University of Tehran
Central Library
and Documentation Center

Academic Librarianship and Information Research

Online ISSN: 2783 - 4638

Homepage: https://jlib.ut.ac.ir/

Conceptualizing Security with the Approach of Sustainability and Resilience of the Organization

Mehrdad Hamidzadeh[1], **Alireza Poorebrahimi**[2✉], **Abbas Toloui Ashlaghi**[3], and **Mohammad Reza Motadel**[4]

1. Department of Information Technology Management, Faculty of Management and Economics, Research & Sciences Branch, Islamic Azad University, Tehran, Iran. E-mail: en.hamidzadeh@gmail.com
2. Corresponding author, Department of Industrial Management, Faculty of Management and Accounting, Karaj Branch, Islamic Azad University, Visiting Professor, Faculty of Management and Economics, Science and Research Unit, Islamic Azad University, Tehran, Iran. E-mail: poorebrahimi@gmail.com
3. Department of Information Technology Management, Faculty of Management and Economics, Research & Sciences Branch, Islamic Azad University, Tehran, Iran. E-mail: toloie@srbiaau.ac.ir
4. Department of Management, Faculty of Management, Islamic Azad University, Central Tehran Branch, Tehran, Iran. E-mail: moh.motadel@iauctb.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 25 March 2024
Received in revised form 28 May 2024
Accepted 20 June 2024
Available online 29 June 2024

Keywords:
conceptualization,
organization,
security,
security maturity,
stability,
ontology

ABSTRACT

Objective: This research adopts an approach that conceptualizes security and develops a comprehensive security model using knowledge representation technologies. It aligns with sustainability and organizational resilience within the context of the fifth industrial revolution, aiming to provide a complete overview of the conceptual components of security.

Methods: The objectives of this applied research are pursued through a conceptualization approach. To achieve this, the latest version of Protégé software was used to develop the ontology. Additionally, a life cycle process for ontology creation was designed to align with international methods and design science. Furthermore, to create a comprehensive representation, the OntoGraf tool was employed with a focus on organizational resilience.

Results: The design of a conceptual model for organizational security requirements, controls, and assets was achieved through ontology engineering using the Protégé tool. This process was based on standards, international frameworks, and the specific conditions and needs of the country. The approach aimed to establish sustainability and resilience within the organization while also creating a comprehensive representation of the conceptual components of security in organizations.

Conclusions: In today's complex environment, smart action is essential. In a large organization like a university, acting intelligently is the most important factor in enhancing competitiveness. Security plays a crucial role across various dimensions of organizations that adopt a smart approach. The field of security is highly dynamic, with new threats constantly emerging. To address these rapidly growing threats, conceptual solutions are needed to enhance organizational security, resilience, and continuity. This research presents the conceptualization and organization of knowledge in security, as well as the creation of a platform for the development and use of common concepts.

Cite this article: Hamidzadeh, M., Poorebrahimi, A., Toloui Ashlaghi, A., & Motadel, M. R. (2024). Conceptualizing security with the approach of sustainability and resilience of the organization. *Academic Librarianship and Information Research*, 58 (2), 87-104. http//doi.org/10.22059/jlib.2024.378155.1745

Publisher: University of Tehran Press.
DOI: http//doi.org/10.22059/jlib.2024.378155.1745

Introduction

In many organizations, cybersecurity is hindered by challenges such as the lack of macro and strategic policies, insufficient focus on optimal methods and existing standards, the increasing prevalence of advanced and complex threats, inadequate processes and procedures for leveraging expert personnel and technologies, excessive dependence on tools, and the existence of security silos in planning and implementation. As a result, organizations are far from achieving the desired level of cybersecurity.

Organizations and governments around the world are increasingly becoming digital. Rapid advances in digital technologies have created a wide range of innovative opportunities to fundamentally change core functions, structures, operations, processes, activities, and relationships with stakeholders. Improving the security of infrastructure and services, as well as protecting users' data and privacy, is one of Iran's seven strategies for creating a smart government.

This research adopts an approach that conceptualizes security and develops a comprehensive security model using knowledge representation technologies. It aligns with sustainability and organizational resilience within the context of the fifth industrial revolution, aiming to provide a complete overview of the conceptual components of security.

Method

The objectives of this applied research are pursued through a conceptualization approach. To achieve this, the latest version of Protégé software was used to develop the ontology. Additionally, a life cycle process for ontology creation was designed to align with international methods and design science. Furthermore, to create a comprehensive representation, the OntoGraf tool was employed with a focus on organizational resilience.

Results

The design of a conceptual model for organizational security requirements, controls, and assets was achieved through ontology engineering using the Protégé tool. This process was based on standards, international frameworks, and the specific conditions and needs of the country. The approach aimed to establish sustainability and resilience within the organization while also creating a comprehensive representation of the conceptual components of security in organizations.

The data for this research is based on a pluralistic approach that incorporates various sources, including organizational and security architecture, international security standards, validated models, best practices, general policies in the fields of technology and security, components of intelligent organizations, relevant research, and comparative studies. Additionally, it draws on tacit knowledge and the experiences of experts. Following an analysis grounded in design science and utilizing ontological engineering in accordance with the life cycle, the design

process for the smart organization security model was executed based on conceptualization and ontology, following the outlined steps.

Conclusions

In today's complex environment, smart action is essential. In a large organization like a university, acting intelligently is the most important factor in enhancing competitiveness. Security plays a crucial role across various dimensions of organizations that adopt a smart approach. The field of security is highly dynamic, with new threats constantly emerging. To address these rapidly growing threats, conceptual solutions are needed to enhance organizational security, resilience, and continuity. This research presents the conceptualization and organization of knowledge in security, as well as the creation of a platform for the development and use of common concepts.

A common understanding is the foundation for the formal coding of entities, attributes, processes, and relationships within a specific domain. To effectively interpret security datasets, it is essential to create and develop conceptual models based on ontology. Reusability, reliability, and characterization are important features that should be considered in the conceptualization of security. On the other hand, smart organizations are those that can exponentially enhance the scale, scope, and speed of their operations in a way that allows them to maintain leadership in the ecosystem. This competitive advantage must be stabilized and secured. Furthermore, assets—especially critical ones—along with security requirements and controls, must ensure business continuity and resilience in accordance with modern models. The continuity, resilience, and sustainability of critical services in intelligent organizations are essential. Therefore, conceptual models should be developed with a holistic and systematic approach to sustainability, emphasizing the two principles of reducing vulnerability and restoring services in the shortest possible time.

Author Contributions

All authors have read and agreed to the published version of the manuscript. All authors contributed equally to the conceptualization of the article and writing of the original and subsequent drafts.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank the anonymous reviewers.

Ethical considerations

The authors avoided data fabrication, falsification, plagiarism, and misconduct.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of interest

The authors declare no conflict of interest.

تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی
شاپا الکترونیکی: ۲۷۸۳-۴۶۳۸
Homepage: https://jlib.ut.ac.ir/

مفهوم‌سازی امنیت با رویکرد پایداری و تاب‌آوری سازمان

مهرداد حمیدزاده[۱]، علیرضا پور ابراهیمی[۲]✉، عباس طلوعی اشلقی[۳]، و محمدرضا معتدل[۴]

۱. دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: en.hamidzadeh@gmail.com

۲. نویسنده مسئول، استادیار، گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه آزاد اسلامی، واحد کرج/ استاد مدعو دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: poorebrahimi@gmail.com

۳. استاد، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: toloie@srbiaau.ac.ir

۴. استادیار، گروه مدیریت، دانشکده مدیریت، دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران. رایانامه: moh.motadel@iauctb.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۱/۰۶
تاریخ بازنگری: ۱۴۰۳/۰۳/۰۸
تاریخ پذیرش: ۱۴۰۳/۰۳/۳۱
تاریخ انتشار: ۱۴۰۳/۰۴/۰۹

کلیدواژه‌ها:
امنیت،
بلوغ امنیت،
پایداری،
سازمان.
مفهوم‌سازی،
هستان‌شناسی

چکیده

هدف: این پژوهش با رویکرد مفهوم‌سازی امنیت و ایجاد مدل امنیت جامع با بهره‌گیری از فناوری‌های بازنمایی دانش با رویکرد پایداری و تاب‌آوری سازمان منطبق بر انقلاب صنعتی پنجم و ایجاد تصویری کامل از مؤلفه‌های مفهومی امنیت صورت پذیرفته است.

روش پژوهش: مقاصد پژوهش از نوع کاربردی است که با رویکرد مفهوم‌سازی صورت پذیرفته است، بدین منظور جهت توسعه هستان‌شناسی از آخرین نسخه نرم‌افزار Protégé استفاده‌شده است و جهت ساخت هستان‌شناسی منطبق بر روش‌های بین‌المللی و همچنین علم طراحی، چرخه حیات فرایند ساخت هستان‌شناسی طراحی گردید، در ادامه جهت ایجاد تصویر جامع از ابزار Ontograf با رویکرد تاب‌آوری سازمان استفاده شده است.

یافته‌ها: طراحی مدل مفهومی الزامات و کنترل‌های امنیت سازمان و همچنین دارایی‌های سازمان با بهره‌گیری از مهندسی هستان‌شناسی و ابزار Protégé مبتنی بر استانداردها، چارچوب‌های بین‌المللی، شرایط و مقتضیات کشور با رویکرد ایجاد پایداری و تاب‌آوری سازمان و ایجاد تصویر جامع از مؤلفه‌های مفهومی امنیت در سازمان‌ها.

نتیجه‌گیری: در محیط‌های پیچیده‌ی عصر کنونی، اقدام هوشمند امری ضروری است. در سازمان بزرگ همانند دانشگاه، هوشمند عمل کردن مهمترین عامل افزایش توان رقابت است. امنیت در ابعاد مختلف سازمان‌هایی که رویکرد هوشمند دارند حائز اهمیت است. دنیای امنیت بسیار پویا بوده و همواره تهدیدهای جدیدی شناسایی می‌گردند، برای مقابله با تهدیدهایی که به‌سرعت در حال رشد هستند به راهکارهای مفهومی جهت افزایش امنیت سازمان و همچنین افزایش تاب‌آوری و تداوم نیاز است. مفهوم‌سازی و سازماندهی دانش در امنیت و همچنین ایجاد بستری جهت توسعه و استفاده از مفاهیم مشترک در این پژوهش ارائه شده است.

استناد: حمیدزاده، مهرداد؛ پورابراهیمی، علیرضا؛ طلوعی‌اشلقی، عباس؛ و معتدل، محمدرضا (۱۴۰۳). مفهوم‌سازی امنیت با رویکرد پایداری و تاب‌آوری سازمان *تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی*، ۵۸ (۲)، ۸۷-۱۰۴. http//doi.org/10.22059/jlib.2024.378155.1745

ناشر: انتشارات دانشگاه تهران.

مقدمه

جهانی‌شدن و تحولات سریع از ویژگی‌های محیطی عصر کنونی است، در این شرایط سازمان‌ها باید انعطاف‌پذیری و قدرت واکنش منطقی در محیط پررقابت را داشته باشند تا با شرایط موجود همسو و بقای خود را حفظ کنند. عامل انسانی هوشمند، گروه‌های هوشمند و در نهایت، سازمان هوشمند اساس موفقیت یک سازمان است (نجاری و دیگران، ۱۳۹۴). تغییرات شتابان فناوری‌های تحول‌آفرین و نوظهور باعث دگرگونی و تحول گسترده در ابعاد مختلف سازمان‌ها و جامعه شده و نیز موجب بازطراحی مدل‌های کسب‌وکار و رشد سازمان‌ها شده‌اند. فناوری‌های تحول‌آفرین، در حال ایجاد تغییرات بنیادی و اساسی در سازمان‌ها و کسب‌وکارها هستند (لنگ[1] و رامسی[2]، ۲۰۱۸). یکی از تحولاتی که در سال‌های اخیر تأثیر شگرفی بر فرایندهای کتابخانه‌ها و مراکز اطلاع‌رسانی داشته، ظهور فناوری‌های وب معنایی به ویژه هستان‌شناسی‌ها[3] است. با ظهور وب معنایی و تمرکز آن بر تولید دانش (به‌جای اطلاعات) و افزایش دسترس‌پذیری اشیای محتوایی کتابخانه‌ها، گرایش مراکز اطلاع‌رسانی و کتابخانه‌های ملی جهان برای استفاده از بستر وب معنایی و به ویژه هستان‌شناسی‌ها به منظور برطرف نمودن بخشی از مشکلات نظام‌های کتابخانه‌ای افزایش یافته است. به طور نمونه هستان‌شناسی‌های مربوط به توصیف منابع کتابشناختی از جمله هستان‌شناسی «دوکو[4]» واژگان ساختاریافته‌ای برای اجزای مدرک، هم از نظر ساختاری و هم از نظر محتوایی/معانی بیان ارائه نموده و امکان توصیف این اجزا و مدارک متشکل از آنها فراهم می‌کند (فتحیان دستگردی، ۱۳۹۹). از مهمترین چالش‌های رویکرد هوشمندی در کتابخانه‌ها و مراکز اطلاع‌رسانی بعد امنیت است و عدم توجه به الزامات و کنترل‌های امنیتی با توجه به دارایی‌ها منجر به واکشی اطلاعات می‌شود.

