند تا با ایجاد سازگاری‌های قانونی و اجرایی و همچنین ایجاد اعتماد در طرفین فرستنده و گیرنده و طراحی کاربر دوست و بی‌خطا، شرایط را برای پیاده‌سازی هرچه زودتر و ایمن امضای دیجیتال در سازمان‌های کنونی ایجاد کنند، چراکه در دنیایی که به سمت‌وسوی دیجیتالی شدن پیش می‌رود، نیاز به امضای دیجیتال بیش‌ازپیش احساس می‌شود و عدم احصا و توجه به مسائل قانونی و کاربری و نداشتن زیرساخت‌های فنی می‌تواند این امر را به تأخیر انداخته یا اجرای آن با خطا مواجه شود که موجب سلب اعتماد و چالش‌های جدی دیگری خواهد شد.

با توجه به نتایج پژوهش، پیشنهاد می‌شود که زیرساخت‌های فنی توسعه یافته و از شرکت‌های دانش‌بنیانی که در این زمینه و دیگر زمینه‌های تحول دیجیتال در حال فعالیت هستند، در پیاده‌سازی امضای دیجیتال دعوت به همکاری شود.. فرهنگ‌سازی دیجیتال و آموزش پیشنهاد دیگر است. با توجه به اینکه مسئله تحول دیجیتال در حال رخ دادن است، نسل قدیمی برای باقی ماندن و همکاری به آموزش نیاز دارند و ناآگاهی از آن باعث می‌شود کار با این ابزار با سختی انجام‌شده یا مقاومت در برابر آن بیشتر شود. با توجه به اهمیت قوانین در روابط بین‌الملل و تجارت، و همچنین چالش‌های قانونی داخلی به‌دست‌آمده، پیشنهاد می‌شود قوانین سایر کشورها در حوزه اجرای امضای دیجیتال بررسی و طی یک طرح تحقیقاتی و مطالعه تطبیقی، شکاف‌های قانونی استخراج و برای آن، راه‌حلی ایجاد شود. در پیاده‌سازی هرچه بهتر و سریع‌تر امضای دیجیتال، توسعه ابزارها و محصولات امنیتی ساخت ایران به‌منظور کاهش هک و حمله‌های سایبری و همچنین الزام سازمان‌ها در به‌روزرسانی و عقد قراردادهای امنیتی با شرکت‌های حوزه امنیت نیز اهمیت خواهد داشت.

مراجع

[1] Zhang, J. (2010). A study on application of digital signature technology. In 2010 International Conference on Networking and Digital Society (Vol. 1, pp. 498-501). IEEE.

[2] Tavakoli Rad, R; Zargaran Khouzani, F (2023). Successful Organizational Digital Transformation Model, the 6th International Conference on Interdisciplinary Studies in Management and Engineering. Tehran.(in Persian).

[3] Kumalo, M. O. (2020). A framework for digital signature implementations for e-government services. Internet in public administration Municipal government -- Data processing. Masters

[4] Pancholi, V. R., Patel, B. P., & Hiran, D. (2018). A Study on Importance of Digital Signature for E-Governance Schemes. vol, 4, 7-10. IJIRST –International Journal for Innovative Research in Science & Technology| Volume 4 | Issue 10 | March 2018

[5] Khashei, V., Zargaran, F., (2018). Strategic Management of Lynch, Fozhan pub, Tehran. .(in Persian).

[6] Singh, S., Iqbal, M. S., & Jaiswal, A. (2015). Survey on techniques developed using digital signature: public key cryptography. International Journal of Computer Applications, 117(16).

[7] Kaur, Ravneet; Kaur, Amandeep (2012). [IEEE 2012 International Conference on Computing Sciences (ICCS) - Phagwara, India (2012.09.14-2012.09.15)] 2012 International Conference on Computing Sciences - Digital Signature. , (), 295–301. doi:10.1109/ICCS.2012.25

[8] Gupta, A., Tung, Y. A., & Marsden, J. R. (2004). Digital signature: use and modification to achieve success in next generational e-business processes. Information & Management, 41(5), 561-575.

Decision Support Systems, 44(1), 350–359. doi:10.1016/j.dss.2007.04.006

[26] Carayannis, E. G., & Turner, E. (2006). Innovation diffusion and technology acceptance: The case of PKI technology. Technovation, 26(7), 847–855. doi:10.1016/j.technovation.2005.06.013

[27] Srivastava, A. (2005). Is internet security a major issue with respect to the slow acceptance rate of digital signatures?. Computer Law & Security Review, 21(5), 392-404.

[28] L. Tkachev Pravovoy status of computer documents: Basic characteristics. Moscow, 2000, p. 8

[29] Dahabiyeh, L., & Constantinides, P. (2022). Legitimating digital technologies in industry exchange fields: the case of digital signatures. Information and Organization, 32(1), 100392.

[30] Costa, A. A., Arantes, A., & Tavares, L. V. (2013). Evidence of the impacts of public e-procurement: The Portuguese experience. Journal of Purchasing and Supply Management, 19(4), 238-246.

[31] Mohungoo, I., Brown, I., & Kabanda, S. (2020). A systematic review of implementation challenges in public E-Procurement. In Responsible Design, Implementation and Use of Information and Communication Technology: 19th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2020, Skukuza, South Africa, April 6–8, 2020, Proceedings, Part II 19 (pp. 46-58). Springer International Publishing.

