Security Horazions

Presentation of a comprehensive information security model in digital media based on blockchain technology (Case study: political digital media)

Faezeh Farhoodi [1*]

1- Corresponding Author: assistant professor, Department of Management, Faculty of Social Sciences, Media, University of Religions and Denominations, Qom, Iran. f.farhudi@urd.ac.ir

Volume info

Vol. 19
Series: 71
Summer 2026
P.P: 179-206

Article Type

Research Paper

Article History

Received:
2025-09-13
Revised:
2025-11-01
Accepted:
2026-08-03
Published:
2026-08-31

ISSN – E-ISSN

ISSN: 2538-1857
E-ISSN: 2645-5250

Abstract

Information security in digital political media holds strategic and vital importance, as any deficiency in data protection can lead to the disclosure of sensitive information, distortion of facts, and disruption of political transparency. Furthermore, due to their sensitive nature and broad influence, digital political media are prime targets for complex and organized cyberattacks from both domestic and foreign adversaries. Therefore, integrating information security management frameworks with blockchain capabilities is an effective step toward creating a comprehensive and sustainable model for protecting digital political media.The aim of this study was to develop a comprehensive information security model for political digital media based on blockchain technology. The research adopted a mixed-methods approach with an applied-developmental purpose. Data collection involved qualitative library research and quantitative fieldwork. The population consisted of 29 digital political media managers and 56 blockchain experts, totaling 85 participants selected through a census method. In the qualitative phase, components related to two variables were extracted using the Meta-synthesis algorithm. In the quantitative phase, expert opinions were collected through the Delphi method and questionnaires. Results revealed that the key indicators forming the final model are organized into four main dimensions: governance of political data in the digital environment, transparency and security of political data within blockchain, technological infrastructure for securing political data, and interactions and communications in digital political contexts. The highest-ranked indicators included information confidentiality, resistance to hacker attacks, security of political social networks, and user authentication. The study recommends developing organizational policies grounded in blockchain and information security, establishing a committee for information security and emerging technologies, and enhancing the expertise of human resources.

Keywords: Block chain, Digital Media, Information security, Political data, Political digital media, Political interactions and communications

Cite this Article: Farhoudi, Faezeh. (1405). Presenting a Comprehensive Information Security Model for Digital Media Based on Blockchain Technology (Case Study: Political Digital Media). Security Horizons, 19(71), 179-206.
Dor: 20.1001.1.25381857.1405.19.71.7.4

Publisher: Imam Hossein University.

«آفاق امنیت»

ارائه مدل جامع امنیت اطلاعات در رسانه‌های دیجیتال مبتنی بر فناوری زنجیره بلوکی (مورد مطالعه: رسانه‌های دیجیتال سیاسی)

فائزه فرهودی[1*]

۱- نویسنده مسئول: استادیار، گروه مدیریت، دانشکده علوم اجتماعی، دانشگاه ادیان و مذاهب، قم، ایران f.farhudi@urd.ac.ir

سال و شماره

سال ۱۹ ، پیاپی: ۷۱
تابستان ۱۴۰۵
صص: ۲۰۶-۱۷۹

نوع مقاله

مقاله پژوهشی

سابقه مقاله

تاریخ دریافت: ۱۴۰۴/۰۶/۲۲
تاریخ بازنگری: ۱۴۰۴/۰۸/۱۰
تاریخ پذیرش: ۱۴۰۵/۰۵/۱۲
تاریخ انتشار: ۱۴۰۵/۰۶/۰۹

شاپا چاپی و الکترونیکی

شاپا چاپی: ۱۸۵۷-۲۵۳۸
الکترونیکی: ۵۲۵۰-۲۶۴۵

چکیده

امنیت اطلاعات در رسانه‌های دیجیتال سیاسی از اهمیت استراتژیک و حیاتی برخوردار است؛ زیرا هرگونه کاستی در حفظ امنیت داده‌ها میتواند موجب افشای اطلاعات حساس، تحریف واقعیت‌ها، و ایجاد اختلال در شفافیت سیاسی شود. نیز رسانه‌های دیجیتال سیاسی به دلیل ماهیت حساس و تأثیرگذاری گسترده، هدف اصلی حملات پیچیده و سازمان‌یافته در فضای سایبری از سوی دشمنان داخلی و خارجی هستند. لذا تلفیق چارچوب‌های مدیریت امنیت اطلاعات با قابلیت‌های زنجیره بلوکی، گامی مؤثر در جهت ایجاد مدلی جامع و پایدار برای حفاظت از رسانه‌های دیجیتال سیاسی است. هدف تحقیق، ارائه مدل جامع امنیت اطلاعات در رسانه‌های دیجیتال سیاسی مبتنی بر فناوری زنجیره بلوکی بود. روش تحقیق ترکیبی و از نظر هدف، توسعه‌ای کاربردی بود. گرداوری اطلاعات در بخش کیفی، کتابخانه‌ای و در بخش کمی، میدانی بود. جامعه آماری، مدیران رسانه‌های دیجیتال سیاسی (۲۹ نفر) و متخصصان زنجیره بلوکی (۵۶ نفر) بود که در مجموع ۸۵ نفر به روش کل شماری انتخاب شدند. در بخش کیفی، با استفاده از الگوریتم فراترکیب، مولفه‌های مربوط به دو متغیر استخراج شد. در بخش کمی با روش دلفی و پرسشنامه نظرات متخصصان دریافت شد. یافته ها حاکی از آن بود که شاخص‌های کلیدی پژوهش حاضر (که مدل نهایی برگرفته از آنها بود) در چهار بعد اصلی حاکمیت داده‌های سیاسی در فضای دیجیتال، شفافیت و امنیت داده‌های سیاسی در زنجیره بلوکی، زیرساخت‌های فناورانه برای امنیت داده های سیاسی و تعاملات و ارتباطات سیاسی دیجیتال، جای گرفته است. نتایج نشان داد، شاخص "محرمانگی اطلاعات"، "مقاومت در برابر نفوذ هکرها"، "امنیت شبکه های اجتماعی سیاسی" و "احراز هویت کاربران" بالاترین رتبه را کسب کردند. تدوین خط مشی سازمانی مبتنی بر زنجیره بلوکی و امنیت اطلاعات، تشکیل کمیته امنیت اطلاعات و فناوری های نوین، و ارتقای تخصص نیروی انسانی از پیشنهادات پژوهش حاضر است.

کلیدواژه‌ها: زنجیره بلوکی، رسانه‌های دیجیتال سیاسی، امنیت اطلاعات، داده های سیاسی، تعاملات و ارتباطات سیاسی

استناد: فرهودی، فائزه . (۱۴۰۵). ارائه مدل جامع امنیت اطلاعات در رسانه‌های دیجیتال مبتنی بر فناوری زنجیره بلوکی (مورد مطالعه: رسانه‌های دیجیتال سیاسی). فصلنامه آفاق امنیت، ۱۹(۷۱)، ۲۰۶-۱۷۹.

Dor: 20.1001.1.25381857.1405.19.71.7.4

مقدمه

در عصر حاضر، رسانه‌های دیجیتال به‌ویژه رسانه‌های دیجیتال سیاسی، به عنوان یکی از مهمترین نهادهای تأثیرگذار در شکل‌دهی افکار عمومی، فرآیندهای تصمیم‌گیری سیاسی و ترویج مشارکت مدنی، نقش بی‌سابقه‌ای یافته‌اند (Khan & et al, 2022). این رسانه‌ها با تولید و توزیع گسترده و سریع اطلاعات، بستری حیاتی برای تبادل نظر و ایجاد هویت جمعی فراهم می‌آورند، اما همزمان با این فرصت‌ها، چالش‌های اساسی نیز امنیت اطلاعات در رسانه‌ها را مورد تهدید قرار داده است. اطلاعات منتشر شده در این رسانه‌ها نه تنها ممکن است از نظر سیاسی حساسیت برانگیز باشد؛ بلکه ناپایدار بودن امنیت داده‌ها و نبود چارچوب منسجم و معین، بعضا تهدیدی برای اعتماد عمومی و سلامت فضای رسانه‌ای محسوب میشود (Chen & et al, 2021). رسانه دیجیتال به هر نوع محتوایی اطلاق می‌شود که از طریق ابزارهای مجهز به پردازشگر دیجیتال (مانند رایانه، تلفن همراه، تبلت) ایجاد، ذخیره و منتشر شود. سازمان‌های خبری، اپلیکیشن‌ها، شبکه‌های اجتماعی (Estakhrian-Haghighi & et al, 2017)، رسانه‌های آنلاین (شامل وب‌سایت‌ها، خبرگزاری‌ها، وبلاگ‌ها و شبکه‌های اجتماعی)، و رسانه‌های تعاملی (مانند پلتفرم‌های ویدیویی مانند آپارات و پیام‌رسان‌ها) از جمله رسانه های دیجیتال محسوب می شوند. رسانه‌های دیجیتال سیاسی، به مجموعه‌ای از زیرساخت‌ها و پلتفرم‌های ارتباطی مبتنی بر فناوری‌های دیجیتال گفته می‌شود که به‌طور تخصصی در حوزه انتقال، انتشار و تبادل اطلاعات سیاسی فعالیت دارند (Zarei & et al, 2019) که امکان تعامل مستقیم و دوسویه میان فعالان سیاسی، نهادهای دولتی، احزاب و عموم جامعه را فراهم می‌آورند (Hamzehpour, 2020) و با ویژگی‌هایی مانند قابلیت فراگیر بودن، دسترسی لحظه‌ای، سرعت بالای دسترس‌پذیری و امکان تولید محتوا توسط کاربران متعدد، ظرفیت بی‌نظیری برای تأثیرگذاری مستقیم بر رفتار سیاسی و کنشهای مدنی فراهم می‌کنند (Khan & et al, 2022). حفظ محرمانگی، یکپارچگی، و امنیت اطلاعات به ویژه در رسانه‌های سیاسی، از اهمیت ویژه‌ای برخوردار است به گونه ای که نقض این اصول میتواند پیامدهای گسترده‌ای از جمله دستکاری اطلاعات، انتشار اخبار جعلی، نفوذ سایبری از جانب دشمنان داخلی و خارجی، و خدشه‌دار شدن امنیت و حریم خصوصی کاربران را به دنبال داشته باشد. امنیت اطلاعات، مجموعه‌ای منسجم از سیاست‌ها، فناوری‌ها و فرایندهای مدیریتی است که به منظور