به طور متداول امنیت سازمان‌ها، بر اساس مجموعه‌ای از اقدامات واکنشی طراحی می‌گردد. به عبارتی، برای یک وضعیت خاص راه‌حل ارائه می‌شود. در نتیجه، سازمان دارای مجموعه راه‌حل‌های مستقل و فنی پیچیده است که تضمینی برای همکاری و سازگاری ندارند. بنابراین، طراحی مدل امنیت و توصیف روابط (مفهوم‌سازی) روشی مهم و ضروری بوده و فراهم‌کننده رفتار امن و قابل‌اعتماد است (علی‌آبادی و دیگران، ۱۳۹۶).

امنیت سایبری، در بسیاری از سازمان‌ها، به دلیل چالش‌هایی همچون نبود سیاست‌های کلان و راهبردی، عدم تمرکز بر بهینه روش‌ها و استانداردهای موجود، روند تصاعدی بروز تهدیدات پیشرفته و پیچیده، فقدان فرایندها و رویه‌های مناسب برای بهره‌برداری نیروهای خبره و متخصص از فناوری‌ها، وابستگی زیاد به ابزارها، وجود جزایر امنیتی در برنامه‌ریزی و در اجرا و غیره فاصله زیادی تا رسیدن به سطح مطلوب دارد (آدینه، ۱۴۰۰). (یکی از مسائل مهم در حوزهٔ امنیت، سازمان‌دهی دانش (مدیریت دانش) است، هستان‌شناسی به‌عنوان کلید حل این مسئله ارائه شده است. برای رسیدن به همبستگی در درک مفاهیم امنیتی باید آنها را به شکلی عمومی مطرح نماییم و جزئیات کافی را برای مفید بودن آنها ارائه دهیم (دونر[5]، ۲۰۰۳). یکی از مهمترین ابزارها برای مدل‌سازی دانش، هستان‌شناسی است که ابزاری بسیار قدرتمند در مقایسه با سایر روش‌های مدل‌سازی که از قدرت بیانگری بالاتر، رسمی‌سازی، سلسله مراتبی بودن، قابلیت توزیع‌شدگی و استنتاج قوی برخوردار است (ثروتی و دیگران، ۱۳۹۳). در مطالعات مدل‌سازی و همچنین شبیه‌سازی کارکردهای هوشمندانه، افزون بر روش‌شناسی‌های متداول، شناخت‌شناسی (معرفت‌شناسی[6]) و هستان‌شناسی (وجودشناسی) به طور ویژه‌ای مورد توجه قرارگرفته است (آسوشه، ۱۳۹۰).

هوشمندی در سازمان را می‌توان در بخش‌های مختلف هوشمندی از جمله فرایندهای سازمانی، اطلاعاتی، منابع فیزیکی، منابع انسانی و منابع مالی بیان نمود (حسینی و یدالهی، ۱۳۹۴). تعاریف و ابعاد متنوع و گسترده‌ای در خصوص سازمان هوشمند ذکرشده است، اما به طور جامع می‌توان بیان نمود سازمان‌های هوشمند، با برخورداری از ساختاری متفاوت با سازمان‌های سنتی، سازمان‌ها را برای بقاء در عصر اطلاعات آماده می‌کنند (صابری‌فر، ۱۳۹۹). سازمان هوشمند باید فرایندها و افراد سازمان را با فناوری پیشرفته

1. Lang
2. Rumsey
3. Ontology
4. DoCO- Document Components Ontology
5. Donner
6. Epistemology

همگام ساخته و نیازهای مراجعه‌کنندگان را در زمان کوتاه رفع کند (نجاری و همکاران ۱۳۹۴). برای اطمینان از در نظر گرفتن ملاحظات امنیتی در تمامی ابعاد سازمان، طراحی مدل جامع مفهومی امنیت امری مهم تلقی می‌شود، در غیر این صورت، ناهماهنگی فناوری اطلاعات با اهداف و استراتژی‌های کسب‌وکار، موجب ایجاد آسیب‌های امنیتی در سازمان خواهد شد. مدل مفهومی امنیت سازمان تصویری جامع، یکپارچه و فراگیر از تمامی جنبه‌های امنیت اطلاعات سازمان فراهم می‌نماید به عبارتی مدل مفهومی امنیت ابزاری برای مسئولین امنیت هستند تا جهت ایجاد بهترین روش و قابلیت‌های امنیتی خاص سازمان مورداستفاده قرار گیرند.

با توجه به اهمیت موضوع و موارد بیان‌شده چارچوب‌های امنیتی مختلفی به صورت مجزا و یا در معماری سازمان‌ها بیان‌شده‌اند که البته هیچ یک از آنها نگاه مفهومی نداشته‌اند از جمله: چارچوب امنیتی SABSA[1] برای ایجاد معماری امنیتی سازمان ساخته‌شده و دارای شش لایه معماری امنیتی و یک ماتریس دوبعدی جهت نگاشت پرسش‌های مختلف در هر لایه است؛ چارچوب امنیتی OSA[2]، مجموعه اطلاعات کلی را ارائه می‌دهد و در آن دیدگاه‌های کسب‌وکار، نرم‌افزار، اطلاعات و تکنولوژی بیان می‌شود. این چارچوب شامل فهرستی از تهدیدات مرتبط با سازمان به همراه الگوها و کنترل‌های امنیتی برای کاهش آن تهدیدات است. معماری امنیت O-ESA[3] پنج حوزهٔ معماری امنیت فرا سازمانی را شرح می‌دهد. البته تمرکز این معماری بر فناوری است و دیدگاهی تک منظوره را ایجاد کرده است. چارچوب TOGAF[4] که چارچوب معماری سازمانی بوده و مواردی را در خصوص توسعه چهار حوزه که زیرمجموعه معماری سازمانی است بیان می‌کند، در این چارچوب به منظور جلوگیری از نادیده گرفته نشدن ملاحظات امنیتی حیاتی راهنمایی‌هایی بیان‌شده است (ون[5]، ۲۰۱۴). چارچوب معماری اطلاعات زاکمن که پراستفاده‌ترین چارچوب در عرصه معماری سازمانی است سازمان را از زوایا و سطوح مختلف (شش جنبه عبارتند از داده، عملیات، شبکه، افراد، زمان و انگیزه) تحلیل می‌کند. چارچوب زاکمن درعین‌حال که بسیار جامع است به موضوع امنیت به صورت جامع پرداخته نشده است. با وجود این، برای اهداف مدل‌سازی معماری امنیت، سه ستون اول از ماتریس زاکمن (داده، عملیات و شبکه) بسیار کاربردی بوده و پاسخ پرسش‌هایی همچون اینکه سازمان چه داده‌های با ارزشی را کنترل می‌کند، داده‌ها چگونه استفاده می‌شوند و در کجا قرار می‌گیرند را می‌توان از این ستون‌ها به دست آورد و چارچوب معماری سازمان فدرال که دارای شش مدل (معماری مرجع عملکرد، کسب‌وکار، داده، برنامه‌کاربردی، زیرساخت و امنیت) است و در مدل مرجع امنیت دارای سه بعد اهداف، ریسک و کنترل است (محروقی و همکاران، ۱۳۹۶).

سازمان‌ها و دولت‌ها در سراسر جهان به طور فزاینده به دیجیتال تبدیل می‌شوند. پیشرفت‌های سریع در حوزهٔ فناوری‌های دیجیتال طیف گسترده‌ای از فرصت‌های نوآورانه را فراهم کرده‌اند تا کارکردهای اصلی، ساختارها، عملیات، فرایندها، فعالیت‌ها و روابط با ذی‌نفعان به طور اساسی تغییر دهند. ارتقاء امنیت زیرساخت‌ها و خدمات و حفاظت از داده‌ها و حریم خصوصی کاربران یکی از راهبردهای هفت‌گانه ایران برای ایجاد دولت هوشمند است (وزارت ارتباطات و فناوری اطلاعات، ۱۴۰۲). مطابق با تحلیل صورت گرفته توسط هشت موسسه برتر مشاوره مدیریت جهان امنیت سایبری به‌عنوان یکی از کلان‌روندهای مهم معرفی‌شده است (قلم‌بر و همکاران، ۱۴۰۱).

مطابق بررسی‌های صورت گرفته طبقه‌بندی و مفهوم‌سازی کنترل‌ها و الزامات امنیتی و همچنین دارایی‌های سازمان به صورت پویا امری ضروری بوده، خلأ پژوهش فوق، یکپارچه‌سازی و مفهوم‌سازی کنترل های امنیتی با رویکرد تاب‌آوری سازمان است که در ادامه در بخش ادبیات موضوع و پیشینه پژوهش هستان‌شناسی، امنیت و پیشینه پژوهش بررسی شده و روش پژوهش، ابزارها، داده‌ها و نحوه طراحی مدل مبتنی بر ابزار مدل‌سازی Protégé صورت گرفته و همچنین نحوه ایجاد تصویر جامع از کنترل‌های بین‌المللی و ارتباط مفهومی آنها با ابزار Ontograf بیان شده است. در بخش یافته‌های پژوهش خروجی طراحی و تحلیل‌های

1. Sherwood Applied Business Security Architecture
2. Open Security Architecture
3. Open Enterprise Security Architecture
4. The Open Group Architecture Framework
5. Van

انجام شده به تفکیک ارائه شده و در نهایت در بخش بحث و نتیجه‌گیری ویژگی‌ها و قابلیت‌های کسب شده در خصوص طبقه‌بندی و مفهوم‌سازی امنیت، بلوغ امنیت سازمان و غیره شرح داده شده است.

ادبیات و پیشینه پژوهش

۱. مفهوم‌سازی (هستان‌شناسی) و امنیت

درک یک حوزه، شامل مفاهیم و روابط بین آنها و همچنین ترکیب مفاهیم جهت حل مسائل مرتبط با آن حوزه، دانش است و از طرفی هوش مصنوعی بر ایجاد برنامه‌هایی برای بازنمایی و پردازش دانش در مورد واقعیت‌ها، قواعد و ساختار مسائل تمرکز دارد. ذخیره دانش، بازیابی دانش و استنتاج دانش از مهمترین مفاهیم پایه در هوش مصنوعی است. پیش‌نیاز این فرایندها اکتساب، جمع‌آوری، سازماندهی و ساختاردهی دانش در مورد یک حوزهٔ مطالعاتی برای قرار دادن آنها در سیستم است.

