



University of
Sistan and Baluchestan

Public Management Researches

Print ISSN: 2538 - 3418 Online ISSN: 2676 - 7880



Iranian Academy of
Management Sciences

Identify Management Codes of Comprehensive Framework for Data Center Cybersecurity Based on the NIST Model with an Integrated and Intelligent Approach

Ahmad Kazemi¹, Ali Moeini*², Saeed Rouhani³,
Nour Mohammad Yaghoubi⁴, Hamid Reza Yazdani⁵

1. Instructor of Computer Science Department, Faculty of Mathematics, Statistics and Computer Science, University of Sistan and Baluchestan, Zahedan, Iran.
2. Professor of School of Engineering Science, College of Engineering, University of Tehran, Tehran, Iran. (Corresponding Author) Email: moeini@ut.ac.ir
3. Assistant Professor of Information Technology Management, Faculty of Management University of Tehran, Tehran, Iran.
4. Professor of School of Management Science, Faculty of Management, University of Sistan and Baluchestan, Zahedan Iran.
5. Assistant Professor of School of Management Science, Faculty of Management, College of Farabi, University of Tehran, Tehran, Iran.

Abstract

In order to facilitate processes and provide innovative services, Most of organizations pay special attention to using data center services to host new platforms, services and tools to manage and run their systems. In the field of data center cybersecurity, all aspects need to be considered to identify the causes and then solve the problems. Therefore, in this study, we seek to identify and provide management codes that consider all internal and external aspects of cyber security.

In this research, using NIST cybersecurity framework and existing localized framework for Identify management codes of Comprehensive framework for data center cybersecurity by systematic literature review (SLR), 1831 documents was extracted by searching the Science direct, Scopus and ISC articles. After necessary examinations, 63 of them were identified as related documents. They were analyzed and coded using the Meta- synthesis method. Finally, the extracted features were classified into 5 main category and 23 sub categories and 108 codes, which were related to data center cyber security, i.e. Identification, protection, detection, response and retrieval.

Introduction

In recent years, the volume of data has increased to such an extent that the 21st century is known as the data century (Calzada & Almirall, 2020). However, this

increase in the volume of data and the need to ensure the security of the production and maintenance center and data services have been raised as an emerging issue in the management of information systems. Utilization of the data center, which is considered as the most important vital infrastructure of the organization, and huge investment has been made and the existential importance of these centers in providing the information and services needed by the society, causes an increase in cyber threats against them and increases the motivation of the threat actors to endanger the security of these centers. (Kazemi et al., 2022). The researcher's main approach is to identify and present data center cyber security management codes with an integrated and intelligent approach.

Problem Statement

Identify management codes of Comprehensive framework for data center cybersecurity Based on the NIST model with an integrated and intelligent approach.

The review of internal research in the field of cyber security also shows that no research has been conducted that has examined the security of the organizational data center separately. Adopting this point of view, which includes all the dimensions and components, and the codes affecting the cyber security of the data center, can be a useful approach in this regard.

Materials and Methods

The current research method is qualitative and Meta- synthesis method. In this research, in order to review data center cyber security literature, Sandelowski and Barroso's seven-step model has been used (Sandelowski & Barroso, 2006).

Research Findings

By systematically reviewing data center cyber security literature and coding and analyzing them, the main categories and components of this framework were identified. In total, the results of coding the sources led to the identification of the components of the framework and its dimensions. Based on the investigations, a total of 108 management codes were classified in the form of 23 components and extracted as components of the intelligent and integrated cyber security framework of the data center, which were identified in the 5 main categories of identification, protection, discovery, response and recovery.

Conclusion

In this research, using NIST cybersecurity framework and existing localized framework for Identify management codes of Comprehensive framework for data center cybersecurity by systematic literature review (SLR), 1831 documents was extracted by searching the Science direct, Scopus and ISC articles. After necessary examinations, 63 of them were identified as related documents. They were analyzed and coded using the Meta- synthesis method.

Finally, the extracted features were classified into 5 main category and 23 sub categories and 108 codes, which were related to data center cyber security, i.e. Identification, protection, detection, response and retrieval.

The innovation of the current research is from the aspect of studying the framework of cyber security with the approach of integrated and intelligent management of data centers, and therefore the development of a framework that can help organizations in facing cyber threats of data centers active in information and communication infrastructures is one of the goals of this research.

Integrity and intelligence in paying attention to each of the components of the above dimensions, which are connected and integrated like the links of a chain, and the continuous and rotating monitoring of that is the necessary intelligence to learn from the previous actions of oneself and others and to prevent the repetition of threats to the cyber security of the organization's data centers.

Keywords: Cyber Security, Comprehensive Framework, Data Center, NIST Model, Integrated and Intelligent Approach.

Article Type: Research Article

Cite this article: Kazemi, A., Moeini, A., Rouhani, S., Yaghoubi, N.M., & Yazdani, H.R. (2022). Identify Management Codes of Comprehensive Framework for Data Center Cybersecurity Based on the NIST Model with an Integrated and Intelligent Approach. *Public Management Researches*, 15 (57), 113-142. (In Persian)

DOI:10.22111/JMR.2022.42211.5774

Received: 22 Apr. 2022

Revised: 29 May. 2022

Accepted: 25 Jun. 2022

© The Author(s).

Publisher: University of Sistan and Baluchestan



شناسایی کدهای مدیریتی چارچوب جامع امنیت سایبری مرکز داده بر اساس الگوی NIST با رویکرد یکپارچه و هوشمند

احمد کاظمی^۱ - علی معینی*^۲ - سعید روحانی^۳ - نور محمد یعقوبی^۴ - حمید رضایزدانی^۵

۱. دانشجوی دکتری مدیریت فناوری اطلاعات دانشگاه تهران، عضو هیات علمی دانشگاه سیستان و بلوچستان، زاهدان، ایران.

۲. نویسنده مسئول، استاد، عضو هیات علمی دانشکده علوم مهندسی، دانشکده فنی، دانشگاه تهران، تهران، ایران.
moeini@ut.ac.ir

۳. دانشیار، عضو هیات علمی دانشکده مدیریت دانشگاه تهران، تهران، ایران.

۴. استاد، عضو هیات علمی دانشکده اقتصاد، مدیریت و حسابداری دانشگاه سیستان و بلوچستان، زاهدان، ایران.

۵. استادیار، عضو هیات علمی دانشکده مدیریت و حسابداری دانشکده فنی دانشگاه تهران، تهران، ایران.

چکیده

بسیاری از سازمان‌ها به منظور تسهیل فرآیندها و ارائه خدمات نوآورانه، توجه ویژه‌ای به استفاده از خدمات مرکز داده جهت میزبانی از سکوها، خدمات و ابزارهای نوین برای مدیریت و راهبری سامانه‌های خود نشان می‌دهند. در حوزه امنیت سایبری مرکز داده، برای شناخت علل تهدیدات سایبری و سپس حل مسائل نیاز است، تمام جوانب در نظر گرفته شوند. بنابراین ما در این پژوهش دنبال شناسایی و ارائه کدهای مدیریتی هستیم که در آن تمامی جوانب درونی و بیرونی امنیت سایبری در نظر گرفته شود. در این پژوهش با الگوگیری از چارچوب کلی امنیت سایبری NIST و چارچوب بسط داده شده موجود، نسبت به شناسایی جامع کدهای تأمین امنیت و حفاظت از زیر ساخت اصلی مرکز داده، اقدام نمودیم تا ضمن اتخاذ راهبرد یکپارچه، هوشمندی لازم با اشتراک اطلاعات و یادگیری از حملات قبلی در سازمانها جهت بهبود فرایند پاسخ و بازیابی ایجاد گردد. در این پژوهش بمنظور شناسایی و ارائه کدهای مدیریتی چارچوب جامع امنیت سایبری مرکز داده با روش مرور نظام‌مند از طریق جستجو در پایگاه وب او ساینس و اسکوپس و مقالات داخلی تعداد ۱۸۳۱ سند استخراج شد که پس از بررسی‌های لازم ۶۳ مورد از آن‌ها به‌عنوان اسناد مرتبط شناسایی و با استفاده از روش فراترکیب، بررسی و کدگذاری شدند و کدهای استخراج شده در ذیل ۵ مقوله اصلی (برگرفته از الگوی NIST)، ۲۳ مولفه و ۱۰۸ کد مدیریتی قرار گرفتند که مربوط به امنیت سایبری مرکز داده یعنی شناسایی، محافظت، کشف، پاسخگویی و بازیابی بودند.