حفاظت از داده‌ها و سیستم‌های اطلاعاتی در برابر انواع تهدیدات، طراحی و پیاده‌سازی می‌گردد (Peltier, 2016). این تهدیدات میتواند منجر به افشای غیرمجاز، دست‌کاری، تخریب یا از دست رفتن اطلاعات شود. امنیت اطلاعات بر پایه سه اصل بنیادین محرمانگی[1]، یکپارچگی[2] و دسترس‌پذیری[3] استوار است که به شکل مثلث CIA شناخته می‌شود (Whitman & Mattord, 2017) و علاوه بر اصول پایه، مفاهیمی نظیر اصالت[4]، عدم انکار[5] و قابلیت پیگیری[6] در تضمین اعتبار و اطمینان از تبادلات اطلاعات نقش بسزایی ایفا می‌کنند (Smith & Brooks, 2019). امنیت اطلاعات افزون بر بعد فناوری دارای جنبه‌های انسانی و فرهنگی نیز هست که می بایست بین ابعاد فنی، مدیریتی، انسانی و فرهنگی هماهنگی لازم ایجاد گردد تا پویایی و جامعیت آن در نهایت منجر به موفقیت نظام های امنیتی شود (Jafarnejad Sani & et al, 2022). در سال های اخیر، فناوری زنجیره بلوکی یا بلاک‌چین با ویژگی‌های ذاتی نظیر ساختار غیرمتمرکز، ثبت تغییرناپذیر تراکنش‌ها، شفافیت، و تضمین امنیت داده‌ها، به عنوان یک راهکار نوآورانه و قدرتمند مطرح شده که می‌تواند تحولی بنیادین در امنیت اطلاعات رسانه‌های دیجیتال ایجاد کند (Sharif Khatibi & et al, 2019). این فناوری با حذف واسطه‌ها، توزیع داده‌ها در میان چندین گره و واحد شبکه ای مستقل و نیز استفاده از الگوریتم‌های رمزنگاری پیشرفته، ضمن افزایش سطح اعتماد کاربران، امکان ردیابی دقیق تراکنش‌ها و جلوگیری از دست‌کاری و جعل داده‌ها را امکان پذیر می‌کند (Wang & et al, 2022). این فناوری داده‌های تراکنش‌ها را به صورت زنجیره‌ای ذخیره می‌کند (Karmakar, 2024) و به عنوان یک پایگاه داده توزیع‌شده می‌تواند امنیت، اعتماد و کارایی در مدیریت داده‌ها و تراکنش‌ها را در صنایع مختلف ایجاد کند (Leng & et al, 2022). مهم‌ترین ویژگی بلاک‌چین، حذف واسطه‌ها و امکان انجام تراکنش‌های همتا به همتا است (Zheng & et al, 2021). در نتیجه، بلاک‌چین نه تنها بستر اصلی ارزهای دیجیتال است بلکه قابلیت به کارگیری در حوزه‌های مختلف مانند قراردادهای هوشمند، سیستم‌های رای‌گیری و مدیریت زنجیره تأمین را دارد (Wang & et al, 2020). زنجیره بلوکی با فراهم آوردن

1 Confidentiality
2 Integrity
6 Accountability
3 Availability
4 Authenticity
5 Non-repudiation
6 Accountability

ساختاری توزیع‌شده، تغییرناپذیر و شفاف، می‌تواند ضمن ارتقاء امنیت داده‌ها، صحت و اعتبار اخبار را تضمین کند (Ferreira & et al, 2020). تدوین مدل‌های عملیاتی که قادر باشد امنیت داده‌ها را در کنار حفظ حریم خصوصی، به صورت همزمان پیاده‌سازی نماید، از اهمیت بسزایی برخوردار است (O'Shields, 2017). همان گونه که می دانیم مشارکت فعال کاربران و انتشار مطالب سیاسی حساس، چالش های امنیتی خاصی مانند دستکاری داده‌ها، نفوذهای سایبری و نقض حریم خصوصی را به همراه دارد که توجه به آنها برای حفظ سلامت فضای رسانه‌ای امری ضروری است (Chen & et al, 2021). در ایران نیز همچون بسیاری از کشورها، با وجود رشد چشمگیر استفاده از رسانه‌های دیجیتال سیاسی، چالش‌های متعددی در زمینه امنیت اطلاعات و مدیریت داده‌ها وجود دارد. تعدد نهادهای سیاستگذار، پراکندگی و ضعف هماهنگی بین دستگاه‌های نظارتی، فقدان زیرساخت‌های فناورانه کارآمد و نیز عدم آگاهی کافی کاربران از تهدیدات سایبری، کاهش کارآمدی محافظت از اطلاعات و اعتماد عمومی را سبب شده است (Lokuge & et al, 2019). همچنین، پیچیدگی فضای رسانه‌های دیجیتال و حضور گسترده و متنوع تولیدکنندگان محتوا، علاوه بر تهدیدات فنی، چالش‌های مدیریتی، حقوقی و فرهنگی نیز به همراه داشته است (Fazli & et al, 2023). به همین دلیل، طراحی مدل جامع و یکپارچه امنیتی که علاوه بر زیرساخت‌های فناورانه، رویکردی مدیریتی و ساختاری متناسب با شرایط خاص رسانه‌های دیجیتال سیاسی کشور داشته باشد، ضروری به نظر می رسد. پژوهش حاضر با هدف ارائه مدل امنیت اطلاعات در رسانه‌های دیجیتال مبتنی بر زنجیره بلوکی، با تأکید بر رسانه‌های دیجیتال سیاسی در ایران، طی بازه زمانی اردیبهشت ۱۴۰۴ تا تیر ۱۴۰۴ انجام شده و محور آن تحلیل مولفه‌های امنیت اطلاعات، قابلیت‌های بلاک‌چین، و طراحی مدل اجرایی برای ارتقای امنیت در رسانه‌های دیجیتال سیاسی استوار است و سوالات فرعی پژوهش عبارتند از:

* مولفه‌ها و معیارهای کلیدی امنیت اطلاعات در رسانه‌های دیجیتال سیاسی ایران کدامند؟

* ویژگی‌ها و قابلیت‌های فناوری زنجیره بلوکی که به ارتقای امنیت اطلاعات در رسانه‌های دیجیتال سیاسی کمک می‌کند کدامند؟

ادبیات نظری

در بخشی از نظریه "اشاعه نوآوری" راجرز به نقش رسانه به عنوان یکی از عوامل گسترش نوآوری تاکید شده و پیش‌فرض این است که نوآوری‌ها مانند ایده‌ها در یک جامعه آغاز می‌شوند و از طریق اشکال متفاوت ارتباطی از جمله شبکه‌های اجتماعی، گسترش می‌یابند (Maharati & Entezarian, 2021). به جهت نقشی که راجرز برای نوآوری در رسانه‌ها قائل است و از سوی دیگر به کارگیری فناوری های نوین در رسانه ها، گامی به سوی فعالیت های نوآورانه در عرصه رسانه ها محسوب می شود؛ لذا از این نظریه استفاده شد. بر اساس نظریه وابستگی، هر چه تعداد و کارکردهای اطلاعات رسانه‌ای توسط رسانه‌های جمعی بیشتر باشد، وابستگی مخاطبان به رسانه بیشتر می‌شود. با استفاده از فناوری‌های نوین مانند بلاک‌چین در رسانه‌های دیجیتال حریم‌خصوصی کاربران بیشتر مورد توجه قرار گرفت لذا میزان وابستگی مخاطبان به رسانه‌های دیجیتال افزایش خواهد یافت. نظریه استفاده و رضامندی، مهم‌ترین نقش رسانه‌ها را برآورده ساختن نیازها و انگیزه‌های مخاطب می‌داند، بنابراین، به هر میزان که رسانه‌ها این نیازهارا برآورده سازند، به همان میزان موجبات رضایتمندی را فراهم می‌کنند (Windahl & et al, 2019, 274). در عصر حاضر، استفاده از فناوری‌های نوین افزایش یافته که باعث شده کاربران و پدیدآورندگان در استفاده از این رسانه‌ها به جهت امنیت اطلاعات که ایجاد شده، احساس خوشنودی داشته باشند. چارچوب تئوریک مکتب امنیتی کپنهاگ بر گسترش مفهوم امنیت فراتر از حوزه نظامی و تأکید بر بخش‌های مختلف امنیتی (حوزه‌هایی همچون بخش نظامی، سیاسی، اقتصادی، زیست‌محیطی و اجتماعی) متمرکز است و مفهوم کلیدی «امنیتی شدن» را برای تحلیل فرایند تبدیل شدن یک مسئله به تهدید امنیتی به کار می‌برد. اقدامات اضطراری، منطق امنیتی، مجموعه ها و بازیگران امنیتی، از دیگر شاخصه های این نظریه محسوب می شوند. هدف اصلی چارچوب نظری کپنهاک که بوزان و همکارانش از جمله نظریه پردازان این مکتب بودند، فراهم آوردن روشی جدید برای تحلیل امنیت است که برخلاف دیدگاه‌های سنتی و محدود به حوزه نظامی، جنبه‌های گسترده‌تر و اجتماعی امنیت را نیز در بر می‌گیرد و به درک بهتر چگونگی شکل‌گیری و مواجهه با تهدیدهای مختلف کمک می‌کند. بوزان بر خلاف دیدگاه های رئالیستی روابط بین الملل که امنیت را امری

عینی تصور می کردند، معتقد است که امنیت مساله ای بین ذهنی و مبتنی بر تصمیم بازیگران است و طبق نظریه بوزان، برداشت و تحلیل بازیگران از امنیت بر تصمیم سازی و واکنش ها و در نهایت رفتار سازمانی آنها در حوزه امنیت نقش بی بدیلی دارد لذا ممکن است یک موضوع در نزد یک بازیگر تهدید امنیتی محسوب شود و همان موضوع نزد دیگر بازیگران امری عادی و طبیعی جلوه کند (Buzan, 1998). از آنجا که رسانه ها امروزه مهمترین ابزار جنگ روانی چه در زمان صلح چه در زمان جنگ هستند و جنگ روانی هم یکی از ابزارهای اثرگذار بر امنیت ملی است عملیات روانی رسانه ای معمولا امنیت یک کشور را خدشه دار خواهد کرد (Caparini, 2004, 65-69).