فرایند اکتساب دانش انسان، درک صحیح آن، تبدیل آن به شکلی مناسب برای اعمال اشکال متنوع با استفاده از فن‌ها، زبان‌ها و ابزار مناسب، تأیید و اعتبارسنجی آن توسط سیستم‌های هوشمند و نگهداری از آن در گذر زمان مهندسی دانش گفته می‌شود. هستان‌شناسی ابزاری برای توصیف صریح مفهوم‌سازی ذهنی پس‌زمینه دانش بازنمایی شده در پایگاه‌های دانش را فراهم می‌آورد (گاسویچ[1] و دیگران، ۲۰۰۹). استدلال و بازنمایی دانش در سیستم‌های هوشمند و ذهن انسان بدین‌صورت است که ذهن انسان از بازنمایی‌هایی همچون قیاس، تطابق و جستجو برای استنتاج استفاده می‌کند و استدلال‌کننده‌های هوش مصنوعی با رویه‌های استنتاج و دانش کد شده سعی بر حل مسائل دارند (گاسویچ و دیگران، ۲۰۰۹). دیدگاه‌ها و تعاریف متعددی از هستان‌شناسی ارائه شده است از جمله. هستان‌شناسی ابزار مناسبی برای مدل‌سازی داده، اطلاعات و دانش است. هستان‌شناسی توصیفی رسمی و صریح از یک مفهوم‌سازی مشترک است (کومار[2]، ۲۰۱۳) همچنین مدلی قابل‌درک برای ماشین است که به صورت شبکه‌ای از مفاهیم پیوندی بازنمایی شده است (ثروتی و همکاران،۱۳۹۳). هستان‌شناسی در حوزهٔ کامپیوتر عبارت است از، چندتایی مرتب O= A,I,R,C که شامل اجزای (C[3]، مجموعه مفاهیم موجود در جهان؛ R[4]، مجموعه روابط بین مفاهیم؛ I[5]، نمونه‌های مفاهیم و A، اصول بدیهی و قواعد استنتاج) است (کالفگلو و شورلمر[6]، ۲۰۰۳). در ریاضیات هستان‌شناسی گرافی پیچیده از روابط است که برای بازنمون دانش در مورد جهان از آن استفاده می‌شود (اریگ[7]، ۲۰۰۷). در دنیای وب معنایی هستان‌شناسی، واژگان مورداستفاده برای توصیف و بازنمایی یک حوزه از دانش را تعریف می‌کند (یو[8]، ۲۰۰۷). یک تعریف مهم دیگر از هستان‌شناسی که توسط بسیاری از پژوهشگران مورداستفاده قرارگرفته است تعریف گارتنر از هستان‌شناسی است. گارتنر مفهوم آن را به صورت"توصیفی صریح از مفهوم‌سازی ذهنی" بیان کرده که مفهوم‌سازی ذهنی دیدی انتزاعی و ساده‌شده از جهانی است که ما برای اهدافی خاص تمایل به بازنمایی آن داریم (گروبر[9]، ۱۹۹۳). و هستان‌شناسی، تحلیل مفهومی و مدل‌سازی دامنه است؛ به عبارتی هستان‌شناسی "توصیفی صوری و صریح از مفهوم‌سازی ذهنی مشترک" بیان‌شده است (استودر[10] و دیگران، ۱۹۹۸).

امنیت از نظر مفهومی به وضعیتی اطلاق می‌شود که نیروهای حفظ‌کننده وضع موجود توان محافظت را از نیروهای شناخته‌شده بر هم زننده آن داشته باشند، ولی محافظت کردن از هر چیزی نیاز به شناختن ماهیت آن و شناختن روش‌ها و چگونگی وقوع، به موردحفاظت شده را خواهد داشت. امنیت مفهومی در حال تغییر است به‌نحوی که میزان فهم امنیت مبتنی بر دانش و اطلاعات تحلیل‌گر گسترش می یابد. کمیته امنیت ملی سیستم‌های اطلاعاتی، امنیت اطلاعات را حفاظت از اطلاعات و عناصر حیاتی آن

1. Gasevic
2. Kumar
3. concepts
4. relations
5. individual
6. Kalfoglou & Schorlemmer
7. Ehrig
8. Yu
9. Gruber
10. Studer

تعریف کرده است، تعریف فوق مبتنی برسه مفهوم محرمانگی، یکپارچگی، دسترس‌پذیری ارائه شده است (ویتمن و ماترد[1]، ۲۰۱۲). امنیت ابعاد مختلفی داشته و دارای مجموعه‌ای از حوزه‌ها همچون امنیت فیزیکی، امنیت کارکنان، امنیت شبکه، امنیت رایانه و غیره است (جیکوبز[2]، ۲۰۱۱). امنیت فناوری اطلاعات، حفاظت از سیستم‌های اطلاعاتی به منظور تأمین محرمانه بودن، تمامیت و دسترس‌پذیری اطلاعات در سازمان است (سیف[3] ، ۲۰۱۴). امنیت اطلاعات سازمان، طیف وسیعی را شامل می‌شود (آلبرتز[4] و همکاران، ۲۰۰۱)، به عبارتی بر رویکرد سطح بالا به امنیت فناوری اطلاعات مبتنی بر انواع چارچوب‌ها تأکید دارد. غالباً سازمان‌ها بیش از آنکه به قضیه‌ی فرایند امنیت فناوری اطلاعات در سطح استراتژیک و همگام با اهداف کسب‌وکار استراتژیک بپردازند، در سطح تاکتیکی به آن می‌پردازند (شروود[5] و همکاران، ۲۰۰۵). یکی از رویکردهای کل‌نگر و مهم در زمینه اطلاعات سازمان، معماری امنیت اطلاعات سازمانی مطابق با چارچوب معماری سازمانی است، رویکرد کل‌نگر قالبی با سطح انتزاع زیاد و جزئیات کم برای پوشش جنبه‌های مختلف امنیت اطلاعات ارائه می‌دهد و روش‌های جزءنگر نیازمندی‌های خاص در حوزۀ امنیت را با تمام جزئیات پوشش می‌دهند. هدف معماری امنیت سازمانی[6]، فراهم ساختن چارچوبی است که سازمان بتواند بر اساس آن نیازمندی‌های امنیت را شناسایی و در مورد بهترین راه‌حل‌های پیاده‌سازی امنیت یکپارچه سازمانی تصمیم‌گیری نماید.

۲. پیشینه تحقیق

به دلیل اهمیت حوزۀ امنیت در تمامی ابعاد سازمان، مطالعات فراوانی در زمینه امنیت صورت پذیرفته و همچنین با توجه به قابلیت‌های علم هستان‌شناسی و توسعه ابزارها و زبان‌های گوناگون جهت توسعه و استفاده مجدد از مدل‌های مبتنی از هستان‌شناسی، سعی شد فقط پژوهش‌ها در هر دو حوزۀ امنیت و هستان‌شناسی مورد بررسی و واکاوی قرار گیرد.

پیشینه پژوهش بیانگر آن است که پژوهشگران، علم و ابزارهای هستان‌شناسی را در ابعاد مختلف سازمان مورد بهره‌برداری داشتند تا بتوانند از مزایا و قابلیت‌های مفهوم‌سازی در راستای ایجاد تصویر شفاف و اشرافیت اطلاعات استفاده نمایند، اما به طور کل‌نگر مورداستفاده قرار نداده‌اند با توجه به مشکلات و الزامات بیان‌شده طراحی و تدوین مدل جامع مفهومی امنیت برای سازمان‌های دیجیتال از جمله کتابخانه‌ها امری ضروری است.

جدول ۱. پیشینه پژوهش مرتبط با امنیت و هستان‌شناسی

نویسنده	سال	موضوع	خلاصه پژوهش انجام‌شده	تحلیل (نقاط ضعف و قوت)پژوهش
(ماوروئیدیس[7] و برومادر[8]، ۲۰۲۱)	۲۰۲۱	مدل اطلاعاتی تهدید سایبری	این تحقیق هستان‌شناسی‌های مرتبط با تهدیدات سایبری، استانداردهای اشتراک‌گذاری و طبقه‌بندی‌های را باهدف اندازه‌گیری بیان مفهومی سطح بالای آنها با توجه به عناصر چه کسی، چه‌چیزی، چرا، کجا، چه‌زمانی و چگونه ارزیابی می‌کند.	برای همبستگی مقادیر زیادی از اطلاعات تهدید و به دست آوردن اطلاعات زمینه‌ای که می‌توانند در زمان‌های معنادار به اشتراک گذاشته شوند، نیاز به استفاده از قالب‌های نمایش دانش قابل‌درک ماشینی دارد، این امر با فناوری‌هایی مانند هستان‌شناسی به دست می‌آید.
(وانگ[9] و دیگران ۲۰۲۱)	۲۰۲۱	مهندسی اجتماعی در امنیت سایبری	مهندسی اجتماعی تهدیدی دیگر برای امنیت فضای مجازی است. این مقاله ابتدا یک هستان‌شناسی دامنه را توسعه می‌دهد هستان‌شناسی دامنه ۱۱ مفهوم از موجودیت‌های اصلی را تعریف می‌کند که به طور قابل‌توجهی مهندسی اجتماعی را تشکیل می‌دهد، همراه با ۲۲ نوع رابطه که چگونگی ارتباط این موجودیت‌ها را توصیف می‌کند.	این مقاله یک طرح دانش رسمی و صریح برای درک، تجزیه‌وتحلیل، استفاده مجدد و اشتراک‌گذاری دانش حوزه مهندسی اجتماعی ارائه می‌دهد بر اساس این هستان‌شناسی دامنه یک نمودار حادثه حمله مهندسی اجتماعی ایجاد می‌کند.
(بیتتون[10] و دیگران، ۲۰۲۱)	۲۰۲۱	ارزیابی ریسک امنیت شبکه سازمانی	در این مقاله برای تجزیه‌وتحلیل از هستان‌شناسی ارائه‌شده توسط NIST برای ارزیابی ریسک امنیت شبکه سازمانی و اعمال آن در سیستم‌های تولید مبتنی بر ML استفاده‌شده است.	به طور خاص فرایندهای ذیل در این مقاله انجام‌شده است. ۱.دارای‌های یک سیستم تولیدML شمرده‌شده است، ۲. مدل تهدید توصیف‌شده است، ۳. تهدیدات مختلف شناسایی‌شده

1. Whitman &Mattord
2. Jacobs
3. Saif
4. Alberts
5. Sherwood
6. Enterprise Information Security Architecture (EISA)
7. Mavroeidis
8. Bromander
9. Wang
10. Bitton

