دوفصلنامه بازی جنگ، سال چهارم، شماره ۸، بهار و تابستان ۱۴۰۰

تاریخ دریافت: ۱۴۰۰/۰۳/۲۷ تاریخ پذیرش: ۱۴۰۰/۰۶/۰۱

از صفحه ۱۰۳ تا صفحه ۱۴۰

چالش‌ها و الزامات امنیتی بکارگیری فناوری کلان داده در توسعه شبکه‌های فرماندهی و کنترل نسل جدید

حمید عظیمی زاده* [۱]

محمدرضا موحدی صفت [۲]

محمدسپهری [۳]

خداداد هلیلی [۴]

نوع مقاله: مروری

چکیده

فناوری کلان‌داده باعث تصمیم‌گیری بلادرنگ، زمان پردازش و هزینه کم، سرعت تحلیل بالا، ارتقای اثربخشی فرمان و تصمیم‌گیری، امکان شبیه‌سازی صحنه نبرد، مدیریت یکپارچه و هوشمندی سامانه فرماندهی و کنترل نسل جدید شده و برای کسب برتری نظامی در جنگ‌های آینده ضروری است. این تحقیق بصورت کیفی، که از نظر هدف کاربردی است و برای گردآوری اطلاعات، از روش کتابخانه‌ای استفاده شده است که با بررسی نقش فناوری نوظهورکلان داده درتوسعه شبکه‌های فرماندهی و کنترل نسل جدید، به این نتیجه رسیده که توسعه کلان‌داده‌ها، چالش‌ها و الزامات امنیتی جدی را به همراه دارد. این فناوری، داده‌های تولیدشده ازمیدان جنگ را جمع‌آوری(لایه تولیدداده)، تجزیه‌وتحلیل(لایه پردازش‌داده) و مدیریت(لایه بهره‌برداری‌داده) می‌نماید و اقدامات امنیتی مورد نیاز برای هر لایه را انجام می‌دهد. دراین تحقیق ابتدا برای افزایش درک کلی از کلان‌داده و محیط نظامی، مروری بر سیستم C2 نسل جدید، ویژگی‌های کلان‌داده‌ها مدل(6V) و چرخه حیات کلان‌داده‌ها مدل پنج فازی را تشریح و ضمن ارائه چارچوبی که سیستم C2 را به سه لایه تقسیم می‌کند، نقش‌ها و اجزای هر لایه با درنظرگرفتن چرخه حیات کلان داده‌ها و چارچوب سیستم به تفصیل شرح داده و در نهایت یک معماری امنیتی با مشخص‌کردن الزامات امنیتی برای هر لایه پیشنهاد می‌گردد.

واژه‌های کلیدی:

فناوری کلان داده، سامانه فرماندهی و کنترل، امنیت کلان داده.

[۱] دانشجوی دکترای مدیریت راهبردی فضای سایبر(گرایش دفاع سایبری)، دانشگاه عالی دفاع ملی، تهران، ایران.

[۲] استادیار مهندسی فناوری اطلاعات، دانشگاه عالی دفاع ملی، تهران، ایران.

[۳] استادیار دانشگاه پدافند هوایی خاتم الانبیاء(ص)، تهران، ایران.

[۴] استادیار دانشگاه هوایی شهیدستاری، تهران، ایران.

* نویسنده مسئول: Email: H. azimizadeh99@sndu. ac. ir

مقدمه

سیستم فرماندهی و کنترل به عنوان‌بخش مهمی از سیستم قدرت نظامی جدید، جایگاه و نقش فوق العاده مهمی دارد. در عصر داده‌های بزرگ، انواع تجهیزات رزمی و حسگرهایی که حجم داده‌ها را جمع‌آوری می‌کنند بیشتر و بیشتر می‌شوند، سرعت تولید داده‌ها سریع‌تر و سریع‌تر می‌شود و به موقع بودن پردازش داده‌ها نیز بالاتر و بالاتر می‌رود.

روند تکامل فرماندهی و کنترل ازفرماندهی و کنترل قدیمی[1](C2) به فرماندهی، کنترل، ارتباطات و اطلاعات[2](C3I) و در مرحله‌ی بعد به فرملندهی، کنترل، ارتباطات، رایلنه و اطلاعات [3](C4I)و سپس فرماندهی، کنترل، ارتباطات، کامپیوتر، اطلاعات، جستجو و مراقبت [4](C4I&ISR) و نهایتاً پیدایش جنگ‌های شبکه محور [5](NCW) نسل جدید فرماندهی و کنترل C2 که از چرخه "داده به تصمیم" صحبت می‌کند تا چرخه "حسگر به تیرانداز" نشان دهنده نقش بی‌بدیل فناوری‌های تاثیرگذار بخصوص هوش مصنوعی و کلان داده در این عرصه می‌باشد [۱]

با توسعه سامانه‌های فرماندهی و کنترل و استفاده از حسگرها و سنسورهای اطلاعاتی، ماهواره‌ها، سامانه‌های جنگ الکترونیک، سامانه‌های رادار فعال و ردیابی غیرفعال، انواع جنگنده‌ها، هواپیماهای بدون سرنشین، جنگ افزارهای هوشمند و... داده‌ها با حجم، سرعت و تنوع بالا تولید و در این سامانه‌ها ذخیره شده و چنانچه از روش‌های تجزیه وتحلیل هوشمند داده‌ها استفاده نکنیم عملا با حجم زیادی از داده‌ها روبرو خواهیم بود که قابلیت استفاده در صحنه نبرد و سامانه فرماندهی و کنترل را نخواهند داشت لذا تحلیل و پردازش حجم بالای این داده‌ها به منظور تصمیم‌گیری دقیق‌تر در مورد نحوه مدیریت صحنه نبرد، اقدامات بلادرنگ، ارتقاء اثربخشی اقدامات نظامی و کسب برتری در میدان جنگ با استفاده از فناوری کلان داده امری اجتناب ناپذیر می‌باشد در نتیجه به کارگیری فناوری کلان داده باعث تصمیم‌گیری به موقع و بلادرنگ، زمان پردازش و هزینه کمتر، سرعت پردازش و تحلیل بالا، آگاهی فراگیر و فهم برتر از فضای نبرد، ارتقای اثربخشی فرمان و تصمیم‌گیری، امکان شبیه‌سازی و تصویرسازی صحنه نبرد، مدیریت یکپارچه و مرکزی و هوشمندی سامانه فرماندهی و کنترل سایبری شده و

---

[1] C2: Command and Control
[2] C3I: Command, Control, Communications AND Intelligence
[3] C4I: Command, Control, Communications, Computer AND Intelligence
[4] C4I&ISR: Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance
[5] NCW: Network Centric Warfare

برای کسب برتری نظامی در جنگ‌های آینده ضروری، که می‌توان گفت که فناوری نوظهور کلان داده‌ها منجر به ارتقاء، توسعه و هوشمندی سامانه‌های نوین فرماندهی و کنترل سایبری شده است.

در این تحقیق با در نظر گرفتن این مطلب که توسعه داده‌های بزرگ چالش‌های جدی را برای توسعه سیستم فرماندهی و کنترل نسل جدید به وجود می‌آورد. چالش داده‌های بزرگ، (تولید داده‌های سامانه فرمان و کنترل) را از سه جنبه (ذخیره‌سازی داده ها– پردازش و تحلیل داده‌ها – امنیت داده ها) بررسی و راهکار مناسب در خصوص چرخه حیات کلان داده‌ها در شبکه‌های فرماندهی وکنترل نسل جدید ارائه می‌گردد.

مبانی نظری

پیشینه تحقیق

۱)آمریکا: جنگ شبکه محور مرزهای جنگ‌های آینده را جابه جا می‌کند. جنگ شبکه محور برای عبور از محدودیت‌هایی که در جنگ های سکو محور و قدیمی وجود داشت مطرح گردیده است. امکان تعامل اطلاعاتی و عملیاتی بین واحدهای صف و ستاد در همه رده‌ها با بهره گیری از خصوصیات ذاتی شبکه به نحوی چشمگیر و به صورت نمایی افزایش یافته است. به این ترتیب سرعت، دقت، پایایی و وسعت میدان عمل جنگ افزارها به میزان قابل توجهی افزایش یافته و در ضمن تحولی بنیادین در مفاهیم سنتی و سلسله مراتب فرماندهی و کنترل ایجاد گردیده است.

استفاده از ابر برای سیستم‌های اطلاعاتی و ارتباطی نظامی از حدود۱۲سال پیش (۲۰۱۰) آغاز شده است. آمریکایی‌ها اولین کسانی بودند که این حرکت را انجام دادند. بنابراین مهاجرت به ابر یکی از ارکان بازنگری کامل در معماری سیستم‌های اطلاعاتی و ارتباطی ایالات متحده، محیط اشترک اطلاعاتی "JIE: Joint Information Environment" است.

پنتاگون و آژانس سیستم‌های اطلاعاتی دفاعی و مدیر ارشد اطلاعات(CIO) این پروژه را راه لندازی کرده است. وزارت دفاع ایالات متحده در تلاش است تا با تعریف یک پلت فرم برای عملیات سیستم‌های کلان داده دربخش دفاعی، یک سیستم کلان داده دفاعی را به طور کارآمد و ایمن ایجاد کند (مارتس ۲۰۱۹). اهمیت داده‌های بزرگ دربخش دفاعی در سطح جهانی در حال افزایش است زیرا هر سرباز و تجهیزات جنگی، اطلاعات ارزشمندی در میدان‌های جنگ تولید و استفاده می‌کند. [۲]

۲) چین: تلاش چین برای دستیابی به قابلیت هوش مصنوعی (AI) برای انجام انواع عملکردهای غیرنظامی و نظامی با تسلط بر تجزیه و تحلیل داده‌های بزرگ شروع می‌شود -

تلاش برای تبدیل شـــدن به یک رهبر جهانی در تجزیه و تحلیل داده‌های بزرگ. در جریان نوزدهمین کنگره ملی حزب کمونیسـت چین در اکتبر ۲۰۱۷، شـی جین پینگ، رئیس جمهور چین بر لزوم "ترویج ادغام عمیق اینترنت، داده‌های بزرگ و هوش مصـــنوعی با اقتصـــاد واقعی تاکید کرد. « برنامه اقدام برای ارتقای توسـعه داده‌های بزرگ» در سـال ۲۰۱۵ توسـط شـورای دولتی جمهوری خلق چین تا حدی رویکرد کلی چین برای توسعه و اسـتفاده از تجزیه و تحلیل داده‌های بزرگ را تشـریح کرد. نشـان می‌دهد که پکن به دنبال اسـتفاده از داده‌های بزرگ برای کمک به چین برای دســـتیابی به موقعیت قدرت بزرگ اســـت. این تجزیه و تحلیل ما را به شناسایی و تمرکز بر روی دو حوزه اولویت مشخص برای رهبران غیر نظامی و نظامی چین سوق داد: "اســـتفاده پکن از تجزیه و تحلیل داده‌های بزرگ در نظارت بر جمعیت داخلی خود و استفاده از آن برای افزایش قابلیت‌های نظامی خود. "

در حوزه نظامی: فرماندهی، کنترل، ارتباطات، رایانه، اطلاعات، نظارت و شـناسـایی. تجهیزات و نگهداری؛ لجسـتیک؛ مراقبت‌های بهداشـتی؛ بسـیج مردمی؛ آموزش؛ اسـتخدام؛ مدل‌سـازی و شـبیه‌سـازی و امنیت سـایبری اسـتفاده از کلان داده‌های دفاع ملی همچنین زیربنای تلاش بلندمدت پکن است که رئیس‌جمهور شی در سخنرانی نوزدهمین کنگره حزب خود بیان کرد تا در نهایت تا سال ۲۰۳۰ به مرکز جهانی هوش مصنوعی تبدیل شود. [۳]

۳) روسیه: اختلافات روسیه و غرب (بخصوص آمریکا)در سال‌های اخیر در زمینه‌های گوناگونی از جمله حوزه سـایبر مشـهودتر شـده اسـت. دقیقاً همان‌طور که در دنیای فیزیکی، مسـکو برای مقاومت در برابر تهدیدها و تحریم‌ها اقدام به ایجاد یک بازدارندگی نظامی کرده و اســـتقلال اقتصـادی از غرب را دنبال می‌کند، زیرسـاخت‌های اینترنتی خود را نیز هم‌زمان شـکل می‌دهد تا بتولند به طور مؤثرتری با چالش‌های داخلی برای حکومت متمرکز خود و همچنین تهدیدهای خارجی در قالب رقابت بین دولتی مقابله کند.

- ✓ امن‌سازی داده‌های ملی
- ✓ قلمروسازی جریان اطلاعات
- ✓ تلاش برای ایجاد کنترل منابع مهم اینترنت در امتداد مرزهای ملی(شـبکه رونت روسی). [۴]

مهمترین پژوهش‌های انجام شده در ارتباط با موضوع این تحقیق عبارتند از:

۴) هلیلی و همکاران در تحقیقاتی لزوم بکارگیری فناوری کلان داده در سـامانه‌های فرماندهی و کنترل و چالش‌های آن و کاربردهای نظامی فناوری کلان داده و نقش آن در مدیریت صـــحنه نبرد را بررسـی نموده و نتیجه گیری کرده‌اند که شـناخت این دو فناوری و چالش‌های مربوط به

تلفیق آنها، زمینه ساز بر نامه‌ریزی مناسب برای بهره گیری از فر صت‌های بکارگیری کلان داده در سامانه‌های فرماندهی و کنترل در کشور خواهد بود و به کار گیری فناوری کلان داده موجب بهینه‌سازی کارایی تجهیزات، تصمیم‌گیری به موقع هدایت نیروها و افزایش توان عملیاتی شده وبرای کسب برتری نظامی در جنگ‌های آینده امری ضروری است. [۵]

۵) مهدی نژاد نوری و همکاران در پژوهشی به بررسی نقش فرماندهی و کنترل هوشمند در دفاع دانش بنیان پرداخته و نتیجه گیری کرده‌اند که رشد سریع فناوری‌ها و ترکیب فناوری‌های جدید در حوزه‌های نظامی، مأموریت‌های متنوع را بهبود بخشیده و در حقیقت دفاع در برابر تهدیدات نظامی را دانش بنیان ساخته است. از سوی دیگر فرایند فرماندهی و کنترل در ذات خود به آگاهی از وضعیت نبرد، نیات دشمن، برنامه‌های خودی و محیط نیازمند است و در صحنه‌های نبرد پیچیده و آشوبناک و پویای امروز این آگاهی می‌بایست به وسیله شبکه‌های مخابراتی تبادل گردیده و با پردازش رایانه تبدیل به دانش شود و تسریع فرایند تصمیم‌گیری فرماندهان را از طریق نرم افزارها و سیستم‌های پشتیبان تصمیم‌گیری میسر سازد و این سرآغاز بعدی بنام فرماندهی و کنترل هوشمند در بستر دفاع دانش بنیان می‌باشد. [۱]