[32] Kittur, A. S., & Pais, A. R. (2017). Batch verification of digital signatures: approaches and challenges. Journal of information security and applications, 37, 15-27.

[33] Țurcanu, D., Popovici, S., & Țurcanu, T. (2020). Digital signature: advantages, challenges and strategies. Journal of Social Sciences, 4(3), 62-72.

[34] Ziaeipour, E; Rajabzadeh Qatari, A; Taghizadeh, A(1401). Explaining the adoption process of software-focused networks (SDN) using a foundational and systemic approach. Iran biannual information technology and communication. 51 (14). 172-194. (In Persian).

[35] Karami,, M., Tabatabaeian, S. H., Hanafizadeh, P. H., & Bamdad Soofi, J. (2018). Factors influencing diffusion of Digital Signature in Iranian public Organizations. Iranian Journal of Public Policy, 4(3), 87-102. doi: 10.22059/ppolicy.2018.68428. (In Persian).

[36] Pourqasmi, M; Hadi Pikani, M (2018). Identifying factors affecting the establishment of digital signature system in Isfahan municipality with phenomenological approach, the fourth international research conference in science and engineering. (In Persian).

[37] Esfahani, F; Sarghi Sharbian, M; Mirftahi, M (2019). Authentication in Internet of Things using digital signature, the third national conference of knowledge and technology of electrical, computer and mechanical engineering of Iran. (In Persian).

[38] Pasalar, I (2015). Identifying factors influencing the acceptance of technology among the citizens of Bushehr city; (Study subject: digital signature). Master's thesis. Persian Gulf University. (In Persian).

[39] Mahmoudkhani, Z (2011) Investigating the impact of effective factors on organizational readiness to use digital signatures in electronic banking. Master's thesis, Payam Noor Tehran Center. (In Persian).

[40] Elsan, M (2004). The role of digital signature in electronic document registration. Center, No. 55. (In Persian).

[41] Sandelowski, M., Barroso, J., & Voils, C. I. (2007). Using qualitative metasummary to synthesize qualitative and quantitative descriptive findings. Research in nursing & health, 30(1), 99-111.

[9] Pooja, M., & Yadav, M. (2018). Digital Signature. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 3(6), 71-75.

[10] Mezher, A. E. (2018). Enhanced RSA cryptosystem based on multiplicity of public and private keys. International Journal of Electrical and Computer Engineering, 8(5), 3949.

[11] Pysarenko, V., Dorohan-Pysarenko, L., & Kantsedal, N. (2019). Application of new data formats for electronic document management in government bodies. In IOP Conference Series: Materials Science and Engineering (Vol. 568, No. 1, p. 012102). IOP Publishing.

[12] Afrianto, I., Heryandi, A., Finandhita, A., & Atin, S. (2018). E-Document Autentification With Digital Signature For Smart City: Reference Model. vol, 407, 1-6.

[13] Roy, A., & Karforma, S. (2014). Authentication of user in E-Governance: A Digital Certificate based approach. International Journal of scientific research and management (IJSRM), 2(8), 1212-1221.

[14] Singh, S., & Karaulia, D. S. (2011). E-governance: Information security issues. In International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya (pp. 120-124).

[15] Na, Z., & Xi, X. G. (2008). The application of a scheme of digital signature in electronic government. In 2008 International Conference on Computer Science and Software Engineering (Vol. 3, pp. 618-621). IEEE.

[16] Blanchette, J. F. (2006). The digital signature dilemma. In Annales des télécommunications (Vol. 61, No. 7, pp. 908-923). Springer-Verlag.

[17] Brown, P. W. (1993). Digital signatures: can they be accepted as legal signatures in EDI?. In Proceedings of the 1st ACM conference on Computer and communications security (pp. 86-92).

[18] Lääveri, L. (2021). Consumer acceptance and usage of digital signature technologies. Jyväskylä University School of Business and Economics, Master's Thesis

[19] Afrianto, I., Heryandi, A., Finandhita, A., & Atin, S. (2021). User Acceptance Test For Digital Signature Application In Academic Domain To Support The Covid-19 Work From Home Program. IJISTECH (International Journal of Information System and Technology), 5(3), 270-280.

[20] Sepashvili, E (2020). Digital Chain of Contemporary Global Economy: E-Commerce through E-Banking and E-Signature. Economia Aziendale Online Business and Management Sciences International Quarterly Vol 11, No 3.

[21] Theuermann, K. ., Tauber, A. and Lenz, T. , (2019). "Mobile-Only Solution for Server-Based Qualified Electronic Signatures," ICC 2019 - IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7, doi: 10.1109/ICC.2019.8762076.

[22] Antolino-Hernandes, Anastacio, Ferreira-Medina, Heberto, Torres-Millarez, Cristhian and OLIVARES Carlos. (2019). Management of digital documents with encrypted signature, through the use of centralized PKI, and distributed using blockchain for a secure exchange. Journal of Research and Development, 5-15: 26-37.

[23] Aydin, S., Handan, Ç. A. M., & Alipour, N. (2018). Analyzing the factors affecting the use of digital signature system with the technology acceptance model. Journal of Economics Bibliography, 5(4), 238-252.

[24] Srivastava, A. (2011). Resistance to change: six reasons why businesses don't use e-signatures. Electronic Commerce Research, 11(4), 357–382. doi:10.1007/s10660-011-9082-4

[25] Chang, I.-C., Hwang, H.-G., Hung, M.-C., Lin, M.-H., & Yen, D. C. (2007). Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department.