نویسنده	سال	موضوع	خلاصه پژوهش انجام‌شده	تحلیل (نقاط ضعف و قوت)پژوهش
				۴، بررسی تعداد زیادی از حملات ،۵. برای تعیین کمیت خطر امتیازدهی جدید معرفی‌شده است.
(ساناگاواراپو[1] و دیگران، ۲۰۲۱)	۲۰۲۱	امنیت اطلاعات	امنیت اطلاعات در دنیای سایبر با افزایش قابل‌توجه تعداد سطوح حمله، یکی از دلایل اصلی نگرانی است. ارائه دانش امنیتی در قالب هستان‌شناسی، تشخیص ناهنجاری، اطلاعات تهدید، استدلال و نسبت دادن ارتباط حملات و بسیاری موارد را تسهیل می‌کند. این کار مستلزم غنی‌سازی پویا هستان‌شناسی‌های امنیت اطلاعات است.	رویکرد اصلی این مقاله غنی‌سازی هستان‌شناسی امنیت اطلاعات مبتنی بر استاندارد است، به عبارتی با معماری یادگیری عمیق آسیب‌پذیری‌ها ، تهدیدات کنترل‌ها و سایر مفاهیم را استخراج کند.
(ارگوندادی[2] و دیگران، ۲۰۲۰)	۲۰۲۰	مدیریت ریسک امنیتی سیستم اطلاعاتی	یک مدل ارتقا یافته معنایی برای مدیریت امنیت در طول عمر سیستم اطلاعاتی پیشنهادشده است. مدل از مجموعه مستمر تهدیدهای شناسایی‌شده پشتیبانی می‌کند. عامل کاوشگر تهدیدهای امنیتی شناسایی‌شده توسط IDS را با استفاده از هستان‌شناسی مبتنی بر توسعه طبقه‌بندی می‌کند.	این مطالعه استفاده از عوامل نرم‌افزاری همراه با بازنمایی دانش معنایی را برای حل پیچیدگی ذاتی در مدیریت امنیت سیستم اطلاعاتی با رویکرد مقرون به صرفه با بازده سرمایه‌گذاری ملموس پیشنهاد می‌کند. تازگی این رویکرد مبتنی بر استفاده از هستان‌شناسی و تجزیه‌وتحلیل ریسک نظام‌مند تهدیدات امنیتی با داده‌های جمع‌آوری‌شده در زمان واقعی است که عینیت تجزیه‌وتحلیل و استدلال سایر عوامل خطر را تضمین می‌کند.
(الخماش[3]، ۲۰۲۰)	۲۰۲۰	توسعه‌سیستم‌ها ی هوشمند ایمن (شهر هوشمند)	توسعه سیستم‌های هوشمند ایمن مطمئن و قابل‌اعتماد برای راه‌حل‌های مؤثر شهر هوشمند ضروری است. در این مقاله یک نمونه اولیه برای توسعه سیستم‌های هوشمند با استفاده از هستان‌شناسی OWL و مدل‌های رسمی ارائه‌شده است.	در این مقاله هستان‌شناسی OWL برای تولید نیازمندی‌های متنی سازگار، کامل و بدون ابهام برای مدل‌سازی رسمی و مدیریت قابلیت ردیابی بین نیازمندی‌ها و مدل‌ها بهره برده است و از ویرایشگر Protégé و ابزار Onto Graf استفاده می‌کند.
(قمر و باوانی[4]، ۲۰۲۰)	۲۰۲۰	امنیت سایبری شهر هوشمند	این مقاله یک معماری لایه‌ای یکپارچه برای امنیت شهرهای هوشمند ارائه می‌دهد. علاوه بر این، مدل معنایی هستان‌شناسی، برای مقابله با پویایی و امنیت شهر هوشمند ارائه‌شده است. مدل توصیف رسمی چهارعنصر اصلی امنیت یعنی آسیب‌پذیری، حمله، الزامات امنیتی و مکانیزم امنیتی را ارائه می‌دهد.	در هستان‌شناسی آسیب پذیری ها و تهدیدهای دارایی‌ها را با اقدامات متقابل مدل می‌کند. یک چارچوب هستی‌شناختی برای امنیت شهر هوشمند Secure-ICADS ارائه شده است، چارچوب پیشنهادی تلاشی برای ارائه داده های ساختار یافته معنایی است. علاوه بر این، حملات بالقوه و آسیب‌پذیری‌های مرتبط با آن‌ها نقشه‌برداری می‌شوند که می تواند احتمال یک حمله خاص را تشخیص دهد.
(مالر[5] و دیگران ۲۰۲۰)	۲۰۲۰	ارزیابی ریسک امنیت اطلاعات برای تجهیزات پزشکی	در این مقاله روش‌شناسی تهدید، احتمال، تجزیه شدت و یکپارچه‌سازی ریسک (TLDR) مبنی بر هستان‌شناسی برای ارزیابی ریسک امنیت اطلاعات برای دستگاه‌های پزشکی ارائه شده است.	روش TLDR ۶از مراحل زیر استفاده می کند: ۱.شناسایی اجزای بالقوه آسیب پذیر دستگاه‌های پزشکی،۲. شناسایی حملات بالقوه، ۳. نقشه حملات کشف شده و طبقه‌بندی الگوی حمله مشترک مبتنی بر هستان‌شناسی،۴. برآورد احتمال، ۵. محاسبه تخمین احتمالات برای هر حمله، ۶. تجزیه هر حمله به چندین جنبه شدت و تعیین وزن، ۷. ارزیابی میزان تاثیر هر یک، ۸. محاسبه ارزیابی‌های شدت مرکب برای هر حمله، ۹.ادغام احتمال و شدت هر حمله و در نتیجه اولویت‌بندی.
(راستوگی[7] و دیگران، ۲۰۲۰)	۲۰۲۰	هوش تهدید بدافزار	تقریباً ۷.۲ میلیارد حمله بدافزار در سراسر جهان در سال ۲۰۱۹ گزارش شد. یک هستان‌شناسی بدافزار می‌تواند از ساخت مدل‌هایی پشتیبانی کند که می‌توانند حملات را از مراحل اولیه (مانند شناسایی آسیب‌پذیری) تا مراحل بعدی شناسایی و ردیابی کنند. یک هستان‌شناسی به عنوان طرحی از یک دامنه خاص عمل می‌کند که حاوی مفاهیم کلیدی (کلاس‌ها) و ویژگی‌های آنها است. هر دو عامل انسانی و نرم‌افزاری می‌توانند از یک هستان‌شناسی برای درک ساختار اطلاعاتی استفاده کنند.	در این مقاله، ما MALont را پیشنهاد شده است. یک هستان‌شناسی برای هوشمندی تهدید بدافزار با تعریف ۶۸ کلاس، ۳۱ ویژگی. نمودار دانش امکان تجزیه و تحلیل، تشخیص ، طبقه‌بندی و نسبت دادن تهدیدات سایبری ناشی از بدافزار را فراهم می‌کند.
(ون و کت[8]، ۲۰۱۹)	۲۰۱۹	امنیت نرم‌افزار	این مقاله یک رویکرد جدید برای مدل‌سازی دانش امنیت نرم‌افزار با رویکرد مبتنی بر زمینه ارائه می‌کند که دانش امنیتی را می‌توان با در نظر گرفتن زمینه برنامه نرم‌افزاری	در آینده انتظار می‌رود هستان‌شناسی به طور مداوم گسترش یافته، محتوای دانش با گنجاندن سناریوهای نرم‌افزاری بیشتر با زمینه کاربردی گسترده غنی‌سازی شده و درعین‌حال

1. Sanagavarapu
2. Arogundade
3. Alkhammash
4. Qamar & Bawany
5. Mahler
6. Threat identification, ontology-based Likelihood, severity Decomposition, and Risk integration
7. Rastogi
8. Wen & Katt

نویسنده	سال	موضوع	خلاصه پژوهش انجام‌شده	تحلیل (نقاط ضعف و قوت)پژوهش
			بازیابی کرد. طراحی این هستان‌شناسی تضمین می‌کند که کاربران جنبه‌های امنیتی مرتبط با ویژگی‌های مهم نرم‌افزار را درک می‌کنند. و توسعه‌دهندگان نرم‌افزار قادرند حملات احتمالی و خطاهای امنیتی مرتبط با عملکرد محصولات نرم‌افزاری خود را بر اساس دامنه برنامه، زبان برنامه‌نویسی یا فناوری‌ها به طور مؤثر شناسایی کنند.	جزئیات زمینه‌ای را در شاخه‌های دانش حوزۀ امنیتی ارائه شود و توضیحات انتزاعی را غنی شود. چنین رویکرد مبتنی بر زمینه در مدل‌سازی هستان‌شناسی می‌تواند به حوزه‌های امنیتی مرزی، مانند امنیت شبکه و رمزنگاری، سود برساند.
(روگوشینا [1] و دیگران، ۲۰۱۹)	۲۰۱۹	امنیت اطلاعات	رویکرد این مقاله تشخیص نتایج یادگیری غیررسمی در حوزۀ امنیت اطلاعات است. ارائه به این حوزۀ توسط ناهمگونی و پویایی منابع اطلاعاتی آن، سلسله مراتب پیچیده دانش و همچنین نیاز روزافزون به متخصصان امنیت اطلاعات تعیین‌شده است.	ساختار سلسله مراتبی پیچیده دانش حوزۀ IS نیازمند استفاده از تحلیل هستی‌شناختی برای پردازش داده است. مدل هستان‌شناسی دامنه IS شامل مفهوم‌سازی دانش، ساختارهای داده ناهمگن و دانش از زیرسیستم‌های مختلف IS و همچنین استانداردها را ادغام می‌کند.
(سیدو ژونگ [2]، ۲۰۱۸)	۲۰۱۸	آسیب‌پذیری امنیت سایبری	یک مدل مفهومی مبتنی بر هستان‌شناسی برای بازنمون دانش رسمی حوزۀ آسیب‌پذیری امنیت سایبری و هوش پیشنهاد کردند که مفاهیم آسیب‌پذیری امنیت سایبری را از چندین منبع یکپارچه می‌کند.	هستان‌شناسی می‌تواند برای استدلال در مورد روابط بین موجودیت‌ها برای صدور هشدارهای امنیت سایبری برای تحلیلگران امنیتی برای تجزیه و تحلیل و مدیریت آسیب‌پذیری‌ها مفید باشد هستان‌شناسی مفاهیم آسیب‌پذیری ارائه‌شده توسط موسسه ملی استاندارد و فناوری NIST گسترش‌یافته است.
(منظور [3] و دیگران، ۲۰۱۸)	۲۰۱۸	مدل‌سازی تهدید ابر	تجزیه‌وتحلیل تهدید با توجه به تعامل پیچیده خدمات محاسباتی و ارتباطی یک کار چالش‌برانگیز است. این مقاله یک هستان‌شناسی را توسعه داده که روابط بین بازیگران مختلف درگیر در اکوسیستم ابر را برای تجزیه‌وتحلیل موارد مختلف نشان می‌دهد.	در این مقاله بیان‌شده است که شناسایی نظام‌مند آسیب‌پذیری‌های مبتنی بر هستان‌شناسی می‌تواند نتیجه بهتری داشته باشد و در آینده بر بهبود هستان‌شناسی و با گنجاندن اقدامات متقابل، آسیب‌پذیری‌های ترکیبی و پیش‌شرط‌های دقیق‌تر اقدام خواهد کرد.
(غریب و میلوپولوس [4]، ۲۰۱۸)	۲۰۱۸	مهندسی الزامات حریم خصوصی	حریم خصوصی یک مفهوم اجتماعی است بر این اساس هستان‌شناسی حریم خصوصی باید الزامات حریم خصوصی را در زمینه اجتماعی و سازمانی خود مفهوم‌سازی کند به‌عبارت‌دیگر هستان‌شناسی نه‌تنها باید جنبه‌های فنی حریم خصوصی بلکه جنبه‌های اجتماعی و سازمانی مرتبط با آن را نیز در نظر بگیرد.	هدف مقاله کمک به مهندسان نرم‌افزار در حین طراحی سیستم‌های آگاه از حریم خصوص با ارائه مجموعه‌ای عمومی و گویا از مفاهیم و روابط کلیدی حریم خصوص است که امکان ثبت نیازهای حریم خصوصی را در زمینه اجتماعی و سازمانی آن‌ها فراهم می‌کند و گام بزرگی در جهت بهبود کیفیت سیستم‌های آگاه از حریم خصوصی است بااین‌حال هنوز کار زیادی باید انجام داد.
(امتیازخان و ندوبواکو [5]، ۲۰۱۸)	۲۰۱۸	دستورالعمل‌های امنیتی برای خانه‌های هوشمند	یکی از استراتژی‌های کاهش ریسک امنیتی، حفاظت از سطح دستگاه است. در این مقاله یک هستان‌شناسی برای نشان دادن دانش در مورد دستورالعمل‌های امنیتی برای قابلیت همکاری و درک در میان بازیگران خانه هوشمند پیشنهادشده است علاوه بر این هستان‌شناسی مبتنی بر زمینه توسعه‌یافته است که با تغییر اطلاعات متنی مانند زمینه کاربر و زمینه فیزیکی سازگار می‌شود.	در این مقاله نیز از ساختارهای اصلی هستان‌شناسی مبتنی بر OWL از کلاس‌ها (مفاهیم) ویژگی‌ها (روابط) و افراد (نمونه/ اعضای کلاس) استفاده‌شده است. همچنین نشان داده که چگونه می‌توان هستان‌شناسی را برای خودکارسازی اعمال کرد.
(گوان [6] و دیگران، ۲۰۱۶)	۲۰۱۶	انتخاب الگوی امنیتی مبتنی بر هستان‌شناسی	یک رویکرد هستان‌شناسی برای مدیریت الزامات امنیتی، الگوهای امنیتی و روابط نگاشت بین آن‌ها پیشنهادشده است. هستان‌شناسی با استفاده از روش‌های توسعه‌یافته و در OWL پیاده‌سازی شده است. به عبارتی یک رویکرد هستی شناختی را پیشنهاد کرد که نگاشت دانش امنیتی را از الزامات امنیتی تا الگوهای امنیتی تسهیل می‌کند.	هستان‌شناسی نگاشت دانش امنیتی را از الزامات امنیتی تا الگوهای امنیتی تسهیل می‌کند. علاوه بر این نمونه اولیه قادر است الگوهای امنیتی با پردازش دانش در هستان‌شناسی پیشنهادی طراحی نماید.
(لیانگ و کانگ [7]، ۲۰۱۳)	۲۰۱۳	هستان‌شناسی امنیتی برای توسعه نرم‌افزار	هستان‌شناسی امنیتی را با اتخاذ روش معماری مدل محور (AMDA) ارائه کردند. هستان‌شناسی پیشنهادی می‌تواند در مدل‌سازی مفهوم امنیتی در هر مرحله از فرایند توسعه (به‌عنوان‌مثال، مراحل نیاز و طراحی) با MDA استفاده شود.	MDA که در توسعه نرم‌افزار مورداستفاده قرارگرفته است تا دغدغه‌ها و مفاهیم امنیتی بتواند در هر مرحله از فرایند توسعه نقش داشته و به‌عنوان اجزای امنیتی در نرم‌افزار گنجانده شود. این هستان‌شناسی و معناشناسی آن را معرفی شده و ثابت کرده که هستان‌شناسی امنیتی پیشنهادی می‌تواند در مدل‌سازی و طراحی مفاهیم امنیتی در هر یک از مراحل فرایند توسعه با MDA مفید باشد.

