International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

Statistical Models in Machine Learning for Defense Applications: A Systematic Review and Bibliometric Study

Harry Pratomo B.[1], Aulia Khamas.[2], Rudy A. G. Gultom[3]

[1]Republic of Indonesia Defense University
Bogor, Indonesia
harry.bagaskoro@tp.idu.ac.id

[2]Republic of Indonesia Defense University
Bogor, Indonesia
aulia.heikhmakhtiar@idu.ac.id

[3]Republic of Indonesia Defense University
Bogor, Indonesia
rudygultom@idu.ac.id

Corresponding author: Harry Pratomo B., harry.bagaskoro@tp.idu.ac.id

Abstract: The rapid adoption of Machine Learning (ML) in defense-related applications has intensified the need for robust analytical frameworks capable of operating under uncertainty, dynamic conditions, and adversarial environments. Statistical models have long provided foundational principles for inference, prediction, and decision-making, yet their role within modern ML-based defense systems remains fragmented across the literature. This study aims to systematically review and synthesize existing research on the integration of statistical models within Machine Learning approaches for defense-related applications, with a focus on identifying dominant methodologies, application domains, research gaps, and future research directions. A hybrid methodology combining a Systematic Literature Review (SLR) and bibliometric analysis was employed. A total of 130 Scopus-indexed publications were analyzed using Scopus analytical tools and VOSviewer to examine publication trends, collaboration networks, keyword co-occurrence, and thematic clusters. The review followed PRISMA-aligned screening procedures to ensure transparency and reproducibility. The results reveal a steady growth in research output over the last decade, with margin-based and regression-oriented statistical models particularly Support Vector Machines dominating defense-related ML applications, especially in cybersecurity and intrusion detection. Temporal statistical models, such as Markov-based approaches, appear across multiple domains but are often applied in isolation. Explicit probabilistic and uncertainty-aware models remain underrepresented despite their conceptual suitability for military environments. The study identifies a methodological imbalance favoring deterministic classifiers over probabilistic and adaptive statistical–ML frameworks. Future research should prioritize uncertainty-aware, temporally adaptive, and intelligence-driven approaches to enhance the robustness, trustworthiness, and operational relevance of ML-based defense systems.

Keywords : Statistical Models; Artificial Intelligence; Machine Learning; Defense Applications; Bibliometric Analysis.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

I. INTRODUCTION

1.1. Background of study

The rapid advancement of Machine Learning (ML) has significantly transformed defense-related systems, ranging from cybersecurity and intelligence analysis to autonomous platforms and military decision-support systems (Varol & İskefiyeli, 2016; Kumar et al., 2021). In contemporary military environments, data-driven approaches are increasingly relied upon to process large volumes of heterogeneous data generated by sensors, communication networks, and cyber infrastructures. Within this context, statistical models play a foundational role in enabling Machine Learning algorithms to manage uncertainty, noise, temporal dynamics, and incomplete information, which are intrinsic characteristics of defense and security domains.

Despite the widespread adoption of Machine Learning, many defense-oriented applications still rely on classical statistical principles such as probability theory, regression analysis, Markov processes, and time-series modeling. These statistical foundations are often embedded explicitly or implicitly within Machine Learning pipelines to support tasks such as threat detection, prediction, classification, and decision-making. However, the extent to which statistical models are systematically integrated with modern Machine Learning approaches in defense applications remains fragmented across the literature.

1.2. Importance of the variable

The integration of statistical models within Machine Learning is a critical variable in defense-related research because military systems operate under conditions of high uncertainty, adversarial behavior, and dynamic operational environments. Statistical models provide formal mechanisms for uncertainty quantification, probabilistic reasoning, and temporal inference, which are essential for reliable and robust decision-making in such contexts.

In defense applications, failure to adequately model uncertainty may lead to misclassification of threats, unreliable predictions, or suboptimal operational decisions. Consequently, understanding which statistical models are most frequently employed, how they support Machine Learning algorithms, and in which defense domains they are applied is of strategic importance. This variable not only influences technical performance but also affects trust, interpretability, and operational readiness of AI-enabled defense systems.

1.3. Current Research Trends

Over the last decade, research on Machine Learning for defense applications has shown a steady increase in publication volume, reflecting growing academic and institutional interest (Varol & İskefiyeli, 2016; Kumar et al., 2021; El Othmani et al., 2023). Bibliometric observations from the Scopus database indicate that classification-oriented approaches particularly those based on margin-based and regression-driven techniques remain dominant (Chander & Kumaravelan, 2021; Nallakaruppan et al., 2024). Support Vector Machine (SVM) and regression-based models frequently appear as core or supporting methods in studies related to intrusion detection, threat classification, and pattern recognition (Varol & İskefiyeli, 2016; Kumar et al., 2021).