پیشینه پژوهش

مولایی و سخائی (۱۴۰۳) در پژوهشی با عنوان "مروری بر کاربردهای منتخب بلاک‌چین در صنعت رسانه و سرگرمی: رویکرد آینده‌پژوهی" اشاره کردند که بلاک چین، پتانسیل زیادی برای توسعه در صنعت رسانه و سرگرمی دارد و مهمترین کاربردهای آن عبارتند از مقابله با اخبار جعلی و شایعات؛ مقابله با سرقت ادبی؛ ارتقای امنیت کاربر؛ حذف واسطه‌های صنعت رسانه؛ احراز هویت مخاطب؛ بستر ایجاد پلتفرم رسانه اجتماعی؛ و ارتقای وفاداری مخاطب. صابری، نظرنیا و خلیلی فر (۱۴۰۳) به بررسی نقش بلاک‌چین در تدوین استراتژی‌های سازمانی و تأثیر آن بر امنیت و شفافیت فرآیندهای استراتژیک پرداختند و به این نتیجه دست یافتند که استفاده از بلاک‌چین به‌عنوان یک فناوری نوین، امکان ایجاد یک سیستم شفاف، غیرمتمرکز با امنیت بالا را فراهم می‌کند که به کاهش ریسک و افزایش امنیت اطلاعات در سازمان کمک شایان توجهی می کند. جوادیان (۱۴۰۳) در مقاله خود چگونگی استفاده از فناوری بلاک چین در بهبود امنیت سیستم های اطلاعات سازمانی را بررسی نموده که نتایج پژوهش او حاکی از این است که استفاده از فناوری بلاک چین بر بهبود امنیت سیستم های اطلاعات سازمانی تاثیر مثبت و معنادار دارد و نیز ویژگی عدم تمرکز بلاک چین، شفافیت داده ها در آن و عدم مداخله گری و دستکاری داده ها در بلاک چین بر بهبود امنیت سیستم های اطلاعات سازمانی اثر مطلوب و مثبت داشته است. جعفرنژاد ثانی و همکاران (۱۴۰۲) به بررسی مولفه های امنیت اطلاعات در تحقیقات پیشین پرداختند و به این نتیجه رسیدند که به دلیل مشکلات امنیتی که علیرغم فناوری های پیشرفته هنوز

هم وجود دارد توجه به فرهنگ امنیت اطلاعات ضروری است و مولفه هایی که به عنوان عوامل سازنده یا تاثیرگذار در فرهنگ امنیت اطلاعات در نظر گرفته شده، از نظر تعداد، شکل گیری و مفهوم متفاوت است و هنوز ابعاد استاندارد و پذیرفته شده ای برای فرهنگ امنیت اطلاعات وجود ندارد. چن و همکاران (۲۰۲۲) در پژوهش خود با عنوان "بررسی کاربرد بلاک‌چین در صنعت رسانه و داده‌های کلان" به این نتیجه رسیدند که بلاک‌چین می‌تواند مشکلاتی مانند کپی‌رایت، جعبه سیاه الگوریتم‌ها، و ضعف در اعتماد و چالش های امنیت داده ها را در رسانه حل کند و آینده روشنی برای کاربرد بلاک‌چین در رسانه رقم بزند. آفتابی (۱۳۹۷) در پایان نامه خود به مدیریت امنیت اطلاعات اشاره کرده که به دلیل فضای رقابتی کنونی، امری ضروری تلقی می شود. او با بهره گیری از روش مدلسازی چندروشی پویاشناسی سیستم و مدلسازی عامل مبنا مدلی ترکیبی از سه عامل سازمان، و نفوذ کنندگان به سیستم امنیتی از خارج و داخل سازمان ارائه کرده تا بتواند درباره میزان خسارات احتمالی و هزینه های امنیتی سازمان ناشی از نفوذهای امنیتی در آینده نزدیک و درک تعاملات میان عامل های شبیه سازی شده به درک درستی دست یابد. نتایج تحقیق نشان می دهد برخلاف تصور، تنها جنبه فنی و مقابله با تهدیدات خارج سازمان منجر به تامین امنیت نمی شود، بلکه تهدیدات از داخل سازمان می تواند محتمل تر و زیان بارتر باشد لذا، مدیران باید به هردو جنبه تهدیدات در داخل و خارج سازمان توجه کافی داشته باشند تا امنیت مورد نظر خود را در سازمان پیاده سازی نمایند. کوسبا[1] و همکاران (۲۰۱۶) به این مطلب پی بردند که پیاده‌سازی زنجیره بلوکی، برخی مشکلات سازمان را از نظر صیانت از حریم خصوصی، شفافیت، امنیت اطلاعات و چالش های سایبری بهبود می‌بخشد. ونپوک و همکاران (۲۰۱۴)، معتقدند یکپارچگی تامین کنندگان و مشتریان از طریق درک یکپارچگی، اجرای یکپارچگی و ارتقا و استمرار یکپارچگی با استفاده از به کارگیری فناوری بلاک چین انجام شدنی است. رستمی و طباخی ممقانی (۱۳۹۰) به ترسیم فضای آینده رسانه با توجه به احتمال رقابتی شدن فضای رسانه ای بدلیل استفاده از انواع فناوری های پیشرفته پرداخته و در راستای ایجاد امنیت ملی، راهبردهای ارشادی- تبلیغی، اطلاعاتی، و سرگرمی-تفریحی ارائه کرده است.

1 Kosba, A., Miller, A., Shi, E., & Chan, D.

جدول ۱. پیشینه پژوهش

ردیف	نویسنده/ نویسندگان (سال پژوهش)	عنوان پژوهش	مهم‌ترین یافته‌ها و نتایج مرتبط با پژوهش
۱	مولایی و سخائی (۱۴۰۳)	مروری بر کاربردهای منتخب بلاک‌چین در صنعت رسانه و سرگرمی: رویکرد آینده‌پژوهی	بلاک چین، پتانسیل زیادی برای توسعه در صنعت رسانه و سرگرمی دارد و مهمترین کاربردهای آن عبارتند از مقابله با اخبار جعلی و شایعات؛ مقابله با سرقت ادبی؛ ارتقای امنیت کاربر؛ حذف واسطه‌های صنعت رسانه؛ احراز هویت مخاطب؛ بستر ایجاد پلتفرم رسانه اجتماعی؛ و ارتقای وفاداری مخاطب
۲	صابری، نظرنیا و خلیلی فر (۱۴۰۳)	استفاده از بلاک چین در تدوین استراتژی های سازمانی: چشم انداز جدید امنیت و شفافیت	استفاده از بلاک‌چین، امکان ایجاد یک سیستم شفاف، غیرمتمرکز با امنیت بالا را فراهم می‌کند که به کاهش ریسک و افزایش امنیت اطلاعات در سازمان کمک شایان توجهی می کند
۳	جوادیان (۱۴۰۳)	استفاده از فناوری بلاک چین برای بهبود امنیت و سیستم های اطلاعات سازمانی	استفاده از فناوری بلاک چین بر بهبود امنیت سیستم های اطلاعات سازمانی تاثیر مثبت و معنادار دارد و نیز ویژگی عدم تمرکز بلاک چین، شفافیت داده ها در آن و عدم مداخله گری و دستکاری داده ها در بلاک چین بر بهبود امنیت سیستم های اطلاعات سازمانی اثر مثبت داشته است.
۴	جعفرنژاد ثانی و همکاران (۱۴۰۲)	ابعاد و مولفه های فرهنگ امنیت اطلاعات: یک مرور نظام مند	به دلیل مشکلات امنیتی که علیرغم فناوری های پیشرفته هنوز هم وجود دارد توجه به فرهنگ امنیت اطلاعات ضروری است و مولفه هایی که به عنوان عوامل تاثیرگذار در فرهنگ امنیت اطلاعات در نظر گرفته شده، از نظر تعداد، شکل گیری و مفهوم متفاوت است و هنوز ابعاد استانداردی برای فرهنگ امنیت اطلاعات وجود ندارد

جدول ۱. پیشینه پژوهش

ردیف	نویسنده/ نویسندگان (سال پژوهش)	عنوان پژوهش	مهم‌ترین یافته‌ها و نتایج مرتبط با پژوهش
۵	چن و همکاران (۲۰۲۲)	پژوهشی در مورد فناوری بلاک‌چین و کاربردهای آن در صنعت رسانه در بستر کلان‌داده	بلاک‌چین می‌تواند مشکلاتی مانند کپی‌رایت، جعبه سیاه الگوریتم‌ها، و ضعف در اعتماد و چالش های امنیت داده ها را در رسانه حل کند و آینده روشنی برای کاربرد بلاک‌چین در رسانه رقم بزند
۶	آفتابی (۱۳۹۷)	یک مدل مدیریت امنیت اطلاعات برای کاهش ریسک های احتمالی در سازمان های مبتنی بر فناوری اطلاعات	برخلاف تصور، تنها جنبه فنی و مقابله با تهدیدات خارج سازمان منجر به تامین امنیت نمی شود، بلکه تهدیدات از داخل سازمان می تواند محتمل تر و زیان بارتر باشد لذا، مدیران باید به هردو جنبه تهدیدات در داخل و خارج سازمان توجه کافی داشته باشند تا امنیت مورد نظر خود را در سازمان پیاده سازی نمایند.
۷	کوسبا و همکاران (۲۰۱۶)	هاوک؛ مدل بلاک‌چین برای رمزنگاری و قراردادهای هوشمند با حفظ حریم خصوصی	پیاده‌سازی زنجیره بلوکی، برخی مشکلات سازمان را از نظر صیانت از حریم خصوصی، شفافیت، امنیت اطلاعات و چالش های سایبری بهبود می‌بخشد
۸	ونپوک و همکاران (۲۰۱۴)	یکپارچه‌سازی تأمین‌کنندگان و مشتریان از طریق درک، پیاده‌سازی و ترویج یکپارچگی با استفاده از فناوری بلاک‌چین	یکپارچگی تامین کنندگان و مشتریان از طریق درک یکپارچگی، اجرای یکپارچگی و ارتقا و استمرار یکپارچگی با استفاده از به کارگیری فناوری بلاک چین انجام شدنی است.
۹	رستمی و طباخی ممقانی (۱۳۹۰)	آینده پژوهی فضای رسانه و امنیت ملی جمهوری اسلامی ایران	به ترسیم فضای آینده رسانه با توجه به احتمال رقابتی شدن فضای رسانه ای بدلیل استفاده از انواع فناوری های پیشرفته پرداخته و در راستای ایجاد امنیت ملی، راهبردهای ارشادی- تبلیغی، اطلاعاتی، و سرگرمی-تفریحی ارائه کرده اند.

مرور پیشینه پژوهش نشان می‌دهد در حوزه امنیت اطلاعات و بلاک چین در داخل و خارج از ایران پژوهش‌های مختلفی انجام شده اما تا کنون هیچ پژوهشی به بررسی تاثیر بلاک‌چین بر امنیت اطلاعات در رسانه‌های دیجیتال سیاسی نپرداخته است. یکی از دلایل، جدید بودن این فناوری و علت دیگر اینکه هنوز فواید این فناوری در رسانه‌های دیجیتال به ویژه رسانه هایی با رویکرد سیاسی بر اندیشمندان، شفاف نیست. لذا پژوهش در این زمینه می‌تواند چالش‌های امنیت اطلاعات در رسانه‌های دیجیتال سیاسی را تا حد زیادی مرتفع نماید.