1. Rogushina
2. Syed & Zhong
3. Manzoor
4. Gharib & Mylopoulos
5. Imtiaz Khan & Ndubuaku
6. Guan
7. Liang & Kang
8. model-driven architecture

نویسنده	سال	موضوع	خلاصه پژوهش انجام‌شده	تحلیل (نقاط ضعف و قوت)پژوهش
(فرای [1] و دیگران، ۲۰۱۲)	۲۰۱۲	شبکه و هستان‌شناسی	این پژوهش باهدف ایجاد یک سیستم تشخیص تهاجم با استدلال مبتنی بر ترافیک با استفاده از هستان‌شناسی برای تشخیص حملات پیچیده مطرح‌شده است. این سیستم، مبتنی بر حملات، دستگاه‌ها، آسیب‌پذیری‌ها و ترافیک است.	در این پژوهش نیز از هستان‌شناسی به‌عنوان یک ساختار ثابت برای واکشی مفاهیم و اطلاعات موجود استفاده‌شده است.
(منیر [2] و دیگران، ۲۰۱۱)	۲۰۱۱	پروتکل Http و شبکه هستان‌شناسی	در این مقاله هستان‌شناسی برای تشخیص آسیب‌پذیری‌های پروتکل Http ایجادشده است و مفاهیم با استفاده از روابط زیر کلاس، شامل بودن۳ به یکدیگر مرتبط شده‌اند؛ ابزار مورداستفاده در این پژوهش Protégé است.	در این پژوهش به طور مناسب مفهوم‌سازی پروتکل Http انجام‌شده است و مفاهیم و روابط با استفاده از هستان‌شناسی مشخص و به صورت وجود و یا عدم وجود حمله برگردانده می‌شود. اما فقط محدود به همین پروتکل است.

روش پژوهش

روش‌شناسی‌های بسیاری توسط پژوهشگران و مهندسان هستان‌شناسی برای ساخت و توسعه هستان‌شناسی معرفی‌شده است. روش‌شناسی‌های سازمانی[4] آن، مهندسی هستان‌شناسی را به صورت سه‌گام اصل تعیین هدف، جمع‌آوری مفاهیم و روابط بین این مفاهیم و تدوین هستان‌شناسی معرفی می‌کند (اسکولد [5]و دیگران، ۱۹۹۸). هستان‌شناسی سازمانی به عنوان یک بستر تعاملی بین افراد مختلف شامل کاربران، طراحان و برنامه‌ریزان در سازمان‌های مختلف عمل می‌نماید (رجبی و دیگران، ۱۳۹۸). روش‌های متعددی جهت طراحی و ساخت هستان‌شناسی ارائه‌شده است، از جمله مهمترین روش‌های عبارتند از: سایک[6]، آسکولد و کینگ[7]، سنسوس[8]، کاکتوس[9]، آنتونالج[10]، نوی[11] (استاب، استودر[12]، ۲۰۱۳). با توجه به اینکه هستان‌شناسی، تحلیل مفهومی و مدل‌سازی دامنه برای تحلیل معنای یک شی در دنیای یک حوزهٔ خاص و فراهم کردن توصیفی صوری برای تشریح آن شی است و به عبارتی توصیفی صوری و صریح از مفهوم‌سازی ذهنی مشترک ارائه می‌نماید (نظامی و همکاران، ۱۳۹۶). مهندسی هستان‌شناسی[13] عبارت است از اصول و ترتیبی که به بررسی قواعد، روش‌ها و ابزار موردنیاز برای ساخت، توسعه و نگهداری هستان‌شناسی‌ها می‌پردازد (شو[14]و دیگران، ۱۳۹۶). منطبق بر مهندسی و همچنین روش‌ها و گام‌های طراحی هستان‌شناسی در پیشینه پژوهش چرخه حیات فرایند ساخت هستان‌شناسی در پنج گام شامل طراحی، مفهوم‌سازی، تحلیل و صوری‌سازی، تولید و پیاده‌سازی و ارزیابی (مطابق با شکل ۱) طراحی شد که در گام طراحی مطالعه امکان سنجی ایجاد هستان‌شناسی، تعیین هدف، تعیین نیازمندی‌ها، مطالعه ابزارها و زبان های بازنمایی دانش و روش استخراج عناصر و در گام دوم (مفهوم‌سازی)، مفهومی‌سازی ذهنی به معنای تعیین مفاهیم و روابط کلیدی و استخراج عناصر اصلی هستان‌شناسی انجام پذیرفته و در ادامه در گام سوم (تحلیل و صوری‌سازی) تحلیل عناصر استخراج شده و پیاده‌سازی مدل مفهومی به صورت صوری و قابل خواندن و پردازش توسط ماشین انجام و در گام چهارم تولید و پیاده‌سازی با استفاده از ابزار مدل‌سازی Protege انجام گرفت. و در نهایت ارزیابی و سنجش مطابق با رهیافت‌های هستان‌شناسی صورت پذیرفت. چرخه فوق منجر می‌شود تا مفهوم‌سازی دانش امنیت سازمان به طور پیوسته بهبود و تکمیل و عملاً فرایند بلوغ امنیت نیز در سازمان پیاده‌سازی گردد.

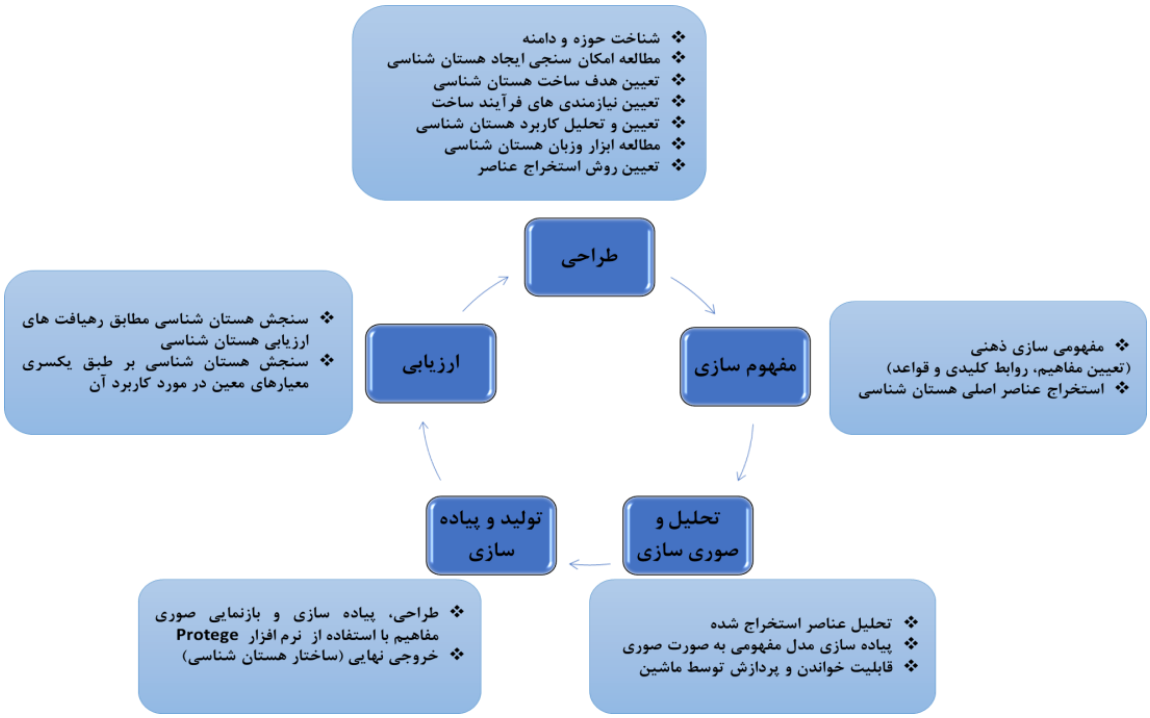
مقاله ارائه‌شده منطبق بر پارادایم تفسیرگرایی انجام شده است. هدف و مقاصد مقاله از نوع کاربردی و همچنین گـردآوری داده‌هـــا به صورت مطالعات کتابخانه‌ای/ تحلیل محتوا و مطابق با استانداردها، بهترین تجربیات، چارچوب‌ها و مدل‌ها و به صورت

1. Frye
2. Munir
3. Comprise of / consist of
4. Enterprise Ontology
5. Uschold
6. Cyc
7. Uschold & King
8. Sensus
9. Kactus
10. On-to-Knowledge
11. Noy
12. Staab & Studer
13. Ontology Engineering
14. Sure

توصیفـــی اســـت، بعد از امکان‌سنجی، تعیین هدف، کاربرد و سازماندهی اطلاعات، مفهوم‌سازی با هدف مفهوم‌سازی ذهنی و روابط کلیدی بین آنها انجام و در ادامه صوری‌سازی منطبق بر مهندسی هستان‌شناسی صورت گرفته و طراحی توسعه هستان‌شناسی با به‌کارگیری ابزارهای بازنمایی دانش از جمله آخرین نسخه نرم‌افزار Protégé صورت گرفت. همچنین در این مقاله، با استفاده از ابزار Ontograf تصویر جامعی از مدل مفهومی امنیت با رویکرد افزایش تداوم، پایداری، تاب‌آوری و امنیت سازمان هوشمند مبتنی بر استنتاج‌های حاصله از مفهوم شناسه‌ها ارائه شد.

یافته‌های پژوهش

داده‌های این پژوهش با رویکرد کثرت منابع منطبق با معماری‌های سازمان و امنیت، استانداردها بین‌المللی امنیت، مدل‌های معتبر، بهترین تجربیات، سیاست‌های کلی نظام در حوزهٔ فناوری و امنیت، مؤلفه‌های سازمان هوشمند، پژوهش‌های مرتبط و مطالعه تطبیقی بوده و از طرفی مبتنی بر تجربه، دانش ضمنی و تجارب خبرگان است. پس از تحلیل مبتنی بر علم طراحی و با استفاده از مهندسی هستان‌شناسی مطابق با چرخه حیات فرایند طراحی مدل امنیت سازمان هوشمند مبتنی بر مفهوم‌سازی و هستان‌شناسی مطابق گام‌های بیان‌شده صورت پذیرفت.



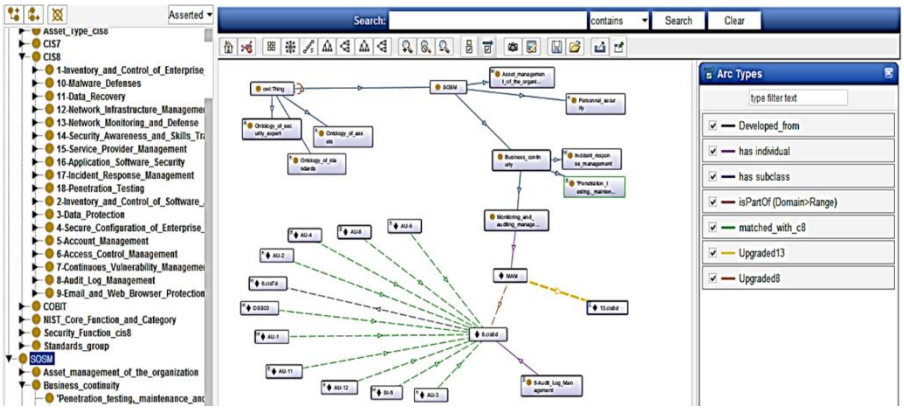
شکل ۱. چرخه حیات فرایند ساخت هستان‌شناسی

مدل امنیت سازمان هوشمند، دارای سه لایه مبتنی بر هستان‌شناسی با رویکرد کل‌نگر بوده، لایه اول کنترل‌ها و الزامات مرتبط با تداوم کسب‌وکار سازمان، لایه دوم مدیریت دارایی‌های سازمان و لایه سوم متخصصان امنیت است و با بهره‌گیری از ابزارهای مهندسی هستان‌شناسی مطابق با شکل ۲ و جدول ۲ طراحی و پیاده‌سازی گردید.