واژه‌های کلیدی: امنیت سایبری، چارچوب جامع، مرکز داده، الگوی NIST، رویکرد یکپارچه و هوشمند.

مقاله مستخرج از رساله دکتری آقای احمد کاظمی است.

استناد: کاظمی، احمد؛ معینی، علی؛ روحانی، سعید؛ یعقوبی، نورمحمد؛ یزدانی، حمیدرضا. (۱۴۰۱). شناسایی کدهای مدیریتی چارچوب جامع امنیت سایبری مرکز داده بر اساس الگوی NIST با رویکرد یکپارچه و هوشمند، پژوهش‌های مدیریت عمومی، ۱۵(۵۷)، ۱۱۳-۱۴۲.

تاریخ دریافت: ۱۴۰۱/۰۲/۰۴ تاریخ ویرایش: ۱۴۰۱/۰۳/۰۸ تاریخ پذیرش: ۱۴۰۱/۰۴/۰۴

DOI:10.22111/JMR.2022.42211.5774

نوع مقاله: علمی پژوهشی

حق مؤلف © نویسندهگان

ناشر: دانشگاه سیستان و بلوچستان



مقدمه

در طی سال‌های اخیر افزایش حجم داده‌ها در حدی است که قرن ۲۱ به عنوان قرن داده شناخته شده است (Calzada & Almirall, 2020). با این حال این افزایش حجم داده‌ها و لزوم تامین امنیت مرکز تولید و نگهداری و خدمات داده به عنوان یک موضوع نوظهور در مدیریت سامانه‌های اطلاعاتی مطرح گردیده است.

بهره‌گیری از مرکز داده که به عنوان مهمترین زیرساخت حیاتی سازمان محسوب می‌شوند و سرمایه‌گذاری هنگفت انجام شده و اهمیت وجودی این مراکز در ارائه اطلاعات و خدمات مورد نیاز جامعه، باعث افزایش تهدیدات سایبری بر علیه آنها و فزونی انگیزه تهدیدکنندگان جهت به خطر انداختن امنیت این مراکز شده است (Kazemi et al., 2022).

در این پژوهش، تمرکز بر نقاط با حساسیت بسیار زیاد و مورد توجه تهدیدکنندگان و مهمترین بخش اطلاعاتی و ارتباطی یک سازمان یعنی مرکز داده آن می‌باشد. این تحلیل بمنظور پایش هوشمند (قبل از وقوع تهدید)، مدیریت یکپارچه (در زمان وقوع تهدید) و مقابله با آثار تهدیدهای امنیتی سایبری (پس از وقوع تهدید) ارائه می‌شود تا در مواجهه با تهدیدها، کاهش آثار بروز و ارتقاء قدرت تصمیم‌گیری در برخورد با آنها و در نتیجه ایجاد و استمرار امنیت، مراکز داده سازمانها موثر بوده و در نهایت موجب ارتقاء سطح امنیت سایبری در کشور گردد (Kazemi et al., 2022).

نقطه قوت این پژوهش، تمرکز بر مرکز داده‌های سازمان است که تهدیدات سایبری، سرمایه‌های اطلاعاتی آنها را خدشه دار می‌کنند و به عنوان تهدیدی جدی جهت تداوم کسب و کار سازمان شناخته می‌شوند. پژوهش حاضر با توجه به کمبود موجود در ادبیات، به دنبال شناسایی و ارائه کدهای مدیریتی با رویکرد یکپارچه و هوشمند برای امنیت سایبری مرکز داده است.

اهمیت اجرای این تحقیق و ارائه کدهای فوق با نگاهی ایجابی و با در نظر داشتن فواید و آثار ناشی از انجام آن بر اساس بررسی و پیش‌بینی محقق نشان‌دهنده موارد ذیل می‌باشد:

- نقص پژوهش در حوزه امنیت سایبری مرکز داده سازمان بصورت جزء نگرانه و لزوم شناخت و توسعه دانش و ادبیات این حوزه به منظور ارتقاء امنیت سایبری مرکز داده

- شناخت مفاهیم و کدهای موجود در چارچوب الگوی هوشمند و یکپارچه امنیت‌سایبری مرکز داده به منظور مواجهه فعال با آنها
- همچنین با در نظر داشتن آثار ناشی از عدم انجام تحقیق و با رویکرد سلبی ضرورت اجرای این تحقیق به شرح ذیل می‌باشد:
- ضعف در شناسایی مفاهیم و کدهای چارچوب امنیت‌سایبری مرکز داده و کاهش قدرت تصمیم‌گیری و افزایش خسارات در این حوزه
- ضعف در اتخاذ دیدگاه جزء نگرانه و شناسایی کلیه کدهای تأثیر گذار در امنیت‌سایبری مرکز داده

- ضعف در ارائه دستورالعمل لازم جهت تامین امنیت مرکز داده در حوزه های مرتبط
- رویکرد اصلی محقق، شناسایی و ارائه کدهای مدیریتی امنیت‌سایبری مرکز داده با رویکرد یکپارچه و هوشمند به شکلی است که با پیروی از روندی علمی در انجام تحقیق، مولفه‌های و کدهای ابعاد امنیت‌سایبری مرکز داده را بر اساس یافته‌های علمی ارائه نماید. بنابراین هدف اصلی و اهداف فرعی در این تحقیق عبارتند از:

هدف اصلی

- " شناسایی و ارائه کدهای مدیریتی چارچوب جامع امنیت‌سایبری مرکز داده بر اساس الگوی^۱ NIST با رویکرد یکپارچه و هوشمند "

اهداف فرعی

- شناسایی و ارائه کدهای مدیریت امنیت سایبری مرکز داده
 - توجه به رویکرد هوشمند و یکپارچه در امنیت‌سایبری مرکز داده
 - و محقق سعی می‌کند با انجام تحقیق به سوالات ذیل پاسخ دهد:
 - " کدهای چارچوب جامع امنیت‌سایبری بسط داده شده مرکز داده کدامند؟ "
 - ساختار، ابعاد و مولفه‌های امنیت‌سایبری مرکز داده چیست؟
 - دسته‌بندی کدهای امنیت‌سایبری مرکز داده کدام است؟
- بررسی پژوهش‌های داخلی در حوزه امنیت‌سایبری نیز نشان می‌دهد تا کنون پژوهشی که امنیت مرکز داده سازمانی را جزء نگرانه مورد بررسی قرار داده باشد، انجام نشده است. این

¹. National Institute of Standards and Technology

در حالی است که ویژگی‌های حوزه امنیت سایبری و وجود روابط تنگاتنگ میان سازمان‌های فعال در این صنعت، ایجاب می‌کند این صنعت مورد بررسی و تجزیه و تحلیل دقیق قرار گیرد؛ اتخاذ دیدگاه جزء نگرانه که دربرگیرنده کلیه ابعاد و مولفه‌ها، و کدهای تأثیر گذار در امنیت سایبری مرکز داده باشد، می‌تواند رویکردی سودمند در این خصوص باشد. در ادامه، بخش اول به بررسی مبانی نظری اختصاص یافته است، بخش بعدی به روش‌شناسی و در نهایت تجزیه و تحلیل یافته‌ها و جمع‌بندی ارائه شده‌اند.

چارچوب نظری و پیشینه پژوهش

امروزه بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشورها، در کلیه سطوح، با تبادلات داده در فضای سایبر انجام می‌شود. مرکز داده، بستری بوجود آورده است تا سازمان‌هایی ناهمگون با سرویس‌ها و خدمات متنوع به یکدیگر متصل شوند. رشد سریع و در عین حال نامتوازن خدمات برخط در فضای سایبر، این زیر ساخت را به یکی از عوامل کارا و در عین حال بالقوه آسیب‌پذیر، تهدیدشونده و دارای اهمیت تبدیل نموده است.

چارچوب جامع امنیت سایبری: در این تحقیق منظور از چارچوب، قالبی است که با ارائه آن زبان مشترک و توانمندی برای درک، مدیریت یکپارچه و هوشمند در پیش‌بینی و پیشگیری، محافظت، مقابله و مدیریت آثار تهدیدهای امنیتی سایبری مرکز داده با ارائه کدهای مدیریتی بر اساس فرهنگ امنیتی، فرایند عملیاتی، فناوری و محیط ایجاد شود.