روش‌شناسی پژوهش

روش تحقیق ترکیبی و از نظر هدف، توسعه‌ای کاربردی است. روش گرداوری اطلاعات در بخش کیفی، کتابخانه‌ای و در بخش کمی، میدانی است. در بخش کیفی، شناسایی مولفه‌های امنیت اطلاعات و زنجیره بلوکی با روش فراترکیب صورت گرفت. در مرحله دوم، با استفاده از روش دلفی، این مولفه‌ها بین متخصصان توزیع شد. جامعه تحقیق، مدیران رسانه‌های دیجیتال سیاسی (انتخاب رسانه‌های متنوع در قالب‌های مختلف، امکان بررسی همه‌جانبه مولفه‌های مدل جامع امنیت اطلاعات را فراهم می‌سازد) و متخصصان زنجیره بلوکی بود که در مجموع ۸۵ نفر به عنوان جامعه آماری به روش کل شماری انتخاب شدند و نیازی به نمونه گیری نبود. در جدول ذیل، لیست جامعه آماری پژوش به تفکیک تخصص ارائه شده است که این افراد به صورت غیرتصادفی و هدفمند انتخاب شده اند.

جدول ۲. جامعه آماری تحقیق به تفکیک تخصص و محل فعالیت

تخصص	محل فعالیت	تعداد	مجموع
	پایگاه خبری «انصاف نیوز» پایگاه خبری-تحلیلی است که تمرکز قابل توجهی بر اخبار و تحلیل‌های سیاسی دارد با رویکردی منصفانه و مستقل به پوشش اخبار عمدتا سیاسی می‌پردازد	۵	
	کانال تلگرام «جهان نیوز» کانال خبری-تحلیلی سیاسی معتبر ایرانی است که اخبار فوری، موثق و تحلیل‌های سیاسی را منتشر می‌کند و به عنوان یک رسانه	۵	

جدول ۲. جامعه آماری تحقیق به تفکیک تخصص و محل فعالیت

تخصص	محل فعالیت	تعداد	مجموع
مدیر و فعال حوزه رسانه های دیجیتال سیاسی	فعال در فضای دیجیتال سیاسی ایران شناخته می‌شود		۲۹
	پایگاه خبری «خبرگزاری فارس» با رویکرد کاملاً سیاسی و تاثیرگذار است که به پوشش و تحلیل مسائل سیاسی کشور می‌پردازد	۶	
	صفحه اینستاگرامی «سیاست روز» صفحه فعال در حوزه تحلیل‌های سیاسی که با حضور پررنگ و مخاطبان قابل توجه فعالیت می‌کند و محتوای آن عمدتاً متکی بر تحلیل و تفسیر رویدادهای سیاسی داخلی و بین‌المللی است	۵	
	کانال تلگرام «رسانه انقلاب» کانال خبری و تحلیلی سیاسی با تأکید بر ارزش‌ها و دیدگاه‌های انقلاب اسلامی انقلابی	۴	
	صفحه اینستاگرامی «خبرگزاری دانشجو» از رسانه‌های فعال و معتبر ایرانی که به انتشار اخبار و تحلیل‌های سیاسی، اقتصادی و اجتماعی می‌پردازد که حضور پررنگ تحلیلگران و کارشناسان سیاسی در محتوای این صفحه، موجب شده به عنوان یکی از منابع خبری تحلیلی سیاسی قابل اعتماد در فضای مجازی شناخته شود	۴	
متخصصان فناوری زنجیره بلوکی	انجمن فناوران زنجیره بلوک	۵۳	۵۶
	خانه بلاک چین ایران (اعضای هیات مدیره)	۳	

در بخش کیفی، با استفاده از الگوریتم هفت مرحله‌ای فراترکیب سندلوسکی و باروسو (۲۰۰۳)[1]، با مطالعه مقالات، پایان‌نامه‌ها و کتاب‌ها، مولفه‌های مربوط به این دو متغیر (امنیت اطلاعات و فناوری زنجیره بلوکی) استخراج شد. در بخش کمی با استفاده از روش دلفی و تنظیم پرسشنامه نظرات متخصصان دریافت شد. در مرحله کمی پرسشنامه طراحی شد که روایی آن با استفاده از نظرات اساتید تأیید شد. همچنین با محاسبه ضریب آلفای کرونباخ، (که برای مالکیت معنوی ۸۳٪ و برای فناوری بلاک چین ۷۹٪ بود)، پایایی پرسشنامه تائید شد.

1 Sandelowski and Barroso

یافته‌های پژوهش

همانطور که اشاره شد از الگوریتم هفت مرحله‌ای فراترکیب جهت استخراج شاخص‌ها استفاده شد که این مراحل عبارت است از طراحی سوال؛ بررسی نظام‌مند ادبیات؛ جستجو و انتخاب مقاله‌های مناسب؛ استخراج اطلاعات مقاله؛ تجزیه و تحلیل و ترکیب یافته‌های کیفی؛ کنترل کیفیت؛ و ارائه یافته‌ها که در مرحله اول، سوالات مورد نظر جهت جستجوی مقالات در جدول ۳ نشان داده شده است.

جدول ۳. سوالات پژوهش در روش فراترکیب

کلمات پرسشی	سوالات پژوهش
What (چه چیزی)	عوامل موثر بر امنیت اطلاعات و فناوری بلاک چین کدامند؟
Who (جامعه مورد مطالعه)	پایگاه های اطلاعاتی علمی معتبر فارسی و لاتین در زمینه موضوع تحقیق کدامند؟
When (بازه زمانی)	مقالات منتشر شده فارسی و لاتین در زمینه موضوع تحقیق ۱۰سال اخیر (۱۴۰۱-۱۳۹۱)
How (چگونگی روش)	با استفاده از روش تحلیل اسناد

در مرحله دوم، کلیدواژه‌ها و پایگاه‌های اطلاعاتی مشخص شد که کلیدواژه‌ها (فارسی و معادل لاتین آنها) عبارتند از امنیت اطلاعات، زنجیره بلوکی، فناوری بلاک‌چین، رسانه‌های دیجیتال، شفافیت اطلاعات، مدیریت محتوا، مدیریت امنیت داده ها، صحت اطلاعات، بلاک‌چین در رسانه‌ها، امنیت سایبری، و رسانه های سیاسی. پایگاه‌های اطلاعاتی مجلات تخصصی نور[۱]، پایگاه مرکز اطلاعات علمی جهاد دانشگاهی[۲]، پرتال جامع علوم انسانی[۳]، پژوهشگاه علوم و فناوری اطلاعات ایران[۴]، و اسکوپوس. در مرحله سوم، ۴۳ مقاله فارسی و ۱۸مقاله لاتین در زمینه مالکیت معنوی و۲۸ مقاله فارسی و ۱۰مقاله لاتین در زمینه بلاک‌چین استخراج شد که از۹۹ مقاله

https://www.noormags.ir/
https://www.sid.ir/fa/journal/
http://ensani.ir/fa
https://irandoc.ac.ir/

اولیه، ۵۴ مقاله متناسب با پژوهش حاضر انتخاب شد. در مرحله چهارم، جهت دستیابی به یافته‌های درون محتواهای مجزایی که در آنها مطالعات اصلی انجام شده، چندین مرتبه مطالعه صورت گرفت. پس از بررسی، مولفه های به دست آمده، به صورت کدهای مشخص دسته‌بندی شد که در جدول۴ نشان شده است:

جدول ۴. کدبندی مطالعات تحقیق

شاخص ها و مولفه ها (کدهای گزینشی)	منابع (مقالات)
محرمانگی اطلاعات سیاسی	بختیاری و لک (۱۳۹۷)، کونگلو (۲۰۲۳)، دان کاولتی (۲۰۱۹)
کنترل توزیع محتوای سیاسی	رضایی میرقائد و همکاران (۱۴۰۱)، شیرز (۲۰۲۳)، کهرامان (۲۰۱۹)
مقابله با جعل هویت	کریمی و همکاران (۱۳۹۳)، شیرز (۲۰۲۳)، لی (۲۰۱۹)
شفافیت انتشار اخبار	رضایی میرقائد و همکاران (۱۴۰۱)، شیرز (۲۰۲۳)
احراز هویت کاربران	کریمی و همکاران (۱۳۹۳)، کونگلو (۲۰۲۳)
دسترسی مستمر	بختیاری و لک (۱۳۹۷)، دان کاولتی (۲۰۱۹)
کنترل دسترسی محتوای محرمانه	رضایی میرقائد و همکاران (۱۴۰۱)
پیشگیری از سانسور	رضایی میرقائد و همکاران (۱۴۰۱)، شیرز (۲۰۲۳)، قاسمی (۱۳۹۳)
حفظ حریم خصوصی فعالان رسانه ای	بختیاری و لک (۱۳۹۷)، کونگلو (۲۰۲۳)
صحت داده‌های رسانه‌ای	باقری و ابراهیمی (۱۴۰۰)، کهرامان (۲۰۱۹)
زیرساخت‌های فناورانه	بیگدلی و همکاران (۱۴۰۴)، ونچرز (۲۰۲۵)، بیرامی و شفیعی (۱۴۰۴)، الهی و همکاران (۱۴۰۳)
امنیت داده‌های عمومی	قاسمی (۱۳۹۳)، بیرامی و شفیعی (۱۴۰۴)، بختیاری و لک (۱۳۹۷)
تحلیل داده‌های بلاک‌چین	رضایی میرقائد و همکاران (۱۴۰۱)، لی (۲۰۱۹)
امنیت محتوای چندرسانه‌ای	بختیاری و لک (۱۳۹۷)، بیرامی و شفیعی (۱۴۰۴)، الهی و همکاران (۱۴۰۳)
حفاظت داده‌های انتخاباتی	رضایی میرقائد و همکاران (۱۴۰۱)، قاسمی (۱۳۹۳)
الگوریتم روانشناختی	علیزاده و همکاران (۱۴۰۲)، لی (۲۰۱۹)، ونچرز (۲۰۲۵)
امنیت شبکه‌های اجتماعی سیاسی	بختیاری و لک (۱۳۹۷)، بیگدلی و همکاران (۱۴۰۴)، بیرامی و شفیعی (۱۴۰۴)