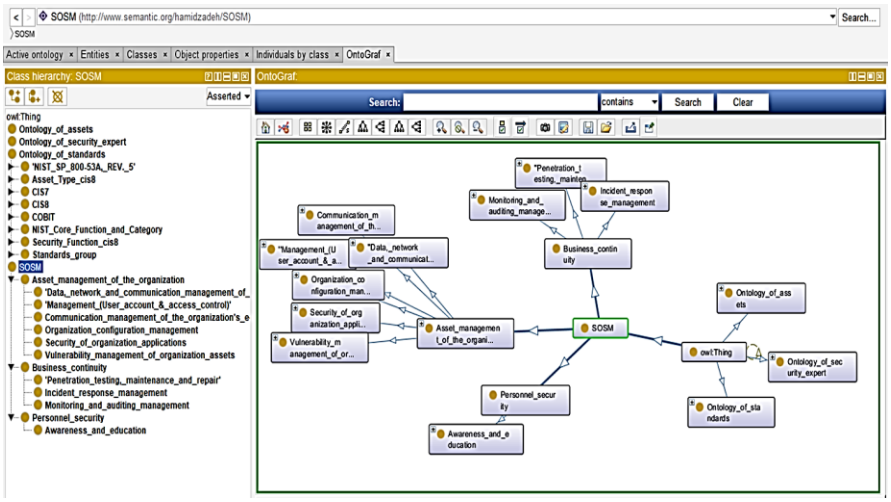
جدول ۲. لایه‌ها، کلاس‌های و اختصارات در مدل امنیت سازمان

لایه هستان شناسی	کلاس های هستان شناسی (مبتنی بر استاندارد)		
Business continuity	Incident response management	مدیریت واکنش به حوادث	IRM
	Monitoring and Auditing Management	مدیریت نظارت و حسابرسی	MAM
	Penetration testing, maintenance and repair	تست نفوذ، نگهداری و تعمیر	PTMR
Asset management of the organization	Vulnerability management of organization assets	مدیریت آسیب پذیری دارایی های سازمان	VMOA
	(User account & access control)Management	مدیریت (حساب کاربری و کنترل دسترسی)	MUAAC
	Organization configuration management	مدیریت پیکربندی سازمان	OCM
	Security of organization applications	امنیت برنامه های کاربردی سازمان	SOA
	Communication management of the organization's ecosystem	مدیریت ارتباطات اکوسیستم سازمان	CMOE
	Data, network and communication management of the organization	مدیریت داده، شبکه و ارتباطات سازمان	DNCM
Personnel security	Awareness and education	آگاهی و آموزش	AE

در لایه‌های مدل امنیت پیشنهادی هر لایه مطابق با مهندسی هستان‌شناسی ایجادشده و مفاهیم، زیر کلاس‌ها، روابط و نمونه‌هایی مطابق با استانداردها و مدل‌های امنیتی داشته و ارتباط معنایی برقرارشده است. از آنجایی‌که هر لایه دارای چندین زیرلایه و نمونه است و نمونه‌ها نیز به کنترل‌های امنیتی منطبق شده‌اند. شکل ۳ نمایی از ارتباط سلسله‌مراتبی و غیر سلسله‌مراتبی را نشان می‌دهد. به طور نمونه کلاس تداوم کسب‌وکار دارای زیر کلاس مدیریت نظارت و حسابرسی است و با اختصار MAM نمایش داده شده است. این زیر کلاس با ارتباط به روز رسانی به کنترل ۱۳و ۸ از چارچوب امنیتی CIS8 هم مفهوم می‌گردد و کنترل ۸ از CIS8 با ارتباط بخشی از به کنترل‌های NIST-VER5 هم مفهوم می‌گردد.



شکل۲. لایه‌های مدل امنیت سازمان هوشمند



شکل۳. ارتباط سلسله‌مراتبی و غیر سلسله‌مراتبی مدل امنیت

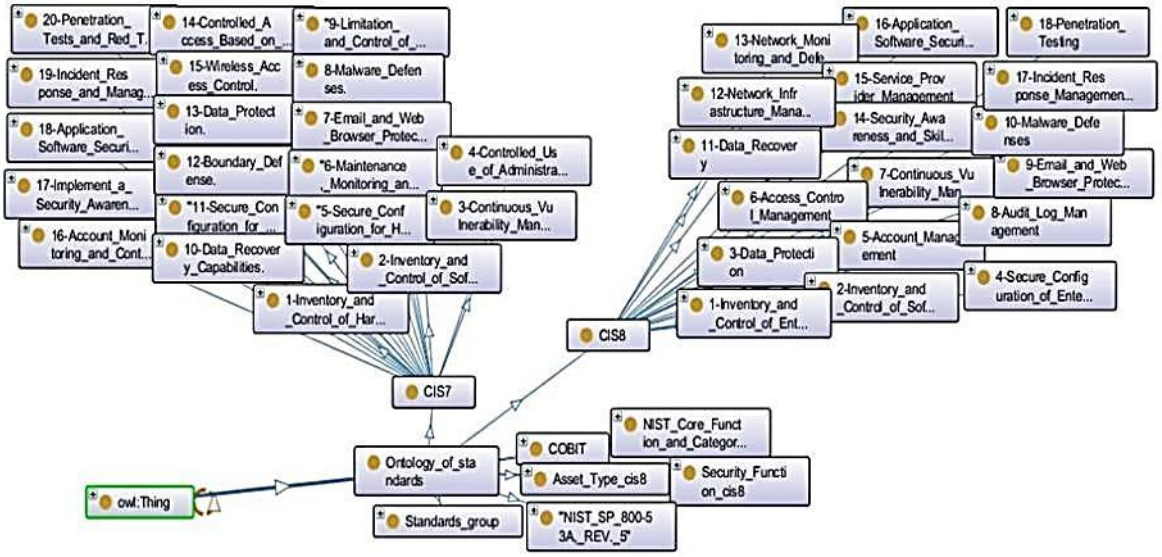
جدول ۴. ۱۸ الزام و ۱۴۷ زیر کلاس CIS8

کلاس و زیر کلاس‌های کنترل امنیتی	کنترل امنیتی
1-Inventory and Control of Enterprise Assets	۵
2-Inventory and Control of Software Assets	۷
3-Data Protection	۱۴
4-Secure Configuration of Enterprise Assets and Software	۱۲
6-Access Control Management	۸
7-Continuous Vulnerability Management	۷
8-Audit Log Management	۱۲
9-Email and Web Browser Protections	۷
6-Access Control Management	۸
10-Malware Defenses	۷
11-Data Recovery	۵
12-Network Infrastructure Management	۸
13-Network Monitoring and Defense	۱۱
14-Security Awareness and Skills Training	۹
15-Service Provider Management	۷
16-Application Software Security	۱۴
17-Incident Response Management	۹
18-Penetration Testing	۵
کل	**۱۴۷**

جدول ۵. ۲۰ الزام و ۱۷۱ زیر کلاس CIS7

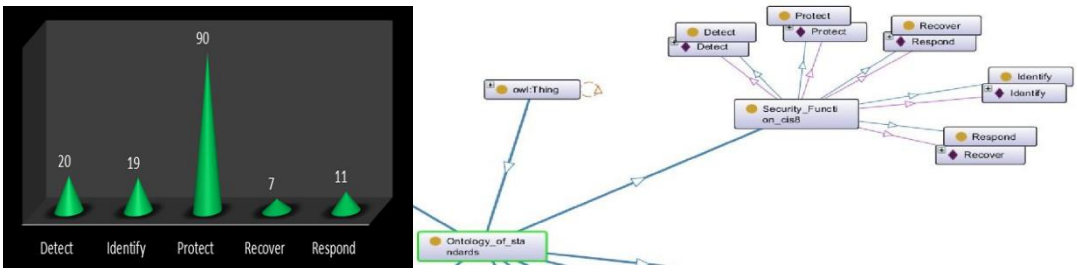
کلاس و زیر کلاس‌های کنترل امنیتی	کنترل‌های امنیتی
1- Inventory and Control of Hardware Assets	۸
2- Inventory and Control of Software Assets	۱۰
3- Continuous Vulnerability Management	۶
4- Continuous Vulnerability Management	۱۰
5- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	۵
6- Maintenance, Monitoring and Analysis of Audit Logs	۸
7- Email and Web Browser Protections	۱۰
8- Malware Defenses	۸
9- Limitation and Control of Network Ports, Protocols, and Services	۵
10- Data Recovery Capabilities	۵
11- Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	۷
12- Boundary Defense	۱۲
13- Data Protection	۹
14- Controlled Access Based on the Need to Know	۹
15- Wireless Access Control	۱۰
16- Account Monitoring and Control	۱۳
17- Implement a Security Awareness and Training Program	۹
18- Establish Secure Coding Practices	۱۱
19- Incident Response and Management	۸
20- Penetration Tests and Red Team Exercises	۸
کل	**۱۷۱**

لایه‌های مدل امنیت طراحی‌شده، مطابق با شکل ۴ دارای پشتوانه کنترل‌ها و الزامات امنیتی چارچوب‌ها و استانداردهای بین‌المللی هستند (به طور نمونه در جدول سه ۱۸ الزامات و ۱۴۷ زیر کلاس CIS8 ارائه شده و در جدول چهار ۲۰ الزامات و ۱۷۱ زیر کلاس CIS7 ارائه شده است.)؛ همان‌طور که بیان شد این مدل، مدلی جامع، کل‌نگر از مجموعه‌ای از استانداردها و مدل‌های امنیت است تا بتواند پوشش کامل و مفهومی در کنترل‌ها و الزامات امنیتی سازمان ارائه دهد.

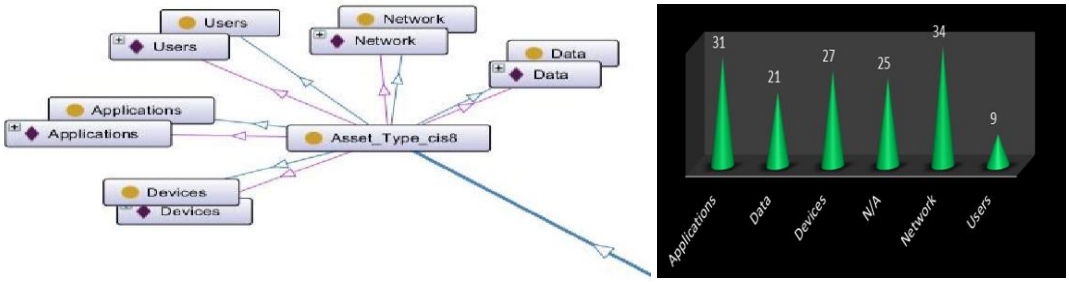


شکل۴. کنترل‌ها و الزامات امنیتی مدل CIS7 و CIS8

همچنین در مدل طراحی‌شده، دسته‌بندی اقدامات امنیتی (شناسایی، تشخیص، محافظت، پاسخ و بازیابی) در شکل ۵ و همچنین دسته‌بندی اقدام منطبق با دارایی‌های امنیتی (برنامه‌های کاربردی، داده، تجهیزات،شبکه و کاربر) با رویکرد پیاده‌سازی الزامات و کنترل‌های سازمان هوشمند مطابق با مقتضیات (شکل ۶) صورت گرفت.

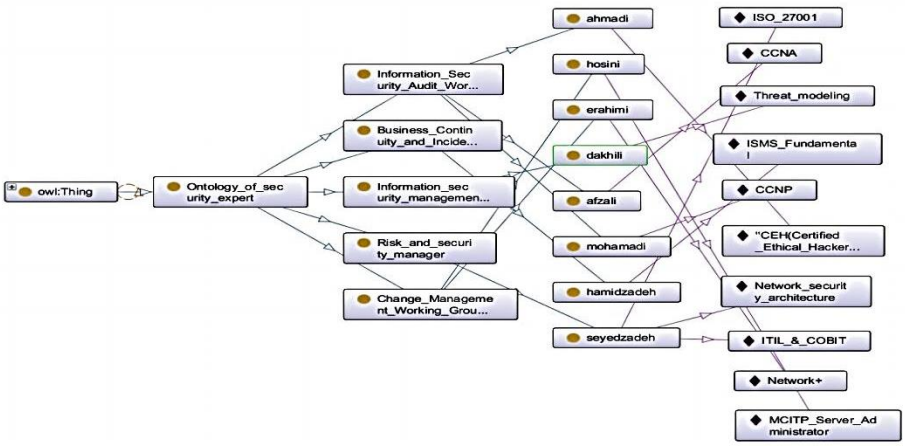


شکل۵. اقدامات و عملکردهای امنیتی و مرتبط با الزامات امنیتی (مطابق با استاندارد)



شکل۶. طبقه‌بندی دارایی‌های سازمان مرتبط با الزامات امنیتی (مطابق با استاندارد)

در نهایت، یکی از مهمترین پشتوانه‌های مدل امنیت، هستان‌شناسی متخصصان امنیت (شکل هفت) و مهارت‌های لازم و موجود در خصوص پیاده‌سازی الزامات امنیتی است، این هستان‌شناسی نیز قابلیت سفارشی‌سازی مطابق با ساختار سازمان را دارد و می‌توان انواع گروه‌های حیاتی از جمله گروه واکنش اضطراری، گروه تداوم کسب‌وکار، گروه پایش و مانیتورینگ و غیره را طراحی و منطبق با نیاز هر گروه مهارت‌های لازم را توسعه داد از طرفی در اجرای دقیق مانورهای مباحثه محور و عملیاتی سازمان نیز بهره برد، همچنین می‌توان برنامه‌ریزی‌های لازم در خصوص پیاده‌سازی اقدامات امنیتی را صورت داد.