رویکرد یکپارچه و هوشمند: کاهش مخاطرات ناشی از حملات امنیتی سایبری به مرکز داده به صورت نظام‌مند با فرایندسازی هوشمند و واکنش سریع و مناسب به حملات سایبری در قالب یک ساختار متمرکز و یکپارچه مانند حلقه‌های یک زنجیر بهم پیوسته با کارایی لازم امکان‌پذیر است. هوشمندی با خصوصیتی نظیر یادگیری، تشخیص الگو، پیش‌بینی، آگاهی بخشی و پایگاه دانش در نظر گرفته می‌شود چشم انداز این یکپارچه‌سازی و هوشمندسازی ایجاد ساختار امن و قوی جهت مقابله با حملات و اختلال در حوزه سایبری مرکز داده خواهد بود.

امنیت سایبری: امنیت سایبری در سطوح یا برای موجودیت‌هایی از قبیل اطلاعات، سامانه‌های اطلاعاتی، شبکه‌های ارتباطی، مراکز داده، سازمان‌های اطلاعات‌محور و ملی مطرح می‌باشد.

مرکز داده: در پروژه تحقیقاتی انجام شده در پژوهشکده امنیت پژوهشگاه فناوری اطلاعات و ارتباطات (۱۳۹۴) مرکز داده معرف مکانی با تجهیزات رایانه‌ای و جانبی مربوطه مانند تجهیزات ذخیره‌سازی و ارتباطی تعریف شده‌است. شرکت سرورایران^۱، مرکز داده را مجموعه خدمت‌دهنده‌ها، زیرساخت‌های ارتباطی/ امنیتی و تجهیزات الکترونیکی برای ارائه، نگهداری و پشتیبانی از خدمات تحت شبکه (اینترنت/ اینترانت/ اکسترانت) معرفی کرده‌است. این مراکز به انواع سازمانی، تجاری و دانشگاهی، خصوصی، فراهم‌کننده‌های خدمت، مراکز داده اینترنتی و فراسازمانی و محلی تقسیم می‌شوند.

بنابراین، پژوهش شناسایی و ارائه کدهای مدیریتی امنیت سایبری مرکز داده با رویکرد یکپارچه و هوشمند بدنبال ارائه کدهای امنیتی لازم در مؤلفه‌های نرم‌افزاری و سخت-افزاری، مأموریت‌ها، وظایف و اعتبار مرکز داده با بکارگیری فرایند تامین امنیت سایبری و ارائه و تداوم خدمات آنها است.

۱. معرفی چارچوب‌های امنیت سایبری اخیر

در دهه های اخیر چارچوب‌ها و معماری های امنیت سایبری مختلفی معرفی گردیده است که ضمن معرفی آنها در جدول (۱)، ویژگیهای آنها به لحاظ سال انتشار و جامعیت مقایسه گردیده است لذا با توجه به قدیمی بودن بعضی‌ها و همپوشانی آنها توسط موارد مطرح شده در چارچوب‌های جدید، ضمن معرفی معماری‌های آنها به چارچوب NIST پرداخته شده است.

^۱ www.serveriran.net

جدول شماره ۱: معرفی چارچوب ها و معماری های امنیت سایبری

معرفی	سال انتشار	امنیت	توضیحات
SABSA	۱۹۹۵	پایه	یک مدل ۶ لایه شامل معماری امنیتی زمینه ای، معماری امنیتی مفهومی، معماری امنیتی منطقی، معماری امنیتی فیزیکی، معماری امنیتی مؤلفه ای و معماری امنیتی عملیاتی.
O-ESA	۲۰۰۴	متوسط	تشریح چند حوزه از معماری امنیت شامل محرکهای کسب و کار مدیریت برنامه امنیت، کنترل‌های امنیتی، معماری تکنولوژی امنیت و عملیات امنیتی.
OSA	۱۹۹۳	متوسط	مجموعه‌ای از الگوها و کنترل های امنیتی را به منظور کاهش تهدیدات سایبری ارائه می‌دهد.
FEAF	۱۹۹۹	پایه	این معماری دارای مدل‌های معماری مرجع عملگرده، کسب و کار، داده، برنامه کاربردی، زیرساخت و امنیت است.
TOGAF	۲۰۰۶	پایه	این چارچوب توسعه چهار حوزه معماری کسب و کار، داده، برنامه کاربردی و فناوری را ارائه میدهد.
Zachman	۱۹۹۹	متوسط	این چارچوب از دو بعد اصلی و پایه تشکیل شده است. بعد اول (ستونها) بیانگر جنبه ها (چه چیز؟ چگونه؟ کجا؟ چه کسی؟ چه وقت و چرا؟) است، و بعد دوم (سطرها) مبین دیدگاه ذینفعان (برنامه ریز، مالک یا دارنده، طراح، سازنده، پیمانکار و کاربر) در سازمان است. به عبارتی دیگر، این چارچوب یک ماتریس دو بعدی را ارائه میدهد.
Clark	۲۰۱۰	متوسط	مدل چهارلایه‌ای فضای سایبر شامل لایه‌های انسانی، اطلاعاتی، منطقی و فیزیکی است در این مدل ضمن تفهیم نقاط کنترل فضای سایبر و اینترنت بر موضوع امنیت فضای سایبر تأکید شده است.
مدل مرکز ملی فضای سجازی	۲۰۱۷	پایه	در این مدل ضمن ترسیم لایه‌های مهم فضای سایبر و اینترنت شامل زیرساخت، خدمات، محتوی، کاربر و حکمرانی، بر بعد امنیت فضای سایبر به عنوان لایه‌ای بسیار مهم تمرکز شده که کلیه لایه‌های دیگر را در بر گرفته است.
Gartner	۲۰۱۴	پایه	چارچوب مشخصی را برای امنیت سایبری معرفی کرد که شامل چهار بخش پیش‌بینی، پیشگیری، کشف و پاسخ در یک فرایند مستمر پایش.
NIST	۲۰۱۸	عالی	چارچوبی توسعه یافته برای شناسایی، کشف و پاسخگویی به حملات سایبری و دنبال رفع کمبود استانداردها در حوزه تأمین امنیت است.

چارچوب امنیت سایبری NIST

یک چارچوب امنیت سایبری که با الهام از الگوی گارنتر و با توسعه آن در سال ۲۰۱۸ در شکل (۱) ارائه شده است.



شکل شماره ۱: چارچوب امنیت سایبری NIST

مجموعه‌ای کلی از دستورالعمل‌ها برای شرکت‌های بخش خصوصی است که توسط مؤسسه ملی استاندارد و فناوری (NIST) ایالات متحده تهیه شده است، تا در شناسایی، کشف و پاسخگویی به حملات سایبری آمادگی بیشتری داشته باشند. چارچوب امنیت سایبری NIST به دنبال رفع کمبود استانداردها در حوزه تأمین امنیت است. در حال حاضر سازمان‌ها شیوه‌های مختلفی از فناوری و قوانین را برای مبارزه با هکرها، سارقان داده و باج افزارها بکار می‌گیرند. حملات سایبری گسترده‌تر و پیچیده‌تر شده و مبارزه با این حملات نیز بسیار سخت‌تر شده است. این مسئله با فقدان یک راهبرد یکپارچه در بین سازمان‌ها همراه است و مجموعه‌های مختلف از سیاست‌ها، دستورالعمل‌ها، شیوه‌ها و فناوری‌های مورد استفاده در امنیت سایبری مشکل دیگری را ایجاد می‌کند و آن اینکه سازمان‌ها قادر به اشتراک‌گذاری اطلاعات در مورد حملات نیستند.

چارچوب هوشمند و یکپارچه امنیت سایبری مرکز داده سازمان

با استناد به چارچوب امنیت سایبری NIST و براساس نتایج بررسی‌های انجام شده در اسناد، مقوله‌های چارچوب هوشمند و یکپارچه امنیت سایبری مرکز داده بسط داده شده که یک چارچوب با پایش و نظارت مستمر می‌باشد بشکل زیر شناسایی شدند (شکل ۲).