جدول ۴. کدبندی مطالعات تحقیق

شاخص ها و مولفه ها (کدهای گزینشی)	منابع (مقالات)
ردیابی منابع داده های سیاسی	رضایی میرقائد و همکاران (۱۴۰۱)، قاسمی (۱۳۹۳)، بیرامی و شفیعی (۱۴۰۴)
حمایت از آزادی بیان	بختیاری و لک (۱۳۹۷)، شیرز (۲۰۲۳)، بیگدلی و همکاران (۱۴۰۴)
مدیریت تعاملات و تسهیل تعامل شفاف	رضایی میرقائد و همکاران (۱۴۰۱)، باقری و همکاران (۱۴۰۲)، ساش و همکاران (۱۳۹۷)
محافظت از اطلاعات محرمانه نظام	تاکی (۱۳۹۲)، باقری و همکاران (۱۴۰۲)، حسین آبادی (۱۴۰۴)، عابدی (۱۳۹۶)، صفری (۱۴۰۳)
امنیت رای‌گیری الکترونیک	رضایی میرقائد و همکاران (۱۴۰۱)، قاسمی (۱۳۹۳)
اعتبار داده‌های سیاسی	حسینی و همکاران (۱۴۰۰)، کورپاس و همکاران (۲۰۲۳)
مقابله با حملات توزیع‌شده سایبری	بیگدلی و همکاران (۲۰۲۴)، موسوی و همکاران (۱۴۰۴)، عابدی (۱۳۹۶)، صفری (۱۴۰۳)
امنیت ویرایش محتوای سیاسی	حسنی (۱۴۰۴)، آفتابی و همکاران (۱۳۹۸)
انطباق پذیری با قوانین فضای مجازی	رضایی میرقائد و همکاران (۱۴۰۱)، بیگدلی و همکاران (۲۰۲۴)، موسوی و همکاران (۱۴۰۴)
خودکارسازی امنیت	حسین آبادی (۱۴۰۴)، عابدی (۱۳۹۶)، صفری (۱۴۰۳)
چارچوب اخلاقی سازمانی	بختیاری و لک (۱۳۹۷)، صابری و دیگران (۱۴۰۳)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
امنیت هویت کاربران	بایر و همکاران (۲۰۲۳)، بیگدلی و همکاران (۲۰۲۴)، موسوی و همکاران (۱۴۰۴)، شیردل و همکاران (۱۴۰۳)، دانش (۱۴۰۴)
کاهش تمرکز مدیریتی	رضایی میرقائد و همکاران (۱۴۰۱)، بیرامی و شفیعی (۱۴۰۴)، الهی و همکاران (۱۴۰۳)
مقابله با اخبار جعلی	نصیری و حسینی (۱۴۰۲)، بایر و همکاران (۲۰۲۳)، موسوی و همکاران (۱۴۰۴)
حکمرانی داده‌های سیاسی	رضایی میرقائد و همکاران (۱۴۰۱)، حسنی (۱۴۰۴)، آفتابی و همکاران (۱۳۹۸)
مالکیت شفاف داده‌های سیاسی	رضایی میرقائد و همکاران (۱۴۰۱)، صابری و دیگران (۱۴۰۳)،

جدول ۴. کدبندی مطالعات تحقیق

شاخص ها و مولفه ها (کدهای گزینشی)	منابع (مقالات)
	جوادیان (۱۴۰۳)
امنیت پلتفرم‌های سیاسی	قاسمی (۱۳۹۳)، یادگاری و همکاران (۱۳۹۶)، باقری کوشا و همکاران (۱۳۹۶)
توسعه تخصص‌های نیروی انسانی	بختیاری و لک (۱۳۹۷)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
حمایت مدیران از متخصصان فناوری	اسفندی ۱۴۰۰، غفاری و همکاران ۱۳۹۵، ساش و همکاران ۱۳۹۷، گوهیل ۱۳۹۲
جلوگیری از جعل	کریمی و همکاران (۱۳۹۳)، بیگدلی و همکاران (۲۰۲۴)، موسوی و همکاران (۱۴۰۴
ردیابی تغییرات محتوای سیاسی	رضایی میرقائد و همکاران (۱۴۰۱)، شیردل و همکاران (۱۴۰۳)
امنیت مشارکت‌های سیاسی	حسنی (۱۴۰۴)، آفتابی و همکاران (۱۳۹۸)
صحت و شفافیت داده‌ها	صابری و دیگران (۱۴۰۳)، جوادیان (۱۴۰۳)، لنگ و همکاران (۲۰۲۲)، شارما و جین (۱۳۹۲)
کنترل امنیت اطلاعات	تاکی (۱۳۹۲)، باقری و همکاران (۱۴۰۲)، حسین آبادی (۱۴۰۴)، عابدی (۱۳۹۶)، صفری (۱۴۰۳)
امنیت ارتباطات	احمدی و حبیب نژاد (۱۴۰۲)، یادگاری و همکاران (۱۳۹۶)، باقری کوشا و همکاران (۱۳۹۶)
یکپارچگی اطلاعات	صابری و دیگران (۱۴۰۳)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
مقاومت در برابر نفوذ هکرها	خسروی و منتظری (۱۴۰۴)، آل بویه و همکاران (۱۳۹۴)، رحیمی و همکاران (۱۴۰۴)، نصیرپور (۱۴۰۴)
داده‌های سیاسی کدگذاری شده	حسینی و همکاران (۱۴۰۰)، کورپاس و همکاران (۲۰۲۳)
عدم شفافیت هویتی	صابری و دیگران (۱۴۰۳)، جوادیان (۱۴۰۳)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
قراردادهای هوشمند امنیتی	سابقی (۱۴۰۴)، اخلاقی درزی و هاشمی (۱۴۰۴)
هوش مصنوعی	صابری و دیگران (۱۴۰۳)، جوادیان (۱۴۰۳)، عظیمی (۲۰۲۳)

جدول ۴. کدبندی مطالعات تحقیق

شاخص ها و مولفه ها (کدهای گزینشی)	منابع (مقالات)
تاب‌آوری و آسیب‌پذیری	ایوز و الخاطب (۲۰۲۳)، کیانیفر و همکاران (۲۰۲۴)
اعتمادسازی عمومی	جوادیان (۱۴۰۳)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
دستکاری ناپذیری اطلاعات محرمانه	بایر و همکاران (۲۰۲۳)، بیگدلی و همکاران (۲۰۲۴)، موسوی و همکاران (۱۴۰۴)، شیردل و همکاران (۱۴۰۳)، دانش (۱۴۰۴)
اعتمادپذیری سیستم	صابری و دیگران (۱۴۰۳)، عظیمی (۲۰۲۳)، لنگ و همکاران (۲۰۲۲)
رمزنگاری اطلاعات و اخبار محرمانه	نصیری و حسینی (۱۴۰۲)، بایر و همکاران (۲۰۲۳)، موسوی و همکاران (۱۴۰۴)
ساختار درختی	رضایی میرقائد و همکاران (۱۴۰۱)، لی (۲۰۱۹)، شیرز (۲۰۲۳)، کهرامان (۲۰۱۹)
توزیع داده های سیاسی غیرمتمرکز	رضایی میرقائد و همکاران (۱۴۰۱)، شیرز (۲۰۲۳)، شیردل و همکاران (۱۴۰۳)

در مرحله پنجم، از روش تحلیل‌زمینه جهت سازماندهی داده ها استفاده شد. فرآیند شش مرحله‌ای برون و کلارک[1] (۲۰۰۶) شامل آشنایی با داده‌ها؛ ایجاد کدهای مفهومی اولیه؛ جستجوی کدهای گزینشی (شاخص‌ها)؛ شکل‌گیری زمینه‌های فرعی (مولفه‌ها)؛ تعریف و نامگذاری زمینه‌های اصلی (بعدهای اصلی)؛ بازبینی نهایی و تهیه گزارش. ۵۵ کد مفهومی اولیه از ۵۴ مقاله فارسی و لاتین بررسی شد که در جدول ۳ ارائه شد. در مرحله جستجوی کدهای گزینشی، تحلیل کدها آغاز و کدهای ناقص یا نامرتبط و تکراری حذف شد که ۴۲ کد گزینشی به دست آمد. در مرحله شکل‌گیری زمینه‌های فرعی، دو مرحله بازبینی و شکل‌دهی به زمینه‌های فرعی انجام شد. در مرحله نام گذاری زمینه‌های اصلی مشخص می شود که هر زمینه اصلی کدام جنبه از داده‌ها را در خود دارد. در این مرحله، ۴ زمینه اصلی به دست آمد (جدول ۵). در مرحله بازبینی نهایی، که شامل بررسی، مقایسه و دریافت مشارکت خبرگان است گزارش نهایی ارائه می‌شود.

1 Braun, V., & Clarke, V

جدول ۵. ابعاد، مولفه‌ها و شاخص‌های نهایی

بعدهای اصلی (زمینه اصلی)	مولفه‌ها (زمینه فرعی)	شاخص (کد گزینشی)
حاکمیت داده‌های سیاسی در فضای دیجیتال	حفاظت از داده‌های سیاسی	محرمانگی اطلاعات سیاسی
		کنترل دسترسی محتوای محرمانه
		حفظ حریم خصوصی فعالان رسانه‌ای
		محافظت از اطلاعات محرمانه نظام
		امنیت هویت کاربران
		رمزنگاری اطلاعات و اخبار محرمانه
		دستکاری ناپذیری اطلاعات محرمانه
	تحلیل و بهینه سازی داده های سیاسی	صحت داده‌های رسانه‌ای
		تحلیل داده‌های بلاک‌چین
		اعتبار داده‌های سیاسی
		ردیابی منابع داده‌های سیاسی
		ردیابی تغییرات محتوای سیاسی
شفافیت و امنیت داده های سیاسی در زنجیره بلوکی	شفافیت داده های سیاسی در زنجیره بلوکی	مقابله با جعل هویت
		مقابله با اخبار جعلی
		شفافیت انتشار اخبار
		مالکیت شفاف داده‌های سیاسی
		صحت و شفافیت داده‌ها
	ساختار امن زنجیره بلوکی	**زیرساخت‌های فناورانه**
		قراردادهای هوشمند امنیتی
		مقاومت در برابر نفوذ هکرها
		ساختار درختی
		توزیع داده های سیاسی غیرمتمرکز
	امنیت شبکه و فناوری اطلاعات	امنیت داده‌های عمومی
		امنیت محتوای چندرسانه‌ای
		امنیت شبکه‌های اجتماعی سیاسی
		امنیت پلتفرم‌های سیاسی

