Military Science and Tactics
https://www.qjmst.ir/ Online ISSN: 4520-2676 Print ISSN: 2008-191x

Designing the Model of Intelligent Command and Control by Using the Military Internet of Things

Mohammad Sepehri[1]✉| Adel Farzaneh[2]

1. Corresponding Author, Assistant Professor, Faculty of Command and Control Engineering, Khatam Al-Anbia University. Tehran. Iran.
Email: sepehri377@chmail. ir
2. Lecturer at the Faculty of Command and Control Engineering, Khatam Al-Anbiya University. Tehran. Iran.
Email: adelfarzaneh313@gmail. com

Article Info

Article type:
Research Article

Article history:
Received
18 August 2023
Received in revised form
12 March 2024
Accepted
10 December 2024
Published online
13 March 2025

Keywords:
Internet of Things, Military IOT, Command and Control, Intelligent Command and Control, Smart Defense.

ABSTRACT

Objective: The primary concern of this study is the lack of codification concerning the indigenous intelligent command and control model. Accordingly, the main objective is to develop such a model using the military Internet of Things (IoT). Secondary objectives include: identifying the dimensions and components of the model, determining the relationships between these dimensions and components, and examining the achievements, consequences, functions, and requirements of the model design.

Methodology: This study adopts an applied-developmental research design, employing a descriptive-case research method with a mixed research approach. Data collection incorporates both field and library research, utilizing books, scholarly articles, official documents, interviews, and questionnaires. The temporal scope spans the years 1402–1403 (Solar Hijri calendar), with projections for the subsequent five years, while the spatial domain encompasses the armed forces of the country. The statistical population consists of 70 subject-matter experts. Structural equation modeling (SEM) is applied to analyze the relationships and correlations between factors.

Conclusion: The dimensions of model design are intelligence, information management, sustainability, interoperability, integration, and network-oriented. The achievements and consequences of designing the model are improvement (intelligence of command and control, decision-making and decision-making, comprehensive defense readiness, deterrence), increasing military authority and capability, and increasing indigenous cyber power. The functions of model design are intelligence-making (action-oriented and strategic command systems, control, monitoring and evaluation systems, communication systems, computer and cyberspace systems, information collection systems, surveillance and identification systems) and online situational awareness on the battlefield. The requirements of designing the model are battlefield intelligence, localization of IoT standards, IoT software security, and funding and credit, training and skill development.

Cite this article: Sepehri, M, Sepehri, Farzaneh, A. Designing the model of intelligent command and control by using the Military Internet of Things. *Military science & Tactics*, 20(70) . 173- 207.
DOI: http//doi. org/10. 22034/qjmst. 2025. 2023165. 2022

Publisher: AJA Command and Staff University
DOI: 10. 22034/qjmst. 2025. 2023165. 2022

Military Science and Tactics
https://www.qjmst.ir/ Online ISSN: 4520-2676 Print ISSN: 2008-191x

طراحی الگوی فرماندهی و کنترل هوشمند بومی با استفاده از اینترنت اشیاء نظامی

محمد سپهری[1]✉ | عادل فرزانه[2]

۱. نویسنده مسؤل، استادیار دانشکده مهندسی فرماندهی و کنترل دانشگاه خاتم‌الانبیا (ص)، تهران، ایران. رایانامه: sepehri377@chmail. ir

۲. مدرس دانشکده مهندسی فرماندهی و کنترل دانشگاه خاتم‌الانبیا (ص)، تهران، ایران. رایانامه: adelfarzaneh313@gmail. com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی
تاریخ دریافت:
۱۴۰۲/۱۱/۲۷
تاریخ بازنگری:
۱۴۰۲/۱۲/۲۲
تاریخ پذیرش:
۱۴۰۳/۰۹/۲۰
تاریخ انتشار:
۱۴۰۳/۱۲/۲۳
کلیدواژه‌ها:
اینترنت اشیاء، اینترنت اشیاء نظامی، فرماندهی و کنترل، فرماندهی و کنترل هوشمند، دفاع هوشمند.

چکیده

هدف: دغدغه اصلی، مدون نبودن الگوی فرماندهی و کنترل هوشمند بومی، هدف اصلی، تدوین الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی، سایر اهداف؛ احصای ابعاد و مؤلفه‌ها، تعیین روابط بین ابعاد و مؤلفه‌های طراحی الگو، احصای دستاوردها، پیامدها، کارکردها و الزامات طراحی الگو می‌باشد.

روش‌شناسی: نوع تحقیق کاربردی-توسعه‌ای، روش تحقیق توصیفی-موردی زمینه‌ای، رویکرد تحقیق آمیخته و روش گردآوری اطلاعات، میدانی و کتابخانه‌ای، با ابزارهای مطالعه کتابخانه‌ای کتب، مقالات، اسناد و مدارک و مصاحبه و پرسش‌نامه و قلمرو زمانی سال‌های۱۴۰۲- ۱۴۰۳ پنج سال آتی و قلمرو مکانی نیروهای مسلح کشور می‌باشد. جامعه آماری۷۰ نفر از خبرگان و صاحب‌نظران، جهت تجزیه و تحلیل و بررسی رابطه و همبستگی بین عوامل، از مدل‌سازی معادلات ساختاری استفاده می‌شود.

یافته‌ها: با آزمون مدل پی. ال. اس در آزمون SRMR، چون کوچک‌تر از ۰/۰۸است، مدل کلی پی ال اس برازش مناسبی دارد بنابراین با مدل مورد نظر در جامعه تطابق دارد.

نتیجه‌گیری: ابعاد طراحی الگو؛ هوشمندسازی، مدیریت اطلاعات، پایداری، تعامل‌پذیری، یکپارچگی و شبکه محوری می‌باشد. دستاوردها و پیامدهای طراحی الگو؛ ارتقای(هوشمندسازی فرماندهی و کنترل، تصمیم‌گیری و تصمیم‌سازی، آمادگی همه جانبه دفاعی، بازدارندگی)، افزایش اقتدار و توانمندی نظامی و افزایش قدرت سایبری بومی می‌باشد. کارکردها طراحی الگو؛ هوشمندسازی (سامانه‌های فرماندهی راه‌کنشی و راهبردی، سامانه‌های کنترل، نظارت و ارزیابی، سامانه‌های ارتباطی، سامانه‌های رایانه‌ای و فضای سایبری، سامانه‌های جمع‌آوری اطلاعات، سامانه‌های مراقبت و شناسایی) و آگاهی وضعیتی برخط میدان نبرد می‌باشد. الزامات طراحی الگو؛ هوشمندی میدان نبرد، بومی‌سازی استانداردهای اینترنت اشیاء، امنیت نرم افزاری اینترنت اشیاء و تأمین هزینه و اعتبارات، آموزش و مهارت‌افزایی می‌باشد.

استناد: سپهری، محمد و فرزانه، عادل (۱۴۰۳)، طراحی الگوی فرماندهی و کنترل هوشمند بومی با استفاده از اینترنت اشیاء نظامی. *علوم و فنون نظامی*. ۲۰(۷۰) ۲۰۷- ۱۷۳.

DOI: http//doi. org/10. 22034/qjmst. 2025. 2023165. 2022

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

DOI: 10. 22034/qjmst. 2025. 2023165. 2022

Military Science and Tactics
https://www.qjmst.ir/

Designing the Model of Intelligent Command and Control by Using the Military Internet of Things

Mohammad Sepehri✉[1]| Adel Farzaneh[2]

Extended Abstract

Introduction

Military superiority, battlefield coordination, and decision-making critically depend on situational awareness facilitated by the integration of the Internet of Military Things (IoMT) and the continuous dissemination of combat intelligence. Elements such as predictive analytics, machine learning, knowledge management, and decision support systems are pivotal to the advancement of command and control (C2) intelligence systems. Intelligent C2, while fundamentally grounded in advanced technologies, also entails a cognitive dimension. The deployment of IoMT significantly enhances intelligence capabilities and introduces innovative methods of warfare. When coupled with artificial intelligence (AI), IoMT transforms traditional C2 paradigms, culminating in a new form of intelligent, adaptive command infrastructure.

The central problem addressed by this study is the absence of a codified model for intelligent command and control tailored to the specific context of the military Internet of Things. Accordingly, the primary objective is the development of a localized, indigenous intelligent C2 model that leverages IoMT capabilities. The development of IoMT technologies is predominantly directed toward enhancing the functionality of C2 systems. Sensors and communication networks serve as critical tools for real-time information gathering and dissemination across the battlefield, thereby

[1] Corresponding Author, Assistant Professor, Faculty of Command and Control Engineering, Khatam Al-Anbia University. Tehran. Iran. Email: sepehri377@chmail. ir

[2] Lecturer at the Faculty of Command and Control Engineering, Khatam Al-Anbiya University. Tehran. Iran. Email: adelfarzaneh313@gmail. com

Online ISSN: 4520-2676 Print ISSN: 2008-191x

enabling more effective command over military assets (Beheshti Atashgah, 2018).

Intelligent command and control refers to the systematic provision of personnel, equipment, infrastructure, and methodologies required for the efficient collection, processing, and distribution of information. These processes inform decision-making, planning, operational execution, and strategic oversight. Key attributes of intelligent C2 include: decisive support for command decisions; efficient information management; rapid planning and responsiveness; swift and secure information dissemination; system integrity; comprehensive situational awareness; strategic foresight; extensive use of information and communication technologies (ICT); and interactive coordination throughout the C2 chain (Rezaei et al., 2020). Therefore, the design of an indigenous intelligent C2 model utilizing IoMT is imperative for enhancing combat capabilities, enabling timely decision-making, establishing dynamic operational protocols, developing integrated command infrastructures, ensuring real-time battlefield awareness, and mitigating strategic vulnerabilities in response to emerging threats.

Methodology

This research employs an applied-developmental framework and adopts a descriptive-case study design with a mixed-methods approach. Data collection was conducted through both fieldwork and library research, utilizing a range of scholarly sources including books, academic articles, research documents, interviews, and questionnaires. The temporal scope of the study spans from 1402 to 1403 (2023–2025), covering a five-year period, while the spatial scope encompasses academic institutions and military centers within the country. The thematic scope includes the dimensions and components of military IoT technology and the design of an indigenous intelligent command and control model.

The study’s target population comprises 70 experts in the fields of cyber operations and command and control, all of whom possess postgraduate qualifications (Master’s or Doctorate) and relevant managerial or strategic experience. To analyze the interrelationships among variables, structural equation modeling (SEM) was employed

Online ISSN: 4520-2676 Print ISSN: 2008-191x

using SmartPLS software. For content validity assessment, the Lawshe method was used. The reliability of the measurement instruments and the correlation among model components were evaluated through factor loading coefficients and Spearman correlation analysis. Cronbach's alpha and composite reliability were used to test internal consistency. Construct validity—including convergent and discriminant validity, as well as model fit—was assessed using co-reliability analyses and the Fornell-Larcker criterion.

Findings

Based on the ranking of dimensions derived from the significance coefficients within the research model, the "intelligence" dimension was ranked highest, while "information management" ranked lowest. Among the components of the network-oriented dimension, "indigenous cyberspace" achieved the highest ranking, whereas "radar networks and smart weapons" were ranked lowest. Within the intelligence dimension, "intelligent control systems" held the top position, while "AI-based unmanned systems" were ranked lowest.

In the integration dimension, the component "expert personnel" ranked first, whereas "technology-based organizational structure" ranked last. For the information management dimension, "management and guidance of information" was ranked highest, while "information exchange" was the lowest-ranked component. Within the interoperability dimension, the "laws and regulations of military command and control" ranked first, while "laws and regulations of national command and control" ranked last. Lastly, in the stability dimension, "security of command and control systems" was the most prominent component, whereas "passive defense" was ranked lowest.

The overall evaluation of the PLS structural model, as measured by the Standardized Root Mean Square Residual (SRMR), yielded a value below the 0.08 threshold, indicating a strong model fit and alignment with the expected conceptual framework.

Conclusion

The primary dimensions influencing the design of an indigenous intelligent command and control model based on military IoT include, in order of significance: intelligence, information management, stability, interoperability, integration, and network orientation. The anticipated outcomes of developing this model encompass the enhancement of C2 intelligence, more effective and timely decision-making, heightened defense readiness, strengthened deterrence capabilities, increased military authority and operational capacity, and the advancement of indigenous cyber power.