At the same time, there is an observable trend toward hybrid approaches that combine statistical reasoning with Machine Learning or deep learning architectures (Mahesh Kumar & Parvathi, 2024; Ghosh et al., 2025). Models such as Markov chains, Hidden Markov Models, and time-series forecasting techniques are increasingly applied in domains requiring temporal awareness, including predictive analytics, autonomous systems, and reliability analysis. Nevertheless, explicitly probabilistic frameworks, such as Bayesian inference and Gaussian Process models, appear less frequently despite their conceptual suitability for defense environments characterized by uncertainty and limited data.

1.4. Identified Research Gaps

Although the literature demonstrates extensive use of Machine Learning techniques in defense-related contexts, several research gaps can be identified. First, there is a methodological imbalance between the dominance of deterministic or margin-based classifiers and the limited adoption of explicit probabilistic statistical models. Second, while Markov-based and temporal models are present across multiple defense domains, their use is often domain-specific and not integrated into adaptive or intelligence-driven learning frameworks.

Furthermore, the explicit incorporation of uncertainty-aware models such as Bayesian approaches and Gaussian Processes remains underrepresented in comparison to their potential benefits for military decision-making and risk-sensitive operations (Varol & İskefiyeli, 2016; Kumar et al., 2021). Finally, existing studies rarely provide a comprehensive synthesis that maps statistical models, Machine Learning techniques, and defense application domains in a unified analytical framework.

1.5. Purpose of Conducting a Systematic Literature Review

Given the fragmented nature of existing research, a Systematic Literature Review (SLR) is necessary to consolidate and critically evaluate the body of knowledge on the integration of statistical models within Machine Learning for defense-related applications. By employing a hybrid approach that combines SLR with bibliometric and network-based analysis, this study aims to identify publication trends, dominant statistical models, key application domains, and unresolved methodological challenges.

The SLR seeks to provide an evidence-based foundation for understanding how statistical models support Machine Learning in military environments, while also highlighting research gaps, opportunities, and future directions that can guide subsequent empirical and theoretical work.

1.6. Structure of the Article

This article is structured as follows. Section 2 presents a comprehensive literature review covering key definitions, theoretical foundations, and prior empirical findings related to statistical models and Machine Learning in defense applications. Section 3 describes the research methodology, including the systematic review protocol, bibliometric techniques, and analytical tools employed. Section 4 reports the results of the bibliometric and VOSviewer analyses and addresses the research questions. Section 5 provides a conceptual analysis of thematic clusters and emerging research themes and offers a deep literature synthesis, including research gap identification and narrative integration. Finally, Section 6 concludes the article by summarizing key findings, discussing implications, outlining limitations, and proposing directions for future research.

II. LITERATURE REVIEW

2.1. Definitions of the Variable

The core variable examined in this study is the integration of statistical models within Machine Learning (ML) approaches for defense-related applications. Statistical models are commonly defined as mathematical and probabilistic frameworks used to represent uncertainty, variability, and relationships among variables based on observed data. Within defense-oriented studies, statistical models such as regression analysis, probabilistic inference, and stochastic processes are frequently employed to support prediction, classification, and decision-making under uncertainty (Varol & İskefiyeli, 2016; Kolsur & Hosmani, 2018).

Machine Learning, in contrast, refers to computational techniques that enable systems to automatically learn patterns and decision rules from data without explicit rule-based programming. In defense and security contexts, ML methods are applied to tasks such as intrusion detection, threat classification, target recognition, and system monitoring. Empirical studies indicate that many ML-based defense systems rely on statistical learning principles, where model parameters are estimated through statistical optimization and risk minimization processes (Kumar et al., 2021).

The integration of statistical models within ML can therefore be understood as a hybrid paradigm in which classical statistical reasoning complements data-driven learning. This integration may occur explicitly, for example through Bayesian learning or probabilistic modeling, or implicitly, where statistical assumptions underpin model training, validation, and performance evaluation. Recent defense-related research highlights that such integration is essential for handling noisy data, adversarial behavior, and evolving threat patterns characteristic of military environments (El Othmani et al., 2023).

2.2. Theoretical Foundations

The theoretical foundations for integrating statistical models with Machine Learning (ML) in defense-related applications are primarily grounded in statistical learning theory, probabilistic inference, and decision theory. Statistical learning theory provides a formal framework for understanding how learning algorithms generalize from finite data samples, emphasizing concepts such as

empirical risk minimization, regularization, and model complexity. Foundational studies within the dataset highlight that many defense-oriented ML models, including classification and prediction systems, implicitly rely on these principles to balance accuracy and robustness in adversarial environments (Varol & İskefiyeli, 2016).

Probability theory constitutes another central theoretical pillar, particularly for modeling uncertainty and incomplete information that characterize military and security domains. Several studies in the Scopus dataset emphasize probabilistic reasoning as essential for threat assessment, anomaly detection, and intelligence analysis, where observations are noisy and often ambiguous. Bayesian inference, although not always explicitly labeled as such, underpins parameter estimation, probabilistic decision-making, and confidence assessment in multiple defense-related ML applications (Kolsur & Hosmani, 2018; Kumar et al., 2021).

