Vol. 5, No. 14, Apr-Jun 2025,(9-16)

Journal of New Achievements in Electrical, Computer and Technology (JNAECT)

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری

دوره ۵، شماره ۱۴، بهار ۱۴۰۴ (۱۶-۹)

journal homepage: https://jnaect.ir

امنیت در سیستم‌های توزیع‌شده: مرور جامع بر اصول، تهدیدات و راهکارهای نوین

علی پاسبان اسدآبادی[1] ، زهرا شهپر*[2] ، حسین باغبان[3]

[1] گروه کامپیوتر، واحد فردوس، دانشگاه آزاد اسلامی، فردوس، ایران، Ali.pasban@iau.ir

[2] گروه کامپیوتر، واحد فردوس، دانشگاه آزاد اسلامی، فردوس، ایران، zahrashahpar@iau.ac.ir

[3] گروه کامپیوتر، واحد فردوس، دانشگاه آزاد اسلامی، فردوس، ایران، Hosein.baghban@iau.ir

چکیده

با گسترش روزافزون فناوری‌های توزیع‌شده مانند اینترنت اشیاء، شبکه‌های 5G، رایانش ابری و بلاک‌چین، موضوع امنیت در این سیستم‌ها به یکی از دغدغه‌های اصلی پژوهشگران و مهندسان تبدیل شده است. این مقاله مروری با استفاده از منابع علمی بین سال‌های 2020 تا 2024، اصول بنیادی امنیت، تهدیدات رایج و راهکارهای نوین در سیستم‌های توزیع‌شده را مورد بررسی قرار می‌دهد. در این مسیر، از فناوری‌هایی مانند یادگیری ماشین، بلاک‌چین، رمزنگاری پیشرفته و مدل‌های اعتماد استفاده شده است. در نهایت نیز مسیرهای آینده تحقیق و چالش‌های پیش رو ارائه می‌شود.

کلیدواژه‌ها: امنیت اطلاعات، سیستم توزیع‌شده، رمزنگاری، یادگیری ماشین، بلاک‌چین، اعتماد، احراز هویت.

1. مقدمه

سیستم‌های توزیع‌شده، زیرساخت اصلی بسیاری از فناوری‌های نوین مانند رایانش ابری، اینترنت اشیاء، و بلاک‌چین را تشکیل می‌دهند. این سیستم‌ها، به‌واسطه ماهیت غیرمتمرکز خود، با تهدیدات امنیتی پیچیده‌ای مواجه‌اند که طراحی راهکارهای جامع و تطبیق‌پذیر را ضروری می‌سازند. پژوهش‌های اخیر نشان می‌دهد که حملات پیچیده‌تر شده‌اند و راهکارهای سنتی دیگر پاسخگوی امنیت این سیستم‌ها نیستند[1].

۲ .اصول امنیت در سیستم‌های توزیع‌شده

امنیت در سیستم‌های توزیع‌شده مبتنی بر مجموعه‌ای از اصول بنیادی است که تضمین‌کننده صحت، قابلیت اطمینان، و ایمنی اطلاعات در یک محیط غیرمتمرکز هستند. این اصول به عنوان پایه‌های امنیت اطلاعات شناخته می‌شوند و رعایت آن‌ها در طراحی، پیاده‌سازی و بهره‌برداری از هر سیستم توزیع‌شده‌ای ضروری است. پنج اصل اصلی که در این حوزه اهمیت ویژه‌ای دارند عبارتند از:

۲,۱ .محرمانگی[1]: محرمانگی به معنای محافظت از داده‌ها در برابر دسترسی افراد غیرمجاز است. در سیستم‌های توزیع‌شده، به‌دلیل پراکندگی گره‌ها و مسیرهای ارتباطی متعدد، خطر نشت اطلاعات بیشتر است. به‌کارگیری روش‌های رمزنگاری قوی مانند AES و رمزنگاری کلید عمومی نقش مهمی در حفظ محرمانگی ایفا می‌کند.

۲,۲ .یکپارچگی[2]: اطمینان از عدم تغییر یا دستکاری غیرمجاز داده‌ها در حین انتقال یا ذخیره‌سازی، تحت عنوان یکپارچگی شناخته می‌شود. الگوریتم‌های هش مانند (SHA-256) و امضای دیجیتال برای بررسی صحت اطلاعات در سیستم‌های توزیع‌شده مورد استفاده قرار می‌گیرند. این مکانیزم‌ها تضمین می‌کنند که هر گونه تغییر در داده‌ها قابل شناسایی خواهد بود.