۶) موحدی صفت و همکارانش در این حوزه به دنبال تبیین جایگاه فناوری کلان داده‌ها در ارتقاء سامانه فرماندهی و کنترل سایبری است که نتایج حاصل می‌تواند در توسعه و ارتقاء سامانه‌های بومی فرماندهی و کنترل مورد استفاده واقع شود. نتایج حاصل از این تحقیق بیانگر آن است که به کارگیری فناوری کلان داده‌ها باعث تصمیم‌گیری به موقع و بلادرنگ، زمان پردازش و هزینه کمتر، سرعت پردازش و تحلیل بالا، آگاهی فراگیر و فهم برتر از فضای نبرد، ارتقای اثربخشی فرمان و تصمیمگیری، امکان شبیهسازی و تصویرسازی صحنه نبرد، مدیریتیکپارچه و مرکزی و هوشمندی سامانه فرماندهی و کنترل سایبری شده و برای کسب برتری نظامی در جنگهای آینده ضروری است لذا با توجه به یافته‌های تحقیق میتوان گفت که فناوری نوظهور کلان داده‌ها منجر به ارتقاء، توسعه و هوشمندی سامانه‌های نوین فرماندهی و کنترل سایبری شده است [۶]

۷) چرخه عمر داده‌ها و ارائه یک برنامه عملیاتی کارآمد در سیستم کلان داده. علاوه بر این، از آنجایی که اهمیت امنیت برای عملکرد ایمن سیستم‌های کلان داده بیشتر مورد تاکید قرار می‌گیرد، تحقیقات در مورد اقداماتی برای کاهش خطرات و تجزیه و تحلیل تهدیدات امنیتی سیستم‌های کلان داده ادامه دارد. یکی از کلمات کلیدی که اغلب در مسائل امنیت داده‌های بزرگ ذکر می‌شود، حفاظت از داده‌های شخصی است. برای مثال ابولمهدی و همکارانش راه‌هایی برای تقویت پیشنهاد می‌کند. [۷]

مفهوم‌شناسی

۲-۲-۱- مفهوم، تعریف، ویژگی و کاربردهای فناوری کلان داده‌ها در شبکه فرماندهی و کنترل

الف)مفهوم کلان داده و تعاریف: کلان داده[1] به مجموعه‌های وسیع و متنوعی از اطلاعات اشاره دارد که با سرعت‌های فزاینده‌ای رشد می‌کنند. کلان داده شامل حجم اطلاعات، سرعت یا شتابی است که در آن ایجاد و جمع‌آوری می‌شود و تنوع یا دامنه نقاط داده‌ای که تحت پوشش قرار می‌گیرند. کلان داده اغلب از داده‌کاوی و در قالب‌های مختلف به‌دست می‌آید. این داده‌ها می‌توانند ساختاری باشند. اغلب این داده‌ها به‌صورت عددی هستند و به‌راحتی قالب‌بندی و ذخیره می‌گردند و یا بدون ساختار به شکل آزادتر با قابلیت اندازه‌گیری کمتر هستند. تقریباً هربخش در یک شرکتیا سازمان می‌تواند از یافته‌های تجزیه‌وتحلیل این داده‌ها استفاده نماید، اما مدیریت آن می‌تواند مشکلاتی ایجاد کند. اصطلاح داده‌های بزرگ در دهه گذشته در فرهنگ لغت ظاهر شد، اما مفهوم آن تقریباً از زمان جنگ جهانی دوم وجود داشته است. داده‌ها در همه جا هستند و میتوانند از همه جا جمع‌آوری شوند. از داده‌هایی که از کاربران یک وب سایت (صفحاتی که بازدید کرده اند)جمع‌آوری شده تا داده‌هایی که توسطِ سنسورهای مختلف از سطح دریا جهتِ به دست آوردنِ میزانِ اکسیژن یا دمای آب در نقاطِ مختلفِ آب به دست می‌آید، همگی نمونه‌ای از جمع آوریِ داده‌ها است. وقتی داده‌ها را جمع‌آوری کردید، حال نیاز دارید که با استفاده از ابزارهایی بر روی آنها عملیاتِ مختلفی انجام دهید تا بتوانید دانش و مفهوم را از آن استخراج کنید.

در واقع اگر بخواهیم مبحث را سادهسازی کنیم، هدفِ اصلی از کلان داده در دو مرحله خلاصه می‌شود:

۱) جمع‌آوری داده‌ها از منابعِ مختلفِ داده ای
۲) پردازشِ آنها و انجام یک سری عملیاتِ مختلف بر روی داده‌ها

تعاریف

تعریف کلان‌داده اولین بار در سال ۲۰۰۱ توسط داگ لنی[2] در موسسه گارنتر مطرح گردید. طبق این تعریف، کلان داده عبارت است از اطلاعات با حجم بالا، سرعت بالا و تنوع زیاد که همانند سرمایه اطلاعاتی با روش‌های نوین پردازشی، ذخیره‌سازی برای درک بهتر از دنیا و

[1] Big data
[2] Doug Laney

روند تصمیم‌گیری مورد استفاده قرار می‌گیرد. وی این سه ویژگی (حجم، سرعت و تنوع) را تحت عنوان 3V [۱]مطرح کرد. [۸]

جدول (۱) تعاریف ارائه شده برای کلان داده ها

۱	مجموعه داده‌های بسیار بزرگ که ممکن است به صورت محاسباتی مورد استفاده قرار گیرد تا الگوها، روندها و ارتباطات را نشان دهد، به خصوص در رابطه با رفتار و تعامل انسان. سرمایه گذاری زیادی در حوزه فناوری و اطلاعات به سمت مدیریت و نگهداری کلان داده‌ها در حال انجام است.	(فرهنگ لغت انگلیسی آکسفورد۲۰۰۷)
۲	دارایی‌های اطلاعاتی با حجم بالا، سرعت بالا و تنوع زیاد که نیازمند پردازش‌های جدید است و تصمیم‌گیری پیشرفته، کشف دانش و بهینه‌سازی فرایند را امکان پذیر می‌سازد.	(موسسه گارنتر ۲۰۲۰)

مرکز داده بزرگ

مرکز داده بزرگ به عنوان پایه اصلی کاربرد و کارایی فناوری کلان داده است مرحله‌ای اجتناب ناپذیر برای ساخت نسل جدید سیستم C2 که عمدتاً برای ذخیره‌سازی و مدیریت داده‌های بزرگ داده‌های کسب و کار در سیستم اطلاعات فرماندهی دارای انواع مختلفی از ویژگی‌ها و ویژگی‌های هر کدام یکسان نیست. لازم است هنجاری و متناظر تدوین شود استانداردهای بین داده‌ها، انجام استانداردسازی و مدیریت علمی مانند کتابخانه و انجام تحقیقات علمی بر روی داده‌ها از طریق فرآیندهای استاندارد و روش‌های ذخیره‌سازی قالب. مدیریت موثر به منظور بهبود کیفیت و کارایی استفاده از داده‌ها و هماهنگی انواع داده‌های ساخت یافته، نیمه ساختاریافته و بدون ساختار. بر این اساس، فضای ذخیره‌سازی ابری فن‌آوری و سیستم فایل توزیع شده برای اطمینان از دسترسی تک نقطه‌ای و جهانی ترکیب شده‌اند به اشتراک گذاری منابع اطلاعاتی برای پاسخگویی به الزامات عملیات مداوم، ظرفیت الاستیک انبساط و تعادل بار معماری سیستم C2 که بر روی داده‌های بزرگ متمرکز است باید به طور جامع منبع را در نظر بگیرد لایه، لایه قابلیت، لایه پلت فرم و لایه مدیریت و سیستم فرماندهی و کنترل نسل جدید را تشکیل می‌دهند. [9]

امنیت داده‌ها و امنیت کلان داده

تعریف امنیت کلان داده: حفاظت از داده‌های اصلی ارتش با ابزارهای قانونی و جلوگیری از فعالیت‌های جمع‌آوری اطلاعات دشمن بر روی اطلاعات اصلی خود. (داوودی فر -۱۳۹۹)

ارتش ایالات متحده از پلت فرم محاسبات ابری برای سیستم C4ISR استفاده می‌کند. تجزیه و تحلیل نشان می‌دهد که پلت فرم محاسبات ابری موجود می‌تواند قابلیت اطمینان و گسترش

---

[۱]. سه «V» یعنی «حجم» (Volume)، «سرعت» (Velocity) و «تنوع» (Variety) است.

عملیات را برآورده کند نرم افزار پردازش داده‌های میدان جنگ، اما الزامات حفظ حریم خصوصی و امنیت داده‌ها را نمی‌توان هنوز برآورد کرد.

جنگ‌های آینده ویژگی‌های اساسی جنگ داده‌های بزرگ را دارند. پیروزی و شکست جنگ به طور فزاینده‌ای بر داده‌های علمی بزرگ، سیستماتیک و بسیار معتبر متکی است. تحلیل جامع داده‌های بزرگ به اوج رقابت میدان نظامی تبدیل شده است، اما اگر منابع داده اصلی نتوانند به درستی محافظت شوند، ممکن است در معرض حملات سایبری با عواقب جدی قرار گیرند که پس از به خطر افتادن. تحت حمایت فناوری داده‌های بزرگ، پایگاه اطلاعاتی عظیمی تبدیل شده است وضعیت حملات سایبری و سیستم‌های نظامی و سیستم‌های داده به هدف تبدیل خواهند شد. بنابراین، حفاظت از داده‌های هسته‌ای نظامی با ابزارهای مشروع و جلوگیری از فعالیت‌های جمع‌آوری اطلاعات دشمن بر روی اطلاعات اصلی خود، در سیستم C2 در عصر داده‌های بزرگ به یک نقطه دشوار تبدیل شده است. [***9***]

فرماندهی و کنترل نسل جدید[۹]

سیستمC2 به عنوان "ضریب" اثربخشی رزمی، فعالیت‌ها نظامی صحنه نبرد را از طریق تعامل بین افراد، ماشین هاو محیط، و همچنین ورودی، پردازش، خروجی و بازخورد اطلاعات را دائما تنظیم می‌کند. (یوانلی کینا- موسسه تحقیقاتی فناوری پیشرفته شیان، چین-۲۰۱۸)

در فرآیند توسعه از سیستم ***C***۲ به ***C***۳، ***C***۴*I*، ***C***۴*I*، ***C***۴*ISR* و ***NCW***[1]، ارتش ایالات متحده به یک جهش از تمرکز به پلت فرم شبکه محور دست یافت.

تنها تحلیل و درک داده‌ها می‌تواند به طور مداوم توانایی "از داده‌ها تا تصمیم‌گیری" را بهبود می‌بخشد و به هدف رزمی "کشف - تخریب است" نزدیک می‌شود.

سیستم یکپارچه C2 برای ارائه پشتیبانی از داده کاوی و پردازش، ایجاد موقعیت و اشتراک اطلاعات و دستیابی به برنده شدن داده‌ها، بر پلت فرم مدیریت کلان داده تکیه خواهد کرد. در حال حاضر نتایج تحقیقات در مورد کاربرد کلان داده در سیستم C2 به سرعت به روز می‌شود، اما در عین حال با مشکلاتی نیز مواجه است. جمع‌بندی به موقع این دستاوردها و مشکلات جدید، اهمیت مرجع مهمی برای ساخت سیستم اطلاعات فرماندهی ارتش ما دارد. [۹]

[1] NCW: Network Centric Warfare

شکل (۱) روند تکامل فرماندهی و کنترل (منبع پژوهشگران)

ب)کاربرد کلان داده‌ها در محیط نظامی

منابع داده نظامی، نظارت اطلاعاتی میدان نبرد داده‌های تولید شده توسط حسگرهای مختلف در میدان نبرد حاوی اطلاعات عملیاتی فراوانی است. که برای تجزیه و تحلیل وضعیت هدف و تلاش رزمی و نظارت اهمیت زیادی دارد اقدام دشمن با این حال، با ادامه فعالیت‌های ردیابی و پایش هدف، داده‌ها حجم تولید شده نیز به صورت تصاعدی افزایش یافته است. فرماندهی و کنترل رزمی تجزیه و تحلیل وضعیت لحظه‌ای در میدان نبرد، فرماندهی و فرماندهی مافوق و اطلاعات تضمینی مختلف نیز حجم زیادی از داده‌های ناهمگن تولید می‌کند. از طریق همجوشی و استخراج این داده‌ها از منابع مختلف، ارتباط داده‌ها و پشتیبانی تصمیم‌گیری قابل تحقق است و کنترل مؤثر موقعیت را می‌توان تحقق بخشید. مشکلات فعلی، ذخیره‌سازی داده‌ها و محاسبه کارآمد کلان داده‌ها الزامات بسیار بالایی را برای ظرفیت ذخیره‌سازی داده‌ها در سیستم C2 ایجاد می‌کند، اما انواع مختلف آن داده‌های درک شده که معمولاً نه تنها شامل ویژگی‌های اطلاعات مفید، بلکه ویژگی‌های دیگر نیز می‌شوند از افزونگی بنابراین، حجم نمونه‌گیری اطلاعات بسیار زیاد است و ادغام اطلاعات کند است. و برنامه‌ریزی پیش‌بینی کند و اجرا ضعیف است. در نتیجه، سیستم فعلی هنوز هم دارد مشکلاتی مانند قابلیت همکاری ضعیف و ظرفیت ضعیف پردازش اطلاعات. از سوی دیگر، بسیاری از داده‌های نیمه ساختاریافته یا بدون ساختار که تاکتیکی پیچیده را توصیف می‌کند. معنی میدان جنگ، از جمله داده‌هایی که از طریق داده‌ها قابل ارائه نیستند، مانند متن، عکس، و انواع گزارش‌ها و گرافیک‌ها، به سختی قابل استفاده هستند. همچنین استفاده از سنتی دشوار است پایگاه داده با فرمت ثابت برای ذخیره‌سازی و ابزارهای مربوطه برای تجزیه و تحلیل داده‌ها. فقدان تحلیل تولنایی این داده‌ها استخراج اطلاعات مفید از این داده‌های با چگالی کم را دشوار می‌کند. که به طور جدی توسعه سیستم فرماندهی و کنترل نسل جدید را محدود می‌کند [9].