پژوهش‌های اخیر در حوزه امنیت مراکز داده منجر به ارائه چارچوب بسط داده شده یکپارچه و هوشمند امنیت‌سایبری مرکز داده گردیده که با در نظر گرفتن مرکز داده سازمان به عنوان حیاتی‌ترین زیرساخت سازمان و پس از بررسی در قالب ۲۳ مولفه و ۵ بعد شناسایی^۱، محافظت، کشف، پاسخگویی و بازیابی ارائه گردیده‌اند (Kazemi et al., 2022). همچنین گروهی از محققان به ساختار تهدیدات سایبری مرکز داده پرداخته و با معرفی انواع مرکز داده سازمانی و پس از بررسی، نسبت به ارائه ساختار تهدیدات سایبری مرکز داده در قالب ۹ بعد فناوری، منشاء، ماهیت، انگیزه، دامنه بروز، آثار و پیامدها، دامنه اثرگذاری، شیوه تحقق و آسیب‌پذیری و ۳۶ مولفه اقدام نموده‌اند (Aghaee et al., 2018). محققان داخلی در تحقیق خود به اصول طراحی یک الگوی امنیتی برای مرکز داده پرداخته و یک الگوی امنیتی برای مرکز داده در سه سطح امنیت فیزیکی، امنیت ارتباطات و امنیت خدمات معرفی و راهکارهایی جهت بهبود امنیت در سطوح مختلف ارائه نموده‌اند (Hossien Zadeh et al., 2016). موسسه انیسا در گزارش سالیانه خود در ژانویه ۲۰۱۹ نسبت به گزارش ۱۵ تهدید پرتکرار در فضای سایبری پرداخته است. شناسایی تهدیدات پرتکرار در حوزه مراکز داده و اندیشیدن تمهیداتی در چارچوب مورد نظر جهت مقابله به یکپارچه و هوشمند می‌تواند موجب تامین امنیت این مراکز گردد (ENISA, 2019). محققان مؤسسه ان‌ای‌اس‌تی^۲ با تالیف مقاله‌ای در سال ۲۰۱۶ نسبت به بررسی شبیه‌سازی تهدیدات برای زیرساخت‌های مرکز داده ابری با محوریت سطح حمله، درخت حمله و نمودار حمله اقدام نموده است (Al Habashi et al., 2016). گزارش سال ۲۰۱۵ مؤسسه سانز بیانگر موارد خاص تهدیدات امنیتی در سطح مراکز داده و ساختارهای ابری است. ۵۰ درصد تهدیدات فوق مربوط به نرم‌افزارهای مخرب و نقص برنامه‌های کاربردی است (Sanz, 2015). براساس گزارش سال ۲۰۱۹ این مؤسسه، تهدیدات فیزیکی نیز از تهدیدات مهم مراکز داده می‌باشد (همان، ۲۰۱۹).

1. Identify, Protect, Detect, Respond, Recovery

2. NIST, National Institute of Standards and technology

روش شناسی پژوهش

روش پژوهش حاضر کیفی و نوعی از فراترکیب است. در فراترکیب اطلاعات و یافته‌های استخراج شده از مطالعات گذشته با موضوع مرتبط و مشابه بررسی می‌شوند (شکل ۳).



شکل شماره ۳: روند انجام روش فراترکیب

در پژوهش حاضر به منظور بررسی ادبیات امنیت سایبری مرکز داده از الگوی هفت مرحله‌ای ساندلوسکی^۱ و باروسو^۲ استفاده شده است (Sandelowski & Barroso, 2006).

۱. گام اول: تنظیم سوال‌های پژوهش

در روش فراترکیب از آنجا که رویکرد محقق اکتشافی است بنابراین به دنبال سوال‌های از جنس چه چیزی است. در پژوهش حاضر سوال پژوهش عبارت است از: «ابعاد، مؤلفه‌ها و کدهای تامین امنیت و حفاظت از زیر ساخت اصلی مرکز داده، چیست؟».

۲. گام دوم: مرور نظام‌مند مبانی نظری

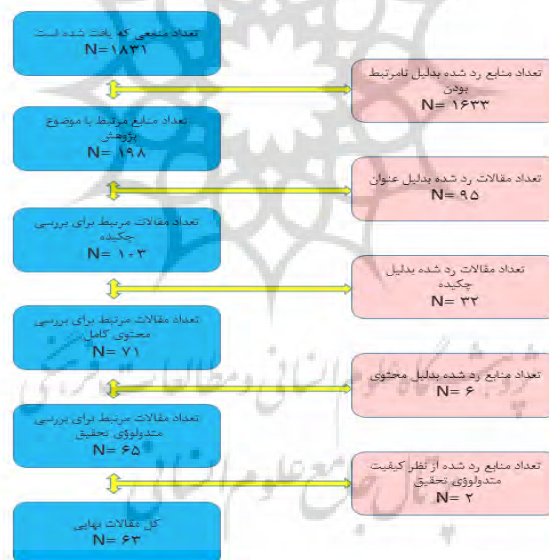
در گام دوم، با استفاده از روش مرور نظام‌مند ادبیات^۳، اسناد معتبر و مرتبط به موضوع پژوهش شناسایی شدند. در پژوهش حاضر جستجو در پایگاه‌های وب او ساینس و اسکپوس و مقالات داخلی انجام شد. با استفاده از کلیدواژه‌های منتخب (Cyber Security Data framework, Integrated and Intelligent Management, Cyber Security, Center, Threats Classification و امنیت سایبری مرکز داده) که در بررسی اولیه مقالات مرتبط با موضوع شناسایی شده بودند، جستجو برای استخراج اسناد معتبر و مرتبط در طی

1. Sandelowski
2. Barroso
3. Systematic Literature Review

بازه زمانی ۲۰۲۱-۲۰۱۰ در پایگاه‌های مذکور انجام شد. در ادامه یک جستجو رو به عقب (بررسی منابع مقالات شناسایی شده) و رو به جلو (بررسی مقالاتی که به منابع شناسایی شده ارجاع دادند) در مورد مقالات نهایی مرحله قبل انجام شد (Abraham et al., 2019). این اقدام به نوعی باعث گردید که مقالات معتبری که در مرحله اول شناسایی نشده بودند (۷ مورد)، به فهرست منابع مورد بررسی اضافه شوند.

۳. گام سوم: جستجو و بررسی مقالات مرتبط

در این گام به منظور بررسی و غربال اسناد حاصل از جستجو مقالات و منابع مرتبط، ابتدا به بررسی تناسب مقالات دریافتی با سؤال پژوهش و بازبینی مجموعه مطالعات منتخب در چندین مرحله و براساس ارتباط با موضوع تحقیق و موارد دیگر اقدام و سپس برخی منابع و مقالات از فرآیند بررسی و تحلیل فراترکیب جدا شدند. این روند در شکل (۴) ارائه شده است.



شکل شماره ۴: روند استخراج منابع معتبر

به منظور غربال اسناد حاصل از جستجو، ابتدا عنوان و کلیدواژه‌های اسناد، منبع انتشار و همچنین ساختار آن بررسی و در نهایت اسناد غیر معتبر و غیر مرتبط با هدف پژوهش از ادامه بررسی‌ها حذف شدند.

در مرحله دوم برای ارزیابی دقیق تر اسناد، با مطالعه چکیده و سپس اصل مقالات باقیمانده، به صورت دقیق تر میزان مطابقت آن‌ها با اهداف و سوال‌های پژوهش بررسی شدند و موارد غیر مرتبط حذف شدند. در نهایت ۶۳ سند به عنوان اسناد معتبر و منتخب برای تحلیل‌های بیشتر باقی ماندند که همه آن‌ها معتبر و مرتبط با موضوع پژوهش بودند. برای استخراج مفاهیم و کدهای مرتبط با موضوع پژوهش، در تمامی مراحل فراترکیب، به‌طور پیوسته مقالات منتخب جهت دستیابی به یافته‌های درون محتوایی مجزا شامل مطالعه‌های اولیه و اصلی چندین بار مرور شدند. در این فرایند محتوای منابع بررسی، کدهای مرتبط انتخاب و مفاهیم و مقوله‌ها شکل گرفتند.

۴. گام چهارم: استخراج اطلاعات مقالات

پس از شناسایی اسناد مورد نظر در این گام اسناد منتخب بررسی شدند و با استفاده از روش کدگذاری سه مرحله‌ای در راستای هدف پژوهش و پاسخگویی به سوال پژوهش، کدهای مربوطه از متن اسناد استخراج گردیدند. در ادامه نیز کدها استخراج شده با توجه به تشابه ماهیت آن‌ها برای استخراج مفاهیم مرتبط، با هم ترکیب و دسته‌بندی شدند و نتایج در قالب مقوله‌ها دسته‌بندی گردیده است.