۲,۳ .دسترس‌پذیری[3]: دسترس‌پذیری به معنای قابلیت استفاده از منابع و خدمات در زمان مورد نیاز است. این اصل در سیستم‌های توزیع‌شده اهمیت دوچندانی دارد، چرا که خرابی یک یا چند گره نباید منجر به توقف کل سیستم شود. استفاده از افزونگی[4]، توازن بار[5] و تحمل‌پذیری خطا[6] از جمله راهکارهایی هستند که برای افزایش دسترس‌پذیری به‌کار می‌روند.

۲,۴ .احراز هویت[7]: احراز هویت فرآیندی است برای تأیید اینکه یک کاربر یا گره واقعاً همان چیزی است که ادعا می‌کند. در سیستم‌های توزیع‌شده، این فرآیند معمولاً از طریق مکانیزم‌هایی مانند رمز عبور، گواهی دیجیتال، یا توکن‌های امن پیاده‌سازی می‌شود. احراز هویت چندمرحله‌ای نیز برای افزایش امنیت پیشنهاد می‌شود.

۲,۵ .کنترل دسترسی[8]: پس از احراز هویت، باید مشخص شود که کاربر یا گره مورد نظر مجاز به انجام چه عملیاتی است. مدل‌های کنترل دسترسی مبتنی بر نقش، کنترل دسترسی مبتنی بر ویژگی و یا سیاست‌های پویا در سیستم‌های توزیع‌شده

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Redundancy
[5] Load Balancing
[6] Fault Tolerance
[7] Authentication
[8] Access Control

کاربرد دارند. همچنین مدل مدل صفر اعتماد [9] نیز به‌صورت گسترده برای کنترل دسترسی بدون اعتماد پیش‌فرض مورد استفاده قرار می‌گیرد. رعایت این اصول، به‌ویژه در محیط‌هایی مانند رایانش ابری و اینترنت اشیاء که مقیاس‌پذیری و ناهمگونی بالا دارند، نقش کلیدی در تأمین امنیت ایفا می‌کند[2].

۳ .تهدیدات رایج در سیستم‌های توزیع‌شده

با افزایش پیچیدگی سیستم‌های توزیع‌شده، انواع متنوعی از تهدیدات امنیتی نیز پدیدار شده‌اند که می‌توانند در لایه‌های مختلف این سیستم‌ها رخ دهند. در این بخش، مهم‌ترین تهدیدات بررسی می‌شود.

۳,۱ .حملات انکار سرویس توزیع‌شده[10]: این نوع حمله با ارسال حجم بالایی از درخواست‌ها از منابع مختلف، باعث اشباع شدن ظرفیت سرورها و قطع دسترسی کاربران قانونی به خدمات می‌شود. در محیط‌های توزیع‌شده مانند رایانش ابری یا شبکه‌های 5G[11]، این حملات می‌توانند باعث اختلال گسترده شوند. روش‌های مبتنی بر یادگیری ماشین، از جمله استفاده از شبکه‌های عصبی پیچشی و بازگشتی، به‌منظور تشخیص الگوهای ناهنجار ترافیک در مقابله با این تهدید بسیار مؤثر بوده‌اند[1].

۳,۲ .تهدیدات داخلی[12]: در این نوع تهدید، عامل تهدید از داخل سازمان یا شبکه عمل می‌کند؛ معمولاً فردی با دسترسی مجاز که از موقعیت خود سوءاستفاده می‌کند. این تهدیدها می‌توانند بسیار خطرناک باشند، زیرا معمولاً از سدهای امنیتی عبور می‌کنند. چارچوب‌های هوش مصنوعی توزیع‌شده می‌توانند با تحلیل رفتار کاربران، الگوهای مشکوک را شناسایی کرده و هشدار دهند[3].

۳,۳ .آسیب‌پذیری نرم‌افزار[13]: نرم‌افزارهایی که به‌درستی طراحی یا به‌روزرسانی نشده‌اند ممکن است دارای آسیب‌پذیری‌هایی باشند که مهاجمان از آن‌ها بهره‌برداری می‌کنند. این آسیب‌پذیری‌ها می‌توانند در کد منبع، واسط‌های API[14] یا پیکربندی‌ها وجود داشته باشند. استفاده از ابزارهای تحلیل ایستا و پویا، و اجرای تست نفوذ به‌صورت مستمر، به کاهش این تهدید کمک می‌کند[3].