The model's functions extend to: the development of intelligent C2 systems at operational and strategic levels; the modernization of control, monitoring, and evaluation mechanisms; and the smart integration of communication, computing, surveillance, and identification systems. Additional functionalities include real-time battlefield data fusion, rapid and intelligent decision-making, improved operational reliability and tactical precision, heightened battlefield efficiency, automated control of military systems, and continuous situational awareness.

Key prerequisites for the implementation of this model include: battlefield intelligence integration, localization of IoT standards, security protocols for IoT software and hardware, establishment of specialized networks and infrastructures, adoption of indigenous IoT communication protocols, integration of intelligent information flows, operational continuity, allocation of financial and technical resources, and specialized training and capacity development.

References

- Anand, L. V., Kotha, M. K., Kannan, N. S., Kumar, S., Meera, M. R., Shawl, R. Q., & Ray, A. P. (2020). Design and development of IoT-based health monitoring system for military applications.
- Rezaei, M., Rashid, G., & Pourdastan, A. (2020). Components and characteristics of intelligent command and control in the battlefield. *Military Science and Technology Quarterly*, *16*(54).

- Beheshti Atashgah, M., Barari, M., Bayat, M., & Aref, M. R. (2018). IoT security concepts and challenges with a focus on the American MIOT mechanism. *Command and Control Quarterly*, *2*(3).

مقدمه

امروزه سرعت بسیار زیاد تحول علوم مختلف باعث حرکت اکثر سامانه‌ها به سمت هوشمندی و هوشمندسازی شده و باعث ایجاد نسلی از تهدیدهای نوین و جنگ‌های نوظهور و مفاهیم جدیدی همانند؛ سامانه هوشمند، ارتش هوشمند، قدرت هوشمند[1]، تهدیدات هوشمند[2]، جنگ هوشمند[3] و فرماندهی و کنترل هوشمند گردیده که ابعاد و زوایای پیچیده‌ای را از خود به نمایش گذاشته‌اند (فرزانه، ۳: ۱۴۰۱). فناوری‌های نوین، باعث ایجاد تغییرات و تحولات اساسی در سازمان‌ها، راهبردها و تدابیر امنیتی و دفاعی شده است. این تحولات فناورانه در حوزه‌های فرماندهی و کنترل که مسئولیت مدیریت و هدایت عملیات نظامی را بر عهده دارد، تأثیرات عمیقی برجای گذاشته است. بر این اساس ارتش‌های دنیا و سازمان‌های دفاعی همواره درصدد استفاده از فناوری‌های نوین و پیشرفته با هدف ارتقاء سطح تجهیزات و سامانه‌های دفاعی و هوشمند نمودن این سامانه‌ها جهت مقابله با تهدیدات هوشمند و نوین شده است. برابر اعلام آژانس دفاعی اروپا در سال ۲۰۲۱، هوش مصنوعی، کلان‌داده، اینترنت اشیاء، بلاک‌چین، رایانش ابری، رباتیک و سامانه‌های بدون سرنشین از جمله فناوری‌های نوین و پیشرفته هستند که می‌توانند تحولات شگرفی را در حوزه‌های امنیتی و دفاعی ایجاد کنند. (همان: ۲) اینترنت اشیاء متشکل از حسگرها، سامانه شناسایی و ردیابی خودکار، ارتباطات بی‌سیم، دسترسی به شبکه و سامانه‌های توزیع‌شده می‌باشد. اینترنت اشیاء فناوری نوظهوری است که در آن برای هر موجودیت امکان ارسال و دریافت داده از طریق شبکه‌های ارتباطی مختلف فراهم می‌گردد. اشیاء به هر چیزی گفته می‌شود که قابلیت جمع‌آوری داده‌ها، کنترل شدن و یا ارتباط از راه دور را داشته باشد. اینترنت اشیاء به بسیاری از کسب‌وکارها نفوذ می‌کند و ابزار ساده‌ای برای جمع‌آوری، تجزیه و تحلیل داده‌های سیستم فنی برای شناسایی و بهینه‌سازی عملکرد بسیاری از اشیاء در زندگی خصوصی و کاری ما فراهم می‌کند (Ploennigs ،2018).

با بهره‌گیری متناسب و به‌موقع از فناوری اینترنت اشیاء نظامی در دفاع هوشمند نیروهای مسلح، تا حدود زیادی می‌تواند امور متنوع نظامی را با دقت و سرعت بیشتر

[1] SMART POWER
[2] SMART THREATS
[3] SMART WAR

پیاده‌سازی و مدیریت نمود تا بحث هوشمندی تجهیزات محقق گردد. با به‌کارگیری اینترنت اشیاء در فرماندهی و کنترل هوشمند، آماد هوشمند، ترابری هوشمند، پایش محیطی، آموزش و شبیه‌سازی، ایجاد سامانه‌های کنترل آتش یکپارچه در زمین، هوا و دریا، تسلیحات هوشمند، مدیریت صحنه نبرد، پایش سلامت و بهداشت، سنجش مشارکتی در میدان نبرد، مدیریت امکانات می‌تواند به قابلیت‌های دفاعی نوین و اثربخش و در واقع به دفاع هوشمند در نیروهای مسلح کشورمان در برابر تهدیدات نوین و هوشمند دست یافت. علی‌رغم پیشرفت‌های چشمگیر به عمل‌آمده در حوزه دفاع هوشمند در نیروهای مسلح، هنوز از قابلیت‌های اینترنت اشیاء و اینترنت اشیاء نظامی به‌طور کامل و مطلوب و از قابلیت‌های فناوری‌های نوین مانند هوش مصنوعی در مراکز فرماندهی و کنترل بهره‌برداری نمی‌گردد. بنابراین دغدغه اصلی محقق، مدون نبودن الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی می‌باشد.

اهمیت طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی موجب ارتقاء توان رزم، هم‌افزایی در تصمیم‌گیری سریع و به موقع، ایجاد دستورالعمل‌ها و روش‌های جاری، بسترسازی لازم جهت ایجاد مراکز فرماندهی و کنترل یکپارچه و هوشمند، کمک به آگاهی وضعیتی میدان نبرد و جلوگیری از غفلت راهبردی و راه‌کنشی در مقابله با تهدیدات آتی می‌شود. همچنین در صورت عدم وجود الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی منجر به؛ کاهش آمادگی رزمی، عدم پاسخگویی مناسب و به موقع به تهدیدات آینده و نوظهور، اختلال و کندی در تصمیم‌گیری، غفلت راه‌کنشی و راهبردی مراکز فرماندهی و کنترل حال و آتی، کاهش سرعت دسترسی به اطلاعات مورد نیاز، عقب ماندن از حرکت بسیار سریع هوشمندسازی در جهان در برابر تهدیدات نوظهورکنترل می‌گردد.

سوال اصلی پژوهش، این است که، الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی چیست؟ سوالات فرعی پژوهش به ترتیب عبارتند از: ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی کدامند؟ روابط بین ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی چیست؟ دستاوردها، پیامدها، کارکردها و الزامات طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی کدامند؟

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

مفهوم الگو

شامل نمادهایی که ویژگی‌های بعضی از پدیده‌های تجربی شامل اجزاء و روابط بین آنها را به شکل منطقی بین مفاهیم نشان می‌دهد (خلیلی شورینی، ۱۳۸۹: ۱۳۲).

اینترنت اشیاء

اتصال اشیاء دنیای فیزیکی توسط فناوری‌های هوشمندساز نظیر شبکه‌های حسگر بیسیم، میکروچیپ‌ست‌ها، دوربین‌های هوشمند، دستگاه‌های موقعیت‌یاب جهانی و غیره اشاره دارد که به‌واسطه شبکه‌های پوشش‌دهنده مبتنی بر اینترنت، قابلیت تعامل با یکدیگر و حوزه اطرافشان را پیداکرده‌اند (Ferreira & et al, 2016: 612).

اینترنت اشیاء نظامی

امروزه، توسعه فناوری‌های مربوط به اینترنت اشیاء در حوزه نظامی بر روی کاربردهای سامانه‌های فرماندهی و کنترل[1] و سامانه کنترل آتش متمرکز شده است. این توسعه با یک نگاه غالب در حوزه نظامی می‌باشد که حسگرها و شبکه‌ها در درجه اول به‌عنوان ابزاری به‌منظور جمع‌آوری و به اشتراک‌گذاری داده در میدان جنگ دیده می‌شوند تا فرامین و کنترل مؤثرتری از دارایی‌های نظامی داشته باشند. فناوری‌های اینترنت اشیاء همچنین در برخی از کاربردها برای مدیریت آماد، آموزش و شبیه‌سازی تطبیق یافته، اما گسترش اینترنت اشیاء در حوزه نظامی محدود بوده و به‌طور ضعیفی یکپارچه‌سازی شده است (بهشتی آتشگاه، ۱۳۹۷).

دفاع هوشمند

دفاعی همه‌جانبه که ثمره همگرایی رهیافت‌های دفاعی خودی (دانش و آگاهی‌محور، شناخت محور، تأثیرمحور، غیرعامل، ناهمگون) و به دنبال همگراکردن آسیب‌های دشمن با کسب تأثیر و نفوذ راهبردی و بازدارندگی از کمترین کنش‌ها در مناسب‌ترین حوزه برای رویارویی با چالش و جنگ‌های هوشمند می‌باشد (حسن‌لو، ۱۳۹۷: ۲۸۵).

---

[1] C4ISR

جنگ‌های شبکه محور[1]

جنگ شبکه محور اجازه می‌دهد بر اساس آگاهی و دانش اشتراکی تمام عناصر از جمله نقش رده‌های پایین پررنگ‌تر شده و امکان همیاری آنها در تصمیم‌گیری فراهم گردد. اینترنت اشیاء نظامی و اینترنت میدان نبرد تجهیزات هوشمند را در یک محیط نظامی و مبتنی بر شبکه به کار می‌گیرد (Ivan et al. , 2021: 2).

فرماندهی و کنترل

اعمال قدرت، اعطای اختیار و هدایت توسط فرماندهی روی نیروهای تحت امر او به منظور اجرای مأموریت واگذاری که ترتیب، آرایش، گسترش نیروی انسانی، تجهیزات، ارتباطات، تسهیلات، امکانات و روش‌هایی را در بر می‌گیرد که توسط فرمانده در طرح‌ریزی، هدایت، ترکیب و کنترل نیروها و عملیات به منظور اجرای یک مأموریت خاص مدنظر قرار گرفته و با عنوان فرماندهی و کنترل بیان می‌شود (جواهری، ۷: ۱۳۸۹).

فرماندهی و کنترل هوشمند

هوشمندی در فرماندهی و کنترل فراهم نمودن کارکنان، تجهیزات، تسهیلات، روش‌ها و شیوه‌های لازم جهت جمع‌آوری، پردازش و توزیع اطلاعات برای تصمیم‌گیرندگان به منظور طرح‌ریزی، برنامه‌ریزی، هدایت عملیات، اعمال کنترل و نظارت می‌باشد که دارای ویژگی‌هایی همچون؛ پشتیبانی قاطع از تصمیم‌گیری، مدیریت کارآمد داده، برنامه‌ریزی سریع جهت واکنش سریع، سرعت توزیع اطلاعات، یکپارچگی(ادغام سامانه‌های فرماندهی و کنترل)، آگاهی فراگیر از فضای نبرد، فهم برتر از فضای نبرد، دانش فعال برتری تصمیم‌گیری، استفاده وسیع از فناوری جدید ICT و تعامل در زنجیره‌ی فرماندهی و کنترل می‌باشد (رضایی و همکاران، ۱۳۹۹: ۱۵۳).