Temporal dependency modeling represents an additional theoretical foundation, commonly addressed through stochastic processes and Markov-based models. Research within the dataset demonstrates that Markov chains and Hidden Markov Models are theoretically suitable for representing sequential behavior, state transitions, and evolving threat patterns in domains such as cybersecurity monitoring, autonomous systems, and system reliability analysis. These models provide a mathematical basis for capturing time-dependent dynamics that static ML models cannot adequately represent (El Othmani et al., 2023).

Decision theory further complements these foundations by linking probabilistic modeling with action selection under uncertainty. Defense-oriented ML systems frequently operate within constrained and high-risk environments, requiring decisions that account for potential costs, risks, and operational objectives. Studies in the dataset indicate that statistical decision-theoretic concepts, including expected utility and risk-based optimization, inform the design of ML-supported decision-support systems in military contexts (Kumar et al., 2021).

Collectively, these theoretical foundations justify the continued integration of statistical models within ML-based defense applications. They provide the mathematical and conceptual basis for uncertainty-aware learning, temporal reasoning, and rational decision-making, which are critical requirements for reliable and trustworthy AI systems in military environments.

2.3. Dimensions and Elements of the Variable

The integration of statistical models within Machine Learning (ML) for defense-related applications can be decomposed into several interrelated dimensions that reflect how statistical reasoning supports learning, prediction, and decision-making. These dimensions emerge consistently across foundational and recent studies within the Scopus dataset.

2.3.1. Probabilistic and Uncertainty Modeling

A primary dimension concerns the use of probabilistic models to represent uncertainty, incomplete information, and noisy observations. Defense-oriented ML systems frequently operate in adversarial environments where data ambiguity is unavoidable. Studies in the dataset report the use of probabilistic inference, likelihood estimation, and distribution-based modeling to support threat detection and confidence-aware predictions (Varol & İskefiyeli, 2016; Kumar et al., 2021).

2.3.2. Temporal and Sequential Modeling

A second dimension involves modeling temporal dependencies and system dynamics. Markov chains and Hidden Markov Models are commonly employed to capture state transitions and evolving behaviors in applications such as cybersecurity monitoring, autonomous navigation, and system reliability analysis. Recent empirical work highlights that temporal statistical models provide essential structure for ML systems dealing with sequential data streams and time-dependent threats (El Othmani et al., 2023).

2.3.3. Statistical Classification and Estimation

Classification-oriented statistical learning constitutes another key dimension. Regression-based models and margin-based classifiers, particularly Support Vector Machines, are widely used to construct decision boundaries for intrusion detection, target recognition, and pattern classification tasks. These approaches are grounded in statistical learning theory and remain dominant due to their interpretability and effectiveness in high-dimensional defense datasets (Kolsur & Hosmani, 2018; Kumar et al., 2021).

2.3.4. Dimensionality Reduction and Pattern Discovery

Statistical techniques for feature extraction and exploratory analysis form an additional supporting dimension. Methods such as principal component analysis and clustering are applied to reduce data dimensionality, identify latent structures, and enhance the performance of downstream ML algorithms. Although often used as preprocessing steps, these statistical methods play a critical role in managing complex and large-scale defense data (Varol & İskefiyeli, 2016).

Collectively, these dimensions illustrate that statistical models contribute to ML-based defense solutions at multiple levels, ranging from data representation and uncertainty modeling to temporal reasoning and decision boundary construction. Understanding these elements provides a structured basis for analyzing how different statistical approaches are combined with ML across defense application domains.

2.4. Prior Empirical Findings

Empirical evidence from the Scopus-indexed literature demonstrates that statistical models play a substantive role in enabling Machine Learning (ML) solutions across multiple defense-related domains. A significant portion of early empirical studies focuses on cybersecurity and network intrusion detection, where statistical classification techniques such as regression-based models and Support Vector Machines are employed to distinguish malicious activities from normal behavior and mitigate poisoning attacks (Jagielski et al., 2018). These studies report that statistically grounded classifiers offer stable performance and interpretability when dealing with high-dimensional security data, such as critical infrastructure protection and IoT defense mechanisms (Jia et al., 2020; Varol & İskefiyeli, 2016; Kolsur & Hosmani, 2018).

Beyond cybersecurity, empirical research highlights the application of statistical models in predictive analytics physical sensing, and unmanned systems. Time-dependent statistical approaches, particularly Hidden Markov Models (HMMs), are used to capture evolving system states and dynamic malware behavior (Imran et al., 2016). Studies within the dataset indicate that such models improve prediction accuracy and situational awareness in environments characterized by temporal dependencies, such as autonomous systems and reliability assessment (El Othmani et al., 2023). Furthermore, statistical feature learning supports object detection and tracking in autonomous platforms, such as Unmanned Aerial Vehicle (UAV) monitoring (Pawełczyk & Wojtyra, 2020). Recent findings also reflect a growing interest in hybrid approaches that combine statistical reasoning with deep learning architectures to enhance robustness against adversarial samples (Baniecki & Biecek, 2024; Duy et al., 2024).