۳,۴ .جعل هویت[15]: در این تهدید، مهاجم با جعل هویت کاربر قانونی، به منابع حساس دسترسی پیدا می‌کند. این حملات می‌توانند با روش‌هایی مانند فیشینگ[16]، مهندسی اجتماعی [17]یا تزریق نشست‌ها [18]انجام شوند. استفاده از فناوری بلاک‌چین در مدیریت هویت دیجیتال به‌دلیل قابلیت تأییدپذیری و تغییرناپذیری اطلاعات، می‌تواند راهکاری مؤثر باشد[4].

9 Zero Trust
10 Distributed Denial-of-Service Attacks-DDOS
11 Fifth-Generation Networks
12 Insider Threats
13 Software Vulnerability
14 Application Programming Interface
15 Identity Fraud
16 Phishing
17 Social Engineering
18 Session Hijacking

۳,۵ .تهدیدات زنجیره تأمین[19]: در معماری‌های توزیع‌شده، بسیاری از مؤلفه‌های نرم‌افزاری از طرف شرکت‌های ثالث تهیه می‌شوند. اگر یکی از این مؤلفه‌ها حاوی کد مخرب باشد، کل سیستم در معرض خطر قرار می‌گیرد. بررسی صحت اجزای واردشده با استفاده از امضای دیجیتال و پایگاه داده‌های معتبر و بررسی خودکار اجزای نرم‌افزاری در این زمینه توصیه می‌شود [5].

۳,۶ .تهدیدات کوانتومی[20]: با ظهور رایانش کوانتومی، الگوریتم‌های رمزنگاری متداول مانند RSA و ECC ممکن است به‌راحتی شکسته شوند. این تهدید هنوز عملیاتی نشده اما در آینده‌ای نزدیک می‌تواند امنیت اطلاعات رمزنگاری‌شده را به خطر اندازد. استفاده از رمزنگاری پساکوانتومی که مبتنی بر مسائل سخت ریاضی جدید مانند رمزنگاری مبتنی بر شبکه‌های هندسی است، به‌عنوان راهکار آینده‌نگر مطرح شده است. الگوریتم‌های رمزنگاری فعلی ممکن است در برابر محاسبات کوانتومی آینده ایمن نباشند. لزوم استفاده از رمزنگاری مقاوم در برابر کوانتوم وجود دارد [6].

۴ .راهکارهای نوین امنیتی

در پاسخ به تهدیدات گسترده در سیستم‌های توزیع‌شده، پژوهشگران و متخصصان امنیت راهکارهای نوینی ارائه کرده‌اند که مبتنی بر فناوری‌های نوظهور هستند. این راهکارها تلاش دارند امنیت را به‌صورت پویا، تطبیق‌پذیر و مقیاس‌پذیر تأمین کنند.

۴,۱ .رمزنگاری پساکوانتومی[21]: با رشد رایانش کوانتومی، الگوریتم‌های رمزنگاری فعلی در معرض خطر هستند. رمزنگاری پساکوانتومی از الگوریتم‌هایی استفاده می‌کند که در برابر حملات کوانتومی مقاوم هستند، مانند رمزنگاری مبتنی بر lattice یا کدهای خطی. این نوع رمزنگاری در حال حاضر توسط نهادهایی مانند NIST[22] برای استانداردسازی در حال بررسی است[6].

۴,۲ .یادگیری ماشین[23]: الگوریتم‌های یادگیری ماشین توانسته‌اند در تشخیص حملات سایبری عملکرد قابل توجهی نشان دهند. با آموزش بر روی داده‌های رفتاری و ترافیک شبکه، این الگوریتم‌ها قادر به شناسایی ناهنجاری‌ها و حملات جدید بدون نیاز به الگوهای از پیش تعریف‌شده هستند. شبکه‌های عصبی عمیق، جنگل‌های تصادفی و ماشین بردار پشتیبان از جمله روش‌های پرکاربرد در این حوزه‌اند [1].