۵. گام پنجم: تجزیه و تحلیل و ترکیب یافته‌های کیفی

در این مرحله با توجه به هدف پژوهش در طی بررسی اسناد منتخب، کدهای مرتبط شناسایی و استخراج گردیدند. سپس کدهای دارای ماهیت مشابه در ذیل یک دسته قرار گرفته و مفاهیم را تشکیل دادند و در ادامه نیز مفاهیم مشابه در ذیل یک مقوله قرار گرفتند.

۶. گام ششم: کنترل کیفیت

نظر به اینکه روند جمع‌آوری داده‌ها به شکلی نظام‌مند انجام شده است و دقت در این فرایند بر میزان اعتبار اجزاء بدست آمده در چارچوب کمک می‌کند ضرورت ایجاد می‌نماید که ترکیب اجزاء در قالب چارچوب نیز اعتبارسنجی شود. براین اساس جهت حفظ کیفیت مطالعه، از شاخص کاپا استفاده شده است. در پژوهش حاضر اسناد منتخب در اختیار یک متخصص قرار داده شد و از وی درخواست شد که با توجه به هدف پژوهش و بدون اطلاع از نحوه ادغام کدها و مفاهیم توسط پژوهشگر، کدگذاری کند. در ادامه برای مقایسه کدهای

احصا شده توسط محقق و یک نفر متخصص با استفاده از نرم‌افزار SPSS ضریب کاپا محاسبه گردید. نتایج حاصل از محاسبه آزمون کاپا، ضریب کاپا را برابر ۰,۷۳ مشخص که بیانگر توافق نسبتاً مناسبی است (Landis & Koch, 1977) و علاوه بر این سطح معناداری کمتر از ۰,۰۵ نیز بیانگر ارتباط بین کدگذاری‌های صورت گرفته بر روی سند منتخب است.

جدول شماره ۲: پایایی روش فراترکیب

نظر محقق		نظر محقق	
مجموع	بله	خیر	
۳	A=۳	B=۰	نظر بله
۲	C=۱	D=۱	خبره خیر
N=۵	۴	۱	دیگر مجموع

$$= [(A+D)/N = ۰/۸] \text{ توافقات مشاهده شده}$$

جدول شماره ۳: وضعیت شاخص کاپا (جنسن و آلن، ۱۹۹۶)

مقدار عددی شاخص	مقدار عددی شاخص	وضعیت توافق	وضعیت توافق
۰-۰/۲۰	کمتر از ۰	بی اهمیت	ضعیف
۰/۰-۴۱/۶۰	۰/۰-۲۱/۴۰	مناسب	متوسط
۰/۱-۸۱	۰/۰-۶۱/۸۰	عالی	معتبر

$$= [(A+B)/N] * [(A+C)/N] * [(C+D)/N] * [(B+D)/N] = ۰/۰۳۸۴ \text{ توافقات شانسی}$$

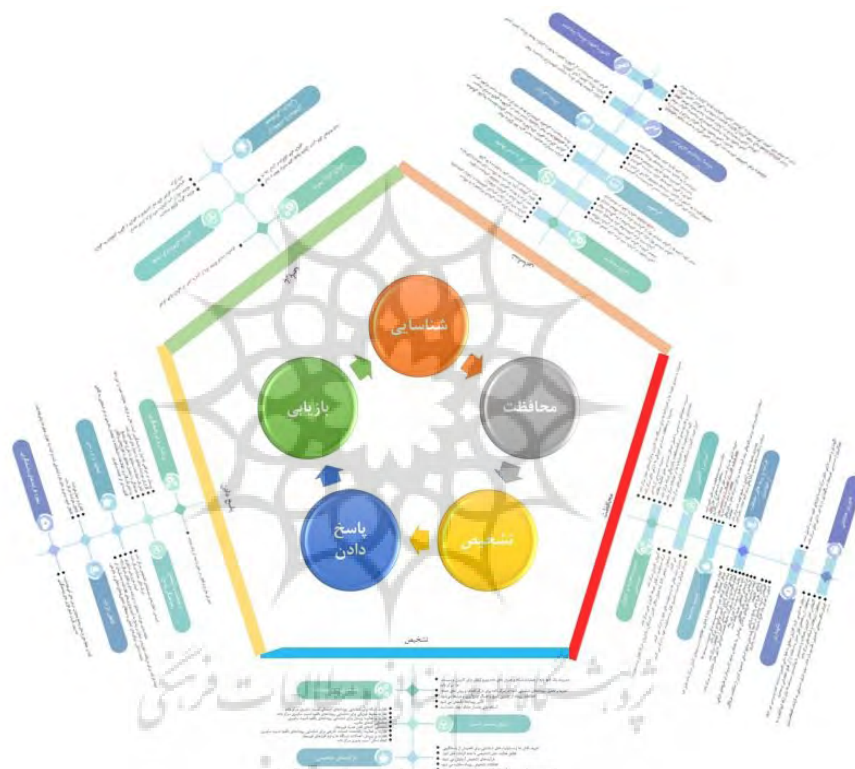
$$= ۰/۷۳ \text{ (توافقات شانسی - ۱) / (توافقات مشاهده شده) = } K$$

نظر به اعتبار میزان بدست آمده عدد K براساس استاندارد اشاره شده در جدول (۳) موارد مستخرجه در قالب شناسایی و ارائه کدهای مدیریتی امنیت سایبری مرکز داده بر اساس الگوی NIST با رویکرد یکپارچه و هوشمند (شکل ۵) صحیح است.

یافته‌های پژوهش

با مرور نظام‌مند ادبیات امنیت سایبری مرکز داده و کدگذاری و تحلیل آن‌ها با روش فراترکیب مقوله‌ها و مولفه‌های اصلی این چارچوب شناسایی شدند. در مجموع نتایج

کدگذاری منابع منجر به شناسایی مولفه‌های چارچوب و ابعاد آن گردید. براساس بررسی‌های صورت گرفته در مجموع ۱۰۸ کدمدیریتی در قالب ۲۳ مولفه دسته بندی و به عنوان مولفه‌های چارچوب هوشمند و یکپارچه امنیت سایبری مرکز داده استخراج شدند که در ۵ مقوله اصلی شناسایی، محافظت، کشف، پاسخ‌گویی و بازیابی مورد شناسایی قرار گرفتند. شکل (۵) نمای کلی این چارچوب جامع را نشان می‌دهد.



شکل شماره ۵: چارچوب جامع امنیت سایبری مرکز داده با رویکرد هوشمند و یکپارچه

همچنین ۲۳ مولفه شناسایی شده، که از تجمیع ۱۰۸ کد منتخب در شکل ۶ بخشی از جدول ۴ شامل کلیه اطلاعات کدهای مدیریتی به تفصیل (جهت اطلاعات کامل به پایان نامه مراجعه شود) بدست آمده اند و پدید آورنده ابعاد چارچوب مورد نظر هستند عبارتند از: مدیریت دارایی، محیط کسب و کار، حکمرانی، ارزیابی ریسک، راهبرد مدیریت ریسک، مدیریت ریسک زنجیره تامین، کنترل دسترسی، آموزش و آگاهی، امنیت داده ها، نگهداری،

فناوری حفاظتی، فرایند و رویه‌های حفاظت از اطلاعات، ناهنجاری‌ها و رویدادها، پایش مستمر امنیت، فرآیندهای تشخیصی، برنامه ریزی پاسخگویی، ارتباطات با ذینفعان (هماهنگی پاسخ)، تحلیل و بررسی، کاهش اثرات، بهبود فرایندهای پاسخگویی، برنامه ریزی بازیابی، بهبود فرایندهای بازیابی، ارتباطات با ذینفعان (هماهنگی بازیابی).