شکل ۷. پشتوانه هستان‌شناسی متخصصان امنیت و مهارت‌های لازم

بحث و نتیجه‌گیری

درک مشترک، پایه‌ای برای کدگذاری رسمی موجودیت‌ها، ویژگی‌ها، فرایندها و ارتباطات در حوزه‌ای خاص است، به منظور درک درست مجموعه داده‌های امنیت، نیاز به ایجاد و توسعه مدل‌های مفهومی بر اساس هستان‌شناسی است، استفاده‌پذیری مجدد، قابلیت اطمینان، مشخصه‌سازی ویژگی‌های مهمی هستند که در مفهوم‌سازی امنیت بایستی مدنظر قرار گیرد؛ از طرفی سازمان هوشمند، سازمان‌هایی هستند که می‌توانند به صورت نمایی مقیاس، دامنه و سرعت کسب‌وکار را توسعه دهند به نحوی‌که در اکوسیستم به عنوان رهبر و پیشرو باقی بمانند، یک مزیت رقابتی که می‌تواند این وضعیت را پایدار و امن نگه دارد رویکرد امنیت سازمان به دارایی‌ها و خصوصاً دارایی‌های حیاتی و همچنین الزامات و کنترل‌های امنیتی است که بایستی مطابق با مدل‌های نوین تداوم و تاب‌آوری کسب‌وکار را ضمانت کند. تداوم، تاب‌آوری و پایداری کسب‌وکار در خدمات حیاتی سازمان هوشمند امری ضروری است و باید مدل‌های مفهومی با رویکرد کل‌نگر و نظام‌مند جهت پایداری با دو اصل کاهش آسیب‌پذیری و همچنین بازگرداندن خدمت در حداقل زمان پیش‌بینی‌شده تدوین گردد.

مدل مفهومی امنیت مبتنی بر هستان‌شناسی دارای سه لایه مهم برگرفته از تحلیل مجموعه استانداردهای بین‌المللی و همچنین شرایط و مقتضیات کشور است به نحوی که لایه اول جهت تداوم کسب‌وکار بایستی عملکردهای امنیتی حفاظت و پیش‌گیری را در ابعاد مختلف به صورت پیوسته انجام داد. بنابراین، در لایه تداوم کسب‌وکار سه گروه کنترل حیاتی مطرح شده است که عبارتند از؛ اولین گروه کنترل امنیتی مدیریت نظارت و حسابرسی است که در کلاس مدیریت نظارت و حسابرسی، دو گروه از اقدامات امنیتی مدیریت لاگ‌های حسابرسی و نظارت، پایش و دفاع از شبکه مطابق با مجموعه استانداردها بیان شده است. یکی دیگر از ابعادی که در تداوم کسب‌وکار اهمیت بسیار حیاتی دارد، مدیریت واکنش به حوادث است و در ادامه گروه تست نفوذ، نگهداری و تعمیرات ارائه شده است به عبارتی، تاب‌آوری و کارایی دارایی‌های سازمانی از طریق شناسایی و استفاده از نقاط ضعف‌های کنترل‌های امنیتی (شامل افراد، فرایند و فناوری‌ها) آزمایش می‌شود و اهداف و کارهای مهاجمان شبیه‌سازی خواهد شد. لایه دوم مدل امنیت مدیریت دارایی سازمان بوده و دارای شش زیر لایه و یا گروه کنترل‌های امنیتی است، این کنترل‌ها عبارتند از:

۱. مدیریت داده، شبکه و ارتباطات سازمان است. امنیت شبکه یکی از مؤلفه‌های حیاتی سازمان است زیرا این محیط همواره در حال تغییر است.

۲. گروه کنترل مدیریت ارتباطات اکوسیستم سازمان، این گروه فرایندی برای ارزیابی ارائه‌دهندگان خدماتی که داده‌های حساس را در اختیار دارند.
۳. امنیت برنامه‌های کاربردی سازمان، که در آن بایستی امنیت چرخه حیات نرم‌افزارهای توسعه یافته و یا خریداری شده را تأمین نمود.
۴. کنترل مدیریت پیکربندی سازمان، که در آن بایستی یک مبنای مشخص برای پیکربندی امن دارایی‌های سازمان و نرم‌افزارها تعیین نماییم.
۵. مدیریت حساب کاربری و کنترل دسترسی سازمان، در سازمان‌ها بایستی از فرایندها و ابزارها برای مدیریت مجوزهای دسترسی حساب‌های مختلف (مدیریتی و کاربری) استفاده شود.
۶. مدیریت آسیب‌پذیری دارایی‌های سازمان،در این گروه طرحی برای ارزیابی مداوم و رسیدگی به آسیب‌پذیری‌های تمام دارایی‌های سازمان ایجاد می‌شود و در نهایت در لایه سوم نیروی انسانی است که در کلاس آگاهی و آموزش، آگاهی بخشی امنیتی و آموزش مهارت‌ها به طور پیوسته صورت می‌پذیرد.

طراحی مدل مفهومی امنیت مبتنی بر هستان‌شناسی ویژگی‌های فراوانی از جمله مفهوم‌سازی امنیت و استاندارد، مدیریت دارایی‌ها و ارتباط دارایی‌های و در نتیجه، اولویت‌بندی دارایی‌ها مبتنی بر رویکرد تداوم کسب‌وکار، به اشتراک‌گذاری دانش و مدیریت کارکنان و غیره در اختیار سازمان‌ها می‌گذارد. از طرفی با توجه به اینکه موضوعات مرتبط با امنیت امری پیوسته است و بایستی به صورت دائم توسعه یابد، ویژگی‌هایی همچون توسعه‌پذیری، انعطاف‌پذیری و افزایش کارایی و اثربخشی کنترل‌های امنیتی را برای سازمان ایجاد می‌نماید.

با توجه به گستردگی مفاهیم مرتبط با امنیت و علم هستان‌شناسی، پژوهش‌های پیشین در زمینه‌هایی همچون هشدارها، حملات، تهدیدات و تحلیل ریسک صورت پذیرفته، اما دید جامع به ابعاد سازمان‌های دیجیتال نداشته و با توجه به بررسی‌های انجام شده در مدل‌ها و ساختارهای سازمان‌های هوشمند، سه بعد سازمان (ساختار)، فناوری و نیروی انسانی ابعاد اساسی در ایجاد تحول سازمان هستند. بنابراین، در این پژوهش با رویکرد مفهوم‌سازی و تحلیل امنیت در سازمان هوشمند مؤلفه‌های مرتبط احصاء و مبتنی بر آن هستان‌شناسی طراحی و پیاده‌سازی گردید. به عبارتی با توجه به ارکان اساسی سازمان هوشمند، مدل مفهومی امنیت یکپارچه، توسعه‌پذیر توسط نرم‌افزار پروتژ در قالب هستان‌شناسی مدل شد.

به کمک مدل مفهومی امنیت طراحی‌شده، می‌توان پیچیدگی‌های مربوط به ابعاد مختلف سازمان را به طور پیوسته کاهش داد و همچنین فرایند بلوغ امنیت را پیاده‌سازی نمود. ساخت مدل مفهومی امنیت مبتنی بر مفهوم‌سازی باعث ایجاد فهم ذهنی مشترکی شده است. چرا که یکی از فواید هستان‌شناسی‌ها ایجاد فهم مشترک در حوزه‌های خاص است. با توجه به اهمیت اشتراک دانش، این پژوهش به دنبال فراهم کردن شرایطی است که خبره‌های دامنه فارغ از محدودیت‌های جغرافیایی قادر به تبادل دانش بر یک بستر مشترک بوده و تصمیمات اتخاذ شده توسط آنها قابل ثبت باشد و بدین طریق در تکامل این هستان‌شناسی موثر واقع شود. همچنین این قابلیت وجود دارد تا بتوان خروجی طراحی شده را در ابزارهای بازنمایی دانش هستان‌شناسی در وب به اشتراک گذاشته و نظر خبرگان را دریافت کرد. با توجه به قابلیت‌ها و ویژگی‌های علم هستان‌شناسی می‌توان در پژوهش‌های آتی مؤلفه‌های بیشتری را با رویکرد غنی‌سازی مفاهیم در مدل مفهومی امنیت سازمان هوشمند در نظر گرفت؛ مؤلفه‌هایی همچون تکنیک‌های امنیتی مبتنی برشکار تهدید و غیره و یا انواع استانداردهای خاص صنعت و یا دستورالعمل‌های خاص سازمانی را نیز اضافه نمود.

رویکرد مفهوم‌شناسی بستری ایجاد می‌نماید که می‌تواند توسط سایر پژوهشگران توسعه‌یافته و هستان‌شناسی‌های دیگری نیز با توجه به شرایط کشور و دنیا به آن اضافه گردد. بنابراین، بایستی با یک برنامه‌ریزی منظم، مراحل توسعه و پیاده‌سازی مفاهیم بنیادی امنیت را در بین کلیه سازمان‌های کشور ایجاد نمود به نحوی‌که از دانش‌های ضمنی و تجربیات مختلف کسب شده در کنار استانداردها و مدل‌ها به همراه استنتاج‌های مؤثر به امنیت بیشتری دست‌یافت تا تمامی خدمات حیاتی کشور را نسبت به موضوعات امنیتی مصون ساخت. لازمه این امر ایجاد یک پلت‌فرم بومی و مستقل یا زیرساخت معنایی است. با توجه به مفاهیم تولیدشده در گام بعدی اقدام به تولید ابزارهای بومی نمود و یا ابزارهای غیربومی را مبتنی بر مفاهیم توسعه داده‌شده استفاده نمود. این اقدام

بنیادی فارق از ایجاد بستری امن در جهت توسعه سازمان‌ها، رویکرد فرهنگ‌سازی را نیز توسعه خواهد داد. به‌کارگیری مدل مفهومی امنیت سازمان مبتنی بر هستان‌شناسی، می‌تواند به‌عنوان یک راهبرد اساسی و مهم در حفاظت از دارایی‌های حیاتی سازمان و به‌تبع خدمات حیاتی سازمان به‌شمار آید چراکه هم‌زمان با ساختارمند کردن استانداردها، دارایی‌ها و متخصصان امنیت، ساختار مدیریت دانش نیز برای آگاهی، آموزش ایجاد می‌نماید و نگرش سیستمی و کل‌نگر را به سازمان تزریق می‌نماید و می‌تواند به صورت پیوسته توسط خبرگان این حوزه به‌روزرسانی و توسعه یابد.

ملاحظات اخلاقی

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

سپاسگزاری

از معاونت محترم پژوهشی دانشگاه دانشگاه آزاد اسلامی واحد علوم و تحقیقات به خاطر حمایت مالی/ حمایت معنوی / همکاری در اجرای پژوهش حاضر سپاسگزاری می‌شود.

منابع

آدینه، رضا (۱۴۰۰). *هوشمندسازی امنیت و مقابله با تهدیدات پیشرفته*. تهران: موسسه فرهنگی هنری دیباگران.

آسوشه، عباس (۱۳۹۰). *هستان‌نگاری:روش‌شناسی، ابزارها و زبان های توسعه*. تهران: انتشارات دانشگاه تربیت مدرس.

ثروتی، لیلا؛ ولوی، محمدرضا؛ و حورعلی، مریم (۱۳۹۳).کاربردهای هستان‌شناسی در امور نظامی و متدولوژی هستان‌شناسی نظامی، *هفتمین کنفرانس ملی انجمن فرماندهی و کنترل (C4I) ایران؛ دانشگاه علوم و فنون هوایی شهید ستاری* https://civilica.com/doc/412525

حسینی، سید یعقوب؛ یدالهی، شهربانو (۱۳۹۴). تبیین و ارزیابی هوشمندی درون سازمانی. *مطالعات مدیریت راهبردی*، ۶(۲۳)، ۱۷۹-۲۰۱

رجبی، زینب؛ و علینقی‌زاده اردستانی، مهدی (۱۳۹۸). ارائه یک روش داده محور برای توسعه معماری سازمانی با استفاده از مدل هستان‌شناسی سازمانی. *فرماندهی و کنترل*، ۳(۳)،۱۶-۴۵ http://ic4i-journal.ir/article-1-163-fa.html

صابری فر، رستم (۱۳۹۹). تعیین و تشخیص عوامل مؤثر در طراحی سازمان هوشمند برای مدیریت شهری. *پژوهش‌های جغرافیایی برنامه‌ریزی شهری*، ۸(۲) ، ۴۴۵-۴۶۷

علی آبادی، سبحان؛ محروقی، حمیدرضا؛ و زارع، مهناز (۱۳۹۶). ارائه مدل مرجع امنیت در چارچوب معماری سازمانی ایران؛ *اولین همایش ملی پیشرفت‌های معماری سازمانی دانشکده مهندسی و علوم کامپیوتر دانشگاه شهید بهشتی*. https://civilica.com/doc/737972/

فتحیان‌دستگردی، اکرم (۱۳۹۹). طراحی الگوی هستان‌شناسی فراداده‌ای برای مدل‌سازی و بازنمون معنایی مقالات نشریات علمی در پایگاه رایسست، *مرکز منطقه‌ای اطلاع رسانی علوم و فناوری (رایسست)*.