کاربرد اینترنت اشیاء در سامانه‌های فرماندهی و کنترل

از حسگرهای مختلف در سامانه‌های فرماندهی و کنترل برای اطمینان از آگاهی موقعیتی از میدان نبرد استفاده می‌شود. شبکه‌ی بسیار پیچیده و گسترده شامل چندین حسگر(حسگرها در سامانه عامل‌های مختلف مانند هواپیماهای بدون سرنشین، رادارها، دوربین‌های تصویربرداری، حسگرهای مادون‌قرمز، حسگرهای زمینی بدون مراقبت، دستگاه‌های قابل‌حمل) داده‌های واقعی را برای نیروهای رزمی و تصمیم‌گیرندگان ارائه

[1] NETWORK CENTRIC WARFARE

می‌دهد. این داده‌ها را می‌توان برای تصویری مشترکی جهت پشتیبانی از تصمیم‌گیری توسط فرماندهان، هماهنگی و کنترل بهتر در منطقه عملیاتی یکپارچه استفاده نمود. این داده‌ها از طریق اینترنت اشیاء به اتاق کنترل منتقل می‌شوند. بنابراین از این سامانه برای اجرای یک رویکرد کم‌هزینه برای مدیریت دقیق، هوشمند در میدان جنگ استفاده می‌شود (Vijay, 2020).

اطلاعات در میدان نبرد

در فناوری‌های رقومی[1]، سه روند جهانی بنام هوش مصنوعی، بلاک چین و داده‌های‌کلان[2] قابل ردیابی هستند که اینترنت اشیاء در مرکزیّت این روندها قرار دارد (Kostin, 2018). تولید داده‌های گسترده جهانی، افزایش قدرت محاسباتی برای پردازش، پیشرفت تحلیل‌های کمی و الگوریتم‌های ریاضی در حوزه فناوری اطلاعات باعث شده است که یک هم‌افزایی بین داده‌های‌کلان، هوش مصنوعی و اینترنت اشیاء به وجود آید و این حوزه‌ها با هم مطرح شوند (Uzair Mehmood et al, 2019).

پیشینه‌های پژوهش

با مطالعه پروژه‌ها، رساله‌ها، مقاله‌های پژوهشی و تحقیق‌های علمی مرتبط که ارتباط بیشتری با موضوع دارند به شرح زیر می‌باشد:

حیدریان و همکار (۱۳۹۸) در مقاله‌ای به بررسی الگوی فرماندهی و کنترل هوایی در جنگ‌های آینده پرداخته که نتایج آن حاکی از آن است که؛ مؤلفه‌های الگوی فرماندهی و کنترل هوایی در جنگ‌های آینده شامل؛ چهار بعد فرماندهی و کنترل، مراقبت، رایانه و ارتباطات، اطلاعات شاناسایی و الکترونیکی به همراه ۳۱ مؤلفه زیرمجموعه در راستای در جنگ‌های آینده می‌باشد. امین‌زاده و همکاران (۱۴۰۲) در مقاله‌ای به بررسی الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مقابله با تهدیدات آینده پرداخته و نتایج آن حاکی از آن است که؛ الگوی نهایی در مجموع برای سه بعد رهبری، نظارت و عملیات، در سطح بلوغ یک، یازده مؤلفه، در سطح بلوغ دو، دوازده مؤلفه، در بلوغ سطح سوم، دوازده مؤلفه، در سطح بلوغ چهارم، نه مؤلفه و در سطح بلوغ پنجم، شش مؤلفه و در مجموع نوزده مؤلفه احصاء و ارائه گردید. الگوی بلوغ سایبری روشی است که سازمانها را قادر به تقویت برنامه امنیت سایبری، اولویت‌بندی اقدامات و

[1] DIGITAL
[2] Big Data

سرمایه‌گذاری‌های امنیت سایبری و حفظ سطح مطلوب امنیت در طول چرخه حیات سیستم‌های فناوری اطلاعات می‌نماید. بر این اساس به منظور نیل به بلوغ تاب‌آوری سایبری بایستی سه بعد راهبری، نظارت و کنترل و عملیات سامانه‌های فرماندهی و کنترل در پنج سطح انجام شده، برنامه‌ریزی‌شده، مدیریت‌شده، اندازه‌گیری شده و نهادینه‌شده) به بلوغ برسد. نسرین تاج و همکار(۱۳۹۶) در پروژه‌ای به الزامات و رویکردهای امنیتی در حوزه اینترنت اشیاء پرداخته که نتایج آن حاکی از آن است که؛ مهم‌ترین چالش، عدم وجود یک معماری امنیتی تأییدشده برای اینترنت اشیاء است. رساله دکتری حسن‌لو (۱۳۹۴) با موضوع دفاع هوشمند در نظام دفاعی جمهوری اسلامی ایران پرداخته که نتایج حاکی از آن است که؛ دفاع هوشمند زمانی به‌صورت کامل بروز و ظهور می‌یابد که در چهار مؤلفه هوشمندسازی با عناوین رهیافت، رفتار، ساختار و ادوات رعایت شده باشد. رمضانی دهقی (۱۳۹۹) در رساله‌ی دکتری با عنوان طرح راهبردی کاربست مفهوم اینترنت اشیاء در حوزه نظامی(مطالعه موردی قرارگاه پدافند هوایی خاتم‌الانبیاء(ص) آجا) پرداخته که نتایج حاکی از آن است که؛ اینترنت اشیاء در حوزه پدافند هوایی آجا به اتصال و ارتباط گسترده تجهیزات و دارایی‌های فیزیکی و کارکنان نظامی از طریق شبکه اینترنت نظامی و با بهره‌گیری از ابزارهای موجود در فناوری‌های اینترنتی اشاره دارد به نحوی که تعامل و همکاری این اشیاء و افراد به ارتقاء بهره‌وری دربخش های مختلف سازمان نظامی منجر می‌شود. زنکیوهانگ (۲۰۱۶) در رساله دکتری با عنوان پیشرفت و چارچوب هوشمندی در لبه برای سامانه‌های اینترنت اشیاء پرداخته که نتایج حاکی از آن است که؛ ویژگی‌های مهم استفاده از اینترنت اشیاء، صرفه‌جویی در انرژی، استقرار و مدیریت کارایی و کم بودن زمان تأخیر می‌باشد. درعین‌حال، مقدار زیادی از داده‌های تولیدشده توسط دستگاه‌ها، بار اضافی را در سامانه داده متمرکز و استفاده از رایانش ابری لبه برای ایجاد اطلاعات در نزدیکی داده‌ها را ضروری می‌نمایند.

رمضانی دهقی و همکاران (۱۴۰۰) در مقاله‌ای با عنوان رتبه‌بندی تهدیدهای اینترنت اشیاء در محیط نظامی پرداخته که نتایج حاکی از آن است که؛ در سازمان‌های نظامی از میان تهدیدهای فناوری اینترنت اشیاء، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها به دلایلی همچون؛ زمان کمتر جهت اثرگذاری، تأثیر کمتر بجا مانده قابل بازگشت، تأثیر بیشتر بر حوزه تصمیم‌گیری، خسارت‌های بیشتر به تجهیزات اینترنت

اشیاء و تأثیر بیشتری به نتیجه نبرد خواهند داشت. عارفی‌نژاد و همکاران (۱۳۹۹) در مقاله‌ای با عنوان بررسی کاربردهای اینترنت اشیاء نظامی در نیروهای مسلح پرداخته که نتایج حاکی از آن است که؛ کاربرد اینترنت اشیاء در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی‌بخش نظامی محسوب می‌گردد. اینترنت اشیاء توسعه حوزه نظامی را به‌طور عمده‌ای پیش خواهد برد و به‌نظر می‌رسد که به زودی شاهد شبکه‌های اینترنت اشیاء نظامی باشیم که در آن نقش انسان کم‌رنگ‌تر از قبل شده و دستگاه‌ها و جنگ‌افزارهای هوشمند با تکیه بر ارتباطات گسترده و متعاقباً توانایی تصمیم‌گیری و انجام فعالیت‌های تصمیم‌گیرانه، نقش‌آفرینی قابل ملاحظه‌ای داشته باشند. فرزین‌فرد و همکاران (۱۳۹۹) در مقاله‌ای با عنوان همگرایی اینترنت اشیاء نظامی و پزشکی و چالش‌های امنیتی پرداخته که نتایج حاکی از آن است که؛ کاربرد اینترنت اشیا در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی‌بخش نظامی محسوب می‌گردد. دوستی‌مطلق (۱۴۰۰) در مقاله‌ای با عنوان سازوکاری جدید برای ارتقاء امنیت شبکه اینترنت اشیاء نظامی با به‌کارگیری رمزنگاری کوانتومی و کلاسیک پرداخته که نتایج حاکی از آن است که؛ بخشی که از رمزنگاری کلاسیک بهره می‌برد و بخشی که از رمزنگاری کوانتومی استفاده می‌کند. با به‌کارگیری طرح جدید معرفی شده می‌توانیم با بهره‌گیری از فناوری رمزنگاری کلاسیک و کوانتومی نیازمندی‌های امنیتی مختلف در شبکه اینترنت اشیاء نظامی را برآورده کنیم. غلام‌نژاد و همکاران (۱۳۹۸) در مقاله‌ای با عنوان کاربردهای نظامی اینترنت اشیاء با تأکید بر مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران پرداخته که نتایج حاکی از آن است که؛ ارتش و اولین پاسخ‌دهندگان باید یک بستر آزمایشی برای تشخیص و آزمایش با فناوری‌هایی که می‌توانند مسیر را تغییر دهند، انجام دهند، تا به‌عنوان پیوندی بین جنگجویان در حوزه کاری و توسعه‌دهندگان اینترنت اشیاء عمل کند. ارتش باید در توسعه فنون جدید امنیتی سرمایه‌گذاری کند که می‌تواند برای دستگاه‌های محصول غیرسفارشی و برنامه‌های سازمانی، از جمله آن‌هایی که در فضای ابری میزبانی می‌شوند، اعمال شود. تمرکز باید بر روی سرمایه‌گذاری در معیارهای امنیتی مقیاس‌پذیر به جای تأمین امنیت سامانه‌های فردی باشد.

قهرمانی‌کوشان و همکار (۱۳۹۵) در مقاله‌ای با عنوان امنیت و چالش‌های پیش روی فناوری اینترنت اشیاء پرداخته که نتایج حاکی از آن است که؛ هرچند اینترنت اشیاء

دروازه بزرگ و مهمی برای ورود به دنیایی با قابلیت‌های بیشتر برای بشر بازکرده، درعین‌حال تهدیداتی بزرگ‌تر از همیشه را نیز متوجه زندگی ما کرده است. در این میان، اولین قدم برای فرار از این تهدیدات این است که هر فرد و نهادی، انفرادی خود را مسئول صیانت و حفاظت از همه اطلاعات بداند. همچنین نکته‌ای که بارها از سوی متخصصان امنیتی به آن اشاره شده، یعنی اقدامات پیشگیرانه و استفاده از عقل سلیم در برقراری ارتباطات مهم‌ترین نکته برای خنثی‌کردن این تهدیدات است. مقاله آقای توکلی و همکاران با عنوان تأثیر به‌کارگیری اینترنت اشیاء بر عملکرد سازمانی حوزه سلامت پرداخته که نتایج حاکی از آن است که؛ استفاده از اینترنت اشیاء از طریق جمع‌آوری پیوسته و دوره‌ای علائم حیاتی و پارامترهای بیماری مزمن و شایع، ارسال محتوای هوشمند به کاربر، مدیریت اطلاعات، خدمات از راه دور، پیگیری و نظارت، فعالیت زیست‌محیطی و یکپارچگی بین سازمانی، بر عملکرد سازمانی تأثیر دارد.