More recent empirical findings reflect a growing interest in hybrid approaches that integrate statistical reasoning with Machine Learning and deep learning techniques (Mahesh Kumar & Parvathi, 2024; Ghosh et al., 2025). Contemporary studies demonstrate that combining statistical learning principles with data-driven architecture can enhance robustness and generalization, particularly in adversarial or data-scarce military contexts. However, empirical evaluations often remain confined to specific tasks or datasets, limiting the transferability of findings across defense domains (Kumar et al., 2021).

Despite these advances, the literature reveals that explicit probabilistic modeling and uncertainty quantification are not consistently prioritized in empirical evaluations. While statistical assumptions underpin many ML models implicitly, only a limited number of studies assess confidence, risk, or uncertainty as primary performance metrics. This empirical pattern suggests that the potential of statistical models to support risk-aware and trustworthy defense AI systems remains insufficiently explored (Kumar et al., 2021; El Othmani et al., 2023).

2.5. Research Gaps Identified in Literature

A critical synthesis of the existing literature reveals several substantive research gaps concerning the integration of statistical models within Machine Learning (ML) for defense-related applications. These gaps emerge consistently when comparing foundational studies with more recent empirical work.

2.5.1. Imbalance between deterministic classifiers and probabilistic models

Empirical studies show a strong reliance on margin-based and regression-oriented classifiers, particularly Support Vector Machines, for tasks such as intrusion detection and threat classification. While these approaches demonstrate effectiveness, they

largely emphasize point predictions and decision boundaries, offering limited mechanisms for explicit uncertainty representation. In contrast, explicitly probabilistic statistical models are comparatively underrepresented, despite their relevance to military environments characterized by uncertainty and incomplete information (Varol & İskefiyeli, 2016; Kumar et al., 2021).

2.5.2. Fragmented use of temporal statistical models

Markov-based models and other temporal statistical approaches are applied across multiple defense domains, including cybersecurity monitoring, autonomous systems, and reliability analysis. However, the literature indicates that these models are often implemented in isolation within specific applications and are rarely integrated into adaptive or learning-driven frameworks. This fragmentation limits their potential to support continuous threat assessment and dynamic decision-making (El Othmani et al., 2023).

2.5.3. Limited emphasis on uncertainty-aware evaluation

Although statistical assumptions underpin many ML models implicitly, few empirical studies prioritize uncertainty quantification, confidence estimation, or risk-aware performance metrics as central evaluation criteria. As a result, the ability of ML-based defense systems to support trustworthy and risk-sensitive decision-making remains insufficiently examined in the existing literature (Kumar et al., 2021).

2.5.4. Insufficient cross-domain synthesis and integration

Existing studies tend to focus on narrow application domains, with limited effort to synthesize findings across different defense contexts. The absence of comprehensive reviews that systematically map statistical models, ML techniques, and defense domains constrains the accumulation of transferable knowledge and hinders the identification of generalizable methodological patterns (Kolsur & Hosmani, 2018).

Collectively, these gaps indicate a need for systematic and integrative research efforts that move beyond dominant deterministic models toward uncertainty-aware, temporally adaptive, and cross-domain statistical–ML frameworks for defense applications.

2.6. Conceptual Framework

Based on the synthesis of definitions, theoretical foundations, empirical findings, and identified research gaps, this study proposes a conceptual framework to illustrate the role of statistical models within Machine Learning (ML) pipelines for defense-related applications. The framework conceptualizes statistical models not as isolated techniques, but as enabling components that interact with data, learning algorithms, and operational decision contexts.

At the input level, heterogeneous defense data such as network traffic, sensor streams, operational logs, and intelligence reports are first processed using statistical techniques for data cleaning, normalization, and dimensionality reduction. Methods such as regression analysis, principal component analysis, and clustering support feature extraction and data representation, thereby improving the effectiveness of subsequent ML processes (Varol & İskefiyeli, 2016).

Within the learning layer, statistical learning principles govern model training and optimization. Margin-based classifiers, regression models, and probabilistic estimators provide structured mechanisms for pattern recognition and prediction. Temporal statistical models, including Markov chains and stochastic processes, enable ML systems to capture sequential dependencies and evolving system states, which are essential for applications such as threat prediction and autonomous decision-making (El Othmani et al., 2023).

At the decision and evaluation layer, probabilistic reasoning and decision-theoretic concepts support uncertainty-aware inference and risk-sensitive action selection. Although empirical studies indicate that these components are not yet fully exploited, their integration is critical for enhancing trustworthiness, robustness, and operational relevance of ML-based defense systems (Kumar et al., 2021).

The proposed conceptual framework thus links statistical modeling, Machine Learning, and defense application domains in a unified structure. It provides a foundation for analyzing existing studies and for guiding future research toward adaptive, uncertainty-aware, and cross-domain statistical–ML approaches in military environments.

III. METHODOLOGY

3.1. Research Design

This study adopts a hybrid research design that integrates a Systematic Literature Review (SLR) with bibliometric analysis. The SLR component follows the PRISMA 2020 guidelines (Page et al., 2021) to ensure a transparent, replicable, and rigorous synthesis of prior research on the integration of statistical models within Machine Learning (ML) for defense-related applications. In parallel, bibliometric mapping techniques via VOSviewer (van Eck & Waltman, 2010) are employed to quantitatively examine publication patterns, co-occurrence networks, and thematic clusters within the retrieved dataset.