قلم بر، محمد امین؛ عبادی، سید محمد علی؛ کرمی، خسرو (۱۴۰۱). *کلان روندهای فناوری به روایت ۸ موسسه برتر مشاوره مدیریت جهان*. تهران: واحد مطالعات راهبردی و آینده پژوهی شرکت سرمایه گذاری دی، انتشارات کاریز.

محروقی، حمیدرضا؛ علی آبادی، سبحان؛ و خیرخواه، محیا (۱۳۹۶). بررسی و مقایسه ی چارچوب ها و مدل‌های امنیت در معماری سازمانی، *اولین همایش ملی پیشرفت معماری سازمانی*https://civilica.com/doc/7379

نجاری، رضا؛ آذر، عادل؛ و جلیلیان، حمیدرضا (۱۳۹۴). ارائه مدل هوشمندی سازمان: مورد مطالعه شرکت های تولیدی. *مطالعات رفتار سازمانی*؛ ۴(۱)، ۱-۲۴.

نظامی، درنا؛ و شمس‌عینی، فریدون (۱۳۹۶). پشتیبانی از تصمیمات معماری سازمانی با استفاده از هستان‌شناسی. *همایش ملی پیشرفت‌های معماری سازمانی*. https://civilica.com/doc/737955

وزارت ارتباطات و فناوری اطلاعات (۱۴۰۲). *برنامه راهبردی دولت هوشمند ایران. تهران: وزارت ارتباطات و فناوری اطلاعات*.

References

Adina, R. (2021). *Smartening security and dealing with advanced threats*. Dibagaran Art Cultural Institute of Tehran. (In Persian)

Alberts, C. J. Dorofee, A. J. & Allen, J. H. (2001). OCTAVE catalog of practices, version 2.0. *Carnegie Mellon University, Software Engineering Institute*. https://doi.org/10.1184/R1/6575834.v1

Aliabadi, S., Mahrooghi, H., & Zare, M. (2016). Presenting the reference model of security in the framework of Iran's organizational architecture; *1st national conference on organizational architecture developments, Faculty of Engineering and Computer Science, Shahid Beheshti University*. (In Persian) https://civilica.com/doc/737972/

Alkhammash, E. (2020). Formal modelling of OWL ontologies-based requirements for the development of safe and secure smart city systems. *Soft Computing*. https://doi.org/10.1007/s00500-020-04688-z

Arogundade, T., Abayomi-Alli, O., & Misra, S. A. (2020). An ontology-based security risk management model for information systems. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-020-04524-4

Assouche, A. (2010). *Ethnography: methodology, development tools and languages.* Tarbiat Modares University Publications. (In Persian)

Bitton, R., Maman, N., Elovici, Y., & Shabta, A. (2021). Evaluating the cybersecurity risk of real world, machine learning production systems. *arXiv*, *arxiv.org/abs/2107.01806* https://doi.org/10.48550/arXiv.2107.01806

Donner, M. (2003). Toward a security ontology. *IEEE Security & Privacy*, 1(3), 6-7 https://doi.org/10.1109/MSP.2003.10004

Ehrig, M. (2007). *Ontology Alignment Bridging the Semantic Gap*. Springer. https://doi.org/10.1007/978-0-387-36501-5

Fethian Tasgardi, A. (2019). Designing a metadata ontology model for modeling and semantic representation of scientific journal articles in the Rice database. *Regional Science and Technology Information Center (RAISEST).* (In Persian)

Frye, L., Cheng, L. & Heflin, H. (2012). An ontology-based system to identify complex network attacks', *IEEE International Conference on Communications (ICC), Canada*. https://doi.org/10.1109/ICC.2012.6364689

Gasevic, D., Djuric, D., & Devedzi, V. (2009). *Model driven engineering and ontology development*. (2nd ed.). Springer.

Gharib, M., & Mylopoulos, J. (2018). A core ontology for privacy requirements engineering. *arXiv:1811.12621v1[cs.SE]*. https://doi.org/10.48550/arXiv.1811.12621

Gruber, T. R. (1993.). A translation approach to portable ontology specifications, Knowledge Acquisition, Knowledge Acquisition. *Current issues in knowledge modeling*, Special issue 5 (2) https://doi.org/10.1006/KNAC.1993.1008

Guan, H., Yang, H., & Wang, J. (2016). An ontology-based approach to security pattern selection. *International Journal of Automation and Computing*, 13, 168-182. DOI:10.1007/s11633-016-0950-1

Hosseini, S. Y., & Yadalhi, S. (2014). Explanation and assessment of intra-organizational intelligence. *Strategic Management Studies*, 6(23), 179-201. (In Persian) 20.1001.1.22286853.1394.6.23.8.6

Imtiaz Khan, Y. & U. Ndubuaku, M. (2018). Ontology-based automation of security guidelines for smart homes. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. https://doi.org/10.1109/WF-IoT.2018.8355214

Jacobs, S. (2011). *Engineering information security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. Wiely.

Kalfoglou, Y., & Schorlemmer, M. (2003). IF-Map: An ontology-mapping method based on information-flow theory. *Journal on data semantics*, 1, 98-127. https://doi.org/10.1007/978-3-540-39733-55

Kang, W., & Liang, Y. (2013). A security ontology with MDA for software development. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. https://doi.org/10.1109/CyberC.2013.20.

Kumar A. (2013). A comparative analysis of taxonomy, thesaurus and ontology. *International Journal of Applied Services Marketing Perspectives*, 2, 251-258.

Lang, D., & Rumsey, C. (2018). Business disruption is here to stay what should learners do? Are Business leaders prepared to handle future business disruptions? *11th IBAB International Conference*.

Mahler, T., Elovici, Y. & Shahar, Y. (2020). A new methodology for information security risk assessment for medical devices and its evaluation. *arXiv:2002.06938v1[CR]*. https://doi.org/10.48550/arXiv.2002.06938

Mahrooqi, H., Aliabadi, S., & Khairkhah, M. (2016). Review and comparison of security frameworks and models in organizational architecture. *1st national conference on the advancement of enterprise architecture*. (In Persian) https://civilica.com/doc/737951.

Manzoor, S., Vateva-Gurova, T., Trapero, R. & Suri, N. (2018). Threat modeling the cloud: An ontology based approach. *In Proceedings of the International Workshop on Information and Operational Technology*, 61-72. (In Persian) https://doi.org/10.1007/978-3-030-12085-6_6

Mavroeidis, V., & Bromander, S. (2021). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. 2017 *European Intelligence and Security Informatics Conference (EISIC).* https://doi.org/10.1109/EISIC.2017.20

Ministry of Communications and Information Technology. (2023). *Iran's Smart Government Strategic Plan*. Tehran: Ministry of Communications and Information Technology. (In Persian)

Munir, R., Ahmed, N., Razzaq, A., Hur, A. & Ahmad, F. (2011). Detect HTTP Specification Attacks using Ontology. *10th International Conference on frontiers of information technology (FIT)*, 75-78. https://doi.org/10.1109/FIT.2011.21

Najari, R., Azar, A., & Jalilian, H. (2014). Presenting the intelligence model of the organization: the study of manufacturing companies. *Organizational Behavior Studies Quarterly*, 4 1 (12) 1-24. (In Persian)

Nizami, D., & Shams Aini, F. (2016). Supporting enterprise architecture decisions using ontology. *National Conference on Organizational Architecture Advances*. (In Persian) https://civilica.com/doc/737955.

Nizami, D.; & Shams Aini, F. (2016). Supporting enterprise architecture decisions using ontology. *National Conference on Organizational Architecture Advances*. (In Persian) https://civilica.com/doc/737955.

Qalambar, M. A., Ebadi, S. M. A., & Karami, K. (2022). *Major technological trends according to the worlds top 8 management consulting institutes.* Strategic Studies and Foresight Unit of D Investment Company, Kariz Publications. (In Persian)

Qamar, T., & Bawany, N. Z. (2020). A cyber security ontology for smart city. *International Journal on Information Technologies & Security*, 3(12), Corpus ID: 235753202

Rajabi, Z., & Alinaghizadehardestani, M. (2018). Presenting a data-driven method for the development of enterprise architecture using the enterprise ontology model. *Command and control of the third year,* 3. (In Persian) http://ic4i-journal.ir/article-1-163-fa.html

Rastogi, N., Dutta, S., J. Zaki, M., Gittens, A., & Aggarwal, C. (2020). MALOnt: An ontology for malware threat intelligence. *arXiv:2006.11446v1 [cs.CR]. Association for Computing Machinery*. https://doi.org/10.48550/arXiv.2006.11446.

Rogushina, J., Gladun, A., Pryima, S. & Strokan, O. (2019). Ontology-based approach to validation of learning outcomes for information security domain. CEUR-WS.org 2577(3). Corpus ID: 215807305. http://www.tsatu.edu.ua/kn/wp-content/uploads/sites/16/skopus_2019.pdf

Saberifar, R. (2019). Determining and identifying effective factors in the design of intelligent organization for urban management. *Urban Planning Geography Research*, 8(2), 445-467. (In Persian)

Saif, A. (2014). Security Architecture as Part of Enterprise Architecture, *School of Information and Communication Technology*. Griffith University, Australia.

Sanagavarapu, L., Iyer, V., & Reddy, Y. (2021). OntoEnricher: A Deep learning approach for ontology enrichment from unstructured text. *arXiv:2102.04081v1*. https://doi.org/10.48550/arXiv.2112.08554

Sarvati, L., Valvi, M., & Hourali, M. (2013). Applications of ontology in military affairs and methodology of military ontology; *The 7th National Conference of the Command and Control Association (C4I) of Iran*; *Shahid Sattari University of Aeronautical Sciences and Techniques; November 2013*. (In Persian). https://civilica.com/doc/412525

Sarvati, L., Valvi, M. & Hourali, M. (2013). Applications of ontology in military affairs and methodology of military ontology; *The 7th National Conference of the Command and Control Association (C4I) of Iran*; *Shahid Sattari University of Aeronautical Sciences and Techniques; November 2013*. (In Persian). https://civilica.com/doc/412525

Sherwood, J., Clark, A. & Lynas, D. (2005). *Enterprise Security architecture: A business-driven approach*. CMP Book.

Studer, R., Benjamins, V. R., & Fensel, D. (1998). Knowledge engineering: Principles and methods, *Data & Knowledge Engineering*, 25(1–2), 161–198. https://doi.org/10.1016/S0169-023X(97)00056-6

Sure, Y., Staab, S. & Studer, R. (2009). Ontology Engineering Methodology. *In Handbook on Ontologies, Staab, S., and Studer, R., (eds.).* Springer. https://doi.org/10.1007/978-3-540-92673-3_6

Syed, R. & Zhong, H. (2018). Cybersecurity vulnerability management: An Ontology-Based Conceptual Model. *In Proceedings of the Twenty-fourth Americas Conference on Information Systems, New Orleans, LA, USA*, 16-18. Corpus ID: 53046758

Uschold, M., King, M., Moralee, S. & Zorgios, Y. (1998). *The enterprise ontology*. Published online by Cambridge University Press. https://doi.org/10.1017/S0269888998001088

Van, R. (2014). Comparing Security Architectures. *Lulea University of Technology, Department of Computer Science, Electrical and Space Engineering*.

Wang, Z., Zhu, H.; Liu, P. & Sun, L. (2021). Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples. *Future issue of cybersecurity (ISSN: 2523-3246)*. https://doi.org/10.1186/s42400-021-00094-6

Wen, S. F., & Katt, B. (2019). Managing Software Security Knowledge in Context: An Ontology Based Approach. *Information*, 10, 216. https://doi.org/10.3390/info10060216

Whitman, M. E. & Mattord, H. J. (2012). *Principles of information security* (4th Ed.). Course Cengage Learning.

Yu, L. (2007). *Introduction to the Semantic Web and Semantic Web Services.* Taylor & Francis, United States of America. https://doi.org/10.1201/978158488934