حاجی شاه‌کرم و همکار(۱۳۹۵) در مقاله‌ای با عنوان معماری پیشنهادی مبتنی بر اینترنت اشیاء و سامانه‌های توصیه‌گر برای هوشمندسازی شهر تهران پرداخته که نتایج حاکی از آن است که؛ پنج‌لایهٔ زیرساخت‌ها، جمع‌آوری داده‌ها، مدیریت و پردازش داده‌ها، خدمات و برنامه‌های کاربردی پیش‌بینی شده که با ایجاد نوآوری در معماری‌های متداول به‌وسیلهٔ بهره‌گیری از ایده‌های جمع‌سپاری و سامانه‌های توصیه‌گر می‌توان باعث بهبود در سامانه حمل و نقل هوشمند، سامانه‌های مدیریت انرژی هوشمند و خانه‌های هوشمند درحوزهٔ شهر هوشمند می‌شود. مهدی‌نژاد نوری و همکاران(۱۳۹۶) در مقاله‌ای با عنوان تأثیر متقابل دفاع دانش‌بنیان و جنگ‌های آینده پرداخته که نتایج حاکی از آن است که؛ با توجه به ویژگی‌های جنگ‌های آینده که دانش محوری جزء مؤلفه‌های اصلی آن محسوب می‌شود، برای مقابله راهی جز دانش‌بنیان کردن دفاع نداریم. برای محقق نمودن دفاع دانش‌بنیان، بایستی ضمن برنامه‌ریزی برای دفاع همه‌جانبه، نسبت به ارتقاء جایگاه فرماندهی و کنترل هوشمند و یکپارچه با به‌کارگیری آخرین فناوری‌ها با هدف بهره‌گیری از تمامی ظرفیت‌های دفاعی اقدام نماییم؛ به‌گونه‌ای که ضمن استفاده از تجربیات قبلی با ایجاد تحول در سامانه جمع‌آوری، تبادل و پردازش اطلاعات و تبدیل آن به دانش جدید، فرماندهان را در راستای اتخاذ تصمیمات درست، به‌موقع و اثربخش یاری رسانده و ضمن تحقق بازدارندگی دفاعی، پایداری ملی را ارتقاء دهیم.

احمدی نوروز محله و همکاران (۲۰۱۶) در مقاله‌ای با عنوان معرفی سبک‌های معماری و تحلیل کاربرد دستگاه‌ها در فناوری اینترنت اشیاء پرداخته که نتایج حاکی از آن است که، اینترنت اشیاء باعث ایجاد تغییر در روش ارتباط و سازمان‌دهی فعالیت و روند صنعتی و تجاری توسط سازمان‌ها شده و کاربرد اینترنت اشیاء بسیار وسیع است. تسنیم یوسف و همکاران (۲۰۱۵) در مقاله‌ای با عنوان امنیت اینترنت اشیاء: وضعیت فعلی، چالش‌ها و اقدامات متقابل پرداخته که نتایج حاکی از آن است که؛ وضعیت کنونی تحقیق در اینترنت اشیاء عمدتاً بر پروتکل‌های تأیید هویت و کنترل دسترسی متمرکز، اما با پیشرفت سریع فنّاوری، لازم است که پروتکل‌های شبکه‌ای جدید مانند IPv6 و v5را برای به‌دست‌آوردن پویایی در توپولوژی اینترنت اشیاء بسنجیم. مهم‌ترین نگرانی در تحقق چارچوبی کاملاً هوشمند، امنیت است. ریکو آراشی[1] (۲۰۱۷) در مقاله‌ای با عنوان سیاست دفاعی و اینترنت اشیاء پرداخته که نتایج حاکی از آن است که؛ بیشتر منابع سایبری، سیاست‌ها و رویه‌های موجود دولت در جهت دفاع از سامانه‌های نظامی و دولتی و زیرساخت‌های مهم و مسئولیت دفاع از سایر اهداف مهم اقتصادی و اجتماعی را به عهده بازیگران خصوصی می‌گذارد که ممکن است منابع لازم برای دفاع مؤثر را نداشته و سیاست‌های دفاعی کنونی در کشورهای غربی در برابر حملاتی که علیه اینترنت اشیاء با رشد سریع انجام می‌شود یا از آن ناشی می‌شود، آسیب‌پذیر هستند.

جمع‌بندی پیشینه‌های تحقیق

ویژگی‌ها و اهمیت دفاع هوشمند و ضروت به‌کارگیری اینترنت اشیاء نظامی در محیط‌های نظامی و نقش آن در ایجاد تحول در زندگی و جامعه امروزی، از نقاط اشتراک می‌باشد. هیچ تحقیقی به طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی اشاره‌ای نداشته و البته مقالات محدودی به مقوله دفاع هوشمند و توانمندی‌های اینترنت اشیاء نظامی پرداخته شده که از نقاط افتراق می‌باشد. طراحی الگوی اینترنت اشیاء نظامی در سامانه‌های فرماندهی و کنترل هوشمند بومی از نوآوری این تحقیق می‌باشد.

[1] Rieko Arashi

روش‌شناسی پژوهش

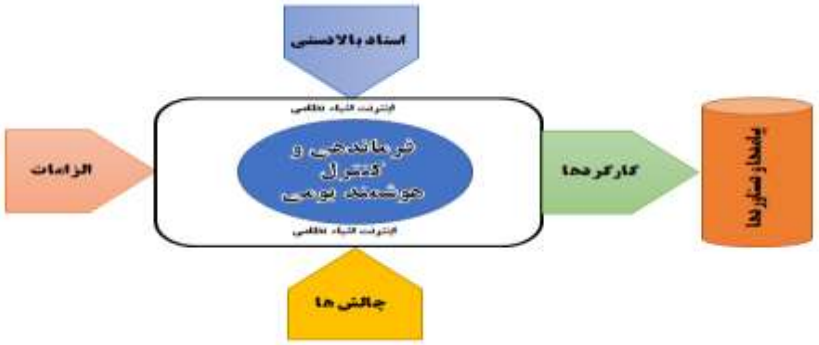
نوع تحقیق کاربردی- توسعه‌ای، روش تحقیق توصیفی- موردی زمینه‌ای، رویکرد تحقیق آمیخته(کمی و کیفی) می‌باشد. گردآوری اطلاعات به روش میدانی و کتابخانه‌ی علمی و تخصصی با ابزارهای مطالعه کتابخانه‌ای کتب و مقالات، همچنین اسناد و مدارک علمی و پژوهشی موجود و با مصاحبه و پرسش‌نامه محقق ساخته و قلمرو زمانی تحقیق از نظر جمع‌آوری داده‌ها بین سال‌های۱۴۰۲- ۱۴۰۳ و از نظر زمان مورد انتظار اجرای تحقیق از سال‌های ۱۴۰۲تا ۱۴۰۳ بوده و قلمرو زمان بهره‌برداری تحقیق تا پایدار بودن نتایج، حدود پنج سال است. قلمرو مکانی، مراکز علمی، دانشگاهی معتبر و نیروهای مسلح کشور و قلمرو موضوعی، ابعاد و مؤلفه‌های فناوری اینترنت اشیاء نظامی و فرماندهی و کنترل هوشمند بومی می‌باشد. جامعه آماری۷۰ نفر از خبرگان و صاحب‌نظران حوزه سایبری و فرماندهی و کنترل که دارای تحصیلات دانشگاهی کارشناسی ارشد و دکتری و سوابق مدیریتی و راهبردی می‌باشند. روش نمونه‌گیری هدفمند همگون، ناهمگون و گلوله برفی تا حد اشباع و با توجه به محدودیت افراد صاحب‌نظر، حجم جامعه آماری کلی تحقیق، زیر صد نفر می‌باشد بنابراین حجم نمونه بر جامعه آماری منطبق بوده و روش نمونه‌گیری به‌صورت تمام شمار می‌باشد. جهت تجزیه و تحلیل آماری و بررسی میزان رابطه و همبستگی بین عوامل احصاء شده، از مدل‌سازی معادلات ساختاری (نرم‌افزار اسمارت‌پی. ال. اس) و برای روایی محتوایی یک آزمون از روش‌های تعیین اعتبار روایی محتوایی، از ضریب لاوشه و برای ارزیابی پایایی ابزار اندازه‌گیری و مشخص نمودن میزان همبستگی مؤلفه‌های الگوی، از محاسبه ضرایب بارعاملی و همبستگی اسپیرمن و جهت سنجش پایایی مدل از آلفای کرونباخ و پایایی ترکیبی[1] اندازه‌گیری و برای روایی سازه شامل روایی همگرا، روایی واگرا، روایی مدل، روایی همگرا و روایی واگرا از طریق محاسبه پایایی اشتراکی[2] و آزمون فورنل-لارکس مورد تجزیه و تحلیل قرار گرفته است.

چارچوب نظری تحقیق

از عوامل بیرونی تاثیرگذار بر فرماندهی و کنترل هوشمند مبتنی بر اینترنت اشیاء که به عنوان عوامل مداخله‌گر بوده و حوزه‌ها، ابعاد و معیارهای آن را تحت تاثیر قرار می‌دهند

[1] COMPOSITE RELIABILITY
[2] AVERAGE VARIANCE EXTRACTED (AVE)

شامل سه مقوله ارکان جهت‌ساز، الزامات و چالش‌ها می‌باشد. ارکان جهت‌ساز، آیات و احادیث، تدابیر و بیانات مقام معظم رهبری(مدظله)، قوانین، مقررات و چارچوب‌های موجود می‌باشد. الزامات، بسترهای مورد نیاز، نیازمندی‌های اعتباری و انسانی و استانداردهای امنیتی و فناوری لازم می‌باشد. چالش‌ها، موانع و مشکلات پیش‌رو را از جنبه‌ها و زوایای مختلف که در فرایند پیاده‌سازی و اجرای الگوی فرماندهی و کنترل هوشمند در نیروهای مسلح جمهوری اسلامی ایران می‌باشد، بنابراین چارچوب نظری تحقیق به شرح ذیل می‌باشد.



شکل (۱) مدل مفهومی تحقیق

تجزیه و تحلیل داده‌ها

جهت احصای ابعاد و مؤلفه‌های الگوی به‌کارگیری اینترنت اشیاء نظامی در سامانه‌های فرماندهی و کنترل هوشمند بومی با مطالعه اکتشافی و مصاحبه‌های انجام شده، ۱۰۰ عامل مؤثر الگو در سه حوزه سخت افزاری، نرم‌افزاری و انسان افزاری استخراج و با هدف اطمینان از تأثیر این عوامل تمامی عوامل احصاء شده در جلسات خبرگی با اساتید مورد ارزیابی قرار گرفت و پس از ترکیب و اصلاح عوامل مؤثر و اعمال نظر اساتید، چهل عامل نهایی به دست آمد.

جدول(۱) مقوله‌ها و مفاهیم طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی

مقوله‌ها	مفاهیم	کدها
سخت افزاری	شبکه محوری	فرماندهی و کنترل، حساسه‌های اپتیکی، حساسه‌های الکترواپتیکی، حساسه‌های اطلاعات سیگنالی (اطلاعات ارتباطی و اطلاعات الکترونیکی)، حساسه‌های اطلاعات تصویری، حساسه‌های اطلاعات سنجشی و علائمی(مسینت)، فضای سایبری بومی، شبکه‌های ارتباطی، شبکه‌های مخابراتی، داده‌پردازی، زیرساخت فیبرنوری، ارتباطات راه‌کنشی، پهپاد، میکروپهپاد، اینترنت اشیاء نظامی، ربات نظامی، کنترل آتش هوشمند، زیرساخت‌های جنگ شبکه محور، شبکه سامانه‌های سلاح، شبکه راداری، مراکز سوئیچینگ، شبکه‌های رادیویی، سامانه‌های پشتیبان سامانه‌ها، پروتکل‌ها، سکوهای بومی.
	هوشمندسازی	فرماندهی و کنترل هوشمند، لینک داده، سامانه کنترل آتش هوشمند، سامانه‌های آگاهی وضعیتی هوشمند، سامانه‌های یادگیری ماشینی، سامانه‌های دفاع سایبری هوشمند، سامانه‌های پایش هوشمند، سامانه کنترل از راه دور هوشمند، شناسایی و مراقبت هوشمند، سامانه کنترل هوشمند، سامانه‌های تحلیل داده، سامانه‌های جنگ سایبرالکترونیک هوشمند، سامانه‌های پیش‌بینی و کنترل هوشمند، سامانه‌های راداری و سلاح‌های هوشمند، سامانه‌های بدون سرنشین هوشمند، سامانه‌های آموزش هوشمند، سامانه اعلام خبرو خطر هوشمند، سامانه کنترل انرژی هوشمند.
انسان افزاری	یکپارچگی[1]	آموزش تخصصی، کارکنان متخصص، تخصص‌های مرتبط اینترنت اشیاء نظامی و فرماندهی و کنترل، ساختار سازمانی فناورپایه، چارچوب‌های سازمان، کاربران، استعداد کارکنان، فرهنگ سازمانی، هرم نیروی انسانی در سازمان، فرهنگ سازمانی، دانش و مهارت کارکنان.
	تعامل‌پذیری	نظام حکمرانی، قوانین و مقررات فرماندهی و کنترل کشوری، قوانین و مقررات فرماندهی و کنترل لشکری، اسناد بالادستی ملی، اسناد بالادستی نیروهای مسلح، فرماندهی و کنترل سایبری صحنه نبرد، مقررات نظامی، رویکرد دولت‌ها، رگولاتوری و حقوق و قوانین.
نرم افزاری	مدیریت اطلاعات	نیازمندی اطلاعات، جمع‌آوری اطلاعات، پردازش اطلاعات، تجزیه و تحلیل اطلاعات، مدیریت و هدایت اطلاعات، تبادل اطلاعات، ادغام اطلاعات، ذخیره‌سازی اطلاعات، چرخه اطلاعات، طبقه‌بندی اطلاعات، عصر اطلاعات، مدیریت دانش، جنگ شناختی، فریب اطلاعاتی، جنگ اطلاعاتی.