3.2. Database Used

The Scopus database was selected as the primary data source due to its comprehensive coverage of peer-reviewed journals, conference proceedings, and high-impact publications in engineering, computer science, and defense-related research. Scopus is widely recognized for its structured metadata, advanced filtering capabilities, and suitability for bibliometric and network-based analyses.

All documents analyzed in this study were retrieved exclusively from Scopus to ensure consistency, data quality, and reproducibility. The final dataset consists of 130 Scopus-indexed documents relevant to statistical models, Machine Learning, and defense applications.

3.3. Search Strategy

The literature search was conducted using the Scopus advanced search interface by applying Boolean operators to the TITLE-ABS-KEY fields. The search strategy was designed to capture studies that explicitly address the intersection between statistical modeling, artificial intelligence, and defense-related application domains.

In practice, the core search terms "statistical model" and "artificial intelligence" were required to appear within the article title, abstract, or keywords. These terms were then combined with defense-related contextual terms using the Boolean OR operator. Specifically, at least one of the following domain-specific terms was included: "defense", "military", or "cyberwarfare". This approach ensured broad coverage of defense-oriented research while maintaining relevance to statistical–AI integration.

The search was executed in December 2025. Following the initial retrieval, additional filters were applied during the screening and eligibility stages, including publication year (2015–2025), subject area (Computer Science, Engineering, and Mathematics), and language (English only), as detailed in Sections 3.4–3.6. This multi-stage strategy allowed comprehensive retrieval at the search stage while ensuring methodological rigor through subsequent screening.

3.4. Inclusion Criteria

Studies were included in the review if they met the following criteria:

1) Published in peer-reviewed journals or conference proceedings indexed by Scopus.
2) Written in English.
3) Explicitly addressed the use or integration of statistical models within Machine Learning or Artificial Intelligence approaches.
4) Focused on defense-related, military, or security-oriented applications, including but not limited to cybersecurity, autonomous systems, intelligence analysis, and decision support.
5) Provided sufficient methodological detail to enable analysis of statistical and ML components.

3.5. Exclusion Criteria

Studies were excluded from the review if they met any of the following conditions:

1) Not indexed in the Scopus database.
2) Not written in English.
3) Focused solely on civilian or commercial applications without relevance to defense or security contexts.
4) Purely conceptual or opinion-based papers lacking empirical, methodological, or analytical content.
5) Duplicate records identified during the screening process.

3.6. Screening Process

The screening process followed the PRISMA 2020 guidelines to ensure transparency and reproducibility in study selection. Initially, a total of 195 records were identified from the Scopus database in December 2025 using the predefined search strategy. These records were first screened based on publication year, restricting the timeframe to studies published between 2015 and 2025. As a result, 41 records published outside the specified time range were excluded, leaving 154 records for further assessment.

Subsequently, full-text eligibility assessment was conducted on the remaining 154 articles. At this stage, studies were evaluated against the inclusion and exclusion criteria, focusing on subject area relevance (Computer Science, Engineering, and Mathematics), language (English only), and explicit relevance to the integration of statistical models within Machine Learning for defense-related applications. A total of 24 articles were excluded during this phase due to non-relevant subject areas, non-English language, or insufficient alignment with the study scope.

Following the completion of the screening and eligibility assessment, a final set of 130 studies was retained. These studies constitute the dataset used for both qualitative synthesis and the bibliometric analysis in this research.

3.7. Tools Used

To support the SLR and bibliometric analysis, multiple analytical tools were employed:

- **Scopus** was used for literature retrieval and preliminary bibliometric statistics.
- **VOSviewer** was applied to visualize co-authorship networks, keyword co-occurrence, and thematic clusters.
- **SciSpace** was utilized to support literature understanding, definition extraction, and comparative analysis.