جدول ۵. ابعاد، مولفه‌ها و شاخص‌های نهایی

بعدهای اصلی (زمینه اصلی)	مولفه‌ها (زمینه فرعی)	شاخص (کد گزینشی)
زیرساخت‌های فناورانه برای امنیت داده‌های سیاسی		امنیت مشارکت‌های سیاسی
		امنیت رای‌گیری الکترونیک
		مقابله با حملات توزیع‌شده سایبری
	مدیریت امنیت در داده‌های سیاسی	چارچوب اخلاقی سازمانی
		یکپارچگی اطلاعات
		خودکارسازی امنیت
		کاهش تمرکز مدیریتی
		حمایت مدیران از متخصصان فناوری
		توسعه تخصص‌های نیروی انسانی
تعاملات و ارتباطات سیاسی دیجیتال	مدیریت تعاملات دیجیتال	احراز هویت کاربران
		مدیریت تعاملات و تسهیل تعامل شفاف
		حمایت از آزادی بیان
	اعتمادسازی دیجیتال	الگوریتم روانشناختی
		تاب‌آوری و آسیب‌پذیری
		توسعه و افزایش اعتماد کاربران و مخاطبان
		اعتمادپذیری سیستم

در مرحله ششم، کنترل کیفیت با استفاده از نظرات چهار نفر از متخصصان رسانه و بلاک چین انجام شد، و ضمن انجام اصلاحات، مراحل انجام شده مورد تائید قرار گرفت. در مرحله هفتم نتیجه نهایی از انجام روش فراترکیب ارائه شد. بررسی کلیه متون و منابع ده سال اخیر (فارسی و لاتین) نشان داد که هنوز محققان نتوانسته‌اند به الگوی مناسب جهت استفاده از زنجیره بلوکی در عرصه امنیت اطلاعات به ویژه در رسانه های دیجیتالی که رویکرد سیاسی دارند دست پیدا کنند. لذا پژوهش حاضر توانسته به شناسایی ابعاد مختلف امنیت اطلاعات با استفاده از فناوری زنجیره

بلوکی کمک کند. همان‌گونه که در جدول ۳ ملاحظه می‌شود از ۴۲ شاخص شناسایی شده، ۱۲ شاخص در بعد "حاکمیت داده‌های سیاسی در فضای دیجیتال" ؛ ۱۰ شاخص در بعد "شفافیت و امنیت داده‌های سیاسی در زنجیره‌بلوکی" ؛ ۱۳ شاخص در بعد "زیرساخت‌های فناورانه برای امنیت داده‌های سیاسی" ؛ ۷ شاخص در بعد "تعاملات و ارتباطات سیاسی دیجیتال" قرار گرفتند. در این مرحله با استفاده از روش دلفی، پانل مورد نظر با ۱۵ مدیر رسانه های دیجیتال سیاسی و ۳۱ نفر متخصص در عرصه فناوری زنجیره بلوکی (در مجموع ۴۶ نفر) شکل گرفت. در این دو مرحله، ارزیابی شاخص های امنیت اطلاعات و زنجیره بلوکی از طریق طیف لیکرت و شامل گزینه‌های تاثیر بسیار زیاد:۵امتیاز/ تاثیر زیاد:۴امتیاز/ تاثیر متوسط: ۳امتیاز/ تاثیر کم:۲امتیاز/ تاثیر بسیار کم: ۱امتیاز انجام گرفت. جهت تعیین سطح اتفاق‌نظر، از ضریب هماهنگی کندال[1] استفاده شد که نشان می‌دهد افرادی که چند مقوله را بر اساس اهمیت مرتب کرده‌اند، معیارهای مشابهی را برای قضاوت درباره اهمیت مقوله‌ها به کار برده‌اند و از این لحاظ اتفاق نظر دارند. در جدول ذیل تفسیر مقادیر ضریب هماهنگی کندال ارائه شده است:

جدول۶. تفاسیر مقادیر ضریب کندال

مقدار ضریب کندال (w)	تفسیر	اطمینان نسبت به ترتیب عوامل
۰/۱	اتفاق نظر بسیار ضعیف	وجود ندارد
۰/۳	اتفاق نظر ضعیف	کم
۰/۵	اتفاق نظر متوسط	متوسط
۰/۷	اتفاق نظر قوی	زیاد
۰/۹	اتفاق نظر بسیار قوی	بسیار زیاد

با توجه به توضیحات جدول۶، ۷۰ درصد به عنوان سطح اتفاق نظر تعیین گردید. بر این اساس هر شاخص که ۷۰ درصد امتیازهای ممکن را کسب می‌نمود، سطح اتفاق نظر را به دست می‌آورد و از آنجایی که بر اساس امتیازدهی ناشی از طیف لیکرت هر شاخص حداکثر ۵ امتیاز می‌تواند به دست آورد، و تعداد مشارکت‌کنندگان نیز ۴۶ نفر بود بنابراین حداکثر امتیاز هر شاخص جهت نیل به امنیت اطلاعات بر اساس زنجیره بلوکی، ۲۳۰ امتیاز می‌توانست باشد و کسب ۷۰درصد از این امتیاز، یعنی دستیابی به ۱۶۱ امتیاز و بیشتر، به منزله کسب سطح اتفاق نظر تلقی می‌شد و

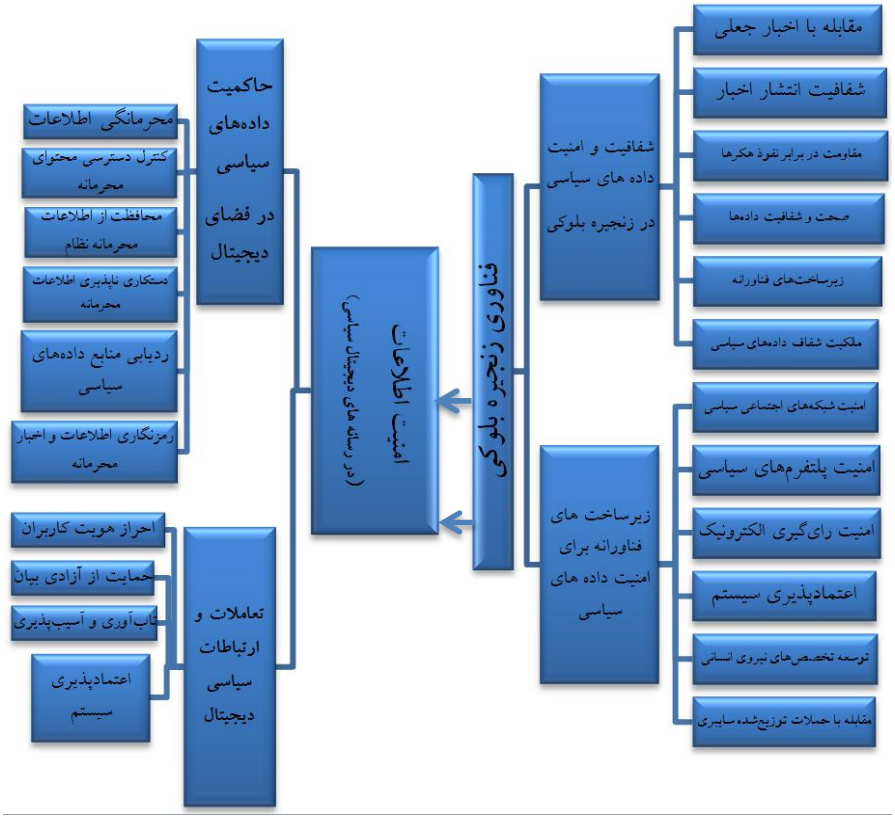
1 Kendall’s coefficient of concordance (w)

شاخص‌هایی که این امتیاز را کسب می‌کردند به عنوان شاخص امنیت اطلاعات در رسانه‌های دیجیتال با استفاده از زنجیره بلوکی که اعضای پانل درباره آن اتفاق نظر دارند در نظر گرفته شدند. نتایج حاصل از دو مرحله دلفی در جدول ذیل آمده است.

جدول ۷. شاخص های نهایی امنیت اطلاعات در رسانه های دیجیتال با استفاده از زنجیره بلوکی توسط اعضای پانل در مرحله دوم

ردیف	زمینه های اصلی	شاخص‌های نهایی **امنیت اطلاعات** با استفاده از زنجیره بلوکی
۱	حاکمیت داده‌های سیاسی در فضای دیجیتال	محرمانگی اطلاعات با امتیاز ۲۲۱ (۰,۹۶درصد امتیاز ممکن)
۲		کنترل دسترسی محتوای محرمانه با امتیاز ۲۱۰ (۹۱ درصد امتیاز ممکن)
۳		محافظت از اطلاعات محرمانه نظام با امتیاز ۱۹۵ (۰,۸۴ درصد امتیاز ممکن)
۴		دستکاری ناپذیری اطلاعات محرمانه با امتیاز ۱۹۱ (۰,۸۳درصد امتیاز ممکن)
۵		ردیابی منابع داده‌های سیاسی با امتیاز ۱۸۱ (۰,۷۸درصد امتیاز ممکن)
۶		رمزنگاری اطلاعات و اخبار محرمانه با امتیاز ۱۸۴ (۰,۸ درصد امتیاز ممکن)
۷	شفافیت و امنیت داده های سیاسی در زنجیره بلوکی	۲. مقابله با اخبار جعلی با امتیاز ۲۱۸ (۰,۹۴درصد امتیاز ممکن)
۸		۳. شفافیت انتشار اخبار با امتیاز ۲۱۱ (۰,۹۱درصد امتیاز ممکن)
۹		مقاومت در برابر نفوذ هکرها با امتیاز ۲۲۳ (۰,۹۶درصد امتیاز ممکن)
۱۰		۵. صحت و شفافیت داده‌ها با امتیاز ۱۹۱ (۰,۸۳ درصد امتیاز ممکن)
۱۱		زیرساخت‌های فناورانه با امتیاز ۱۸۰ (۰,۷۸ درصد امتیاز ممکن)
۱۲		۴. مالکیت شفاف داده‌های سیاسی با امتیاز ۲۰۹ (۰,۹درصد امتیاز ممکن)
۱۳	زیرساخت‌های فناورانه برای امنیت داده‌های سیاسی	امنیت شبکه‌های اجتماعی سیاسی با امتیاز ۲۲۵ (۰,۹۷درصد امتیاز ممکن)
۱۴		امنیت پلتفرم‌های سیاسی با امتیاز ۲۲۳ (۰,۹۶ درصد امتیاز ممکن)
۱۵		امنیت رای‌گیری الکترونیک با امتیاز ۲۲۰ (۰,۹۵ درصد امتیاز ممکن)
۱۶		اعتمادپذیری سیستم با امتیاز ۲۱۴(۰,۹۳ درصد امتیاز ممکن)
۱۷		توسعه تخصص‌های نیروی انسانی با امتیاز ۲۰۱ (۰,۸۷ درصد امتیاز ممکن)
۱۸		مقابله با حملات توزیع‌شده سایبری با امتیاز ۲۲۰ (۰,۹۵ درصد امتیاز ممکن)
۱۹	تعاملات و ارتباطات سیاسی دیجیتال	احراز هویت کاربران با امتیاز ۲۱۹ (۰,۹۵درصد امتیاز ممکن)
۲۰		حمایت از آزادی بیان با امتیاز۱۷۵ (۰,۷۶درصد امتیاز ممکن)
۲۱		تاب‌آوری و آسیب‌پذیری با امتیاز ۲۰۲ (۰,۸۷ درصد امتیاز ممکن)
۲۲		اعتمادپذیری سیستم با امتیاز ۱۸۳ (۰,۷۹ درصد امتیاز ممکن)

از میان مولفه‌های "زیرساخت‌های فناورانه برای امنیت داده‌های سیاسی"، ۶ شاخص حاصل گردید که با میانگین امتیاز ۲۱۷/۱۶ بیشترین امتیاز را داشت. "شفافیت و امنیت داده های سیاسی در زنجیره بلوکی" با۶ شاخص و میانگین امتیاز ۲۰۵/۳۳ در رتبه دوم، "حاکمیت داده‌های سیاسی در فضای دیجیتال" با ۶ شاخص و میانگین ۱۹۷ و "تعاملات و ارتباطات سیاسی دیجیتال" با ۴ شاخص و میانگین ۱۹۴/۷۵ در اولویت های سوم و چهارم قرار گرفتند که مدل حاصل در ذیل ارائه شده است.