ج) ویژگی‌های کلان داده‌ها در محیط نظامی

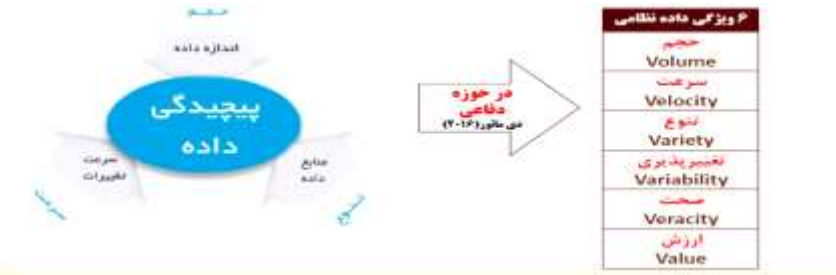
دی مائورو و همکارانش [۱۱] تعریف کلان داده را به عنوان «دارایی اطلاعاتی با حجم، سرعت و تنوع بالا برای نیاز به فناوری و روش‌های تحلیلی خاص برای تبدیل آن به ارزش» پیشنهاد کرد. اساساً این تعریف به کلان داده به عنوان دارایی‌های اطلاعاتی، و چهار ویژگی اساسی داده‌های بزرگ، اطلاعات، فناوری، روش و تأثیر، در نظر گرفته می‌شود که این تعریف را شامل می‌شود. با این حال، به طور کلی، ماهیت داده‌های بزرگ معمولاً با چند کلمه توصیف می‌شود که با ***V*** شروع می‌شود. از زمانی که داگ لین در سال ۲۰۰۱ [۸] داده‌های بزرگ را با استفاده از***3V***، یعنی حجم، سرعت، و تنوع تعریف کرد، بسیاری از **V** ها تا 11V پدید آمده‌اند. و پیچیدگی[1] کلان داده اضافه شد که می‌توان آن را به اختصار (11V+C) نامید. اگرچه برای توصیف داده‌های بزرگ، بسیاری از مطالعات دیگر ارزشمند است. به ویژگی‌های داده‌های بزرگ با استفاده از 6V اشاره می‌کند: حجم، سرعت، تنوع، تغییرپذیری، صحت و ارزش. سیستم‌های کلان داده که در سیستم‌های*C2* پیاده‌سازی می‌شوند، ویژگی‌های ***6V*** را نیز دارند که در زیر به تفصیل توضیح داده شده و به اختصار به آنها اشاره می‌شود. [۱۰] در جدول ۲ مشخصات کلان داده 6V می‌تواند برای سیستم نظامی C2 قابل استفاده باشد.

جدول (۲) مشخصات کلان‌داده *V۶* برای سیستم نظامی *C2*

	توضیح مختصر	در سیستم نظامی*C2*
حجم Volume	حجم زیادی از داده ها	- خاستگاه مفهوم *Network Centric Warfare* و ظهور بسیاری از دستگاه‌ها مانند *IoBT* در میدان جنگ - دارایی‌های نظارتی حجم زیادی از داده‌ها مانند ویدئو/تصویر، سیگنال رادیویی و غیره تولید می‌کنند.
سرعت Velocity	سرعت رشد داده ها نرخ جریان داده	-افزایش *IoBT* و توسعه دارایی‌های اطلاعاتی در میدان نبرد، افزایش داده‌های میدان نبرد را تسریع می‌کند. - عملکرد بالا برای پشتیبانی از تصمیم‌گیری در زمان واقعی (یا تقریباً واقعی) در یک عملیات نظامی
تنوع Variety	انواع مختلف داده از انواع مختلف منبع داده.	عناصر هوشمند مانند*HUMINT* (انواع اطلاعات نظامی شامل هوش انسانی است)، (هوش سیگنال)*SIGINT*، (هوش اندازه گیری و امضاء)*MASINT*، *GEOINT*(هوش جغرافیایی)، *OSINT*(هوش منبع باز) و غیره انواع مختلف، حجم داده‌های میدان جنگ را ایجاد می‌کنند.
تغییرپذیری Variability	تغییر نرخ جریان داده،	- مرکز داده دفاعی با معرفی یک سیستم ابری، مقیاس‌پذیری را ایمن می‌کند. - تبدیل به داده در فرمی مناسب برای دستگاه‌های ترمینال سیستم*C2*

[1]Complexity

	توضیح مختصر	در سیستم نظامی *C2*
	فرمت، ساختار، حجم و غیره	
صحت Veracity	دقت داده ها	در میدان نبرد، مهم است که اطمینان حاصل شود که داده‌ها برای عملیات نظامی و تصمیم‌گیری نظامی قابل اعتماد هستند.
ارزش Value	داده‌های ورودی/خروجی با ارزش	-داده‌های ورودی توسط دارایی‌های موجود در میدان جنگ ارائه می‌شود. -داده‌های خروجی برای دارایی‌های رزمی با تصمیم‌گیری استفاده می‌شود.



شکل (۲) مفهوم *6V* در داده‌های نظامی بزرگ(منبع پژوهشگران)

حجم: حجم عظیمی از داده‌ها (یا مجموعه داده ها) ذخیره شده و پردازش شده در یک سیستم کلان داد. از زمانی که ارتش ایالات متحده مفهوم جنگ محوری شبکه را در سال ۱۹۹۸ برجسته کرد، به اشتراک گذاری اطلاعات بین عناصر میدان نبرد فعال‌تر شده است، به ویژه ***IoBT*** و دارایی‌های نظارتی که فیلم/تصویر فیلمبرداری می‌کنند، به طور تصاعدی میزان داده‌هایی را که باید پردازش شوند افزایش داده است. یک سیستم ***C4I*** به عنوان مثال، ترابایت (۱۰۱۲) از حجم داده برای مدیریت در سطح کاربر نهایی رایج شده است، و زتابایت (۱۰۲۱) از حجم داده دیگر واژه‌ای ناآشنا برای مدیران داده‌های نظامی نیست. با توجه به افزایش حجم داده‌ها در میدان نبرد، مرکز داده دفاعی به فضای ذخیره‌سازی کافی برای ذخیره آن و فناوری برای مدیریت کارآمد آن نیاز دارد.

سرعت: سرعت، در کلان داده، عمدتاً به دو جنبه مربوط می‌شود: سرعت رشد داده و سرعت جریان داده. سرعت رشد داده‌ها ارتباط نزدیکی با ویژگی‌های حجم داده معرفی شده در بالا دارد. افزایش ***IoBT*** و توسعه دارایی‌های اطلاعاتی در میدان نبرد، افزایش داده‌های میدان نبرد را تسریع می‌کند. نرخ جریان داده به این معنی است که برای اجرای ***Observe*** به قابلیت‌های انتقال/دریافت و پردازش در زمان واقعی (یا تقریباً واقعی) نیاز است. در یک عملیات نظامی بلادرنگ شبکه ارتباطی سیمی/بی‌سیم بهبود یافته در ساختار، انتقال داده‌ها را با حداقل تأخیر

فراهم می‌کند و فناوری محاسباتی پیشرفته پردازش (یا تجزیه و تحلیل) داده‌ها را در زمان واقعی امکان‌پذیر می‌سازد.

تنوع: انواع اطلاعات نظامی شامل هوش انسانی ***(HUMINT)*** ، هوش سیگن ***(SIGINT)*** ، هوش اندازه گیری وامضاء ***(MASINT)***، هوش مکانی ***(GEOINT)*** ، اطلاعات منبع باز ***(OSINT)***و غیره است. این اطلاعات از انسان، ***IoBT***، حسگرها، وسایل نقلیه هوایی بدون سرنشین (پهپاد)، ماهواره‌ها و غیره در میدان نبرد عمل می‌کنند و داده‌های جمع‌آوری‌شده در قالب‌های ساختاریافته، بدون ساختار یا نیمه‌ساختار یافته در پایگاه داده ذخیره می‌شوند. در نتیجه، سیستم‌های ***C2*** باید بتوانند اشکال مختلفی از داده‌ها را از انواع منابع مختلف در میدان جنگ پردازش کنند.

تغییرپذیری: این ویژگی به تغییر در یک مجموعه داده، چه در نرخ جریان داده، فرمت، ساختار و/یا حجم اشاره دارد. به عنوان مثال، حجم داده مستلزم نیاز به افزایش یا کاهش مقیاس منابع مجازی برای مدیریت کارآمد بار پردازشی اضافی است. به عنوان یک معماری سیستم برای مدیریت تغییرپذیری داده‌ها، ابر می‌تواند به صورت پویا سیستم‌ها را در محیط‌های مجازی مقیاس کند. همچنین پایگاه داده‌های رابطه‌ای و ***DB*** های ***NoSQL***را با تغییر انواع داده‌ها اعمال می‌کند.

صحت: همانطور که ورودی (داده) باید در سیستم‌های ورودی/خروجی دقیق و قابل اعتماد باشد تا به نتایج مورد نظر دست یابد، دقت داده نیز یکی از مهم‌ترین الزامات در سیستم‌های کلان داده ***C2*** است. به عنوان مثال، از آنجایی که کلان داده‌ها برای تصمیم‌گیری استفاده می‌شوند، مهم است که اطمینان حاصل شود که می‌توان به آنها اعتماد کرد. داده‌های نادرست مانند تکرار داده‌های بی‌معنی، نویز یا اشتباهات تایپی ممکن است منجر به داده‌های خروجی با کیفیت پایین شود. این سیستم برای حذف داده‌های نادرست به فناوری نیاز دارد. به عنوان مثال، روش‌های آماری، ادغام/تجمیع داده‌ها با فناوری با دقت بالا، حتی الگوریتم‌های یادگیری ماشین و غیره، فناوری‌هایی هستند که برای اطمینان از کیفیت داده‌ها استفاده می‌شوند.

ارزش: از نقطه نظر داده، هم داده‌های ورودی جمع‌آوری شده در یک سیستم ***C2*** و هم داده‌های خروجی تولید شده پس از تجزیه و تحلیل کلان داده باید از ارزش کافی برخوردار باشند. بنابراین فرمانده باید با استفاده از سیستم ***C2*** با داده‌های بزرگ بتواند تصمیم گرفته و به طور موثر از فعالیت‌های رزمندگان پشتیبانی کند.

چرخه حیات کلان داده‌های در شبکه‌های فرماندهی و کنترل (مدل پنج فازی) [۱۰]

داده‌ها، منبع ورودی داده‌های بزرگ، را می‌توان بر اساس رویه‌ای که در سیستم انجام می‌شود تقسیم کرد. در تحقیقات موسسه ملی استاندارد و فناور ***(NIST)*** [۱۲]، داده‌ها توسط ارائه‌دهنده برنامه کاربردی کلان داده در پنج مرحله پردازش شدند: جمع‌آوری، آماده‌سازی/تعیین، تجزیه و تحلیل، تجسم و دسترسی. پاتگیری[۱۳] به عنوان یک چرخه مدیریت کلان داده پنج مرحله‌ای دیگر پیشنهاد کرد: اکتساب، پیش پردازش، ذخیره‌سازی تجزیه و تحلیل و تجسم. هر دو مطالعه فرآیند مدیریت داده را از تولید/جمع‌آوری داده تا تجسم/استفاده ارائه می‌دهند. با این حال، با افزایش اخیر در الزامات امنیت و حریم خصوصی برای داده‌های مورد استفاده در سیستم داده‌های بزرگ، در صورتی که داده‌ها دیگر برای هدف مورد نظر ضروری نباشند یا ارائه‌دهنده داده رضایت خود را پس بگیرد، باید تخریب داده‌ها در نظر گرفته شود. کو و همکاران [۱۴] یک چرخه حیات داده پنج مرحله‌ای را پیشنهاد کرد که دفع داده‌ها را در نظر می‌گیرد: جمع‌آوری ذخیره‌سازی تجزیه و تحلیل، استفاده شده و تخریب. بنابراین، ما آن چرخه‌های عمر پنج فازی را در یک سیستم کلان داده ***C2*** اعمال خواهیم کرد.

جدول(۳) چرخه حیات داده‌های بزرگ پنج فازی

چرخه حیات داده‌های بزرگ پنج فازی		
۱	جمع آوری	۱- داده‌های ساختاریافته (مطابق با یک مدل پایگاه داده است، که عمدتاً با فیلدهای مختلفی که داده‌ها به آنها تعلق دارند، مانند نام، آدرس، سن و غیره، و با نوع داده برای هر فیلد مانند مشخص می‌شود. عدد، واحد پول، حروف الفبا، نام، تاریخ و آدرس) ۲- داده‌های بدون ساختار (به اطلاعاتی اطلاق می‌شود که یا مدل داده‌ای از پیش تعریف شده ندارند یا به روشی از پیش تعریف شده سازماندهی نشده‌اند. عکس‌ها، تصاویر گرافیکی، ویدئو، متن، ضبط صدا، داده‌های حسگر جریانی و غیره را می‌توان به عنوان داده‌های بدون ساختار طبقه‌بندی کرد.) ۳- داده‌های نیمه ساختاریافته (نوعی داده است که در آن هر دو ویژگی داده‌های ساختاریافته و بدون ساختار منعکس می‌شود. اسناد پردازش کلمه، از جمله ابرداده‌ها مانند نام نویسنده و تاریخ ایجاد، و عکس‌های آپلود شده در سرویس شبکه اجتماعی (*SNS*) با برچسب‌ها نمونه‌های معرف داده‌های نیمه ساختاریافته هستند.)
۲	ذخیره‌سازی	مرحله ذخیره‌سازی فرآیند آماده‌سازی داده‌ها (یعنی تجمیع و ادغام داده‌ها، پاکسازی/پاکسازی داده‌ها، پارتیشن‌بندی داده‌ها، نمایه‌سازی داده‌ها و غیره) باید گنجانده شود تا حجم زیاد و فرمت‌های متنوع داده‌ها به طور مناسب ذخیره شوند. این مرحله به طور خلاصه دو فناوری اصلی (یعنی سیستم فایل توزیع شده و *MapReduce*) را برای پیاده‌سازی ذخیره‌سازی داده‌ها معرفی می‌کند.

		چرخه حیات داده‌های بزرگ پنج فازی
		۱- سیستم‌های فایل توزیع شده محبوب‌ترین زیرساختی هستند که می‌توانند مجموعه‌های عظیم داده را در چندین مخزن ذخیره‌سازی توزیع شده ذخیره کنند. ۲- *MapReduce* یک مدل برنامه نویسی فشرده داده برای پردازش مجموعه داده‌های بزرگ در یک خوشه از گره‌های ذخیره‌سازی توزیع شده است. به غیر از چارچوب *MapReduce*، چندین پروژه منبع باز آپاچی دیگر مربوط به اکوسیستم *Hadoop* هستند، از جمله *Zookeeper*، *Hive*، *Hbase*، *Pig*، *Mahout*، *Avro* و *Spark*
۳	تجزیه و تحلیل	هوسامالدین و همکاران. (۲۰۱۰) پیشنهاد کرد که تجزیه و تحلیل داده‌های بزرگ را می‌توان به چهار جنبه طبقه‌بندی کرد: تجزیه و تحلیل توصیفی، تجزیه و تحلیل تشخیصی، تجزیه و تحلیل پیش‌بینی و تجزیه و تحلیل تجویزی. برای به دست آوردن اطلاعات یا دانش معنی دار، از تکنیک‌های مختلفی مانند تجزیه و تحلیل آماری، تجمیع داده‌ها، خوشه‌بندی داده‌ها، یادگیری ماشین و غیره استفاده می‌شود.
۴	بهره‌برداری	هدف اولیه مرحله بهره‌برداری تولید اطلاعات و دانش ارزشمند از طریق تجزیه و تحلیل داده‌ها است. برای استفاده موثر از کلان داده، یک ابزار تجسم یا یک ابزار تصمیم‌گیری که نیازهای کاربران را به طور دقیق درک و بیان کند، ضروری است.
۵	تخریب	اساساً، داده‌های حریم خصوصی باید پس از گذشت بیش از مدت زمان نگهداری داده‌ها، بدون تأخیر از بین بروند. در زمینه نظامی، تخریب داده‌ها بر اساس مقررات امنیتی یک عنصر ضروری برای تضمین ایمنی عملیات نظامی و حفاظت از سیستم فرماندهی و کنترل است.