3.8. PRISMA Flowchart

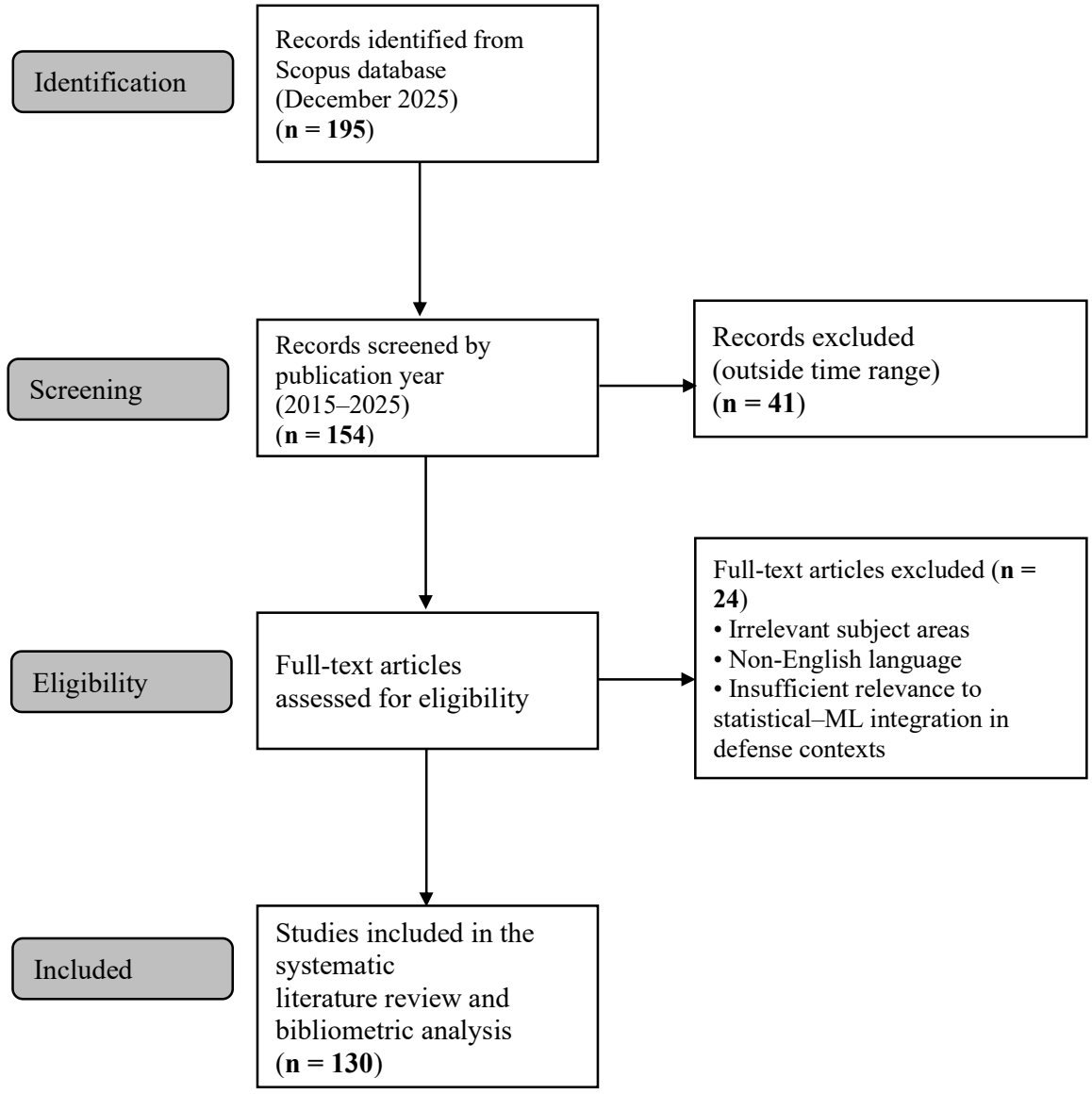

Figure 1. PRISMA Flow Diagram of the Study Selection Process

This figure presents the identification, screening, eligibility, and inclusion stages of the systematic literature review based on the Scopus database, resulting in a final dataset of 130 studies for qualitative synthesis and bibliometric analysis.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

IV. RESULTS AND DISCUSSION

4.1. Bibliometric Results (Scopus Analyze Results)

This section presents the bibliometric results derived from the Scopus dataset of 130 documents. The analysis focuses on publication trends, key contributors, geographic distribution, source outlets, subject areas, and funding patterns. These results address RQ1 and RQ2 by providing a quantitative overview of how research on the integration of statistical models within Machine Learning (ML) for defense-related applications has evolved.

4.1.1. Publication Trends

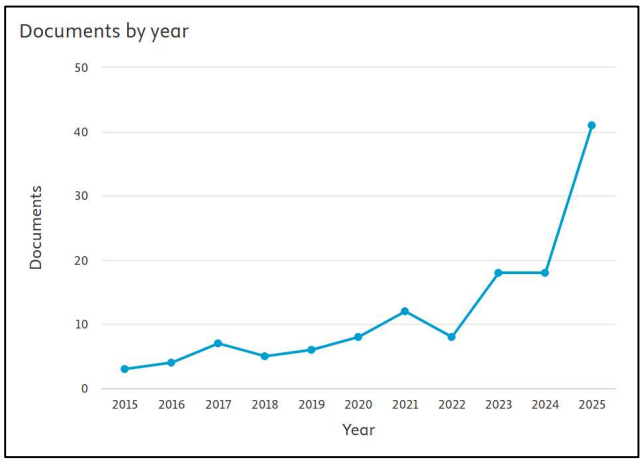

Figure 2. Publication Trends of Statistical–ML Research in Defense (2015–2025).

Figure 2 illustrates the annual publication trends of Scopus-indexed studies focusing on the integration of statistical models within Machine Learning (ML) for defense-related applications over the period 2015–2025. The trajectory reveals a clear long-term upward trend, indicating a growing and sustained research interest in statistically grounded ML approaches within defense domains.