[1] Integration

مقوله‌ها	مفاهیم	کدها
	پایداری	امنیت اطلاعات سامانه‌های اینترنت اشیاء نظامی، امنیت سامانه‌های فرماندهی و کنترل، پدافند غیرعامل در فرماندهی و کنترل، استتار اطلاعات، پنهان‌نگاری، خفیفه‌نگاری، کدگذاری، رمزنگاری، محرمانگی، کنترل امنیتی، سامانه‌های کنترلی، یکپارچه‌سازی، دسترسی، کنترل دسترسی، رصد و پایش، احراز هویت، امنیت شبکه‌ها و زیرساخت‌ها، امنیت و پایداری سخت‌افزاری، امنیت و پایداری نرم‌افزاری، تیم امداد سایبری، حریم خصوصی، اعتماد، عدم انکار.

پس از بهره‌گیری از نظرات خبرگان و صاحب‌نظران، در نهایت شش بعد و ۴۰ مؤلفه مرتبط با ابعاد مورد نظر احصاء گردید که در جدول زیر نشان داده شده‌اند.

جدول(۲) مفاهیم، ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی

مفهوم	ابعاد	مولفه‌ها
الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی	شبکه‌محوری	شبکه رادار‌ی-سلاح‌های هوشمند-حساسه‌های جمع‌آوری اطلاعات(اپتیکی، سیگنالی، تصویری، سنجشی و علائمی)- فضای سایبری بومی- مراکز داده پردازی- شبکه‌های ارتباطی امن و پایدار باسیم و بی‌سیم- پروتکل‌ها بومی- اینترنت اشیاء نظامی.
	هوشمندسازی	هوش مصنوعی در فرماندهی و کنترل- هوش مصنوعی در تحلیل داده- سامانه‌های دفاع سایبری هوشمند- سامانه‌های اینترنت اشیاء - سامانه‌های هوشمند پشتیبان سامانه- جنگ سایبرالکترونیک هوشمند- سامانه‌های کنترل هوشمند- سامانه‌های دفاع هوشمند- سامانه‌های آگاهی وضعیتی هوشمند- سامانه‌های بدون سرنشین مبتنی بر هوش مصنوعی - سامانه‌های آموزش هوشمند مبتنی بر هوش مصنوعی.
	یکپارچگی	آموزش تخصصی- کارکنان متخصص- ساختار سازمانی فناورپایه- فرهنگ سازمانی- دانش و مهارت کارکنان.
	مدیریت اطلاعات	پردازش و تجزیه و تحلیل اطلاعات-مدیریت و هدایت اطلاعات- تبادل اطلاعات- ادغام اطلاعات-ذخیره‌سازی اطلاعات.
	تعامل پذیری	نظام حکمرانی- قوانین و مقررات فرماندهی و کنترل لشکری - قوانین و مقررات فرماندهی و کنترل کشوری- رگولاتوری و حقوق و قوانین.
	پایداری	پدافند غیرعامل در فرماندهی و کنترل- امنیت سامانه‌های فرماندهی و کنترل- امنیت اطلاعات سامانه‌های اینترنت اشیاء نظامی- رصد و پایش- کنترل دسترسی- امنیت شبکه‌ها و زیرساخت‌ها- امنیت و پایداری سخت‌افزاری - امنیت و پایداری نرم‌افزاری.

تجزیه و تحلیل آماری ابعاد و مؤلفه‌ها

با هدف بررسی میزان تأثیر ابعاد و مولفه‌های احصاء شده از پرسش‌نامه محقق ساخته مبتنی بر طیف لیکرت استفاده و پس از بررسی روایی و پایایی نتایج عبارتند از:

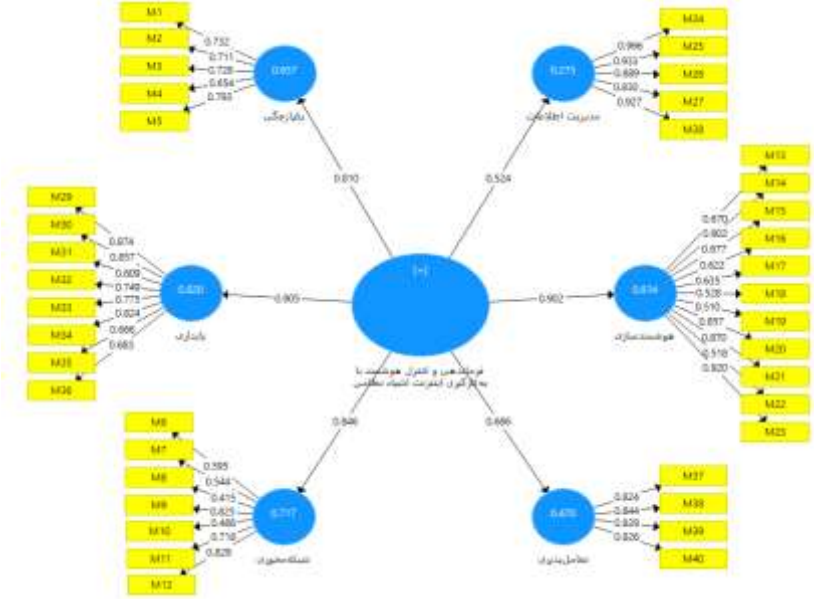
[1] Survivability

الف- روایی و پایایی ابزار اندازه‌گیری

از روایی صوری و محتوایی جهت روایی پرسشنامه استفاده و همچنین با هدف تضمین روایی محتوایی و ارزیابی میزان هماهنگی محتوای ابزار اندازه‌گیری توسط پرسش‌نامه با هدف مورد نظر از قضاوت ۱۲نفر از متخصصین و خبرگان استفاده گردید. معیار ارزیابی روایی محتوایی ضریب نسبی[1] است. بر اساس جدول لاشه حداقل مقدار ضریب محتوایی قابل قبول با توجه به تعداد متخصصان ۵۹٪ در نظر گرفته شد، بر این اساس سوالات با ضریب CVR پایین‌تر از این مقدار قبل از اجرای آزمون حذف و در مرحله آخر پرسش‌نامه نهایی که گویه‌های آن شامل شش بعد و ۴۰ مؤلفه مهم است بین جامعه آماری توزیع و پس از دریافت جواب‌های پرسش‌نامه نسبت به تحلیل آماری یافته‌های تحقیق از نرم‌افزارSmart PLS استفاده گردید.

ب- برازش مدل اندازه‌گیری

ضرایب بار عاملی مورد قبول برای هر شاخص مقادیر بیشتر از ۰/۴می‌باشد. پس از اجرای نرم‌افزار PLS Algorithm، ضرایب بار عاملی تمام مؤلفه‌ها بالاتر از ۰/۴ به دست آمد و برازش مدل اندازه‌گیری کلی نیز مورد تأیید مطابق شکل زیر قرار گرفت.



[1] Content Validity Ratio (CVR)

شکل(۱)ضرایب بار عاملی مؤلفه‌های الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی

پ-سنجش پایایی

برای سنجش پایایی مدل از بارهای عاملی آلفای کرونباخ و پایایی ترکیبی اندازه‌گیری می‌شود. در صورتی که مقدار پایایی ترکیبی برای هر سازه بیشتر از ۰/۷شود علیرغم وجود ضرایب آلفای کرونباخ کمتر از ۰/۷پایداری درونی مدل اندازه‌گیری مناسب استنباط می‌شود.

جدول(۳) آزمون‌های پایایی مدل

ابعاد	تعداد گویه	آلفای کرونباخ	همبستگی اسپیرمن	پایایی ترکیبی	پایایی اشتراکی
شبکه محوری	۷	۰/۷۵۲	۰/۸۷۲	۰/۸۴۰	۰/۶۷۱
هوشمندسازی	۱۱	۰/۸۴۵	۰/۸۲۳	۸۰۲ .۰	۰/۹۵۲
یکپارچگی	۵	۰/۸۶۷	۹۲۱ .۰	۰/۸۵۹	۰/۸۰۲
مدیریت اطلاعات	۵	۰/۷۴۷	۰/۹۶۱	۰/۷۹۳	۰/۶۶۶
تعامل پذیری	۴	۰/۸۳۴	۰/۹۳۳	۰/۷۴۴	۰/۸۶۷
پایداری	۸	۰/۸۴۸	۰/۷۲۱	۰/۸۷۷	۰/۵۶۷

آزمون آلفای‌کرونباخ: ضرایب آلفای کرونباخ برای متغیرهای تحقیق، بالای ۰/۷است، بنابراین پایایی مدل تأیید می‌شود.

آزمون همبستگی اسپیرمن بین سوالات هر متغیر: تمامی ضرایب اسپیرمن بالای ۰/۷ هستند بنابراین پایایی بر اساس آزمون(Rho-a) نیز تأیید می‌شود.

آزمون پایایی ترکیبی(CR): کلیه ضرایب پایایی ترکیبی برای متغیرهای پژوهش بالای ۰/۷است و پایایی مدل تأیید می‌شود.

آزمون پایایی اشتراکی(AVE)[1]: برای همه متغیرها میانگین شاخص‌های اشتراکی سوالات بالای ۰/۵ است بنابراین پایایی بر اساس این آزمون تأیید می‌شود.

روایی همگرا با متوسط واریانس استخراج شده: چون مقادیر متوسط واریانس استخراج شده همه متغیرها در جدول، بیشتر از ۰/۵ است در نتیجه همگرایی مدل اندازه‌گیری، مناسب ارزیابی می‌شود.

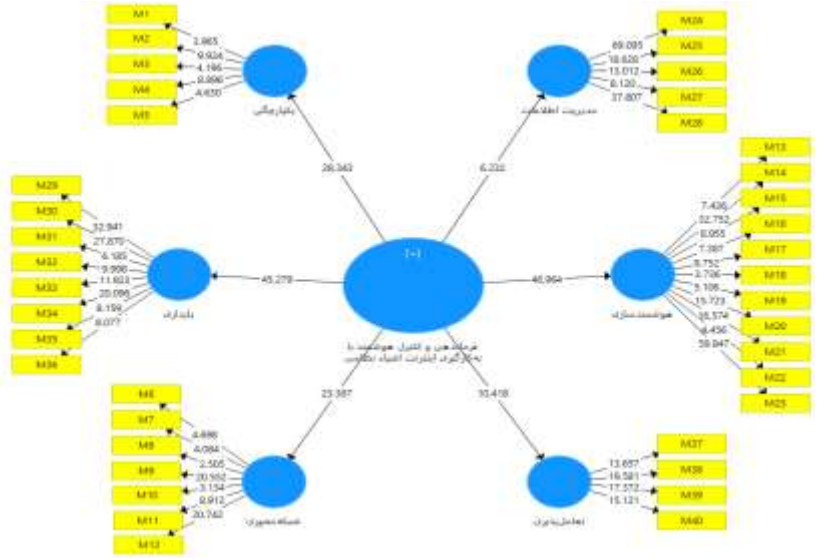
[1] Average Variance Extracted

روایی واگرا: چون جذر مقدار متوسط واریانس استخراج شده برای هر متغیر یعنی قطر جدول از مقدار ضرایب همبستگی آن متغیر با سایر متغیرها (مقادیر مندرج در زیر و سمت راست همان مقدار در ستون) بیشتر است روایی واگرا، قابل قبول ارزیابی می‌شود.