جمع‌آوری: در عمل، سیستم‌های کلان داده حجم‌های بزرگ و فرمت‌های متنوع داده‌ها را از چندین حوزه منحصربه‌فرد مانند مراقبت‌های بهداشتی، اقتصاد/صنعت، شهرهای هوشمند، علوم، ارتش و غیره جمع‌آوری می‌کنند. در یک مدل رابطه‌ای. داده‌های ساخت یافته مطابق با یک مدل پایگاه داده است که عمدتاً با فیلدهای مختلفی که داده‌ها به آنها تعلق دارند، مانند نام، آدرس، سن و غیره، و با نوع داده برای هر فیلد مانند عدد، واحد پول، حروف الفبا، نام، مشخص می‌شود. تاریخ و آدرس. داده‌های بدون ساختار به اطلاعاتی اطلاق می‌شود که یا مدل داده‌ای از پیش تعریف شده ندارند یا به روشی از پیش تعریف شده سازماندهی نشده‌اند. عکس‌ها، تصاویر گرافیکی، ویدئو، متن، ضبط صدا، داده‌های حسگر جریانی و غیره را می‌توان به عنوان داده‌های بدون ساختار طبقه‌بندی کرد. داده‌های نیمه ساختاریافته نوعی داده است که در آن هر دو ویژگی داده‌های ساختاریافته و بدون ساختار منعکس می‌شود. اسناد پردازش کلمه، از جمله ابرداده‌ها مانند نام نویسنده و تاریخ ایجاد، و عکس‌های آپلود شده در سرویس شبکه اجتماعی (***SNS***) با برچسب‌ها نمونه‌های معرف داده‌های نیمه ساختاریافته هستند.

ذخیره‌سازی سیستم‌های کلان داده صرفاً با ذخیره‌سازی داده‌های خام جمع‌آوری شده در مرحله قبل راضی نمی‌شوند. در مرحله ذخیره‌سازی فرآیند آماده‌سازی داده‌ها (یعنی تجمیع و ادغام داده‌ها، پاکسازی/پاکسازی داده‌ها، پارتیشن داده‌ها، نمایه‌سازی داده‌ها و غیره) باید

گنجانده شود تا حجم زیاد و فرمت‌های متنوع داده‌ها به طور مناسب ذخیره شود. این مرحله به طور خلاصه دو فناوری اصلی (یعنی سیستم فایل توزیع شده و ***MapReduce***) را برای پیاده‌سازی ذخیره‌سازی داده‌ها معرفی می‌کند. سیستم‌های فایل توزیع شده محبوب‌ترین زیرساختی هستند که می‌توانند مجموعه‌های عظیم داده را در چندین مخزن ذخیره‌سازی توزیع شده ذخیره کنند [۱۵، ۱۶]. ***MapReduce*** یک مدل برنامه نویسی فشرده داده برای پردازش مجموعه داده‌های بزرگ در یک خوشه از گره‌های ذخیره‌سازی توزیع شده است [۱۵، ۱۷]. در عمل، ***Hadoop*** چارچوبی برای سیستم فایل توزیع شده و ***MapReduce*** فراهم می‌کند.

تجزیه و تحلیل: این مرحله، تجزیه و تحلیل داده‌های بزرگ، دانش مفیدی را با تجزیه و تحلیل مقدار زیادی از داده‌های قبلا جمع‌آوری و ذخیره شده تولید می‌کند. برای مثال، هوسامالدین و همکاران. [۱۸] پیشنهاد کرد که تجزیه و تحلیل داده‌های بزرگ را می‌توان به چهار جنبه طبقه‌بندی کرد: تجزیه و تحلیل توصیفی، تجزیه و تحلیل تشخیصی، تجزیه و تحلیل پیش‌بینی و تجزیه و تحلیل تجویزی. برای به دست آوردن اطلاعات یا دانش معنی دار، از تکنیک‌های مختلفی مانند تجزیه و تحلیل آماری، تجمیع داده‌ها، خوشه‌بندی داده‌ها، یادگیری ماشین و غیره استفاده می‌شود.

بهره‌برداری: در هر زمینه‌ای که فناوری کلان داده در آن اعمال می‌شود، هدف اولیه مرحله بهره‌برداری تولید اطلاعات و دانش ارزشمند از طریق تجزیه و تحلیل داده‌ها است. به عنوان مثال، با تجزیه و تحلیل روند خرید در حین خرید اینترنتی، تولید محصولات مورد نظر مصرف کنندگان در زمینه تجاری برای شرکت آسان‌تر است. علاوه بر این، داده‌های جمع‌آوری شده برای تحقیقات دانشگاهی را می‌توان به سرعت و با دقت تجزیه و تحلیل کرد تا نتایج ارزشمندی ارائه دهد. در حوزه نظامی، شواهدی را برای تصمیم‌گیری فرماندهان فراهم می‌کند و جهتی را که هر عنصر رزمی در آن عمل می‌کند، پیشنهاد می‌کند. بنابراین، برای استفاده موثر از کلان داده، یک ابزار تجسم یا یک ابزار تصمیم‌گیری که نیازهای کاربران را به طور دقیق درک کرده و بیان می‌کند، ضروری است.

تخریب: با سخت‌تر شدن الزامات مربوط به امنیت و حریم خصوصی داده‌های بزرگ، مدیریت داده‌ها طبق مقررات بسیار مهم شده است. اساساً، داده‌های حریم خصوصی باید پس از گذشت بیش از مدت زمان نگهداری داده‌ها، بدون تأخیر از بین بروند، مگر اینکه در قوانین و مقررات دیگر تصریح شده باشد. علاوه بر این، اگر داده‌ها دیگر برای هدف مورد نظر ضروری نیستند یا اگر ارائه دهنده داده رضایت خود را پس بگیرد، باید از بین بروند [۱۹]. در زمینه نظامی،

تخریب داده‌ها بر اساس مقررات امنیتی یک عنصر ضروری برای تضمین ایمنی عملیات نظامی و حفاظت از سیستم ***C2*** است.

ساختار شبکه‌های فرماندهی و کنترل مبتنی بر کلان داده‌ها در محیط صحنه نبرد [۱۰]

در این‌بخش ویژگی‌های ساختاری سیستم کلان داده و سیستم ***C2*** به وضوح درک می‌شود و چارچوب سیستم کلان داده ***C2*** به تازگی با در نظر گرفتن رابطه بین دو سیستم ارائه می‌شود. اول، بخش الف. یک چارچوب سیستمی را تعریف می‌کند که به چهار لایه طبقه‌بندی شده است، با تفسیر داده‌های بزرگ از دیدگاه سیستم به منظور درک ویژگی‌های ساختاری یک سیستم کلان داده عمومی. چارچوب کلی سیستم کلان داده یک راهنمای اساسی برای بکارگیری فناوری کلان داده در سیستم ***C2*** که در میدان جنگ عمل می‌کند، ارائه می‌دهد. بخش ب. سیستم ***C2***را با توجه به جریان داده‌های ایجاد شده و مدیریت شده در میدان جنگ به سه لایه طبقه‌بندی می‌کند. با طبقه‌بندی سیستم ***C2*** که شامل اجزای پیچیده و متنوعی است از نظر داده به سه لایه می‌توان گفت که استانداردی واضح برای بکارگیری فناوری کلان داده ارائه شد. در نتیجه، بخش ج. به تازگی چارچوب سیستم کلان داده ***C2*** را از طریق ترکیب ساختاری بر اساس همبستگی بین چارچوب سیستم کلان داده تعریف شده قبلی و چارچوب سیستم ***C2*** ارائه می‌دهد. علاوه بر این، امکان پیاده‌سازی عملی سیستم را با ارائه اجزای لازم برای هر قسمت از چارچوب ارائه شده به تفصیل بررسی می‌کنیم.

الف) چارچوب سیستم داده‌های بزرگ لایه‌ای از دیدگاه سیستم

چارچوب سیستم داده‌های بزرگ لایه‌ای به ساختار سیستمی اشاره دارد که به اندازه کافی برای مدیریت داده‌های تحت پوشش چرخه عمر کلان داده پیاده‌سازی شده است. با توجه به دیدگاه پیکربندی سیستم داده‌های بزرگ، این مقاله چهار لایه از یک چارچوب را پیشنهاد می‌کند: زیرساخت، داده، پلت فرم و لایه‌های کاربردی. این طبقه‌بندی از سه چارچوب (یعنی زیرساخت، پلتفرم و پردازش) سیستم‌های کلان داده ذکر شده در (***NIST***) [۱۲] و سه لایه (یعنی زیرساخت، بافت‌های کلان داده، و پلت فرم داده‌های بزرگ به عنوان یک سرویس و برنامه) ارائه شده است. توسط ***Kune*** و همکاران[۱۴].

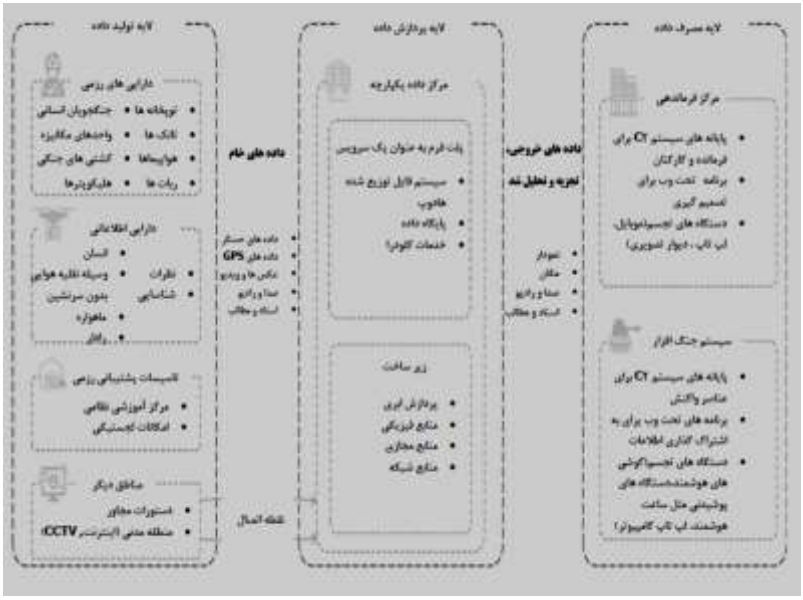
- **لایه زیرساخت:** این لایه به منابع فیزیکی یا مجازی مورد نیاز در کل فرآیند چرخه حیات داده‌های بزرگ برای جمع‌آوری ذخیره‌سازی تجزیه و تحلیل، استفاده و تخریب داده‌ها اشاره دارد. زیرساخت شامل سرور، ذخیره‌سازی دستگاه‌های شبکه، اینترنت اشیا، حسگرها، سرویس‌های وب اینترنتی و غیره است. علاوه بر این، در سال‌های اخیر، محاسبات ابری، که با مقیاس‌پذیری عالی و استفاده از منابع سیستم

اطلاعاتی، تأمین منابع بر حسب تقاضا، و سهولت محاسبات موازی مشخص می‌شود، به عنوان یک زیرساخت کلان داده که ۶ ولت را تضمین می‌کند، در کانون توجه قرار گرفته است.

- **لایه داده:** این لایه داده‌ها را در یک سیستم کلان داده ذخیره و مدیریت می‌کند. برای مقابله با حجم زیاد و اشکال مختلف داده در لایه داده، داشتن یک سیستم مناسب ضروری است. به عنوان مثال، فن‌آوری‌های پارتیشن‌بندی نمایه‌سازی و ***MapReduce*** در سیستم‌های فایل توزیع شده برای ذخیره مقادیر زیادی از داده‌ها در مخازن متعدد و مدیریت کارآمد داده‌ها استفاده شده است. علاوه بر این، پایگاه‌های داده‌ای مانند پایگاه‌های داده رابطه‌ای و ***NoSQL*** برای انواع مختلف داده‌ها مورد نیاز هستند.
- **لایه بستر داده بزرگ:** پلتفرم کلان داده ممکن است به عنوان میان افزار برای اجرای عملکرد کلان داده سیستم تعریف شود [۱۵]. اکوسیستم ***Hadoop*** یک پلتفرم نماینده برای پیاده‌سازی کلان داده است. به عنوان مثال، ***HDFS***، ***MapReduce***، ***YARN***، و غیره، عملکردهایی را به عنوان ماژول‌های منحصر به فرد برای ذخیره، پردازش و مدیریت داده‌ها در سیستم‌های داده بزرگ ارائه می‌دهند. ***Cloudera*** که یک محصول تجاری است که امنیت و مدیریت را افزایش می‌دهد، نماینده یک پلتفرم به عنوان سرویس (***PaaS***) است.
- **لایه کاربردی:** بسته به زمینه‌ای که سیستم کلان داده و داده‌های پردازش شده در آن استفاده می‌شود، باید از روش‌های تحلیل مناسب و ابزارهای بصری استفاده شود که توسط لایه کاربردی پوشش داده می‌شود. به عبارت دیگر، الگوریتم‌هایی برای به دست آوردن نتایج تحلیل مورد نیاز کاربران یا تجهیزات و نرم‌افزارهایی که کاربران می‌توانند مستقیماً از آنها استفاده کنند، در لایه کاربردی ضروری هستند.

ب) چارچوب سیستم سه لایه *C2* از نظر جریان داده‌های میدان نبرد

در میدان نبرد، یک سیستم ***C2*** ابزاری است که اطلاعات را بین عناصر متعدد میدان نبرد تحت شبکه تحت مفهوم «سنسور به تیرانداز» مبادله می‌کند و از عزم فرمانده و اقدام تیرانداز به طور مؤثر پشتیبانی می‌کند. به طور خاص، با توجه به فرآیندهای تولید، پردازش و استفاده از داده‌های میدان جنگ مورد استفاده در سیستم ***C2*** به سه لایه تقسیم می‌شود که در لایه‌های تولید داده، پردازش داده و استفاده از داده بیان می‌شود. جزئیات هر لایه در زیر ارائه شده و در شکل ۳ نشان داده شده است.