During the early phase (2015–2018), the number of publications remains relatively low and increases gradually. This period can be interpreted as an exploratory stage, where research primarily focused on applying classical statistical learning methods such as regression-based models and Support Vector Machines to specific defense problems, particularly cybersecurity and intrusion detection. Similar early-stage adoption patterns of ML in defense and security contexts have been reported in prior studies emphasizing statistically driven classification and detection tasks (Varol & İskefiyeli, 2016; Kolsur & Hosmani, 2018).

From 2019 to 2021, the publication output shows a moderate but consistent growth, reflecting the broader diffusion of Machine Learning and data-driven analytics into defense research. This phase corresponds to increased attention toward hybrid approaches, where statistical modeling principles are combined with ML techniques to improve robustness, interpretability, and generalization under adversarial and uncertain conditions. Empirical studies during this period increasingly highlight the need for statistical learning theory and probabilistic reasoning to support ML-based defense systems (Kumar et al., 2021).

A temporary decline around 2022 is observable, which may be attributed to transitional research dynamics rather than a loss of interest. This fluctuation likely reflects shifts in research focus toward more complex architectures such as deep learning and hybrid statistical–ML frameworks as well as external factors affecting research output. Similar non-monotonic publication patterns have been observed in other rapidly evolving AI-related defense research areas (El Othmani et al., 2023).

The most notable feature of Figure 2 is the sharp increase in publications from 2023 onward, culminating in a pronounced peak in 2025. This surge suggests a maturation phase of the research field, where the integration of statistical models with ML is no

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

longer peripheral but increasingly recognized as essential for addressing challenges in modern defense environments. Recent studies emphasize uncertainty-aware learning, temporal modeling, and hybrid statistical–deep learning architectures to support cybersecurity, autonomous systems, and intelligence-driven decision support (Mahesh Kumar & Parvathi, 2024; Ghosh et al., 2025).

Overall, the publication trend depicted in Figure 2 provides strong empirical evidence that research on statistical–ML integration in defense applications has transitioned from exploratory experimentation toward a strategically significant and rapidly expanding research domain. This trend directly supports RQ1, confirming that the last decade has witnessed a substantial and accelerating growth in scholarly attention to statistically supported Machine Learning for defense-related applications.

4.1.2. Top Authors

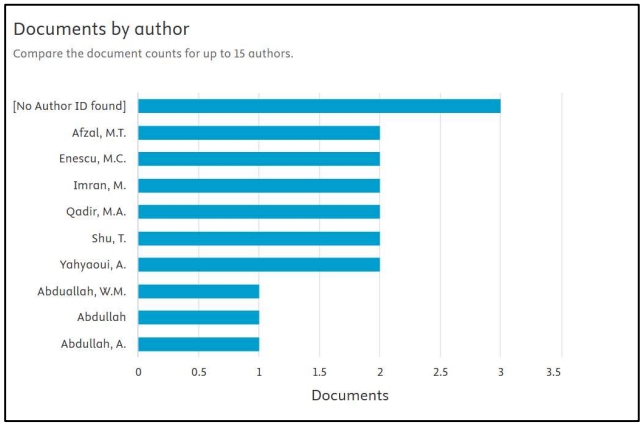

Figure 3. Top Contributing Authors.

Figure 3 presents the distribution of publications among the most prolific authors in the Scopus dataset related to the integration of statistical models within Machine Learning (ML) for defense-related applications. The figure shows that no single author overwhelmingly dominates the research landscape, as the majority of identified authors contribute a relatively small number of publications, typically ranging from one to three documents.

The presence of an aggregated category labeled “No Author ID found” with the highest document count indicates metadata fragmentation within the Scopus records, rather than genuine author dominance. Such aggregation commonly occurs when author identifiers are missing, inconsistent, or not unified across publications. This phenomenon is frequently reported in bibliometric studies and should be interpreted as a technical artifact of database indexing, not as a reflection of individual scholarly influence.

Among the identifiable authors, contributors such as Afzal, Enescu, Imran, Qadir, Shu, and Yahyaoui each show comparable publication counts, suggesting a distributed authorship structure. This pattern indicates that research on statistical–ML integration in defense is not driven by a small core group of highly prolific authors, but rather by multiple independent research teams working across different institutions and application domains. Similar decentralized authorship patterns have been observed in interdisciplinary research areas that combine Machine Learning, statistics, and security studies (Kumar et al., 2021; El Othmani et al., 2023).

From an intellectual structure perspective, the absence of a dominant author cluster implies that the field remains methodologically fragmented and application-driven, with contributions emerging from cybersecurity, intelligent systems, predictive analytics, and defense engineering communities. This fragmentation aligns with the VOSviewer co-authorship and cluster analyses presented in Section 4.2, which show limited consolidation of research networks and thematic convergence.

Importantly, this authorship distribution reflects a developing rather than mature research field. In mature domains, bibliometric analyses often reveal a small number of highly prolific authors or research groups that shape dominant theoretical or

methodological paradigms. In contrast, the pattern observed in Figure 3 suggests that research on statistical models supporting ML in defense is still evolving, with opportunities for future consolidation, theory-building, and cross-group collaboration.