جدول ۴. چارچوب جامع امنیت سایبری مرکز داده

منبع	کدها	مؤلفه‌ها	مقوله‌ها
CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5	دستگاه‌ها و تجهیزات فیزیکی درون مرکز داده سازمان	مدیریت دارایی	شناسایی
CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5	پلتفرم‌های نرم‌افزار و برنامه‌های کاربردی درون مرکز داده سازمان		
CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	ارتباطات سازمانی و جریان‌های داده		
CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9	منابع و سرورهای اطلاعات خارجی مرتبط با مرکز داده		

شکل شماره ۶: بخشی از جدول چارچوب جامع امنیت سایبری مرکز داده

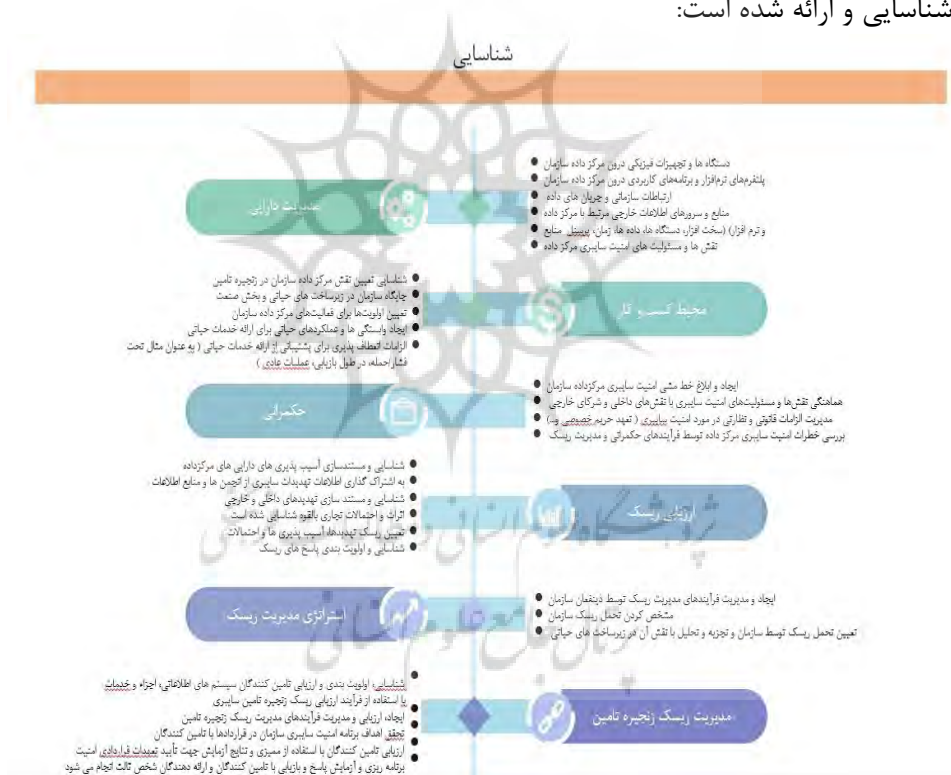
یکپارچگی از آنجایی نتیجه‌گیری می‌شود که در صورت عدم توجه به هر کدام از مولفه ابعاد فوق که مانند حلقه‌های یک زنجیر بهم پیوسته ترسیم شده‌اند چارچوب کارایی لازم را در امنیت سایبری از دست خواهد داد و ساختار امنیت ایجاد شده از هم خواهد گسست. همچنین اگر به فرایند طراحی چارچوب فوق توجه کنیم انجام مستمر و پایش چرخشی آن هوشمندی لازم را جهت درس گرفتن از اقدامات قبلی خود و دیگران و جلوگیری از تکرار تهدیدات امنیت سایبری لازم برای مراکز داده سازمان را فراهم می‌نماید.

مسئله هوشمندی با خصوصیتی نظیر یادگیری، تشخیص الگو تهدیدات سایبری، پیش‌بینی، آگاهی بخشی و پایگاه دانش تهدیدات پیش رو برای توسعه امنیت مرکز داده بعنوان مهمترین زیرساخت ارتباطی و اطلاعاتی سازمان در نظر گرفته شده است و تلاش بر این موضوع متمرکز است که مراکز داده سازمانی در سطح ملی دارای عملکرد امنیتی به شکل یکپارچه بوده و این موضوع به پایداری آنها کمک نماید در این خصوص میتوان

مباحثی همچون بازدارندگی و تاب آوری سایبری را در این نوع زیرساخت ها مورد توجه قرار داد که در این مورد پیشنهادهایی در بخش مربوطه ارائه خواهد شد. در ادامه به صورت مختصر توضیحات لازم در مورد برخی از مهمترین کدهای مدیریتی مربوط به مولفه های چارچوب هوشمند و یکپارچه امنیت سایبری مرکز داده ارائه شده است.

۱. کدهای مدیریتی مقوله شناسایی

همانطوری که در شکل ۷ مشاهده می شود مقوله شناسایی کلیت مرکز داده و مولفه های امنیتی و تجهیزاتی آن دارای اهمیت بسیاری است و کدهای مربوط به آن شناسایی و ارائه شده است:



شکل شماره ۷: کدهای مدیریتی بعد شناسایی چارچوب جامع هوشمند و یکپارچه امنیت سایبری مرکز داده

تشخیص



شکل شماره ۹: کدهای مدیریتی بعد کشف چارچوب جامع هوشمند و یکپارچه امنیت سایبری مرکز داده

۴. کدهای مدیریتی مقوله پاسخگویی

همانطوری که در شکل ۱۰ مشاهده می‌شود مقوله پاسخگویی به تهدیدات در مرکز داده و مولفه‌های آن دارای اهمیت بسیاری است و کدهای مربوط به آن شناسایی و ارائه شده است:

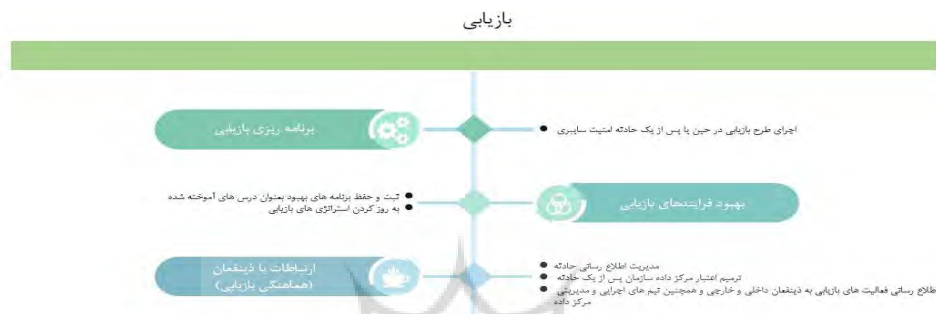
پاسخ دادن



شکل شماره ۱۰: کدهای مدیریتی بعد پاسخگویی چارچوب جامع هوشمند و یکپارچه امنیت سایبری مرکز داده

۵. کدهای مدیریتی مقوله بازیابی

همانطوری که در شکل ۱۱ مشاهده می‌شود مقوله بازیابی مرکز داده و تداوم ارائه سرویسها و خدمات آن دارای اهمیت بسیاری است و کدهای مربوط به آن شناسایی و ارائه شده است:



شکل شماره ۱۱: کدهای مدیریتی بعد بازیابی چارچوب جامع هوشمند و یکپارچه امنیت سایبری مرکز داده

بحث و نتیجه‌گیری

پژوهش حاضر به دنبال ارائه کدهای مدیریتی چارچوب جامع امنیت سایبری مرکز داده با رویکرد هوشمند و یکپارچه است از این رو سعی گردید با مرور نظام‌مند ادبیات امنیت سایبری مرکز داده و کدگذاری و تحلیل آن‌ها با روش فراترکیب و بر مبنای الگوی NIST کدهای مدیریتی مقوله‌ها و مولفه‌های اصلی این چارچوب شناسایی شوند. بر مبنای مطالعه منابع فوق، تحقیقی با عنوان و حوزه معرفی شده به شکل تحقیق حاضر انجام نشده است و نوآوری تحقیق حاضر از جنبه مطالعه در مورد چارچوب امنیت سایبری با رویکرد مدیریت یکپارچه و هوشمند در مورد مراکز داده سازمانی بوده و لذا توسعه چارچوبی که بتواند به سازمانها در مواجهه با تهدیدات سایبری مراکز داده فعال در زیرساخت‌های اطلاعاتی و ارتباطی کمک کند از اهداف این تحقیق محسوب می‌شود. علاوه بر این در پژوهش حاضر برخلاف مطالعات قبلی یک دسته‌بندی جامع از مولفه‌های چارچوب امنیت سایبری مرکز داده و در مجموع ۱۰۸ کدمدیریتی در قالب ۲۳ مولفه در ۵ مقوله اصلی شناسایی، محافظت، کشف، پاسخگویی و بازیابی مورد شناسایی قرار گرفتند.