جدول(۴) ماتریس فورنل - لارکر

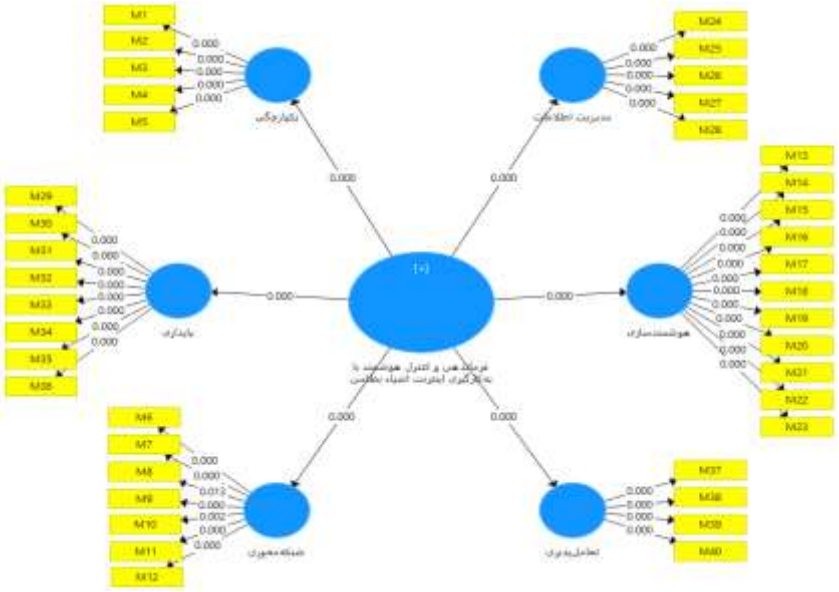
ابعاد	شبکه محوری	هوشمندسازی	یکپارچگی	مدیریت اطلاعات	تعامل پذیری	پایداری
شبکه محوری	۰/۸۷۱					
هوشمندسازی	۰/۶۵۲	۰/۸۸۳				
یکپارچگی	۰/۶۴۵	۰/۶۴۲	۰/۶۸۹			
مدیریت اطلاعات	۰/۶۷۶	۰/۶۶۱	۰/۶۹۶	۰/۷۶۵		
تعامل پذیری	۰/۳۲۱	۰/۳۲۴	۰/۱۱۲	۰/۳۲۱	۰/۵۷۸	
پایداری	۰/۶۵۲	۰/۲۷۴	۰/۳۱۴	۰/۲۲۳	۰/۲۴۱	۰/۶۵۴

برازش مدل ساختاری: ضرایب معنی‌داری به دست آمده از ۱/۹۶ بیشتر است، بنابراین در سطح اطمینان ۵٪ همبستگی‌های مشاهده شده معنی‌دار است.



شکل(۲) محاسبه ضرایب معناداری (T-Value) به شیوه بوت استرپینگ

چون همه مقادیر ضرایب معناداری Z، بیشتر از ۱/۹۶می‌باشد، رابطه بین متغیرها تأیید می‌شود.



شکل(۳) محاسبه سطح معناداری (P-Value) به شیوه بوت استرپینگ

با محاسبه ضرایبZ برای مولفه‌ها و ابعاد و تفسیر نتایج آن از این ضرایب می‌توان برای رتبه‌بندی متغیرهای تحقیق استفاده نمود.

جدول(۵) رتبه‌بندی ابعاد الگوی پژوهش بر اساس ضرایب معناداری (T-Value)

ابعاد	T-Value	رتبه
شبکه محوری	۲۳/۶۷	۴
هوشمندسازی	۴۶/۹۶۴	۱
یکپارچگی	۲۸/۳۴۳	۳
مدیریت اطلاعات	۶/۲۲۲	۶
تعامل پذیری	۱۰/۴۱۸	۵
پایداری	۴۵/۲۷۹	۲

بعد «هوشمندسازی»رتبه اول و بعد «مدیریت اطلاعات» رتبه آخر را دارد.

جدول(۶) رتبه‌بندی مؤلفه‌های بعد« شبکه محوری » بر اساس ضرایب معناداری (T-Value)

مؤلفه	ضریب T-Value	رتبه
فضای سایبری بومی	۲۰/۷۴۲	۱
حساسه‌های جمع‌آوری اطلاعات(اپتیکی، سیگنالی، تصویری، سنجشی و علائمی)	۲۰/۵۵۲	۲
مراکز داده پردازی	۸/۹۱۲	۳
شبکه‌های ارتباطی امن و پایدار باسیم و بی‌سیم	۴/۶۹۸	۴

زیرساخت‌های جنگ شبکه محور	۴/۰۸۴	۵
پروتکل‌ها بومی	۳/۱۳۴	۶
شبکه راداری و سلاح‌های هوشمند	۲/۵۰۵	۷

مؤلفه« فضای سایبر بومی» رتبه اول و مؤلفه« شبکه راداری و سلاح‌های هوشمند» رتبه آخر را در میان مؤلفه‌های بعد « شبکه محوری» دارد.

جدول(۷) رتبه‌بندی مؤلفه‌های بعد «هوشمندسازی» بر اساس ضرایب معناداری (T-Value)

مؤلفه	ضریب T-Value	رتبه
سامانه‌های کنترل هوشمند	۵۹/۸۴۶	۱
سامانه‌های دفاع سایبری هوشمند	۳۲/۷۵۲	۲
سامانه‌های آگاهی وضعیتی هوشمند	۱۶/۵۷۴	۳
اینترنت اشیاء نظامی	۱۵/۷۲۳	۴
هوش مصنوعی در فرماندهی و کنترل	۸/۹۵۵	۵
سامانه‌های هوشمند پشتیبان سامانه	۸/۷۵۲	۶
سامانه‌های دفاع هوشمند	۷/۴۳۶	۷
جنگ سایبرالکترونیک هوشمند	۷/۳۸۷	۸
سامانه‌های آموزش هوشمند مبتنی بر هوش مصنوعی	۵/۱۰۶	۹
هوش مصنوعی در تحلیل داده	۴/۴۵۶	۱۰
سامانه‌های بدون سرنشین مبتنی بر هوش مصنوعی	۳/۷۳۶	۱۱

با توجه به نتایج بدست آمده مؤلفه « سامانه‌های کنترل هوشمند » رتبه اول و مؤلفه «سامانه‌های بدون سرنشین مبتنی بر هوش مصنوعی» رتبه آخر را در میان مؤلفه‌های بعد «هوشمندسازی» دارد.

جدول (۸) رتبه‌بندی مؤلفه‌های بعد «یکپارچگی» بر اساس ضرایب معناداری (T-Value)

مؤلفه	ضریب T-Value	رتبه
کارکنان متخصص	۹/۹۲۴	۱
دانش و مهارت کاربران	۸/۸۹۶	۲
فرهنگ سازمانی	۴/۶۳۰	۳
آموزش تخصصی	۴/۱۹۶	۴
ساختار سازمانی فناورپایه	۳/۹۶۵	۵

مؤلفه«کارکنان متخصص» رتبه اول و مؤلفه«ساختار سازمانی فناورپایه» رتبه آخر را در میان مؤلفه‌های بعد «یکپارچگی» دارد.

جدول(۹) رتبه‌بندی مؤلفه‌های بعد«مدیریت‌اطلاعات» بر اساس ضرایب معناداری (**T-Value**)

مؤلفه	ضریب T-Value	رتبه
مدیریت و هدایت اطلاعات	۶۹/۰۹۵	۱
ذخیره‌سازی اطلاعات	۳۷/۸۰۷	۲
پردازش و تجزیه و تحلیل اطلاعات	۱۸/۶۲۸	۳
ادغام اطلاعات	۱۳/۰۱۲	۴
تبادل اطلاعات	۸/۱۲۰	۵

مؤلفه «مدیریت و هدایت اطلاعات» رتبه اول و مؤلفه «تبادل اطلاعات» رتبه آخر را در میان مؤلفه‌های بعد «مدیریت اطلاعات» دارد.

جدول(۱۰) رتبه‌بندی مؤلفه‌های بعد«تعامل‌پذیری بر اساس ضرایب معناداری (T-Value)

مؤلفه	ضریب T-Value	رتبه
قوانین و مقررات فرماندهی و کنترل لشگری	۱۹/۵۸۱	۱
رگولاتوری و حقوق و قوانین	۱۷/۳۷۲	۲
نظام حکمرانی	۱۵/۱۲۱	۳
قوانین و مقررات فرماندهی و کنترل کشوری	۱۳/۶۵۷	۴

با توجه به نتایج بدست آمده در جدول فوق از دیدگاه جامعه آماری مؤلفه «قوانین و مقررات فرماندهی و کنترل لشگری» رتبه اول را دارد و مؤلفه«قوانین و مقررات فرماندهی و کنترل کشوری» رتبه آخر را در میان مؤلفه‌های بعد«تعامل‌پذیری دارد.

جدول(۱۱) رتبه‌بندی مؤلفه‌های بعد«پایداری» بر اساس ضرایب معناداری (T-Value)

مؤلفه	ضریب T-Value	رتبه
امنیت سامانه‌های فرماندهی و کنترل	۳۲/۹۴۱	۱
امنیت اطلاعات سامانه‌های اینترنت اشیاء نظامی	۲۷/۸۷۰	۲
امنیت و پایداری نرم‌افزاری	۲۰/۰۹۶	۳
امنیت و پایداری سخت‌افزاری	۱۱/۹۲۳	۴
امنیت شبکه‌ها و زیرساخت‌ها	۹/۹۹۸	۵
رصد و پایش	۸/۱۵۹	۶
کنترل دسترسی	۸/۰۷۷	۷
پدافند غیرعامل در فرماندهی و کنترل	۶/۱۸۵	۸

با توجه به نتایج بدست آمده مؤلفه « امنیت سامانه‌های فرماندهی و کنترل» رتبه اول و مؤلفه «پدافند غیرعامل در فرماندهی و کنترل» رتبه آخر را در میان مؤلفه‌های بعد «پایداری» دارد.

آزمون همگنی: اگر بارهای عاملی بیشتر ۰/۷باشد سوالات آن متغیر همگن و از یک جنس و در صورتی که سؤالی مقدار معین را نداشت باید از مدل حذف می‌شود. به این فرایند تحلیل عامل تأییدی گفته می‌شود. تا مطمئن شود سوالات یک متغیر دقیقاً همان متغیر را می‌سنجد و هم‌جنس با همان مجموعه است. این آزمون در جدول زیر نشان داده شده است.