۴,۳ .بلاک‌چین[24]: بلاک‌چین با فراهم‌سازی یک دفترکل تغییرناپذیر و شفاف، امکان ثبت و رهگیری ایمن تراکنش‌ها و تعاملات بین گره‌ها را فراهم می‌آورد. این فناوری به‌ویژه در مدیریت هویت، تأیید اعتبار و تضمین یکپارچگی داده‌ها کاربرد دارد. ویژگی توزیع‌شدگی بلاک‌چین آن را به گزینه‌ای مناسب برای زیرساخت‌های بدون اعتماد مرکزی تبدیل کرده است[4].

۴,۴ .معماری چندلایه[25]: در این رویکرد، امنیت در لایه‌های مختلف سیستم مانند لایه شبکه، انتقال و کاربرد به‌صورت مجزا و مکمل اعمال می‌شود. به‌کارگیری مکانیزم‌های رمزنگاری، احراز هویت، دیواره‌های آتش، سیستم‌های تشخیص نفوذ و سیاست‌های کنترل دسترسی در سطوح مختلف باعث افزایش امنیت کلی می‌شود[7].

19 Supply Chain Threats
20 Quantum Threats
21 Post-Quantum Cryptography
22 National Institute of Standards and Technology
23 Machine Learning
24 Blockchain

۴,۵ .مدل اعتماد صفر: در این مدل هیچ موجودیتی (کاربر، دستگاه یا اپلیکیشن) به‌صورت پیش‌فرض مورد اعتماد قرار نمی‌گیرد. دسترسی به منابع فقط پس از احراز هویت دقیق و بررسی مداوم مجاز است. این مدل، به‌ویژه در محیط‌های ابری و کاری از راه دور، امنیت را به شکل چشمگیری افزایش می‌دهد[7].

۴,۶ .اعتماد فازی[۲۶]: در بسیاری از سیستم‌های توزیع‌شده مانند شبکه‌های حسگر یا اینترنت اشیا، استفاده از مدل‌های اعتماد فازی باعث می‌شود تا تصمیم‌گیری در مورد تعامل با گره‌های دیگر بر اساس معیارهایی مانند سابقه، صحت پاسخ و تعاملات قبلی انجام گیرد. این مدل‌ها با محاسبات ساده، انعطاف‌پذیری بالایی ارائه می‌دهند[5].

۴,۷ .هوش مصنوعی توزیع‌شده[۲۷]: در این رویکرد، تحلیل داده‌ها به‌صورت محلی در گره‌ها انجام می‌شود و تنها نتایج آموزش یا ویژگی‌ها بین گره‌ها به اشتراک گذاشته می‌شود. این روش علاوه بر حفظ حریم خصوصی، باعث کاهش مصرف پهنای باند و بهبود مقیاس‌پذیری می‌شود. چارچوب‌های یادگیری فدرال[28] نمونه‌ای از پیاده‌سازی این ایده هستند. داده‌ها در محل خود تحلیل می‌شوند و فقط نتایج تحلیل میان گره‌ها به اشتراک گذاشته می‌شود[2].

۵ .مطالعات موردی

۵,۱ .استفاده از بلاک‌چین: برای هویت دیجیتال در یکی از پژوهش‌های سال ۲۰۲۳، از فناوری بلاک‌چین برای ایجاد سیستم مدیریت هویت غیرمتمرکز استفاده شده است. در این سامانه، از قراردادهای هوشمند برای تأیید هویت کاربران بهره گرفته شده و دسترسی‌ها به صورت ایمن ثبت و پیگیری می‌شوند. نتایج این مطالعه نشان می‌دهد که استفاده از بلاک‌چین باعث کاهش قابل توجه جعل هویت و افزایش شفافیت در ثبت تعاملات شده است[4].

۵,۲ .تشخیص DDoS به کمک شبکه عصبی در شبکه 5G : در تحقیقی دیگر، الگوریتم‌های یادگیری عمیق مانند شبکه‌های عصبی پیچشی (CNN) و بازگشتی (RNN) برای شناسایی حملات انکار سرویس در شبکه‌های 5G به‌کار رفته‌اند. مدل ارائه‌شده توانسته است با دقت بالا الگوهای حمله را از الگوهای عادی ترافیک متمایز کند و در نتیجه زمان پاسخگویی را بهبود ببخشد. پیاده‌سازی این روش در محیط واقعی عملکرد مؤثر آن را اثبات کرده است[1].