یکپارچگی از آنجایی نتیجه‌گیری می‌شود که در صورت عدم توجه به هر کدام از مولفه ابعاد فوق که مانند حلقه‌های یک زنجیر بهم پیوسته ترسیم شده‌اند چارچوب کارایی لازم را در امنیت سایبری از دست خواهد داد و ساختار امنیت ایجاد شده از هم خواهد گسست. همچنین اگر به فرایند طراحی چارچوب فوق توجه کنیم انجام مستمر و پایش چرخشی آن هوشمندی لازم را جهت درس گرفتن از اقدامات قبلی خود و دیگران و جلوگیری از تکرار تهدیدات امنیت سایبری لازم برای مراکز داده سازمان را فراهم می‌نماید.

مسئله هوشمندی با خصوصیات نظیر یادگیری، تشخیص الگو تهدیدات سایبری، پیش‌بینی، آگاهی بخشی و پایگاه دانش تهدیدات پیش رو برای توسعه امنیت مرکز داده بعنوان مهمترین زیرساخت ارتباطی و اطلاعاتی سازمان در نظر گرفته شده است و تلاش بر این موضوع متمرکز است که مراکز داده سازمانی در سطح ملی دارای عملکرد امنیتی به شکل یکپارچه بوده و این موضوع به پایداری آنها کمک نماید در این خصوص میتوان مباحثی همچون بازدارندگی و تاب آوری سایبری را در این نوع زیرساخت ها مورد توجه قرار داد که در این مورد پیشنهادهایی در بخش مربوطه ارائه خواهد شد.

در مورد دانش‌افزایی مقاله باید توجه داشت، مطالعات قبلی عمدتاً در مورد چارچوب کلی امنیت سایبری و متمرکز بر ابعادی مانند تهدید، منشاء تهدید، شیوه تهدید بودند و به چارچوبی با ویژگی یکپارچه و هوشمند با خصوصیات نظیر یادگیری، تشخیص الگو، پیش‌بینی، آگاهی بخشی و توسعه پایگاه دانش توجه نکرده بودند ضمن اینکه چارچوب جامع امنیت سایبری هوشمند و یکپارچه مرکز داده با نگاه جزءنگر انجام نشده است. علاوه بر این در پژوهش حاضر برخلاف مطالعات قبلی یک دسته‌بندی جامع از کدها و مولفه‌های چارچوب امنیت سایبری مرکز داده ارائه شده است.

پیشنهادهای اجرایی و پژوهشی زیر می‌تواند در ادامه کار پژوهشی فوق مورد نظر قرار گیرد:

- رویکرد کل‌گرایانه و شناسایی چارچوب زیست بوم موجود امنیت سایبری مراکز داده سازمانی در کشور.

- رویکرد کل‌گرایانه و ارائه چارچوب زیست بوم مطلوب امنیت سایبری مراکز داده سازمانی در کشور با رویکرد مدیریت هوشمند و یکپارچه.

منابع فارسی

- کاظمی، احمد؛ معینی، علی؛ روحانی، سعید؛ یعقوبی، نورمحمد؛ یزدانی، حمیدرضا. (۱۴۰۰) چارچوب هوشمند و یکپارچه امنیت سایبری مرکز داده سازمان در سطح ملی، فصلنامه علمی پژوهشی، امنیت ملی.
- آقایی، محسن؛ معینی، علی؛ عرب‌سرخی، ابوذر؛ محمدیان، ایوب؛ زارعی، علی‌اصغر. (۱۳۹۸). ارائه مدل مفهومی ساختار تهدیدات سایبری مراکز داده. فصلنامه امنیت پژوهی دانشگاه فارابی.
- بازرگان، عباس. (۱۳۷۸). مقدمه‌ای بر روش‌های تحقیق کیفی و آمیخته، رویکردهای متداول در علوم رفتاری، تهران، چاپ اول، نشر دیدار.
- حسین‌زاده، محمد؛ حسنی آهنگر، محمدرضا. (۱۳۹۵). اصول طراحی یک مدل امنیتی برای مراکز داده، یازدهمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی.

References

- Abraham, R., Schneider, J., & vom Brocke, J. (2019). A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424-438 .
- Abraham S., Nair S. (2018). Comparative analysis and patch optimization using the cyber security analytics framework. *Journal of Defense Modeling and Simulation*.
- Accenture Technology Vision 2019.
- Accenture Trend 4: Secure US to Secure ME .
- Aghaei, M., and Moini, A., and Arabsarkhi, A., and Mohammadian, A., and Zarei, A. (2018). Providing a conceptual model of the structure of cyber threats in data centers. *Farabi University Security Research Quarterly*. (In Persian)
- Ahmed M., Rama Mohan Babu G. (2019). Cyber security framework for big data environment using support vector machine. *Journal of Advanced Research in Dynamical and Control Systems*.
- Ahmed AlKalbani., Hepu Deng., Booi Kam., (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development , *25th Australasian Conference on Information Systems, 8th - 10th Dec 2014, Auckland, New Zealand*.
- Al-Badi, A., Tarhini, A., & Khan, A. I. (2018). Exploring big data governance frameworks. *Procedia Computer Science*, 141, 271-277 .
- Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*, 25(sup1), 64-75.

- Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: a theory building approach. *Information Systems Management*, 36(2), 98-110.
- Ashtiani M., Abdollahi Azgomi M. (2014). A distributed simulation framework for modeling cyber attacks and the evaluation of security measures. *SIMULATION*.
- Al-Muhtadi J., Saleem K., Al-Rabiaah S., Imran M., Gawanmeh A., Rodrigues J.J.P.C. (2020). A lightweight cyber security framework with context-awareness for pervasive computing environments. *Sustainable Cities and Society*.
- Attard, J., Orlandi, F., & Auer, S. (2016). Data driven governments: Creating value through open government data *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII* (pp. 84-110): Springer.
- Atoum I., Ootom A. (2016). Effective belief network for cyber security frameworks. *International Journal of Security and its Applications*.
- Atoum I., Ootom A., Ali A.A. (2014). A holistic cyber security implementation framework. *Information Management and Computer Security*.
- Australian Government. (2020). *Data Governance framework 2020*.
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program:
<https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731>
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels:
<https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785>
- Baggott S.S., Santos J.R. (2020). A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid. *Risk Analysis*.
- Baig Z., Zeadally S. (2019). Cyber-security risk assessment framework for critical infrastructures. *Intelligent Automation and Soft Computing*.
- Bazargan, Abbas. (1999). An introduction to qualitative and mixed research methods; Common approaches in behavioral sciences, Tehran, First Edition, Didar Publishing. (In Persian)
- Benfeldt, O., Persson, J. S., & Madsen, S. (2019). Data governance as a collective action problem. *Information Systems Frontiers*, 1-15.

- Bhardwaj A., Goundar S. (2019). A framework to define the relationship between cyber security and cloud performance. *Fraud and Security*.
- Bonina, C., & Eaton, B. (2020). Cultivating open government data platform ecosystems: Lessons from Buenos Aires, Mexico City and Montevideo. *Government Information Quarterly*, 37(3), 101479.
- Calzada, I., & Almirall, E. (2020). Data ecosystems for protecting European citizens' digital rights. *Transforming Government: People, Process and Policy*.
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls):
<https://www.cisecurity.org>
- Collier J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*
- Control Objectives for Information and Related Technology (COBIT):
<http://www.isaca.org/COBIT/Pages/default.aspx>
- Cyber Threatscape Report 2019. Accenture
- Dawes, S. S., Vidasova, L., & Parkhimovich, O. (2016). Planning and designing open government data programs: An ecosystem approach. *Government Information Quarterly*, 33(1), 15-27.
- Diran, D., Hoppe, T., Ubacht, J., Slob, A., & Blok, K. (2020). A data ecosystem for data-driven thermal energy transition: Reflection on current practice and suggestions for re-design. *Energies*, 13(2), 444.
- Efthymiopoulos M.P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*.
- European Commission. (2020). *Data governance and data policies at the European Commission*.
- ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, FINAL VERSION 1.0 ETL 2018, JANUARY 2019
- Evangelou M., Adams N.M. (2020). An anomaly detection framework for cyber-security data. *Computers and Security*.
- Georgiadou A., Mouzakis S., Bounas K., Askounis D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*.
- Gupta, A., Panagiotopoulos, P., & Bowen, F. (2020). An orchestration approach to smart city data ecosystems. *Technological Forecasting and Social Change*, 153, 119929.
- Hadji-Janev M., Bogdanoski M. (2017). Swarming-based cyber defence under the framework of collective security. *Security Journal*.