شکل ۱. مدل امنیت اطلاعات در رسانه‌های دیجیتال سیاسی بر اساس بهره‌گیری از فناوری زنجیره بلوکی

جهت اعتبارسنجی مدل به دست آمده، این مدل در اختیار ۳۰ نفر از مدیران رسانه های دیجیتال سیاسی و متخصصان زنجیره بلوکی قرار گرفت که نظرات خود را درباره مولفه‌های موجود در این مدل بر اساس طیف لیکرت ارائه کردند (خیلی کم ۱؛ کم ۲؛ متوسط ۳؛ زیاد ۴؛

خیلی زیاد ۵). پاسخ‌های متخصصان عمدتا ۴و۵ بوده و به ندرت گزینه ۳ و متوسط را انتخاب کرده‌اند. برای مشخص کردن تفاوت نظر متخصصان در هر مولفه، از آزمون ناپارامتریک تک نمونه‌ای ویلکاکسون استفاده شد و مولفه‌هایی که از نظر متخصصان اهمیت بالایی داشت به دست آمد (جدول ۸). در نهایت مدل طراحی شده با عنوان مدل جامع امنیت اطلاعات در رسانه‌های دیجیتال سیاسی بر مبنای مولفه‌های زنجیره بلوکی، معتبر شناخته شد.

جدول ۸. نتایج آزمون تک نمونه‌ای ویلکاکسون برای مولفه‌ها

مولفه ها	ملاک	میانگین رتبه	z	P
محرمانگی اطلاعات	بزرگتر از ۳ کوچکتر از۳	۲/۵۰ ۰/۰۰	-۲/۰۰۰	۰/۰۳۶
کنترل دسترسی محتوای محرمانه	بزرگتر از ۳ کوچکتر از ۳	۲/۰۰ ۰/۰۰	-۱/۷۳۲	۰/۰۱۸
محافظت از اطلاعات محرمانه نظام	بزرگتر از ۳ کوچکتر از ۳	۳/۰۰ ۳/۰۰	-۱/۳۴۲	۰/۰۲۵
دستکاری ناپذیری اطلاعات محرمانه	بزرگتر از ۳ کوچکتر از ۳	۲/۵۰ ۰/۰۰	-۲/۰۰۰	۰/۰۴۶
ردیابی منابع داده های سیاسی	بزرگتر از ۳ کوچکتر از ۳	۳/۰۰ ۰/۰۰	-۲/۲۳۶	۰/۰۲۵
رمزنگاری اطلاعات و اخبار محرمانه	بزرگتر از ۳ کوچکتر از ۳	۲/۰۰ ۲/۰۰	-۰/۵۷۷	۰/۰۳۳
احراز هویت کاربران	بزرگتر از ۳ کوچکتر از ۳	۲/۵۰ ۰/۰۰	-۲/۰۰۰	۰/۰۴۶
حمایت از آزادی بیان	بزرگتر از ۳ کوچکتر از ۳	۴/۵۰ ۷/۸۳	-۰/۴۳۲	۰/۰۳۶
تاب آوری و آسیب پذیری	بزرگتر از ۳ کوچکتر از ۳	۲/۵۰ ۴/۶۰	-۱/۵۵۲	۰/۰۲۱
اعتمادپذیری سیستم	بزرگتر از ۳ کوچکتر از ۳	۳/۵۰ ۶/۱۷	-۰/۰۷۳	۰/۰۳۸
مقابله با اخبار جعلی	بزرگتر از ۳ کوچکتر از ۳	۴/۵۰ ۴/۵۰	-۲/۱۲۱	۰/۰۳۴
شفافیت انتشار اخبار	بزرگتر از ۳ کوچکتر از ۳	۴/۵۰ ۴/۵۰	-۱/۴۱۴	۰/۰۳۷
مقاومت در برابر نفوذ هکرها	بزرگتر از ۳ کوچکتر از ۳	۳/۵۰ ۰/۰۰	-۲/۴۴۹	۰/۰۱۴
صحت و شفافیت داده‌ها	بزرگتر از ۳ کوچکتر از ۳	۴/۰۰ ۴/۰۰	-۱/۱۳۴	۰/۰۴۵

جدول ۸. نتایج آزمون تک نمونه‌ای ویلکاکسون برای مولفه‌ها

مولفه ها	ملاک	میانگین رتبه	z	P
زیرساخت های فناورانه	بزرگتر از ۳ کوچکتر از ۳	۳/۵۰ ۰/۰۰	-۲/۴۴۹	۰/۰۱
مالکیت شفاف داده های سیاسی	بزرگتر از ۳ کوچکتر از ۳	۳/۰۰ ۰/۰۰	-۲/۲۳۶	۰/۰۱۵
امنیت شبکه های اجتماعی سیاسی	بزرگتر از ۳ کوچکتر از ۳	۲/۰۰ ۴/۵۰	-۰/۴۱۴	۰/۰۳۹
امنیت پلتفرم های سیاسی	بزرگتر از ۳ کوچکتر از ۳	۳/۰۰ ۰/۰۰	-۰/۴۴۷	۰/۰۲۷
امنیت رای گیری الکترونیک	بزرگتر از ۳ کوچکتر از ۳	۳/۰۰ ۵/۳۳	-۰/۳۵۱	۰/۰۴۹
اعتمادپذیری سیستم	بزرگتر از ۳ کوچکتر از ۳	۳/۵۰ ۶/۱۷	-۰/۰۷۳	۰/۰۳۲
توسعه تخصص های نیروی انسانی	بزرگتر از ۳ کوچکتر از ۳	۴/۰۰ ۴/۰۰	-۱/۱۳۴	۰/۰۳۸
مقابله با حملات توزیع شده سایبری	بزرگتر از ۳ کوچکتر از ۳	۳/۵۰ ۰/۰۰	-۲/۴۴۹	۰/۰۱۴

بر اساس جدول ۸، تمامی شاخص‌های امنیت اطلاعات و زنجیره بلوکی مورد تائید متخصصان بوده است ($p<0/05$). به عبارت دیگر میانگین اعتبار مولفه‌های مربوط به مدل جامع امنیت اطلاعات در رسانه های دیجیتال سیاسی بر مبنای فناوری زنجیره بلوکی بالاتر از ۳ است.

نتیجه‌گیری و پیشنهادها

پژوهش حاضر با هدف طراحی مدل جامع امنیت اطلاعات در رسانه‌های دیجیتال سیاسی مبتنی بر فناوری زنجیره بلوکی، توانست مولفه‌ها و شاخص‌های کلیدی این حوزه را شناسایی و احصا کند. این مدل، ابعاد و شاخص‌های کلیدی حوزه پژوهش حاضر را در چهار بعد اصلی شامل حاکمیت داده‌های سیاسی در فضای دیجیتال، شفافیت و امنیت داده‌های سیاسی در زنجیره بلوکی، زیرساخت‌های فناورانه برای امنیت داده های سیاسی و تعاملات و ارتباطات سیاسی دیجیتال، به خوبی نمایش می دهد. در بعد حاکمیت داده های سیاسی، شاخص "محرمانگی اطلاعات" بالاترین امتیاز را داشته و در بعد شفافیت و امنیت داده‌های سیاسی در زنجیره بلوکی، شاخص "مقاومت در برابر نفوذ هکرها" رتبه اول، و در بعد زیرساخت های فناورانه، شاخص "امنیت

شبکه های اجتماعی سیاسی" بالاترین امتیاز و در بعد تعاملات و ارتباطات سیاسی دیجیتال، شاخص "احراز هویت کاربران" بالاترین رتبه را کسب کرده است. مولایی و سخائی (۱۴۰۳) و نیز جوادیان (۱۴۰۳) بر پتانسیل بلاک‌چین در افزایش امنیت و غیرقابل دستکاری بودن داده‌ها تأکید کرده‌اند که در مدل ارائه شده در پژوهش حاضر نیز شاخص‌هایی چون «دستکاری ناپذیری اطلاعات محرمانه» و «مقاومت در برابر نفوذ هکرها» وجود دارد. پژوهش آفتابی (۱۳۹۷) اشاره شده که علاوه بر تهدیدات خارجی، تهدیدات داخلی سازمان‌ها نیز ممکن است در امنیت اطلاعات سازمان مشکلاتی را ایجاد کنند. همانطور که در پژوهش حاضر نیز به مولفه‌هایی مانند «تاب‌آوری و آسیب‌پذیری» و «اعتمادپذیری سیستم» تاکید شده است. در پژوهش حاضر به شاخص‌هایی چون «امنیت شبکه‌های اجتماعی سیاسی» و «اعتمادپذیری سیستم»اشاره شده و حاکی از آن است که زیرساخت‌های فناورانه و اعتمادپذیری سیستم از اهمیت بالایی برخوردارند. همان گونه که صابری، نظرنیا و خلیلی‌فر (۱۴۰۳) بر نقش بلاک‌چین در تدوین استراتژی‌های سازمانی امنیت محور تأکید کرده‌اند و اشاره دارند که بلاک‌چین با ایجاد سیستم شفاف و غیرمتمرکز، امنیت اطلاعات را افزایش می‌دهد. جعفرنژاد ثانی و همکاران (۱۴۰۲) نشان دادند که علی‌رغم فناوری‌های پیشرفته، مشکلات امنیتی همچنان وجود دارد و فرهنگ امنیت اطلاعات نیاز به توجه بیشتر دارد. این نکته در پژوهش حاضر با تاکید بر "توسعه تخصص‌های نیروی انسانی" و "تاب‌آوری سیستم" بازتاب یافته است که به اهمیت آموزش و فرهنگ امنیتی اشاره دارد. کوسبا و همکاران (۲۰۱۶) به نقش مهم و اثرگذار پیاده سازی بلاک چین در بهبود مشکلاتی مانند حریم خصوصی، شفافیت و امنیت داده ها اشاره کردند. همان گونه که در مدل ارائه شده در پژوهش حاضر نیز شاخص‌های مختلف مربوط به امنیت داده‌ها و شفافیت داده‌های سیاسی تحقق این یافته‌ها است. ونپوک و همکاران (۲۰۱۴) معتقدند که فناوری بلاک‌چین می‌تواند یکپارچگی تامین‌کنندگان و مشتریان را ارتقا دهد که در پژوهش حاضر نیز این موضوع در شاخص‌های مربوط به "اعتمادپذیری سیستم" و "تعاملات سیاسی دیجیتال" مورد تاکید بوده است.