۵,۳ .رمزنگاری سبک برای دستگاه‌های IoT[۲۹] با منابع محدود: دستگاه‌های اینترنت اشیاء معمولاً از نظر توان محاسباتی و باتری محدود هستند. در این زمینه، روش‌هایی مبتنی بر رمزنگاری سبک و تقسیم داده به قطعات کوچک‌تر پیشنهاد شده‌اند. این روش‌ها ضمن حفظ امنیت داده‌ها، موجب افزایش بهره‌وری و کاهش مصرف انرژی شده‌اند. همچنین از الگوریتم‌هایی مانند ChaCha20به عنوان جایگزینی سریع و امن استفاده شده است [5].

۵,۴ .پیاده‌سازی مدل Zero Trust در زیرساختAWS[۳۰]: مدل اعتماد صفر در محیط ابری AWS به‌صورت عملیاتی پیاده‌سازی شده است. این مدل شامل استفاده از احراز هویت چندعاملی، رمزنگاری بین گره‌ای، نظارت مستمر بر ترافیک و

25 Layered Architecture
26 Fuzzy trust models
27 Distributed Artificial Intelligence
28 Federated Learning
29 Internet of Things
30 Amazon Web Services

استفاده از سیاست‌های دسترسی پویا است. نتایج نشان دادند که پیاده‌سازی Zero Trust موجب کاهش چشمگیر نفوذها و بهبود پاسخ به حوادث شده است[7].

۵،۵ .چارچوب AI توزیع‌شده برای تشخیص تهدیدات داخلی: در این مطالعه، از یادگیری توزیع‌شده برای تشخیص رفتارهای مشکوک کاربران در شبکه استفاده شده است. هر گره به‌صورت مستقل داده‌های خود را پردازش می‌کند و فقط نتایج تحلیل به اشتراک گذاشته می‌شود. این روش موجب افزایش دقت در شناسایی تهدیدات و حفظ حریم خصوصی کاربران شده است. این چارچوب به‌ویژه برای سازمان‌های بزرگ و حساس کاربردی است [2].

۶ .چالش‌ها و مسیرهای آینده

علیرغم پیشرفت‌های قابل‌توجه در حوزه امنیت سیستم‌های توزیع‌شده، چالش‌های متعددی همچنان وجود دارد که باید مورد توجه محققان و توسعه‌دهندگان قرار گیرد:

- **مقیاس‌پذیری راهکارها :**با افزایش گره‌ها و ترافیک داده در سیستم‌های توزیع‌شده، بسیاری از راهکارهای امنیتی سنتی قابلیت مقیاس‌پذیری ندارند و موجب کندی عملکرد یا ایجاد گلوگاه امنیتی می‌شوند.
- **سازگاری بین‌پلتفرمی :**وجود سیستم‌ها، دستگاه‌ها و نرم‌افزارهای مختلف با استانداردهای متفاوت، یکپارچه‌سازی راهکارهای امنیتی را دشوار می‌سازد. عدم سازگاری بین پروتکل‌ها یا الگوریتم‌ها می‌تواند باعث ایجاد نقاط ضعف شود.
- **حفظ حریم خصوصی :**در بسیاری از موارد، داده‌های حساس کاربران در سیستم‌های توزیع‌شده پردازش و ذخیره می‌شود. حفظ حریم خصوصی کاربران و انطباق با مقرراتی نظیر GDPR [۳۱]نیازمند توسعه راهکارهایی مانند یادگیری فدرال یا رمزنگاری همریخت است.
- **تهدیدات ناشناخته و نوظهور:** مهاجمان به‌طور مداوم روش‌های جدیدی برای حمله طراحی می‌کنند. عدم توانایی سیستم‌های دفاعی در شناسایی تهدیدات ناشناخته باعث آسیب‌پذیری می‌شود. استفاده از یادگیری بدون ناظر یا تحلیل رفتار می‌تواند در تشخیص تهدیدات جدید مؤثر باشد.
- **محدودیت منابع در IoT** [۳۲]: بسیاری از دستگاه‌های IoT دارای منابع پردازشی، حافظه و انرژی محدود هستند که اجرای الگوریتم‌های امنیتی سنگین را دشوار می‌سازد. استفاده از الگوریتم‌های سبک و کارآمد رمزنگاری برای این حوزه ضروری است [3، 5].

برای غلبه بر این چالش‌ها، توسعه چارچوب‌های استاندارد، آموزش نیروهای متخصص، و ارتقاء زیرساخت‌ها نیز از جمله مسیرهای تحقیقاتی پیشنهادی در آینده است.