جدول(۱۲) آزمون همگن بودن

مولفه / ابعاد	شبکه محوری	هوشمندسازی	یکپارچگی	مدیریت اطلاعات	تعامل پذیری	پایداری
شبکه‌های ارتباطی امن و پایدار باسیم و بی‌سیم	۰/۸۶۶					
شبکه راداری و سلاح‌های هوشمند	۰/۷۶۵					
حساسه‌های جمع‌آوری اطلاعات(اپتیکی، سیگنالی، تصویری، سنجشی و علائمی)	۰/۸۷۶					
پروتکل‌ها بومی	۰/۷۴۱					
مراکز داده پردازی	۰/۸۱۴					
فضای سایبری بومی	۰/۸۹۷					
سامانه‌های دفاع هوشمند		۰/۸۴۷				
سامانه‌های دفاع سایبری هوشمند		۰/۸۷۶				
هوش مصنوعی در فرماندهی و کنترل		۰/۸۴۵				
جنگ سایبرالکترونیک هوشمند		۰/۸۰۹				
سامانه‌های هوشمند پشتیبان سامانه		۰/۸۸۸				
سامانه‌های بدون سرنشین مبتنی بر هوش مصنوعی		۰/۷۸۹				
سامانه‌های آموزش هوشمند مبتنی بر هوش مصنوعی		۰/۷۶۸				
اینترنت اشیاء نظامی		۰/۷۸۹				
سامانه‌های آگاهی وضعیتی هوشمند		۰/۷۶۵				
هوش مصنوعی در تحلیل داده		۰/۸۹۷				
سامانه‌های کنترل هوشمند		۰/۷۸۴				
ساختار سازمانی فناورپایه			۰/۷۸۸			
کارکنان متخصص			۰/۹۹۱			
آموزش تخصصی			۰/۹۰۶			
دانش و مهارت کاربران			۰/۷۲۳			

فرهنگ سازمانی			۰/۷۶۸			
مدیریت و هدایت اطلاعات				۰/۹۹۴		
پردازش و تجزیه و تحلیل اطلاعات				۰/۷۸۹		
ادغام اطلاعات				۰/۸۶۵		
تبادل اطلاعات				۰/۷۰۰		
ذخیره‌سازی اطلاعات				۰/۸۰۹		
قوانین و مقررات فرماندهی و کنترل لشکری					۰/۹۰۳	
قوانین و مقررات فرماندهی و کنترل کشوری					۰/۸۹۹	
رگولاتوری و حقوق و قوانین					۰/۷۳۰	
نظام حکمرانی					۰/۷۶۸	
امنیت سامانه‌های فرماندهی و کنترل						۰/۷۱۱
امنیت اطلاعات سامانه‌های اینترنت اشیاء نظامی						۰/۸۴۳
پدافند غیرعامل در فرماندهی و کنترل						۰/۷۹۹
امنیت شبکه‌ها و زیرساخت‌ها						۰/۸۰۹
امنیت و پایداری سخت‌افزاری						۰/۷۲۹
امنیت و پایداری نرم‌افزاری						۰/۸۸۸
رصد و پایش						۰/۷۵۵
کنترل دسترسی						۰/۹۸۷

آزمون کلی مدل پی. ال. اس: در آزمون SRMR (ریشه میانگین‌های مجذور خطاهای باقی‌مانده)، اگر SRMR کوچک‌تر از ۰/۰۸ باشد بنابراین مدل کلیPLS برازش مناسبی دارد یعنی با مدل مورد نظر در جامعه تطابق دارد.

جدول (۱۳) آزمون کلی مدل پی ال اس

Fit Summary		
	Saturated Model	Estimated Model
SRMR	۰/۱۶۳	۰/۰۶۸

SRMR کوچک‌تر از ۰/۰۸است بنابراین مدل کلی پی ال اس برازش مناسبی دارد یعنی با مدل مورد نظر در جامعه تطابق دارد.

نتیجه‌گیری و پیشنهادها

الف- پاسخ به سؤالات تحقیق

پاسخ به سؤال اول فرعی تحقیق: ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی کدام‌اند؟ ابعاد و مؤلفه‌ها در جدول ذیل بیان شده است:

جدول(۱۴) ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمندبومی با به‌کارگیری اینترنت اشیاء نظامی

مفهوم	ابعاد	مؤلفه‌ها	ضریب اطمینان	بار عاملی
فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی	شبکه محوری	شبکه‌های ارتباطی امن و پایدار باسیم و بی‌سیم	۰/۹۹	۰/۵۹۵
		زیرساخت‌های جنگ شبکه محور	۰/۹۹	۰/۵۴۴
		شبکه راداری و سلاح‌های هوشمند	۰/۹۹	۰/۴۱۵
		حساسه‌های جمع‌آوری اطلاعات(اپتیکی، سیگنالی، تصویری، سنجشی و علائمی)	۰/۹۹	۰/۸۲۵
		پروتکل‌ها بومی	۰/۹۹	۰/۴۶۶
		مراکز داده پردازی	۰/۹۹	۰/۷۱۸
		فضای سایبری بومی	۰/۹۹	۰/۸۲۹
	هوشمندسازی	سامانه‌های دفاع هوشمند	۰/۹۹	۰/۶۷۰
		سامانه‌های دفاع سایبری هوشمند	۰/۹۹	۰/۹۰۲
		هوش مصنوعی در فرماندهی و کنترل	۰/۹۹	۰/۶۷۷
		جنگ سایبرالکترونیک هوشمند	۰/۹۹	۰/۶۲۲
		سامانه‌های هوشمند پشتیبان سامانه	۰/۹۹	۰/۶۳۵
		سامانه‌های بدون سرنشین مبتنی بر هوش مصنوعی	۰/۹۹	۰/۵۲۸
		سامانه‌های آموزش هوشمند مبتنی بر هوش مصنوعی	۰/۹۹	۰/۵۱۰
		اینترنت اشیاء نظامی	۰/۹۹	۰/۸۵۷
		سامانه‌های آگاهی وضعیتی هوشمند	۰/۹۹	۰/۸۷۰
		هوش مصنوعی در تحلیل داده	۰/۹۹	۰/۵۱۸
		سامانه‌های کنترل هوشمند	۰/۹۹	۰/۹۲۰
	یکپارچگی	ساختار سازمانی فناورپایه	۰/۹۹	۰/۷۳۲
		کارکنان متخصص	۰/۹۹	۰/۷۱۱
		آموزش تخصصی	۰/۹۹	۰/۷۲۸
		دانش و مهارت کاربران	۰/۹۹	۰/۶۵۴

مفهوم	ابعاد	مؤلفه‌ها	ضریب اطمینان	بار عاملی
		فرهنگ سازمانی	۰/۹۹	۰/۷۹۳
	مدیریت اطلاعات	مدیریت و هدایت اطلاعات	۰/۹۹	۰/۹۶۶
		پردازش و تجزیه و تحلیل اطلاعات	۰/۹۹	۰/۹۳۳
		ادغام اطلاعات	۰/۹۹	۰/۸۸۹
		تبادل اطلاعات	۰/۹۹	۰/۸۳۰
		ذخیره‌سازی اطلاعات	۰/۹۹	۰/۹۲۷
	تعامل پذیری	قوانین و مقررات فرماندهی و کنترل لشکری	۰/۹۹	۰/۸۲۴
		قوانین و مقررات فرماندهی و کنترل کشوری	۰/۹۹	۰/۸۴۴
		رگولاتوری و حقوق و قوانین	۰/۹۹	۰/۸۲۹
		نظام حکمرانی	۰/۹۹	۰/۸۲۶
	پایداری	امنیت سامانه‌های فرماندهی و کنترل	۰/۹۹	۰/۸۷۴
		امنیت اطلاعات سامانه‌های اینترنت اشیاء نظامی	۰/۹۹	۰/۸۵۷
		پدافند غیرعامل در فرماندهی و کنترل	۰/۹۹	۰/۶۰۹
		امنیت شبکه‌ها و زیرساخت‌ها	۰/۹۹	۰/۷۴۹
		امنیت و پایداری سخت‌افزاری	۰/۹۹	۰/۷۷۵
		امنیت و پایداری نرم‌افزاری	۰/۹۹	۰/۸۲۴
		رصد و پایش	۰/۹۹	۰/۶۶۶
		کنترل دسترسی	۰/۹۹	۰/۶۸۳

پاسخ به سؤال دوم فرعی تحقیق: روابط بین ابعاد و مؤلفه‌های طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی چیست؟ روابط بین ابعاد و مؤلفه‌های مطابق با الگوی نهایی تحقیق می‌باشد که در الگو قابل ملاحظه می‌باشد.

پاسخ به سؤال سوم فرعی تحقیق: دستاوردها، پیامدها، کارکردها و الزامات طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی چیست؟

الف-دستاوردها و پیامدهای طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی عبارتند از:

۱.ارتقاء هوشمندسازی فرماندهی و کنترل

۲. ارتقاء تصمیم‌گیری و تصمیم‌سازی

۳.ارتقاء آمادگی همه جانبه دفاعی

۴.ارتقاء بازدارندگی

۵.افزایش اقتدار و توانمندی نظامی

۶.افزایش قدرت سایبری بومی

ب- کارکردها طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی عبارتند از؛

۱.هوشمندسازی سامانه‌های فرماندهی در کلیه سطوح راه‌کنشی و راهبردی

۲.هوشمندسازی سامانه‌های کنترل، نظارت و ارزیابی

۳.هوشمندسازی سامانه‌های ارتباطی

۴.هوشمندسازی سامانه‌های رایانه‌ای و فضای سایبری

۵.هوشمندسازی سامانه‌های جمع‌آوری اطلاعات

۶.هوشمندسازی سامانه‌های مراقبت و شناسایی

۷.هوشمندسازی، اشتراک‌گذاری و یکپارچگی سامانه‌ها و حساسه‌های میدان نبرد

۸.تجزیه و تحلیل‌های برخط و تصمیم‌گیری هوشمند و سریع

۹.هوشمندسازی، افزایش اطمینان و دقت عملیات و تاکتی‌ک‌ه‌ای نظامی

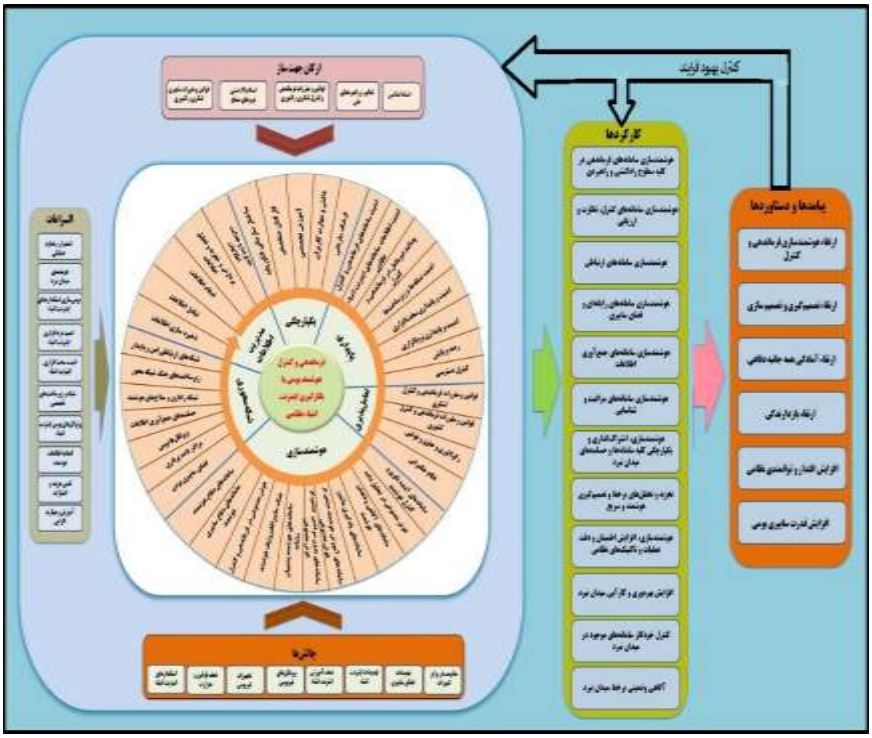
۱۰. افزایش بهره‌وری و کارآیی میدان نبرد

۱۱. کنترل خودکار سامانه‌های موجود در میدان نبرد

۱۲. آگاهی وضعیتی برخط میدان نبرد

ج- الزامات طراحی الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی شامل؛ هوشمندی میدان نبرد، بومی‌سازی استانداردهای اینترنت اشیاء، امنیت نرم افزاری اینترنت اشیاء، امنیت سخت افزاری اینترنت اشیاء، شبکه و زیرساخت‌های تخصصی، پرتکل‌های بومی اینترنت اشیاء، ادغام اطلاعات هوشمند، استمرار و تداوم عملیات، تامین هزینه و اعتبارات، آموزش و مهارت افزایی می‌باشد.

پاسخ به سؤال اصلی تحقیق: الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی چیست؟ الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی با توجه به تمامی عوامل تأثیرگذار بشرح ذیل می‌باشد:



شکل (۴) الگوی فرماندهی و کنترل هوشمند بومی با به‌کارگیری اینترنت اشیاء نظامی (برمبنای ابعاد، مولفه‌ها، کارکردها و پیامدها)

پیشنهادها

الف- پیشنهادهای اجرایی

۱. پیاده‌سازی الگوی فرماندهی و کنترل یکپارچه و هوشمند بومی کشور در بین سازمان‌های نظامی و غیرنظامی.