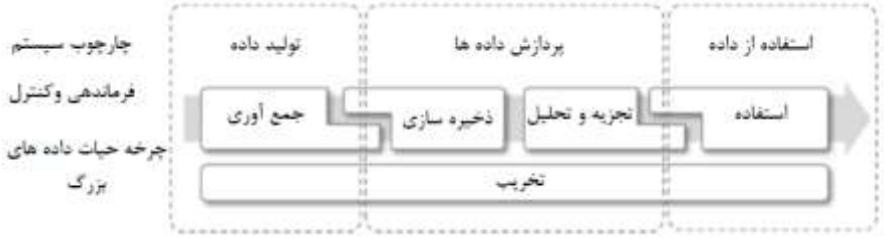


شکل (۳) چارچوب سیستم سه لایه C2 که بر اساس جریان داده‌های میدان نبرد طبقه‌بندی شده است. [۱۰]

- **لایه تولید داده:** این لایه حجم زیادی و انواع مختلفی از داده‌های میدان نبرد را تولید می‌کند و این داده‌ها را به مرحله بعدی یعنی لایه پردازش داده‌ها منتقل می‌کند. عناصری که داده‌های جنگی را تولید می‌کنند در مکان‌های متنوعی مانند مناطق جنگی، مناطق اردوگاه نظامی و مناطق غیرنظامی عمل می‌کنند. نمونه‌هایی از تولیدکننده‌های داده رزمی عبارتند از: دارایی‌های اطلاعاتی، دارایی‌های رزمی، امکانات پشتیبانی رزمی، سایر دستورات، اینترنت و غیره. داده‌های رزمی همچنین شامل داده‌های حسگر از ***IoBT***های مختلف، سیگنال ***GPS***، تصویر/ویدئو، سیگنال صوتی/رادیویی، متن/اسناد می‌شوند. و غیره. تقریباً تمام اشکال داده تحت پوشش یک سیستم کلان داده معمولی را شامل می‌شود.
- **لایه پردازش داده:** این لایه در مرکز داده یکپارچه اجرا می‌شود، جایی که مراحل اصلی چرخه عمر داده‌های بزرگ برای ذخیره و تجزیه و تحلیل داده‌های جمع‌آوری شده پیاده‌سازی می‌شوند. لایه پردازش داده را می‌توان به زیرساخت و پلتفرم (یا پلتفرم به عنوان سرویس (***PaaS***)) تقسیم کرد. زیرساخت به معنای منابع فیزیکی/مجازی مانند محاسبات ابری، دستگاه‌های شبکه و غیره است و پلتفرم سیستم کلان داده ممکن است مانند ***Hadoop***، ***Cloudera*** و غیره باشد.

- **لایه استفاده از داده:** این لایه به فرماندهان کمک می‌کند تا با تجسم داده‌های تجزیه و تحلیل شده در لایه پردازش داده به عنوان اطلاعات ارزشمند، تصمیم‌گیری کنند. اطلاعات رزمی بلادرنگ مستقیماً در دسترس فرمانده و کارکنانی است که در مقر فرماندهی و دارایی‌های جنگی/اطلاعاتی در میدان نبرد قضاوت و تصمیم‌گیری می‌کنند.

ج) چارچوب سیستم کلان داده C2 پیشنهادی[10]



شکل (۴) شرح ارتباط بین چارچوب سیستم سه لایه C2 و چرخه عمر کلان داده.

همان‌طور که قبلاً ذکر شد، چارچوب سیستم سه لایه ***C2*** بر اساس جریان داده برای تولید، پردازش و استفاده از داده‌های میدان نبرد طبقه‌بندی شد و رابطه نزدیکی با هر مرحله از چرخه حیات داده‌های بزرگ و معماری سیستم لایه‌ای داشت. بخش الف و ب. به ترتیب. همبستگی بین چارچوب سیستم ***C2*** و چرخه عمر کلان داده در شکل ۳ ارائه شده است. اول، لایه تولید داده عمدتاً با جمع‌آوری داده‌ها مطابقت دارد. لایه پردازش داده در ذخیره و تجزیه و تحلیل داده‌های جمع‌آوری شده نقش دارد و لایه استفاده از داده گامی است که شامل استفاده از اطلاعات ارزشمند ارائه شده توسط داده‌های بزرگ است. در نهایت، تخریب، در چرخه حیات داده‌های بزرگ، عملی است که در تمام لایه‌های چارچوب رخ می‌دهد. همانطور که در مطالعه قبلی [۱۹] ذکر شد، امنیت داده‌ها یک عامل اساسی در چرخه حیات است. هر لایه از یک سیستم ***C2*** باید بتواند داده‌های غیر ضروری یا غیرقانونی را بلافاصله حذف کند. مراحل چرخه حیات به خوبی روی هر لایه همپوشانی دارند، به این معنی که موارد لازم برای پیوند مراحل چارچوب در مراحل متقابل وجود دارد.

چارچوب چهار لایه کلان داده نیز مربوط به چارچوب سیستم ***C2*** است که بر اساس جریان داده‌های میدان نبرد طبقه‌بندی شده است و شکل ۴ این ارتباط را بیان می‌کند. به عنوان مثال، در لایه تولید داده یک سیستم ***C2***، زیرساخت را می‌توان دستگاه‌های ***IoBT*** و شبکه‌ای که آن دستگاه‌ها را به هم متصل می‌کند، نام برد. در نتیجه، شکل ۳ اجزای مورد نیاز در هر لایه از یک سیستم ***C2*** را برای هر چارچوب کلان داده اعمال شده در سیستم سه لایه ***C2*** نشان

می‌دهد. با این حال، لایه پلت فرم داده‌های بزرگ، پلتفرمی است که به عنوان سرویسی برای پیاده‌سازی یک سیستم کلان داده ارائه می‌شود و بنابراین، لایه تولید داده و لایه مصرف داده قابل اجرا نیستند.

شکل (۵) شرح ارتباط بین چارچوب سیستم سه لایه C2 و معماری سیستم داده‌های بزرگ. [۱۰]

د) معماری امنیتی برای سیستم کلان داده نظامی *C2*

برای راه اندازی ایمن سیستم‌های کلان داده در محدوده مقررات مربوط به حفاظت از اطلاعات، دامیان و همکاران. [***20***] و ***Cloud Security Alliance [21]*** تهدیدات امنیتی را تجزیه و تحلیل کرده‌اند و چندین سازمان بین المللی استانداردها و دستورالعمل‌های امنیتی را پیشنهاد کرده‌اند [***22***-***23***]. علاوه بر این، برخی از مطالعات [***24***، ***25***] ملاحظات امنیتی قابل اجرا در سیستم‌های کلان داده را ارائه کرده‌اند، در حالی که ابولمهدی و همکاران. [***26***] و حسین و همکاران. [***27***] الزامات امنیتی را ذکر کنید که باید به طور منحصر به فرد در زمینه‌های خاص مانند مراقبت‌های بهداشتی و شبکه‌های هوشمند اعمال شوند. این‌بخش به طور دقیق تری امنیت یک سیستم نظامی ***C2*** با داده‌های بزرگ را بررسی می‌کند. با تجزیه و تحلیل تهدیدات امنیتی که باید در لایه‌های چارچوب سیستم ***C2*** طبقه‌بندی شده دربخش ۳ در نظر گرفته شوند و الزامات ارائه شده است، ما یک معماری امنیتی مناسب برای یک سیستم ***C2*** با داده‌های بزرگ پیشنهاد می‌کنیم.

ه) چارچوب سیستم سه لایه *C2* از نظر جریان داده‌های میدان نبرد

C2یک سیستم اطلاعات دفاعی است که در عملیات نظامی استفاده می‌شود و دارای ویژگی‌های امنیتی سختی است. اولاً، تمام اطلاعات تحت پوشش سیستم ***C2*** اطلاعات مهم و حساسی هستند که می‌توانند بر امنیت ملی تأثیر بگذارند. بنابراین، یک سیستم ***C2*** باید با حفظ سطح بالایی از امنیت تحت هر شرایطی، داده‌ها را به صورت ایمن مدیریت کند. ثانیاً تهدید جدی دشمن برای سامانه ***C2*** نیروهای دوست مستمر است. مدیران مسئول امنیت اطلاعات در یک سیستم ***C2*** باید تهدیدات دشمن را ترجیحا تجزیه و تحلیل کنند و آنها را به طور فعال تکمیل کنند. سوم، مانند ساختار سلسله مراتبی متمایز سازمان‌های نظامی، تفاوت‌ها در اختیار کاربر سیستم ***C4I*** نیز آشکار است. به دلیل این تفاوت‌ها در اختیارات کاربران، سیستم نیاز به احراز هویت واضح دارد و استفاده از داده‌ها و دامنه دسترسی را متمایز می‌کند. در نهایت، در صورت نیاز، یک سیستم ***C4I*** یک شبکه ایزوله است و دارای یک نقطه اتصال با یک شبکه خارجی است. بنابراین، اقدامات امنیتی برای نقاط تماس با شبکه‌های خارجی ضروری است و تأیید داده‌های وارد شده از خارج ضروری است.

چالش‌های امنیتی و الزامات مرتبط با کلان داده‌ها در شبکه‌های فرماندهی و کنترل

در این‌بخش تهدیدات امنیتی را تجزیه و تحلیل می‌کنیم و الزامات امنیتی را برای هر یک از سه لایه طبقه‌بندی شده در چارچوب سیستم کلان داده ***C2*** ارائه می‌کنیم. شکل ۶ به طور جامع الزامات امنیتی اعمال شده برای هر لایه از چارچوب سیستم ***C2*** را نشان می‌دهد و جزئیات دربخش فرعی ارائه شده است.

شکل (۶) الزامات امنیتی پیشنهادی اعمال شده در چارچوب ۳ لایه. [۱۰]

۱. لایه تولید داده

در لایه تولید داده‌ها، بسیاری از دارایی‌های نظامی شبکه‌ای، انواع و مقدار زیادی داده‌های میدان جنگ را تولید می‌کنند. جنگنده‌های انسانی، واحدهای مکانیزه، پهپادها، رادارها و غیره، دارایی‌های نظامی هستند که به عنوان ***IoBT*** در نظر گرفته می‌شوند و داده‌های میدان نبرد را ارائه می‌دهند. بر اساس ویژگی‌های اینترنت اشیاء نظامی، مطالعات مختلفی در مورد الزامات امنیتی انجام شده است. به طور خاص، در میان مطالعاتی که الزامات امنیتی سیستماتیک را ارائه کردند، ***Mavroeidakos*** و همکاران. [***28***] به تهدیدات امنیتی، مانند بدافزار، بات نت، باج افزار، و غیره، و حملات سایبری مانند حمله لایه فیزیکی، حمله شبکه، و حمله انسان در وسط و غیره پرداخت. [۲۹] همچنین تهدیدات امنیتی احتمالی برنامه‌های ***IoT*** را بر اساس محرمانه بودن، یکپارچگی و در دسترس بودن پیشنهاد کرد که به عنوان سه‌گانه سیا شناخته می‌شود. بنابراین، ما قصد داریم با تحلیل تهدیدات امنیتی ***IoBT*** که در محدوده سیستم ***C2*** عمل می‌کند، الزامات امنیتی را به شرح زیر ارائه کنیم. همانند اینترنت اشیا عمومی، ***IoBT*** نیز در برابر عفونت‌های بدافزار آسیب پذیر است. بنابراین، اقداماتی باید برای جلوگیری از آلودگی با باج افزار یا سوء استفاده به عنوان یک بات نت انجام شود. علاوه بر این، فضای فیزیکی این لایه یک منطقه رزمی است و دشمنان در همان فضا عمل می‌کنند. اگر دشمن تجهیزات ***IoBT*** نیروهای دوست را بدست آورد، دسترسی غیرمجاز به شبکه‌های ما، سرقت اطلاعات

داخلی و ارائه اطلاعات نادرست خواهد داشت. علاوه بر این، دشمن می‌تواند سیگنال‌های شبکه سیمی و بی‌سیم را برای حمله به دسترسی غیرمجاز شبکه از طریق استشمام و جعل، ربوده باشد. یک سیستم ***C2*** یک شبکه ایزوله است. با این حال، گاهی اوقات داده‌های مربوط به یک منطقه دیگر، مانند سطوح دیگر سیستم‌های ***C2*** یا اینترنت در منطقه مدنی نیز مورد نیاز است. یعنی نقاط اتصال با شبکه‌های خارجی وجود دارد. بنابراین، مدیریت امنیتی آن اتصالات، که می‌توانند کانال‌های ورودی داده خارجی باشند، بسیار مهم است. بنابراین، ما شش الزام امنیتی را برای لایه تولید داده پیشنهاد می‌کنیم.

- **امنیت نقطه پایانی:** دستگاه‌های نقطه پایانی که داده‌ها را تولید می‌کنند ممکن است به عنوان ***IoBT*** نامیده شوند که از طریق یک شبکه به هم متصل می‌شوند. ***IoBT*** اساساً به عملکرد ضد بدافزار نیاز دارد تا آسیب‌پذیری در برابر عفونت باج افزار را جبران کند. علاوه بر این، با توجه به محیط عملیاتی میدان نبرد، در دسترس بودن دستگاه باید افزایش یابد و داده‌ها برای آماده شدن برای موقعیت‌های خطرناک فوراً پاک شوند.
- احراز هویت: دو ملاحظات برای احراز هویت در لایه تولید داده وجود دارد: اولین مورد احراز هویت کاربر در دستگاه است. دستگاه می‌تواند با اعمال احراز هویت چندعاملی مانند نام کاربری/رمز عبور و احراز هویت بیومتریک تأیید کند که کاربر به دستگاه دسترسی دارد. دوم مجوز دسترسی به سیستم است. با بررسی اینکه آیا دستگاه به عنوان بخشی از سیستم ثبت شده است، کنترل دسترسی شبکه (***NAC***) ممکن است برای تأیید شناسه‌های منحصر به فرد مانند آدرس‌های ***IP*** و ***MAC*** دستگاه اعمال شود.
- **رمزگذاری داده‌ها:** رمزگذاری برای اطمینان از محرمانه بودن داده‌ها ضروری است و دو دیدگاه نیز باید در نظر گرفته شود: زمانی که داده‌ها در یک دستگاه جمع‌آوری و ذخیره می‌شوند و زمانی که داده‌ها از طریق شبکه منتقل و دریافت می‌شوند.
- **مسئله حفظ حریم خصوصی:** مسائل حفظ حریم خصوصی برای داده‌های بزرگ جمع‌آوری‌شده‌بخش حیاتی امنیت است. اگر اطلاعات شخصی رزمندگان تحت پوشش یک سیستم ***C4I*** جمع‌آوری شود، مسائل مربوط به حریم خصوصی نیز باید به طور کامل در نظر گرفته شود. برای مثال، نه تنها اطلاعات شخصی عمومی (مثلاً نام، طبقه و جنسیت رزمنده) بلکه اطلاعات مکان و سیگنال‌های زیستی نیز باید با حساسیت مدیریت شوند. بنابراین، سیستم باید با مقررات حفظ حریم خصوصی کشور مانند

مقررات حفاظت از داده‌های عمومی (***GDPR***) و قانون حفظ حریم خصوصی مصرف کنندگان کالیفرنیا (***CCPA***) مطابقت داشته باشد.