31 General Data Protection Regulation

۷ .نتیجه‌گیری

امنیت در سیستم‌های توزیع‌شده به‌عنوان یکی از حیاتی‌ترین مؤلفه‌های طراحی و بهره‌برداری از این نوع سیستم‌ها مطرح است. با توجه به ماهیت غیرمتمرکز، مقیاس‌پذیر و پویا بودن این معماری‌ها، تهدیدات متنوعی آن‌ها را هدف قرار می‌دهند. در این مقاله، با بررسی اصول امنیتی، انواع تهدیدات رایج، و راهکارهای نوین مقابله، نشان دادیم که استفاده از فناوری‌هایی همچون رمزنگاری پساکوانتومی، بلاک‌چین، یادگیری ماشین و مدل صفر اعتماد می‌تواند نقش مهمی در افزایش تاب‌آوری سیستم‌های توزیع‌شده در برابر حملات ایفا کند.

علاوه بر این، مطالعات موردی مختلف اثبات کرده‌اند که این فناوری‌ها، هنگامی که به‌درستی پیاده‌سازی شوند، می‌توانند نه تنها سطح امنیت را بالا ببرند بلکه عملکرد و قابلیت اطمینان سیستم را نیز حفظ نمایند. همچنین توجه به چالش‌هایی مانند مقیاس‌پذیری، حریم خصوصی، و تهدیدات نوظهور باید در مرکز تحقیقات آینده قرار گیرد.

در نهایت، برای دستیابی به سیستم‌های توزیع‌شده امن، باید رویکردی چندلایه، تطبیق‌پذیر و بر پایه تحلیل داده اتخاذ کرد. تلفیق فناوری‌های نوین و توسعه چارچوب‌های استاندارد، همراه با آموزش مستمر نیروی انسانی، کلید موفقیت در مسیر ایجاد محیط‌های دیجیتال ایمن و قابل‌اعتماد خواهد بود.

۸- منابع و مراجع:

[1] Li, Y., Wang, J., & Chen, F. (2024). Deep Learning Approaches for Detecting DDoS Attacks in 5G Networks: A Comprehensive Review. Elsevier.

[2] Patel, D., & Shah, N. (2022). A Distributed AI Framework for Detecting Insider Threats Using Collaborative Learning. arXiv.

[3] Kumar, R., & Singh, M. (2020). Techniques for Secure Distributed Systems: A Review. ResearchGate.

[4] Zhang, Y., Wu, X., & Lin, X. (2023). Blockchain-based Identity Management: A Survey. Springer.

[5] Rahman, M. A., et al. (2023). Securing IoT Devices with Lightweight Cryptography and Data Fragmentation: A Survey. MDPI.

[6] Chen, L., et al. (2021). Post-Quantum Cryptography: Current State and Future Directions. NIST.

[7] Alshamrani, A., et al. (2023). Zero Trust Architecture for Cloud Infrastructure. IEEE.

Security in Distributed Systems: A Comprehensive Analysis of Principles, Threats, and Modern Solutions

Ali Pasban Asadabadi[1], Zahra Shahpar*[2], Hosein Baghban[3]

[1]Department of Computer, Ferdows Branch, Islamic Azad University, Ferdows, Iran, ali.pasban@iau.ir
[2]Department of Computer, Ferdows Branch, Islamic Azad University, Ferdows, Iran, Zahra.shahpar@iau.ir
[3]Department of Computer, Ferdows Branch, Islamic Azad University, Ferdows, Iran, hosein.baghban@iau.ir

Abstract— With the rapid expansion of distributed technologies such as the Internet of Things (IoT), 5G networks, cloud computing, and blockchain, ensuring the security of these systems has become a top priority for researchers and engineers. This review article examines the fundamental principles of security, common cyber threats, and state-of-the-art solutions applied to distributed systems based on scientific sources published between 2020 and 2024. The study highlights the role of advanced technologies such as machine learning, blockchain, post-quantum cryptography, and trust-based models in enhancing distributed security. Furthermore, several case studies are presented to demonstrate the practical implementation of these approaches. Finally, the article discusses existing challenges and future research directions toward developing more secure and resilient distributed environments.

Keywords: Distributed Systems, Cybersecurity, Blockchain, Machine Learning, Post-Quantum Cryptography, Access Control, Trust Models.