پیشنهادات پژوهش

- تقویت زیرساخت‌های فناورانه به ویژه امنیت شبکه‌ها، پلتفرم‌ها و رای‌گیری الکترونیک جهت افزایش مقاومت در برابر حملات سایبری.
- ارتقای تخصص و آموزش نیروی انسانی (از طریق آموزش های ضمن خدمت) برای بهبود فرهنگ امنیت و افزایش تاب‌آوری سیستم‌ها.
- افزایش شفافیت و صحت انتشار اخبار با استفاده از مکانیزم‌های زنجیره بلوکی برای مقابله با اخبار جعلی و افزایش اعتماد مخاطبان و کاربران رسانه ها.
- بهبود تعاملات سازمانی با تمرکز بر احراز هویت کاربران، حمایت از آزادی بیان و تاب‌آوری در برابر آسیب‌های فضای مجازی.
- اعمال ارزیابی‌های دوره‌ای مدل امنیتی به منظور به‌روزرسانی و انطباق با تهدیدات نوین سایبری.
- تدوین خط مشی رسانه های دیجیتال سیاسی به نحوی که عمده فعالیت ها با بهره گیری از زنجیره بلوکی تبیین شده باشد
- تشکیل کمیته امنیت اطلاعات و فناوری‌های نوین و تعیین وظایف و اختیارات

محدودیت‌های پژوهش

از جمله محدودیت‌های پژوهش، دسترسی و تعامل با جامعه آماری پژوهش بود و محقق، جهت تشکیل پنل دلفی و هماهنگی با متخصصان، با محدودیت‌ها و موانعی مواجه بود. همچنین با توجه به جدیدبودن بحث بلاک‌چین در رسانه‌های دیجیتال به ویژه حساسیت خاص در مورد رسانه ها با محتوای سیاسی، متخصصین این حوزه اطلاعات گسترده‌ای در این زمینه ارائه نمی‌کردند.

فهرست منابع

Eftekhari, Asghar, (2016), National Security: Approaches and Strategies, Tehran: Strategic Studies Research Institute Publications.

Bozan, Bari, (2005), People, States and Fear: An Introduction to Contemporary Security Studies, Tehran: Strategic Studies Research Institute Publications.

Dehshiri, Mohammad Reza, Janparvar, Mohsen and Mohammadi, Hamzeh, (2019), Conceptual and Exemplary Analysis of New Threats to the National Security of the Islamic Republic of Iran, Strategic Studies Quarterly, Volume: 22, Issue 84, 7-34.

Dehghani Firouzabadi, Seyed Jalal, (2012), Principles and Foundations of International Relations of the Islamic Republic of Iran. In the collection of articles on the foreign policy of the Islamic Republic of Iran, Tehran: Samt Publications.

Rahimi, Hossein, (1999), The Role of Parties in Political Development and National Security, Strategic Studies Journal, No. 4.

Rafi, Hossein, (1991), Geopolitics and Security Challenges of Iran, Tehran: Ghomes Publications.

Samiei, Ahmad, (2010), Sociological study of the causes of the tendency towards terrorism in Iran, Iranian Journal of Sociological Studies, Volume: 2, Issue 3, 115-140

Ghanbari, Mohammad, (2019), The effective components of non-physical threats of terrorism on the sense of public security at the national level, Journal of Strategic Defense Studies, Volume: 17, Issue 77, 325-344.

Karimi Firouzjaei, Ali et al., (2018), Iran's legislative criminal policy towards terrorism in light of international documents, Political Studies Quarterly, Volume: 11, Issue 41, 195-234

Mandel, Robert, (2010), The changing face of national security, Tehran: Institute for Strategic Studies Publications.

Mottaqi, Ebrahim, Shafiee, Nozar and Karimi, Asghar, (2017), Analysis of the National Security Threats of the Islamic Republic of Iran in the Regional Environment of West Asia, Quarterly Journal of Strategic Policy Research, Volume: 6, Number 22, 139-166.

Adderley, Richard, & Musgrove, Peter, (2001), Data mining case study: Modeling the behavior of offenders who commit serious sexual assaults, Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining, 215-220.

Asal, Victor, LaFree, Gray, & Russell, Sarah, (2016), Empirically understanding the enemies list: A comparative analysis of designated foreign terrorist organizations, Behavioral Sciences of Terrorism and Political Aggression, Vol.8, No.2, 83-104.

Brayne, Sarah, (2017), Big data surveillance: The case of policing, American Sociological Review, Vol.82, No.5, 977-1008.

Buzan, Barry, Wæver, Ole, & de Wilde, Jaap, (1998), Security: A new framework for analysis,Colorado: Lynne Rienner Publishers.

Byman, Daniel, (2008), Iran, terrorism, and weapons of mass destruction, Studies in Conflict & Terrorism, Vol.31, No.3, 169-181.

Byman, Daniel, (2019), Road warriors: Foreign fighters in the armies of jihad, NewYork: Oxford University Press.

Clarke, Ronaldo, & Newman, Graeme, (2006),Outsmarting the terrorists, Westport: Praeger Publishers.

Cordesman, Anthony, (2016), Iran's evolving military forces, Washington D.C: Center for Strategic and International Studies (CSIS).

Crenshaw, Martha, (1981), The causes of terrorism. Comparative Politics, Vol.13,No.4, 379-399.
Dugan, Laura, LaFree, Gray, & Piquero, Alex, (2005), Testing a rational choice model of airline hijackings, Criminology, Vol.43, No.4, 1031-1065.
Ekblom, Paul, (2005), Designing out crime by understanding the mechanisms, Handbook of crime prevention and community safety, New York: Willan Publishing.
Enders, Walters, & Sandler, Todd,(2012), The political economy of terrorism, Cambridge: Cambridge University Press.
Eubank, William, & Weinberg, Leonard, (1994),Does democracy encourage terrorism?, Terrorism and Political Violence, Vol. 6, No.4, 417-435.
Gurr, Robert, (1970), Why men rebel, Princeton: Princeton University Press.
Hoffman, Bruce, (2017),Inside terrorism, New York: Columbia University Press.
Hoffman, Frank, (2009), Hybrid warfare and challenges. Joint Force Quarterly, No. 52, 34-39.
Horgan, John, et al, (2016). Putting terrorism in context: Lessons from the Global Terrorism Database, London: Routledge.
Kaplan, Stanely, & Garrick, John, (1981), On the quantitative definition of risk, Risk Analysis,Vol.1,No.1, 11-27.
Katzman, Kenneth, (2021), Iran: Politics, human rights, and U.S. policy, Congressional Research Service (CRS): Report RL32048
Keohane, Robert, & Nye, Joseph, (1971), Transnational Relations and World Politics,Cambridge: Harvard University Press.
LaFree, Gray, & Dugan, Laura, (2007), Introducing the Global Terrorism Database, Terrorism and Political Violence, Vol. 19, No. 2, 181-204.
LaFree, Gray, & Dugan, Laura, (2010), Research on Terrorism and Countering Terrorism, Oxford: Oxford University Press.
LaFree, Gray, Dugan, Laura, & Korte, Raven, (2010),The impact of British counterterrorist strategies on political violence in Northern Ireland, Criminology & Public Policy, Vol. 9, No.3, 501-530.
Martin, Gus, (2018), Understanding terrorism: Challenges, perspectives, and issues, New York : Sage publications.
McCormick, Gordon, (2003), Terrorist decision making, Annual Review of Political Science, Vol.6, No.1, 473-507.
Menkhaus, Ken, (2018), Elite bargains and political deals in fragile states, Washington D.C: United States Institute of Peace.
Morselli, Carlo, (2009), Inside criminal networks, Berlin: Springer Science & Business Media.
Mumford, Andrew, (2013), The strategy and practice of hybrid warfare, London: Routledge.
National Consortium for the Study of Terrorism and Responses to Terrorism (START), (2022), Global Terrorism Database (GTD) Dec 2022 release,College Park: University of Maryland.
Pape, Robert, (2005), Dying to win: The strategic logic of suicide terrorism, New York: Random House.
Perry, Walter, et al, (2013), Predictive policing: The role of crime forecasting, Santa Monica: Rand Corporation.
Provost, Foster, & Fawcett, Tom, (2013), Data science for business, Sebastopol: O'Reilly Media, Inc.
Saaty, Thomas, (1980), The Analytic Hierarchy Process, New York: McGraw-Hill.
Schmid, Alex, (2011), The Routledge handbook of terrorism research, London: Routledge.
Siegel, Eric, (2016), Predictive analytics, Hoboken: John Wiley & Sons.

Walt, Stephen, (1987), The Origins of Alliances, Ithaka: Cornell University Press.
Walt, Stephen, (1991), The renaissance of security studies. International Studies Quarterly, Vol.35, No.2, 211-239.
Waltz, Kenneth, (1979), Theory of International Politics, Boston: Addison-Wesley.
Wigan, Marcus, & Clarke, Roger, (2013), Big data's big unintended consequences, Computer, Vol. 46, No. 6, 46-53.
Zammit-Mangion, Andrew, et al, (2012), Point process modelling of improvised explosive device attacks in Iraq, Annals of Applied Statistics, Vol.6, No. 4, 1510-1531.
Zhao, Hui, et al, (2015), A machine learning-based approach for prediction of terrorism attacks, Security Informatics, Vol. 4, No.1, 1-11.