- Hashim M.S., Masrek M.N., Yunos Z. (2016). Elements in the cyber security framework for protecting the Critical Information Infrastructure against cyber threats. *Information (Japan)*.
- Hahn A., Thomas R.K., Lozano I., Cardenas A. (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*.
- Hosseinzadeh, Mohammad; Hosni Ahangar, Mohammad Reza. (2015). Principles of Designing a Security Model for Data Centers, 11th Symposium on Advances in Science and Technology. (In Persian)
- Immonen, A., & Kalaoja, J. (2019). Requirements of an Energy Data Ecosystem. *IEEE access*, 7, 111692-111708.
- Immonen, A., Palviainen, M., & Ovaska, E. (2014). Requirements of an open data based business ecosystem. *IEEE access*, 2, 88-103.
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements:
<https://www.iso.org/standard/54534.html>
- Jang, K.-a., & Kim, W.-J. (2020). Development of data governance components using DEMATEL and content analysis. *The Journal of Supercomputing*, 1-15 .
- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, 37(3), 101493.
- Jetzek, T. (2017). Innovation in the open data ecosystem: Exploring the role of real options thinking and multi-sided platforms for sustainable value generation through open data *Analytics, Innovation, and Excellence-Driven Enterprise Sustainability* (pp. 137-168): Springer.
- Kapletia D., Felici M., Wainwright N. (2014). An integrated framework for innovation management in cyber security and privacy. *Communications in Computer and Information Science*.
- Kampars, J., Zdravkovic, J., Stirna, J., & Grabis, J. (2020). Extending organizational capabilities with Open Data to support sustainable and dynamic business ecosystems. *Software and Systems Modeling*, 19(2), 371-398 .
- Kazemi, A., and Moini, A., and Rohani, S., and Yagoubi, N., and Yazdani, H. (2022) Intelligent and integrated cyber security framework of the organization's data center at the national level. *Farabi University Security Research Quarterly*. (In Persian)
- Kim I., Park N. (2019). A study on cyber security framework by life cycle for safety system based on information and communication technology. *Journal of Advanced Research in Dynamical and Control Systems*.

- Khalid A., Kirisci P., Khan Z.H., Ghrairi Z., Thoben K.-D., Pannek J. (2018). Security framework for industrial collaborative robotic cyber-physical systems *Computers in Industry*.
- Knight R., Nurse J.R.C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers and Security*.
- Kassen, M. (2017). Open data and e-government-related or competing ecosystems: a paradox of open government and promise of civic engagement in Estonia. *Information Technology for Development, 25*(3), 552-578 .
- Le N.T., Hoang D.B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing*.
- Li, S., & Yu, H. (2020). Big data and financial information analytics ecosystem: strengthening personal information under legal regulation. *Information Systems and e-Business Management, 18*(4), 891-909.
- Lillie, T., & Eybers, S. (2018). *Identifying the constructs and agile capabilities of data governance and data management: A review of the literature*. Paper presented at the International Development Informatics Association Conference.
- Lindman, J., Kinnari, T., & Rossi, M. (2015). Business roles in the emerging open-data ecosystem. *IEEE Software, 33*(5), 54-59.
- Lu T., Zhao J., Zhao L., Li Y., Zhang X. (2015). Towards a framework for assuring cyber physical system security. *International Journal of Security and its Applications*.
- Madaan, N., Ahad, M. A., & Sastry, S. M. (2018). Data integration in IoT ecosystem: Information linkage as a privacy threat. *Computer law & security review, 34*(1), 125-133.
- Mazumdar, S., Seybold, D., Kritikos, K., & Verginadis, Y. (2019). A survey on data storage and placement methodologies for cloud-big data ecosystem. *Journal of Big Data, 6*(1), 1-37.
- McBride, K., Olesk, M., Kütt, A., & Shysh, D. (2020). Systemic change, open data ecosystem performance improvements, and empirical insights from Estonia: A country-level action research study. *Information Polity*(Preprint), 1-26.
- Methodology of business ecosystems network analysis: A case study in Telecom Italia Future Centre, *Technological Forecasting and Social Change*, Elsevier, vol. 80(6), pages 1194-1210.
- Mendhurwar S., Mishra R. (2019). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*.

- Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2), 2053951720948087.
- Moreno, J., Fernandez, E. B., Serrano, M. A., & Fernández-Medina, E. (2019). Secure development of big data ecosystems. *IEEE access*, 7, 96604-96619 .
- National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity”, January 10, 2017
- National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity”, April 16, 2018
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015).
<https://doi.org/10.6028/NIST.SP.800-53r4>.
- Noorman, M. (2017). Institutions in the Data Ecosystem: Actors in the public knowledge domain and in private data companies. *Open Data and the Knowledge Society*, 85-103 .
- Oliveira, M. I. S., Lima, G. d. F. B., & Lóscio, B. F. (2019). Investigations into Data Ecosystems: a systematic mapping study. *Knowledge and Information Systems*, 1-42 .
- Otoom A., Atoum I. (2013). An implementation framework (IF) for the National Information Assurance and Cyber Security Strategy (NIACSS) of Jordan. *International Arab Journal of Information Technology*.
- Panda A., Bower A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*.
- Pandey S., Singh R.K., Gunasekaran A., Kaushik A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*.
- Porcedda M.G. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law and Security Review*.
- Rowe B., Halpern M., Lentz T. (2012). Is a public health framework the cure for cyber security?. *CrossTalk*.
- Royalsociety. (2020). *The UK data governance landscape*.
- Sandelowski, M., & Barroso, J. (2006). *Handbook for synthesizing qualitative research*: springer publishing company.
- Sani A.S., Yuan D., Jin J., Gao L., Yu S., Dong Z.Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*.

- SANS, The State of Dynamic Data Center and Cloud Security in the Modern Enterprise, A SANS Survey, Dave Shackleford, October 2015
- Specht, A., Guru, S., Houghton, L., Keniger, L., Driver, P., Ritchie, E. G Treloar, A. (2015). Data management challenges in analysis and synthesis in the ecosystem sciences. *Science of the Total Environment*, 534, 144-158.
- Srinivas J., Das A.K., Kumar N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*.
- Strauss, A., & Corbin, J. (1994). Grounded theory methodology: An overview.
- Svilicic B., Kamahara J., Celic J., Bolmsten J. (2019). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*.
- Styrin, E., Luna-Reyes, L. F., & Harrison, T. M. (2017). Open data ecosystems: an international comparison. *Transforming Government: People, Process and Policy*.
- Tikk-Ringas E. (2015). Legal framework of cyber security. *Intelligent Systems, Control and Automation: Science and Engineering*.
- Topal O.A., Demir M.O., Liang Z., Pusane A.E., Dartmann G., Ascheid G., Kur G.K. (2020). A Physical Layer Security Framework for Cognitive Cyber-Physical Systems. *IEEE Wireless Communications*.
- Vaishnavi, V., Kuechler, W., and Petter, S. (Eds.) (2004/19). "Design Science Research in Information Systems" January 20, 2004 (created in 2004 and updated until 2015 by Vaishnavi, V. and Kuechler, W.); last updated (by Vaishnavi, V. and Petter, S.), June 30, 2019. URL: <http://www.desrist.org/design-research-in-information-systems/>.
- Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all---a contingency approach to data governance. *Journal of Data and Information Quality (JDIQ)*, 1(1), 1-27.
- Wei J. (2010). Knowledge management framework for cyber security learning. *International Journal of Management in Education*.
- Yoon, A., & Copeland, A. (2020). Toward community-inclusive data ecosystems: Challenges and opportunities of open data for community-based organizations. *Journal of the Association for Information Science and Technology*, 71(12), 1439-1454.
- Zhai L., Vamvoudakis K.G. (2020). A data-based private learning framework for enhanced security against replay attacks in cyber-physical systems. *International Journal of Robust and Nonlinear Control*.
- Zimmer, L. (2006). Qualitative meta-synthesis: a question of dialoguing with texts. *Journal of advanced nursing*, 53(3), 311-318.