- **امنیت شبکه بی‌سیم:** اطمینان، در دسترس بودن و یکپارچگی باید برای ارتباطات ترافیکی بی‌سیم در میدان جنگ تضمین شود. محرمانه بودن را می‌توان از طریق رمزگذاری داده‌ها (در حین انتقال یا در حالت استراحت) که در بالا ارائه شد تقویت کرد، اما اقدامات تکمیلی بیشتری برای جلوگیری از وقفه در دسترس بودن ناشی از حملات پارازیت و هرگونه آسیب به یکپارچگی ناشی از سرقت ترافیک یا حملات تزریق از طرف دشمن مورد نیاز است. . بنابراین، برای محافظت از شبکه بی‌سیم در لایه تولید داده، لازم است توانایی غلبه بر حملات ترافیکی را داشته باشیم و با تأیید ترافیک داده ثابت کنیم که ترافیک در حین انتقال/دریافت تحت تأثیر قرار نگرفته است.
- امنیت نقطه اتصال: در یک شبکه ایزوله، نقاط اتصال با شبکه‌های خارجی عوامل آسیب‌پذیری هستند که باید با دقت با آنها برخورد کرد. به طور خاص، برای انتقال داده‌ها از شبکه خارجی به داخل، شبکه برای نقطه اتصال باید به طور ایمن پیکربندی شود و فرمت و ایمنی داده‌ها باید تأیید و ارسال شود.

۲. لایه پردازش داده

۱)زیرساخت ارائه شده توسط رایانش ابری

رایانش ابری مقیاس‌پذیری عالی دارد. ابر می‌تولند منابع فیزیکی محدود را با تقسیم عملکرد سرور و فضای ذخیره‌سازی کارآمد به کار گیرد. بنابراین، محاسبات ابری یک زیرساخت نماینده برای پیاده‌سازی یک سیستم کلان داده است که توسط ۶ ولت مشخص می‌شود. گروه تحقیقاتی ما قبلاً الزامات امنیتی برای یک سیستم دفاعی ***C4I*** مبتنی بر ابر را مطالعه کرده بود [***30, 31***]. برای استخراج الزامات امنیتی در تحقیقات قبلی خود، به الزامات امنیتی شناسایی شده توسط خط پایه کنترل‌های امنیتی (***FedRAMP([32]***، راهنمای الزامات امنیت محاسبات ابری***[33] (DISA)***، راهنمای گواهینامه امنیتی برای سرویس ابری (اینترنت کره و اینترنت کره) اشاره کردیم. آژانس مورد امنیت) [***34***]، الزامات امنیتی برای سیستم مجازی‌سازی سرور (انجمن فناوری ارتباطات) [***35***]، و دستورالعمل‌های امنیتی مؤسسه ملی و عمومی برای رایانش ابری (سرویس اطلاعات ملی) [***36***]. الزامات شامل پنج دسته با ۲۸ مورد است. امنیت مجازی‌سازی (۹ مورد)، امنیت داده‌ها (۹ مورد)، امنیت شبکه (۱ مورد)، کنترل دسترسی (۴ مورد) و مدیریت ریسک (۵ مورد) [***20***]. در این مقاله دو مورد اضافی برای نقطه اتصال پیشنهاد

شده است. تماس‌های فیزیکی با سطوح مختلف سیستم‌های ***C2*** یا اینترنت در لایه تولید داده در زیرساخت مرکز داده وجود دارد. بنابراین، اضافه شد: تأیید جریان داده از طریق نقاط اتصال برای امنیت داده‌ها و مدیریت امنیت نقاط اتصال موجود در شبکه ایزوله در امنیت شبکه. مطالب اضافه شده با فونت پررنگ در شکل ۶ نمایش داده شده است.

۲)پلتفرم به عنوان سرویس Hadoop، Cloudera - (PaaS)

پیش از این، دربخش ۴. ۲. ۱. ما امنیت زیرساخت را بررسی کردیم که سیستم‌های کلان داده را به عنوان منابع فیزیکی یا مجازی پیاده‌سازی می‌کند. ما روی امنیت ***Hadoop*** و در این‌بخش پلتفرمی به عنوان سرویس (***PaaS***) از لایه‌های پردازشی که داده‌های بزرگ را ذخیره، مدیریت و تجزیه و تحلیل می‌کند، تمرکز می‌کنیم. بررسی اجمالی امنیتی [***37***]، منتشر شده توسط ***Cloudera***، که خدمات مبتنی بر ***Hadoop*** ارائه می‌دهد، سه موضوع امنیتی (یعنی احراز هویت، رمزگذاری و مجوز) را شرح می‌دهد. علاوه بر این، برخی از مطالعات [***38***-***40***] معانی مانند احراز هویت، مجوز، رمزگذاری، نظارت بر سیستم را با بیان آنها از قبیل کنترل دسترسی، مجوز، امنیت داده در زمان استراحت، ارتباطات بین گره‌ای امنیت داده، بازرسی و طبقه‌بندی منتقل می‌کنند. . بنابراین، الزامات امنیتی برای یک پلت فرم پردازش داده یک سیستم کلان داده ***C2*** را می‌توان در چهار دسته سازماندهی کرد: احراز هویت، مجوز، رمزگذاری، و نظارت و ممیزی امنیتی.

- احراز هویت: این یک الزام امنیتی اساسی برای هر سیستم اطلاعاتی است، کاربران باید هویت خود را ثابت کنند، و سیستم لزوماً بررسی می‌کند که آیا سیستم کلان داده ***C2*** می‌تواند در چهار دسته سازماندهی شود: احراز هویت، مجوز، رمزگذاری، و نظارت و ممیزی امنیتی
- **احراز هویت:** این یک الزام امنیتی اساسی برای هر سیستم اطلاعاتی است، کاربران باید هویت خود را ثابت کنند، و سیستم لزوماً بررسی می‌کند که آیا کاربر قابلیت دسترسی دارد یا خیر. روشن کردن هویت کاربرانی که به سیستم دسترسی دارند در میان تهدید نفوذ مداوم دشمن به شبکه، یک عامل امنیتی ضروری برای اطمینان از اینکه مدیران سیستم داده‌های بزرگ ***C2*** می‌توانند کل سیستم را به طور پایدار اداره کنند، است. احراز هویت در پلتفرم ***Hadoop*** از بسیاری از فناوری‌های کنترل دسترسی مختلف استفاده می‌کند (مانند لیست‌های کنترل دسترسی (***ACL***، ***ACL***های توسعه‌یافته ***HDFS*** و کنترل دسترسی مبتنی بر نقش (***RBAC***)) و مکانیسم ***Kerberos*** را اعمال می‌کند. ***Kerberos*** به طور گسترده‌ای به عنوان

مکانیزم احراز هویت قابل استفاده برای اکثر خوشه‌های ***Hadoop*** مانند ***HDFS***، ***MapReduce*** و ***YARN*** استفاده می‌شود [***37***].

- **مجوز:** در یک سیستم ***C2*** نظامی، محدوده دسترسی به داده‌های اختصاص داده شده به کاربران بسته به تفاوت‌های سلسله مراتبی در سازمان و نقش کارکنان، به طور گسترده‌ای متفاوت است. تمام فعالیت‌های درون خوشه ***Hadoop***، مانند دسترسی به داده‌ها، استفاده، مشاهده و اصلاحات اداری، باید به درستی در چارچوب اختیاری که به کاربر یا مدیر اختصاص داده شده است، اجرا شود و مکانیزم مجوز باید برای این منظور اعمال شود. در خوشه‌های ***Hadoop*** مانند ***HDFS***، ***MapReduce*** و ***YARN***، کنترل دسترسی از طریق مجوزهای سبک ***POSIX*** اعمال می‌شود که به هر فایل و دایرکتوری اجازه می‌دهد. ***ACL***های تقسیم شده نیز اعمال می‌شوند، یا ***Apache RANGER*** برای مدیریت مجوز برای هر خوشه استفاده می‌شود [***37***].
- **رمزگذاری:** رمزگذاری آخرین خط دفاعی است که یک هکر به داده‌های ما دسترسی کامل پیدا می‌کند [***41***]. داده‌های حساسی که نیاز به محافظت دارند، چه در ذخیره‌سازی یا در حین حمل و نقل ذخیره شوند، باید رمزگذاری شوند تا محتویات آن فاش نشود و نباید توسط کاربران غیرمجاز رمزگشایی شوند. در سیستم‌های نظامی ***C4I***، رمزگذاری داده‌ها یک الزام امنیتی حیاتی است که در برابر نقض محرمانه بودن به دلیل تهدیدات دشمن محافظت می‌کند. خوشه ***Hadoop*** با اعمال امنیت لایه انتقال (***TLS***) و لایه سوکت ایمن (***SSL***) نه تنها برای داده در حالت استراحت بلکه برای داده در حال انتقال نیز رمزگذاری را تضمین می‌کند [***37***].
- **گزارش نظارت و حسابرسی امنیتی:** مدیر امنیت سیستم باید رفتار خوشه ***Hadoop*** را نظارت کند و به سرعت رویدادهایی را که از معیارهای امنیتی تعیین شده منحرف می‌شوند، تشخیص دهد. گاهی اوقات با ترک تمام اقدامات تولید شده در خوشه ***Hadoop***، گزارش ذخیره شده برای یافتن علت و معلول مشکل تجزیه و تحلیل می‌شود. ***Ganglia*** و ***Nagios*** ابزارهای نظارتی مبتنی بر منبع باز [***38***] هستند که می‌توانند برای ***Hadoop*** نیز اعمال شوند، و مدیر کلودرا نیز قابلیت‌های نظارت امنیتی با کارایی بالا را برای پلتفرم کلان داده فراهم می‌کند [***37***].

۳. لایه استفاده از داده

نتایج تجزیه و تحلیل داده‌های بزرگ در یک سیستم ***C2*** برای استفاده از دارایی‌های جنگی/اطلاعاتی در ستاد فرماندهی کنترل تجسم می‌شود. بنابراین، هم ابزار تصمیم‌گیری و هم

دستگاه تجسم که در سیستم نظامی ***C2*** کار می‌کنند باید الزامات امنیتی دستگاه نقطه پایانی را برآورده کنند. به این معنا که تمام پایانه‌هایی که در این لایه کار می‌کنند بخشی از ***IoBT*** متصل به شبکه هستند و دارای ویژگی‌های امنیتی مشابه دستگاه‌های مورد استفاده در لایه تولید داده هستند. با این حال، به دلیل ویژگی‌های سیستم‌های ***C2***، نقطه اتصال در لایه استفاده از داده وجود ندارد. بنابراین، امنیت نقطه اتصال از شش الزامات امنیتی پیشنهاد شده دربخش ۴. ۲. ۱ مستثنی شده است. سپس، از آنجایی که محدوده اطلاعات ارائه شده با توجه به اختیارات کاربر محدود است، مجوز به عنوان یک نیاز امنیتی اضافه می‌شود. بنابراین، شش الزام امنیتی (به عنوان مثال، امنیت دستگاه نقطه پایانی، احراز هویت، رمزگذاری داده‌ها، مسئله حریم خصوصی، امنیت شبکه بی‌سیم و مجوز) باید برآورده شود تا از عملکرد ایمن سیستم اطمینان حاصل شود. [۴۲و۴۳]

جدول (۴) الزامات امنیتی سیستم فرماندهی و کنترل *C2* دفاع مبتنی بر شبکه ابری [۴۲و۴۳]

امنیت مجازی‌سازی	امنیت داده ها	امنیت شبکه	کنترل دسترسی	مدیریت ریسک
• طرح مدیریت منابع مجازی • نظارت بر رفتار منابع • کنترل دسترسی ***Hypervisor*** و بروز رسانی وصله‌های امنیتی • ضد بدافزار • به طور دوره‌ای آسیب‌پذیری امنیتی را در رابط و ***apis*** تجزیه و تحلیل و محافظت کنید. • ردیابی شناسایی و چرخه بقا را برای ماشین مجازی نظارت کنید. • تنظیمات اجزای اولیه ماشین	• جلوگیری از نشت اطلاعات. • سیاست مدیریت رمزگذاری برای دارایی‌های اطلاعاتی و مدیریت لیست دارایی‌های اطلاعاتی • ازکلیدهای رمزگذاری مختلف در محیط‌های مختلف استفاده کنید. • از الگوریتم رمزنگاری تایید شده نظامی استفاده کنید. • سازمان مدیریت سیستم باید به	• حفاظت برای انکار سرویس توزیع شده(***DDos***) • مدیریت شبکه برای نقاط اتصالی که در شبکه ایزوله وجود دارد.	• سیاست و فناوری کنترل برای وضعیت دسترسی از دستگاه‌های قابل حمل و موبایل. • شناسایی کاربران و مدیران با ایجاد مجوز و لغو وظایف. • انتقال و دریافت غیر مجاز داده را مسدود کنید. • احراز هویت و مدیریت یکپارچه دسترسی بیسیم.	کنترل کاربرانی که چندین جلسه را بطور هم زمان دارند. نظارت بر اهداف و مکان ها پیام خطا را به درستی ارائه دهید. شناسایی علت حوادث امنیتی بر اساس داده‌های نظارتی جمع‌آوری شده و ایجاد برنامه‌ای برای واکنش

امنیت مجازی‌سازی	امنیت داده ها	امنیت شبکه	کنترل دسترسی	مدیریت ریسک
مجازی را بدون تغییر نگه دارید. • ترافیک عبوری از ماشین مجازی را نظارت کنید. • لیست استفاده از منابع مجازی را حفظ کنید.	کابران اجازه دهد تا کلیدها را در فواصل زمانی منظم تغییر دهند. • اقداماتی را برای اطمینان از محرمانه بودن داده‌ها هنگام انتقال داده‌ها انجام دهید. • پیاده‌سازی مکانیسم‌هایی برای اعتبارسنجی اطلاعات ورودی و تحویل در سیستم ابری. • دوبلکس کردن تجهیزات حیاتی. • کنترل و مدیریت جریان اطلاعات. • اعتبارسنجی داده‌هایی که از طریق نقطه اتصال می‌آیند.			سریع به حوادث امنیتی آینده. مدیر سیستم امنیت اطلاعات نظامی باید اقدامات امنیتی را در برابر هک داده‌ها و جعل در هنگام کار بر سرور مجازی ایجاد و اجرا کند.