۲. پیاده‌سازی الگوی فرماندهی و کنترل یکپارچه و هوشمند بومی کشور در بین نیروهای مسلح جمهوری اسلامی ایران (آجا- سپاه- فراجا- ودجا).

۳. پیاده‌سازی، نهادینه‌سازی و فرهنگ‌سازی قوانین و مقرارت یکپارچه‌سازی فرماندهی و کنترل هوشمند بومی کشور در بین نیروهای مسلح جمهوری اسلامی ایران.

۴. پیاده‌سازی الگوی فرماندهی و کنترل یکپارچه و هوشمند بومی در بین نیروهای چهارگانه آجا.

۵. هوشمندسازی آماد و پشتیبانی آجا با استفاده از فناوری اینترنت اشیاء.

۶. هوشمندسازی بهداشت و درمان با استفاده از فناوری اینترنت اشیاء در بین سازمان‌های نظامی و غیرنظامی.

۷. هم‌افزایی بین دانشگاه‌های نظامی، غیرنظامی،بخش صنعت و وزارت دفاع در طراحی، ساخت و به‌کارگیری زیرساخت‌های نرم‌افزاری و سخت افزاری سامانه‌های فرماندهی و کنترل هوشمند بومی با به‌کارگیری فناوری اینترنت اشیاء نظامی.

ب- پیشنهادهای پژوهشی

پژوهش‌های زیر پیشنهاد می‌گردد:

۱. طراحی الگوی راهبردی ایمن‌سازی اینترنت اشیاء نظامی در لایه‌های مختلف فیزیکی، اطلاعاتی و شناختی.

۲. طراحی الگوی راهبردی دفاع هوافضایی هوشمند با به‌کارگیری اینترنت اشیاء نظامی.

۳. تدوین راهبردهای دفاع هوافضایی هوشمند با به‌کارگیری اینترنت اشیاء نظامی.

قدردانی

از زحمات و تلاش‌های بسیار ارزنده‌ی آقای دکتر عادل فرزانه که تلاش بسیار زیـادی در در تهیه و آماده‌سازی مقاله کشیدند، نهایت تشکر و امتنان را دارم.

منابع

- احمدی نوروزمحله، لیلا، میرابراهیمی، سید محمدحسین، مؤذن رضامحله، محمدحسین، پوربهرام، علیرضا. (۲۰۱۶). مقاله: معرفی سبک‌های معماری و تحلیل کاربرد دستگاه‌ها در فناوری اینترنت اشیاء، پاریس فرانسه، *پنجمین کنفرانس بین‌المللی علوم و مهندسی*.
- آقانژاد، لیلا، بابایی، شهرام. (۱۳۹۸). مروری بر امنیت در اینترنت اشیاء، *سومین کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران*.
- امین‌زاده، علی محمد. رمضانی دهقی، رسول. سپهری، محمد. (۱۴۰۲). الگوی بلوغ تاب‌آوری سایبری سامانه فرماندهی و کنترل در مقابله با تهدیدات آینده- *آینده‌پژوهی دفاعی*- دافوس آجا. تهران، ۸(۳۰): ۳۹- ۶۶.
- باقری‌منش، محمد، غلامی، محمود، کاویانی، حسن، امکان‌سنجی پیاده‌سازی فناوری اینترنت اشیاء در آماد یک سازمان دفاعی، *نشریه علوم و فنون نظامی*، ۱۵(۴۸): ۵- ۲۵.

- بدری، رامین. (۱۳۹۸). کاربردها و چالش‌های مورد بحث در اینترنت اشیاء، *کنفرانس بین‌المللی پیشرفت‌های اخیر در علوم اطلاعات، مهندسی و فناوری.*
- بهشتی آتشگاه، محمد، براری، مرتضی، بیات، مجید، عارف، محمدرضا. (۱۳۹۷). مفاهیم و چالش‌های امنیتی اینترنت اشیاء با محوریت مکانیزم MIOT آمریکا، *فصلنامه فرماندهی و کنترل*، سال دوم، شماره ۳.
- تاج، نسرین، معدنی، افسانه. (۱۳۹۶). عنوان پروژه: *الزامات و رویکردهای امنیتی در حوزه اینترنت اشیاء، پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران).*
- توکلی، مسعود، رزقی شیرسوار، هادی، نصیری پور، امیراشکان. (۱۳۹۶). مقاله: تأثیر به‌کارگیری اینترنت اشیاء بر عملکرد سازمانی حوزه سلامت، *فصلنامه علمی‌پژوهشی مدیریت بهداشت و درمان*، ۸(۲): ۶-۴۵.
- جمشیدی، حمداله، نیازی، علی، لونی، محمدرضا، اسکندری‌پور، تورج، توکلی، ابوالفضل. (۱۳۹۰). *روش تحقیق با رویکرد نظامی*، تهران، انتشارات دافوس آجا.
- جواهری، علیرضا. (۱۳۸۹). تدابیر فرماندهی: نظریه‌ای برگرفته از تمرین فرماندهی و کنترل. طرح فراسازمانی فاوا نیروهای‌مسلح ـ *موسسه آموزشی و تحقیقاتی صنایع دفاع*. تهران.
- حاجی شاه کرم، مریم، محمدی، شهریار. (۱۳۹۵). مقاله: معماری پیشنهادی مبتنی بر اینترنت اشیاء و سامانه‌های توصیه‌گر برای هوشمندسازی شهر تهران، پائیز، پژوهشگاه علوم و فنّاوری اطلاعات ایران، *فصلنامه علمی- پژوهشی پردازش و مدیریت اطلاعات*، ۳۲(۸۷).
- حسن‌لو، خسرو. (۱۳۹۵). مقاله: نظریهٔ دفاع هوشمند در سپهر اندیشه‌های دفاعی. *فصلنامه مطالعات دفاعی استراتژیک.*
- حسن‌لو، خسرو. (۱۳۹۴). رساله: *دفاع هوشمند در نظام دفاعی جمهوری اسلامی ایران*، دانشگاه و پژوهشگاه عالی دفاع ملی.
- حسینی، امید، محیط، مریم. (۱۳۹۹). نقش اینترنت اشیاء در کاهش شیوع بیماری همه‌گیر کووید۱۹، *هفتمین کنفرانس بین‌المللی نوآوری و تحقیق در علوم مهندسی، گرجستان، تفلیس.*
- حیدریان، محسن. خادم دقیق، امیرهوشنگ. (۱۳۹۸). الگوی فرماندهی و کنترل هوایی در جنگ‌های آینده. *آینده پژوهی دفاعی*، دافوس. ۴(۱۴): ۶۱- ۸۶.
- درافشانیان، محبوبه. (۱۳۹۷). کاربردهای اینترنت اشیا در مراقبت از بیماران، *کنگره ملی سالانه ایده‌های نوین پژوهشی در علوم مهندسی و تکنولوژی، برق و کامپیوتر.*

- دوستی مطلق، سید نصیب‌اله. (۱۴۰۰). مقاله: سازوکاری جدید برای ارتقاء امنیت شبکه اینترنت اشیاء نظامی با به‌کارگیری رمزنگاری کوانتومی و کلاسیک، *نشریه علمی پدافند الکترونیکی و سایبری.*
- رضایی، محسن. رشید، غلامعلی. پوردستان، احمدرضا. (۱۳۹۹). مولفه‌ها و ویژگی‌های فرماندهی و کنترل هوشمند در صحنه نبرد. *فصلنامه علوم و فنون نظامی*. ۱۶(۵۴): ۱۴۹- ۱۷۱.
- رمضانی دهقی، رسول. (۱۳۹۹). رساله: طرح راهبردی کاربست مفهوم اینترنت اشیاء در حوزه نظامی (مطالعه موردی قرارگاه پدافند هوایی خاتم‌الانبیاء (ص) آجا، دانشگاه و پژوهشگاه عالی دفاع ملی.
- رمضانی، رسول، موحدی‌صفت، محمدرضا. (۱۴۰۰). مقاله: رتبه‌بندی تهدیدهای اینترنت اشیاء در محیط نظامی، *فصلنامه امنیت ملی دانشگاه و پژوهشگاه عالی دفاع ملی.*
- ریکو، آراشی. (۲۰۱۷). مقاله: سیاست دفاعی و اینترنت اشیاء/www. deloitte. com ,
- زیبنده، حسین. (۱۳۹۹). دستور کار پژوهش در مورد خط‌مشی در حوزه حکمرانی اینترنت اشیاء، *فصلنامه سیاست‌نامه علم و فناوری*، دوره ۱۰، شماره ۳.
- سازمند، بهاره. (۱۳۹۸). هوش مصنوعی در جهان ۳ (جمهوری خلق چین)، *مرکز پژوهش‌های مجلس شورای اسلامی*، گروه مطالعات بنیادین حکومتی.
- شهبازی، محمد، جهانیان، مجتبی، سیفی، علی. (۱۳۹۸). امنیت اینترنت اشیاء، *هفتمین کنفرانس ملی علوم مهندسی و فناوری اطلاعات.*
- صیادی، محمدکاظم، جهانی، میثم، فولادی سقاواز، ساناز، عابدی، معصومه، فرازمند، عاطفه، محقق، نجلا. (۱۳۹۶). *برنامه‌های مرتبط با اینترنت اشیاء در چند کشور، مرکز تحقیقات مجلس شورای اسلامی.*
- عارفی‌نژاد، سیدمجید، موسوی، سعید، رفیق‌دوست، مهدی. (۱۳۹۹). مقاله: بررسی کاربردهای اینترنت اشیاء نظامی در نیروهای مسلح، *دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران.*
- غلام‌نژاد، پژمان، غلامی، محمود، پورمکاری، علیرضا. (۱۳۹۸). مقاله: کاربردهای نظامی اینترنت اشیا با تأکید بر مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران، *فصلنامه علوم و فنون نظامی*. ۱۵(۴۹): ۱۴۱- ۱۶۳.
- فرزانه، عادل. (۱۴۰۱). *رساله دکتری الگوی دفاع هوشمند نیروهای مسلح جمهوری اسلامی ایران مبتنی بر اینترنت اشیاء*، دانشگاه عالی دفاع ملی.

- فرزین‌فرد، منصور، کریمی قهرودی، محمدرضا. (۱۳۹۹). مقاله: همگرایی اینترنت اشیاء نظامی و پزشکی و چالش‌های امنیتی، دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران.
- قهرمانی کوشان، فرزانه، رسول روستایی. (۱۳۹۵). مقاله: امنیت و چالش‌های پیش روی فناوری اینترنت اشیاء، *کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات*.
- مهدی‌نژاد نوری، رشیدی، علی جبار، تیلا، محمد شعبان، احمدی حاجی آبادی، سید احمد. (۱۳۹۶). مقاله: تأثیر متقابل دفاع دانش‌بنیان و جنگ‌های آینده، *فصلنامه مطالعات دفاعی استراتژیک*.
- هانگ، زنکیو. (۲۰۱۶). رساله: پیشرفت و چارچوب هوشمندی در لبه برای سیستم‌های اینترنت اشیاء، *دانشگاه کالیفرنیا آمریکا*.
- یوسف، تسنیم. (۲۰۱۵). مقاله: امنیت اینترنت اشیاء: وضعیت فعلی، چالش‌ها و اقدامات متقابل، امارات متحده عربی، دانشگاه آمریکایی‌شارجه، *مجله بین‌المللی تحقیقات امنیت اطلاعات*، دوره ۴، شماره ۵.
- Joern Ploennigs, John Cohn, and Andy Stanford-Clark, IBM(2018) IEEE. *Internet of Things Magazine* • September.
- L. Vijay Anand ,Murali Krishna Kotha,Nimmati Satheesh Kannan,Sunil Kumar,M. R. Meera,Rashed Qayoom Shawl, Abhra Pratip Ray Design and development of IoT based health monitoring system for military applications, *Available online 25 December 2020*.
- Mehmood, M. U. , Chun, D. , Han, H. , Jeon, G. , & Chen, K. (2019). A review of the applications of artificial intelligence and big data to buildings for energy-efficiency and a comfortable indoor living environment. *Energy and Buildings*, 202, 109383.