معماری امنیتی پیشنهادی برای داده‌های بزرگ پیاده‌سازی شده در یک سیستم $C2$ نظامی

معماری امنیتی یک چارچوب متحد کننده و خدمات قابل استفاده مجدد است که سیاست‌ها، استانداردها و تصمیمات مدیریت ریسک را اجرا می‌کند [۴۱]. طراحی معماری امنیتی مستلزم درک ساختار کلی سیستم و الزامات امنیتی خاص است. به عبارت دیگر، معماری امنیتی نحوه قرارگیری اقدامات متقابل امنیتی و نحوه ارتباط آنها با معماری کلی سیستم را توصیف می‌کند. از آنجایی که ما یک چارچوب سیستم سه لایه ***C2***، معماری چهار لایه کلان داده و الزامات

امنیتی را پیشنهاد کردیم، می‌توان یک معماری امنیتی برای داده‌های بزرگ پیاده‌سازی شده در یک سیستم ***C2*** نظامی طراحی کرد. برای درک سیستم‌های کلان داده ***C2***، نحوه پیکربندی اجزای هر لایه از یک سیستم ***C2*** را در معماری سیستم کلان داده بررسی کردیم. لایه‌های معماری امنیتی بر اساس لایه‌های ارائه شده در معماری کلان داده طبقه‌بندی می‌شوند. امنیت زیرساخت، امنیت داده‌ها، امنیت پلت فرم داده‌های بزرگ و لایه‌های امنیتی برنامه. برای هر لایه، الزامات امنیتی خاصی در نظر گرفته شده است. شکل ***7*** معماری امنیتی سیستم ***C2*** پیاده‌سازی شده با داده‌های بزرگ را نشان می‌دهد. معماری امنیتی پیشنهادی مبتنی بر ساختار سیستم ***C2*** می‌تواند به اجرای فنی الزامات امنیتی، ارائه خط‌مشی‌ها و دستورالعمل‌های امنیتی و مدیریت ریسک در زمانی که سیستم ***C2*** داده‌های بزرگ را اعمال می‌کند، کمک کند. [44]

شکل (۷) معماری امنیتی پیشنهادی برای داده‌های بزرگ پیاده‌سازی شده در یک سیستم [10] .C2

اول، لایه امنیت زیرساخت به اقدامات امنیتی برای منابع و شبکه‌های فیزیکی یا مجازی نیاز دارد که لایه هر چارچوب سیستم ***C2*** را تشکیل می‌دهند. زیرساخت لایه‌های تولید داده و استفاده از داده عمدتاً از دستگاه‌های فیزیکی نقطه پایانی تشکیل شده‌اند و از طریق یک شبکه بی‌سیم ارتباط برقرار می‌کنند. بنابراین، امنیت دستگاه و امنیت شبکه مورد نیاز است. از آنجایی

که زیرساخت لایه پردازش داده، سیستم رایانش ابری را اعمال می‌کند، معیارهای امنیتی برای سیستم ابری معرفی شده در حوزه نظامی باید اعمال شود. لایه امنیت داده، سطح امنیت کل داده‌های تحت پوشش سیستم را افزایش می‌دهد. رمزگذاری مناسب و تأیید داده‌ها ضروری است زیرا محرمانه بودن و یکپارچگی داده‌ها در سیستم ***C2*** باید کاملاً تضمین شود. هر سه لایه سیستم ***C2*** باید هنگام ذخیره، انتقال و دریافت داده‌ها از طریق شبکه رمزگذاری شوند، که نه تنها برای اطمینان از محرمانه بودن داده‌ها بلکه برای رعایت الزامات حفظ حریم خصوصی ضروری است. علاوه بر این، در لایه پردازش داده‌ها، امنیت داده‌ها به تلاش بیشتری برای مدیریت ایمن داده‌ها نسبت به سایر لایه‌ها نیاز دارد زیرا داده‌های بزرگ برای تجزیه و تحلیل در لایه پردازش داده ذخیره و مدیریت می‌شوند. لایه امنیتی پلتفرم داده‌های بزرگ برای پردازش داده‌ها با پلتفرم‌های کلان داده مانند ***Hadoop*** و ***Cloudera*** اعمال می‌شود. چهار الزام امنیتی برای این لایه امنیتی ارائه شده است: احراز هویت، مجوز، رمزگذاری، و نظارت و ممیزی. با این حال، همانطور که قبلا ذکر شد، لایه‌های تولید و استفاده از داده‌ها از ***Hadoop*** یا ***Cloudera*** به عنوان یک پلتفرم کلان داده استفاده نمی‌کنند. ***[45]*** بنابراین نیازی به در نظر گرفتن فاکتورهای امنیتی نیست. در یک لایه امنیتی برنامه، امنیت برای نرم افزار و سخت افزار کاربر محور برای هر لایه تعریف شده است. به عنوان مثال، احراز هویت نرم افزارهایی که به طور مستقیم توسط کاربران به آنها دسترسی دارند تقویت می‌شود و امنیت محیط وب برای تولید داده‌ها و لایه‌های استفاده مورد نیاز است. در لایه پردازش داده که معادل تجزیه و تحلیل داده‌های بزرگ است، عوامل امنیتی لایه پلتفرم کلان داده نیز در نظر گرفته می‌شود که به همان سطح امنیت نیاز دارد زیرا خدمات مبتنی بر ***Hadoop*** را ارائه می‌دهد. ***[46,47]***

در نتیجه، می‌توان گفت که معماری امنیتی سیستم ***C2*** داده‌های بزرگ پیشنهادی، ساختاری از یک سیستم امنیتی است که برای هر ساختار سلسله مراتبی ضروری است. هنگام طراحی یک سیستم ***C2*** با فناوری داده‌های بزرگ، معماری امنیتی نکات امنیتی را ارائه می‌دهد که باید در نظر گرفته شود.

روش‌شناسی تحقیق

این پژوهش از منظر هدف کاربردی می‌باشد. روش تحقیق مورداستفاده در این پژوهش توصیفی تحلیلی است. از نظر روش تجزیه و تحلیل داده‌ها، این پژوهش کیفی است. داده‌های کیفی بدست آمده از مطالعه و بررسی اسناد و منابع کتابخانه‌ای در این حوزه، نقش فناوری نوظهور کلان داده در توسعه شبکه‌های فرماندهی و کنترل نسل جدید را نشان می‌دهد. نتایج حاصل می‌تواند در توسعه و ارتقاء سامانه‌های بومی فرماندهی و کنترل در کشورمان مورد

استفاده قرار گیرد. ابزار و روش تجزیه و تحلیل داده‌ها از نوع اکتشافی است. محقق با جستجوی ادبیات تحقیق، مصاحبه با خبرگان و مشورت با اساتید به جمع‌آوری اطلاعات کتابخانه‌ای از متون علمی و مقالات مرتبط با موضوع تحقیق و بررسی جامعی انجام داده است. در ادامه جدیدترین و معتبرترین آنها انتخاب و مفاهیم مرتبط با کلان داده، روند تکامل شبکه‌های فرماندهی وکنترل، توسعه داده‌های بزرگ برای توسعه سیستم ***C2***، با استفاده از فناوری داده‌های بزرگ، از سه جنبه مرکز داده بزرگ، محاسبات ابری و امنیت داده‌ها مورد بررسی وتجزیه و تحلیل قرار گرفت و سپس نتیجه‌گیری انجام و پیشنهادهایی به منظور استفاده از یافته‌های این پژوهش در توسعه و ارتقاءسامانه‌های فرماندهی و کنترل در جمهوری اسلامی ایران ارائه شده است.

تجزیه وتحلیل داده‌ها

این مقاله یک چارچوب سیستم جدید و معماری امنیتی بهبود یافته را برای کلان داده‌های نظامی اعمال شده در سیستم ***C2*** پیشنهاد می‌کند. چارچوب سیستم و معماری امنیتی یک چارچوب عملی و سیستماتیک برای ایجاد یک ***C2*** امن‌تر خواهد بود.

۱- معماری امنیتی یک چارچوب متحد کننده و خدمات قابل استفاده مجدد است که سیاست‌ها، استانداردها و تصمیمات مدیریت ریسک را اجرا می‌کند [۴۱]. طراحی معماری امنیتی مستلزم درک ساختار کلی سیستم و الزامات امنیتی خاص است. به عبارت دیگر، معماری امنیتی نحوه قرارگیری اقدامات متقابل امنیتی و نحوه ارتباط آنها با معماری کلی سیستم را توصیف می‌کند. از آنجایی که ما یک چارچوب سیستم سه لایه ***C2***، معماری چهار لایه کلان داده و الزامات امنیتی را پیشنهاد کردیم، می‌توان یک معماری امنیتی برای داده‌های بزرگ پیاده‌سازی شده در یک سیستم***C2*** نظامی طراحی کرد. برای درک سیستم‌های کلان داده ***C2***، نحوه پیکربندی اجزای هر لایه از یک سیستم ***C2*** را در معماری سیستم کلان داده بررسی کردیم. لایه‌های معماری امنیتی بر اساس لایه‌های ارائه شده در معماری کلان داده طبقه‌بندی می‌شوند. امنیت زیرساخت، امنیت داده‌ها، امنیت پلت فرم داده‌های بزرگ و لایه‌های امنیتی برنامه. برای هر لایه، الزامات امنیتی خاصی در نظر گرفته شده است. شکل ۷ معماری امنیتی سیستم ***C2*** پیاده‌سازی شده با داده‌های بزرگ را نشان می‌دهد. معماری امنیتی پیشنهادی مبتنی بر ساختار سیستم ***C2*** می‌تواند به اجرای فنی الزامات امنیتی، ارائه خط‌مشی‌ها و دستورالعمل‌های امنیتی و مدیریت ریسک در زمانی که سیستم ***C2*** داده‌های بزرگ را اعمال می‌کند، کمک کند. ***[44]***

۲- **اول**، لایه امنیت زیرساخت به اقدامات امنیتی برای منابع و شبکه‌های فیزیکی یا مجازی نیاز دارد که لایه هر چارچوب سیستم ***C2*** را تشکیل می‌دهند. زیرساخت لایه‌های تولید داده و استفاده از داده عمدتاً از دستگاه‌های فیزیکی نقطه پایانی تشکیل شده‌اند و از طریق یک شبکه بی‌سیم ارتباط برقرار می‌کنند. بنابراین، امنیت دستگاه و امنیت شبکه مورد نیاز است. از آنجایی که زیرساخت لایه پردازش داده، سیستم رایانش ابری را اعمال می‌کند، معیارهای امنیتی برای سیستم ابری معرفی شده در حوزه نظامی باید اعمال شود. لایه امنیت داده، سطح امنیت کل داده‌های تحت پوشش سیستم را افزایش می‌دهد. رمزگذاری مناسب و تأیید داده‌ها ضروری است زیرا محرمانه بودن و یکپارچگی داده‌ها در سیستم ***C2*** باید کاملاً تضمین شود. هر سه لایه سیستم ***C2*** باید هنگام ذخیره، انتقال و دریافت داده‌ها از طریق شبکه رمزگذاری شوند، که نه تنها برای اطمینان از محرمانه بودن داده‌ها بلکه برای رعایت الزامات حفظ حریم خصوصی ضروری است. علاوه بر این، در لایه پردازش داده‌ها، امنیت داده‌ها به تلاش بیشتری برای مدیریت ایمن داده‌ها نسبت به سایر لایه‌ها نیاز دارد زیرا داده‌های بزرگ برای تجزیه و تحلیل در لایه پردازش داده ذخیره و مدیریت می‌شوند. لایه امنیتی پلتفرم داده‌های بزرگ برای پردازش داده‌ها با پلتفرم‌های کلان داده مانند ***Hadoop*** و ***Cloudera*** اعمال می‌شود. چهار الزام امنیتی برای این لایه امنیتی ارائه شده است: احراز هویت، مجوز، رمزگذاری، و نظارت و ممیزی. با این حال، همانطور که قبلا ذکر شد، لایه‌های تولید و استفاده از داده‌ها از ***Hadoop*** یا ***Cloudera*** به عنوان یک پلتفرم کلان داده استفاده نمی‌کنند. [۴۵] بنابراین نیازی به در نظر گرفتن فاکتورهای امنیتی نیست. در یک لایه امنیتی برنامه، امنیت برای نرم افزار و سخت افزار کاربر محور برای هر لایه تعریف شده است. به عنوان مثال، احراز هویت نرم افزارهایی که به طور مستقیم توسط کاربران به آنها دسترسی دارند تقویت می‌شود و امنیت محیط وب برای تولید داده‌ها و لایه‌های استفاده مورد نیاز است. در لایه پردازش داده که معادل تجزیه و تحلیل داده‌های بزرگ است، عوامل امنیتی لایه پلتفرم کلان داده نیز در نظر گرفته می‌شود که به همان سطح امنیت نیاز دارد زیرا خدمات مبتنی بر ***Hadoop*** را ارائه می‌دهد. [۴۶,۴۷]

نتیجه‌گیری

۱- سیستم فرماندهی و کنترل به عنوان‌بخش مهمی از سیستم قدرت نظامی جدید، جایگاه و نقش فوق العاده مهمی دارد. در عصر داده‌های بزرگ، انواع قدرت رزمی و حسگرهایی که حجم داده‌ها را جمع‌آوری می‌کنند بیشتر و بیشتر می‌شوند، سرعت تولید داده‌ها سریع‌تر و سریع‌تر می‌شود و به موقع بودن پردازش داده‌ها نیز بالاتر و بالاتر می‌رود. سیستم یکپارچه ***C2*** برای ارائه پشتیبانی از داده کاوی و پردازش، ایجاد موقعیت و اشتراک اطلاعات و دستیابی به برنده شدن داده‌ها، بر پلت فرم مدیریت کلان داده تکیه خواهد کرد. در حال حاضر نتایج تحقیقات در مورد کاربرد کلان داده در سیستم ***C2*** به سرعت به روز می‌شود، اما در عین حال با مشکلاتی نیز مواجه است. جمع‌بندی به موقع این دستاوردها و مشکلات جدید، اهمیت مرجع مهمی برای ساخت سیستم اطلاعات فرماندهی ارتش دارد.

۲- توسعه داده‌های بزرگ چالش‌های جدی را برای توسعه سیستم ***C2*** به همراه دارد. که در در ترکیب با استفاده از فناوری داده‌های بزرگ، پیشنهادات مربوطه ارائه می‌شود از سه جنبه مرکز داده بزرگ، محاسبات ابری و امنیت داده‌ها.

۳- ین مقاله به استفاده ایمن و کارآمد از داده‌های بزرگ در حوزه دفاعی با ارائه خاص الزامات امنیتی لازم برای اعمال فناوری داده‌های بزرگ در یک سیستم دفاعی ***C2*** کمک می‌کند. سیستم‌های دفاعی ***C2*** حاوی اطلاعات بسیار حساسی هستند که می‌تواند بر امنیت ملی و زندگی هر یک از رزمندگان تأثیر بگذارد. بنابراین، آنها به سطح بالایی از حفاظت نیاز دارند زیرا حضور دشمن تهدیدی شدید و مداوم است. بنابراین، برای تحقیق در مورد نحوه عملکرد ایمن یک سیستم دفاعی ***C2*** با داده‌های بزرگ، ابتدا این سیستم در سه لایه (لایه‌های تولید داده، پردازش داده و استفاده از داده) طبقه‌بندی شد و این چارچوب سیستم سه لایه ارائه شد. این طبقه‌بندی سیستم ***C2*** را در راستای عملکردهای جمع‌آوری، پردازش و استفاده از داده‌های تولید شده در میدان نبرد مورد بررسی قرار داد و سیستم ***C2*** به عنوان یک سیستم کلان داده با ارائه ارتباط با چرخه حیات داده‌های بزرگ و چهار لایه تحلیل شد. معماری سیستم داده‌های بزرگ با مشخص کردن رابطه متقابل بین چارچوب سیستم سه لایه ***C2*** و معماری سیستم داده‌های بزرگ چهار لایه، اجزای تشکیل دهنده هر لایه به وضوح شناسایی شد و الزامات امنیتی لازم ارائه شد. معماری امنیتی شامل امنیت زیرساخت، امنیت داده، امنیت پلتفرم داده‌های بزرگ و امنیت برنامه‌ها بود. در نتیجه، فناوری داده‌های بزرگ را می‌توان با ارائه عناصر امنیتی خاص برای سیستم‌های ***C2*** که بر

اساس عملکردها و نقش‌ها از حسگرها تا تیراندازها تقسیم‌بندی شده‌اند، به طور ایمن‌تر و مؤثرتر در سیستم‌های ***C2*** اعمال کرد.

پیشنهاد

در راستای مفاهیم مطرح شده در این مقاله در خصوص نقش فناوری نوظهور کلان داده در توسعه شبکه‌های فرماندهی و کنترل نسل جدید و به منظور استفاده از یافته‌های این تحقیق در راهکار نیروها و سازمان‌های نظامی ج. ا. ایران برای پیشرفت فزآینده به سمت فناوری نوظهور کلان داده وارتقاء سامانه‌های فرماندهی و کنترل هوشمند نیروهای مسلح جمهوری اسلامی ایران شایسته است:

۱- سیستم‌های اطلاعات دفاعی، به ویژه سیستم‌های ***C2***، بر اساس سیاست‌های امنیتی در ارتش، دسترسی و افشای اطلاعات بسیار محدودی دارند. به ویژه، به دست آوردن نتایج با پیکربندی یک محیط عملیاتی برای تأیید آن بسیار دشوار است اثربخشی چارچوب کل سیستم و معماری‌های امنیتی سیستم کلان داده***C2*** . در این مطالعه چارچوب سیستم لایه‌ای و معماری امنیتی با تجزیه و تحلیل ویژگی‌های سیستم پیشنهاد شد، اما در آینده باید نحوه اعمال هر نیاز در یک سیستم عامل کاربردی به طور دقیق مورد مطالعه قرار گیرد. اول، برای تجزیه و تحلیل داده‌های بزرگ مورد استفاده نظامی، تهدیدات امنیتی و الزامات امنیتی که هنگام استفاده وجود دارد فن‌آوری‌های تحلیلی مانند روش‌های استاتیک، طبقه‌بندی داده‌ها، داده‌کاوی، یادگیری ماشینی و غیره باید در حوزه داده‌های بزرگ نظامی توسعه بیشتری پیدا کنند. دوم، علاوه بر الزامات امنیتی ارائه شده در این مقاله، لازم است مشخص شود الگوریتم‌های فنی مناسب برای‌بخش دفاع برای هر نیاز. به عنوان مثال، احراز هویت به عنوان یک اقدام امنیتی ضروری برای همه لایه‌های ارائه شده پیشنهاد شد، اما الگوریتم‌های فنی مورد استفاده برای احراز هویت در هر لایه متفاوت است. ارائه مناسب‌ترین الگوریتم برای هر محیط چالشی است که نیاز به تحقیقات بیشتری دارد. بنابراین، برای پیاده‌سازی احراز هویت، رمزگذاری، اعتبارسنجی داده‌ها و حفظ خصوصی برای هربخش از کل سیستم، اگر یک الگوریتم عملی با توجه به محیط نظامی مورد مطالعه قرار گیرد، می‌توان یک سیستم کلان داده***C2*** امن‌تر را پیاده‌سازی کرد. در نهایت، باید بتوان ملاحظات امنیتی را برای تقویت قابلیت همکاری بین ***IoBT*** و سیستم‌های کلان داده که به عنوان بخشی از یک سیستم دفاعی ***C2*** عمل می‌کنند، تجزیه و تحلیل کرد. اینترنت اشیا در حال حاضر منبعی است که داده‌های ورودی را به سیستم ارائه می‌دهد و مطالعات زیادی در ارتباط با سیستم‌های کلان داده انجام شده است. با این حال، تحقیق در زمینه امنیتی برای استفاده ایمن و کارآمد از ***IoBT*** و داده‌های بزرگ نظامی نیاز به توسعه بیشتر دارد.

۲- از یافته‌های این تحقیق به منظورمکانیزه نمودن فعالیت‌های حوزه فرماندهی و کنترل بومی برای پشتیبانی از عملیات مشترک فرا سازمانی و مرکب (خدماتی، پشتیبانی و رزمی در حوزه زمینی، هوایی، دریایی و فضایی).

۳- با یک مدیریت صحیح و استفاده از توان و استعدادهای داخلی کشور می‌توان چالش‌های مرتبط به اتصالات انواع سنسورها و حسگرهارا با قابلیت همکاری و اشتراک اطلاعات با مرجع‌دهی تنظیم استانداردهای مشترک بومی، همجوشی اطلاعات، تحلیل کلان داده هوشمند، شبکه‌های ابر نظامی بومی و دیتا لینک‌های تاکتیکی بومی، را برطرف کرد.

قدردانی

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است بسیار سپاسگزاریم.

منابع

[۱] مهدی نژاد نوری، محمد و علی جبار رشیدی، مجید فخری ومهدی علی نژاد، (زمستان۱۳۹۶)، بررسی نقش فرماندهی وکنترل هوشمند در دفاع دانش بنیان *فصلنامه مطالعات دفاعی استراتژیک*، سال پانزدهم، شماره ۷۰، صص ۴ – ۹۱.

[۵] خداداد هلیلی، جلیل مظلوم، بهرنگ هادیان. (۱۳۹۴). بررسی کاربردهای نظامی فناوری کلان داده و نقش آن در مدیریت صحنه نبرد" *فصل نامه علوم و فنون نظامی*، سال یازدهم، شمارهٔ ۳۳، پاییز ۱۳۹۴، صص ۴۷- ۶۲.

[۶] حافظ محمدی، محمد رضا موحدی صفت. (۱۳۹۹). جایگاه فناوری کلان داده‌ها درارتقاء سامانه فرماندهی و کنترل سایبری در جمهوری اسلامی ایرا ن"، *دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران*، بهمن ماه۱۳۹۹.

[2] Philippe Gros, Senior Research Fellow, Foundation for Strategic Research, October 2, (2019). "The "tactical cloud", a key element of the future combat air system", www. frstrategie. org/home /Notes de la FRS/ (Apr. 16, 2020).

[3] DEREK GROSSMAN, CHRISTIAN CURRIDEN," Chinese Views of Big Data Analytics" Published by the RAND Corporation, Santa Monica, Calif, www. rand. org/t/RRA176-1, *Copyright 2020 RAND Corporation.*

[4] Alena Epifanova"is program officer at the Robert Bosch Center forCentral and Eastern Europe, Russia, and Central Asia","*Deciphering Russia's "Sovereign Internet Law",2020, Auswärtige Politik e. V*, ISSN 1611-7034.

[7] Fazal-e-Amin, Abdullah S. Alghamdi, Iftikhar Ahmad, Tazar Hussain"Big Data for C4I Systems: Goals, Applications,Challenges and Tools","*Deciphering Russia's* ", Fifth international conference on Innovative Computing Technology (INTECH 2015).

[8] Doug Laney. , (2001). "*3D Data Management: Volume, Velocity and Variety*", Application Delivery Strategies (Meta Group)p2.

[9] Jiarui Zhang,a, Gang Wang and Siyuan Wang"Command and Control System Construction in Big Data Era",”*Journal of Physics*: Conf. Series 1168 (2019) 032022-doi: 10. 1088/1742-6596/1168/3/032022.
[10] Seungjin Baek and Young-Gab Kim"*C4I System Security Architecture: A Perspective on Big Data.*
Lifecycle in a Military Environment", *Sustainability2021,* 13, 13827. http: //doi. org/10. 3390/su132413827.
[11] De Mauro, A. ; Greco, M. ; Grimaldi, M. *A formal definition of Big Data based on its essential features*. Libr. Rev. 2016, 65, 122‑135.
[12] Chang, W. L. Grady, N. NIST big data interoperability framework: Volume 2 *Big Data Taxonomy*. NIST Spec. Publ. 2017, 1500, 10.
[13] Patgiri, R. *A Taxonomy on Big Data: Su*rvey. ARXIV 2018, arXiv: 1808. 08474.
[14] Koo, J. ; Kang, G. ; Kim, Y. -G. *Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges*. Sustainability 2020, 12,10571.
[15] Kune, R. ; Konugurthi, P. K. ; Agarwal, A. ; Chillarige, R. R. ; Buyya, R. The anatomy of big data computing. *Softw. Pract. Exp*. 2016,46, 79‑105. [CrossRef]
[16] Shvachko, K. ; Kuang, H. ; Radia, S. ; Chansler, R. The Hadoop Distributed File System. *In Proceedings of the IEEE 26th Symposium.*
[17] Dean, J. ; Ghemawat, S. *MapReduce: Simplified data processing on large cluster. Commu*n. ACM 2008, 51, 107–113. [CrossRef]
[18] Husamaldin, L. ; Saeed, N. *Big Data Analytics Correlation Taxonomy*. Information 2010, 11, 17. [CrossRef]
[19] Koo, J. ; Kang, G. ; Kim, Y. -G. *Security and Privacy in Big Data Life Cycle: A Survey and Open Challenge*s. Sustainability 2020, 12,10571. [CrossRef]
[20] Damiani, E. ; Ardagna, C. A. ; Zavatarelli, F. ; Rekleitis, E. ; Marinos, L. *Big Data Threat Landscape and Good Practice Guide*; European Union Agency for Network and Information Security (ENISA): Athens, Greece, 2016.
[21] Big Data Working Group. *Expanded Top Ten Big Data Security and Privacy Challenges*. Cloud Security Alliance. 2013. Availableonline: https: //downloads. cloudsecurityalliance. org/ initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges . PDF(accessed on 25 August 2021).
[22] Greene, T. ; Shmueli, G. ; Ray, S. ; Fell, J. *Adjusting to the GDPR: The Impact on Data Scientists and Behavioral Researc*hers. BigData 2019, 7, 140‑162. [CrossRef]
[23]Khan, R. A; Alka, K. An Improved Security Threat Model for Big Data Life Cycle. Asian J. *Comput. Sci. Technol*. 2018, 7, 33‑39. [CrossRef]
[24] Rajan, S. (Ed.) Top 10 Big Data Security and Privacy Challenges; *Cloud Security Alliance*: Seattle, WA, USA, 2012;
[25] Yang, K; Lee, D; Kim, K; Yoon, H. *Analysis of Security Threat and Security Requirements of the Bigdata System*. J. Secur. Eng. 2016, 13, 501‑514. [CrossRef]
[26] Abouelmehdi, K; Beni-Hssane, A; Khaloufi, H; Saadi, M. Big data security and privacy in healthcare: A Review. *Procedia Comput*. Sci. 2017, 113, 73‑80. [CrossRef]

[27] Hossain, E. ; Khan, I. ; Un-Noor, F. ; Sikander, S. S. ; Sunny, S. H. Application of Big Data and Machine in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access 2019*, 7, 13960‑13988. [CrossRef]
[28]Mavroeidakos, T; Chaldeakis, V. Threat landscape of next generation IoT-enabled smart grids. In IFIP International Conference onArtificial Intelligence Applications and Innovations; Springer: Cham, Switzerland, 2020.
[29] Puthal, D; Ranjan, R; Chen, J. Big Data Stream Security Classification for IoT Applications. *In Encyclopedia of Big Data Technologies*; Springer: Cham, Switzerland, 2018. [CrossRef]
[30] Koo, J; Kim, Y. –G: Lee, S. H. Design of Security Architecture for the Cloud-Based Korea Military Command and Control System. J. Korean Inst. *Commun. Inf. Sci*. 2020, 45, 400‑408. [CrossRef]
[31]Koo, J. ; Oh, S. -R. ; Lee, S. H. ; Kim, Y. -G. *Security Architecture for Cloud-Based Command and Control System in IoT Environment*. Appl. Sci. 2020, 10, 1035. [CrossRef]
[۳۱] *FedRAMP Security Controls Baseline. Available online: https: //www. fedramp. gov/documents/ (accessed on 11August 2021).*
[۳۲] *FedRAMP Security Controls Baseline. Available online: https: //www. fedramp. gov/documents/ (accessed on 11August 2021).*
[۳۳] Cloud Computing Security Requirements Guide. *Available online: https: //public. cyber. mil/dccs/dccsdocuments/ (accessed on11 August 2021).*
[۳۴]SecurityCertificationGuideforCloudService. *Availableonline: https: //www. kisa.* or. kr/public/laws/laws3_View. jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=91&ST=&SV= (accessed on 11 August 2021).
[۳۵]SecurityRequirementsforServerVirtualizationSystem. *Availableonline: http: //www. tta. or. kr/data/ttas_view. jsp?rn=1&pk_num=TTAK. KO-10. 0708 (accessed on 11 August 2021).*
[۳۶] Security Guidelines of National and Public Institution for Cloud Computing; *National Intelligence Servic*e*:* Seoul, Korea, 2016; pp. 101–103.
[۳۷] Cloudera Inc. Cloudera Security Overview. August 2020. *Available online: https: //docs. cloudera. com/cdp private-cloud-base/7. 1. 3/security-overview/cm-security-overview. pdf (accessed on 15 August 2021).*
[۳۸] Perwej, Y. The Hadoop Security in Big Data A Technological Viewpoint and Analysis. *Int. J. Sci. Res. Comput. Sci. Eng*. IJSRCSE2019, 7, 1‑14.
[۳۹] Shrihari, M. R. ; Manjunath, T. N. ; Archana, R. A. ; Hegadi, R. S. Research Challenges in Big Data Security with Hadoop Platform. *In International Conference on Recent Trends in Image Processing and Pattern Recognition;Springer: Singapore*, 2019; Volume 1037. [CrossRef]

[۴۰] Martis, M. ; Pai, N. V. ; Pragathi, R. S. ; Rakshatha, S. ; Dixit, S. *Comprehensive Survey on Hadoop Security*. Emerg. Res. Comput. Inf. Commun. Appl. 2019, 227-236. [CrossRef].

[۴۱] Peterson, G. Security Architecture Blueprint; Arctec Group, LLC.: Graz, Austria, 2007.

[۴۲] Koo, J. ; Kim, Y. -G. ; Lee, S. H. *Design of Security Architecture for the Cloud-Based Korea Military Command and Control System*. J. Korean Inst. Commun. Inf. Sci. 2020, 45, 400-408. [CrossRef]

[۴۳]. Koo, J. ; Oh, S. -R. ; Lee, S. H. ; Kim, Y. -G. *Security Architecture for Cloud-Based Command and Control System in IoT Environment*. Appl. Sci. 2020, 10, 1035. [CrossRef]

[۴۴]. Shrihari, M. R. ; Manjunath, T. N. ; Archana, R. A. ; Hegadi, R. S. *Research Challenges in Big Data Security with Hadoop Platform.*

[۴۵]. Perwej, Y. *The Hadoop Security in Big Data A Technological Viewpoint and Analysis. Int. J. Sci. Res. Comput*. Sci. Eng. IJSRCSE2019, 7, 1–14.

[۴۶]. *In International Conference on Recent Trends in Image Processing and Pattern Recognition; Springer: Singapore*, 2019; Volume 1037. [CrossRef]

[۴۷]. Martis, M. ; Pai, N. V. ; Pragathi, R. S. ; Rakshatha, S. ; Dixit, S. *Comprehensive Survey on Hadoop Security. Emerg. Res. Comput. Inf. Commun. Appl. 2019, 227–236. [CrossRef]*