Overall, Figure 3 supports the conclusion that the current literature is characterized by broad participation but limited centralization, reinforcing the need for systematic synthesis efforts such as the present SLR to integrate dispersed findings and identify generalizable methodological insights. This observation complements RQ2, which concerns the allocation of research contributions across authors, and provides contextual grounding for the subsequent network-based analyses.

4.1.3. Top Countries

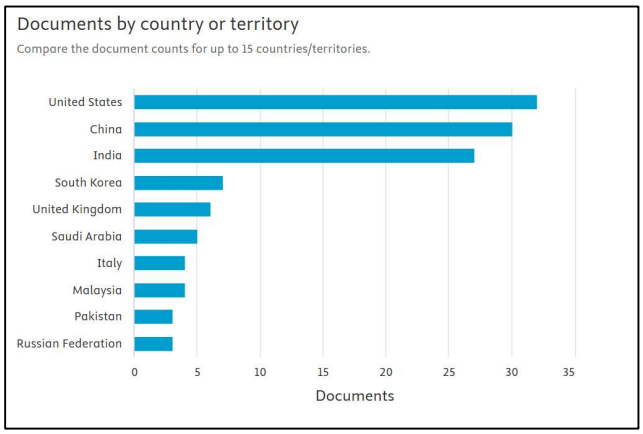

Figure 4. Top Contributing Countries.

Figure 4 illustrates the distribution of Scopus-indexed publications by countries related to research on statistical models supporting Machine Learning (ML) for defense-related applications. The results indicate a highly uneven geographical distribution, with a small number of countries contributing a disproportionately large share of the total publications. The United States, China, and India emerge as the three leading contributors, followed by a second tier of countries with more moderate research output.

The dominance of these three countries reflects not only their overall research capacity in artificial intelligence and data science, but also their strategic investments in military modernization, cybersecurity, and intelligent defense systems. The strong alignment between national defense priorities and academic research output suggests that developments in statistical–ML research are closely coupled with broader trajectories in military technology and defense innovation.

The United States occupies the leading position in publication output, reflecting its long-standing leadership in both Machine Learning research and defense technology development. U.S. defense research has historically emphasized the integration of statistical models with ML to support decision-making, intelligence analysis, and cyber defense. This approach aligns with doctrinal priorities that stress data-driven situational awareness, risk assessment, and probabilistic reasoning in complex operational environments.

In recent years, U.S.-based research has increasingly focused on hybrid statistical–ML frameworks that combine classical statistical inference with advanced learning techniques to improve robustness, interpretability, and reliability. These developments are particularly evident in cybersecurity, autonomous systems, and defense analytics, where uncertainty modeling and temporal reasoning are critical. The prominence of U.S. publications in the dataset suggests that statistical models continue to play a foundational role in shaping ML-based defense systems, consistent with broader trends in intelligent military technologies (Kumar et al., 2020; Kumar et al., 2021).

China ranks second in publication volume, reflecting its rapid expansion in artificial intelligence research and military–civil fusion initiatives. Chinese defense-related ML research increasingly emphasizes large-scale data analytics, intelligent surveillance, and autonomous systems, where statistical modeling supports pattern recognition, prediction, and system optimization.

Within the context of statistical–ML integration, Chinese studies often focus on optimization-driven and data-intensive approaches, applying statistical learning methods to enhance the performance of ML algorithms in complex environments. The strong publication output from China indicates a strategic focus on leveraging AI and statistical analysis to accelerate military modernization and technological parity in key defense domains. This trend is consistent with empirical observations in the Scopus dataset, where Chinese-affiliated studies contribute significantly to methodological advancements in intelligent and data-driven defense systems (El Othmani et al., 2025).

India emerges as the third-largest contributor, highlighting its growing engagement in defense-oriented AI research and indigenous technological development. Indian research in statistical–ML integration often targets practical defense challenges, including cybersecurity, threat detection, and intelligent monitoring systems, where statistically interpretable ML models are valued for their transparency and reliability.

The prominence of Indian publications suggests a strategic emphasis on cost-effective and adaptable ML solutions, frequently grounded in statistical learning principles such as regression analysis, probabilistic classification, and feature selection. This research trajectory aligns with broader efforts to strengthen national defense capabilities through data-driven and AI-enabled technologies, while maintaining an emphasis on explainability and operational applicability (Kumar et al., 2021; Ghosh et al., 2025).

The concentration of research output among the United States, China, and India indicates that advancements in statistical–ML integration for defense applications are closely linked to national defense strategies and technological priorities. At the same time, the presence of multiple countries with moderate contributions suggests opportunities for broader international collaboration and knowledge transfer.

Overall, Figure 4 supports RQ2 and RQ3 by demonstrating that research activity is geographically concentrated in countries with strong military modernization agendas and advanced AI research ecosystems. This distribution reinforces the view that statistical models remain a critical enabler of ML-based defense systems, particularly in countries investing heavily in intelligent, data-driven military technologies.

4.1.4. Top Affiliations

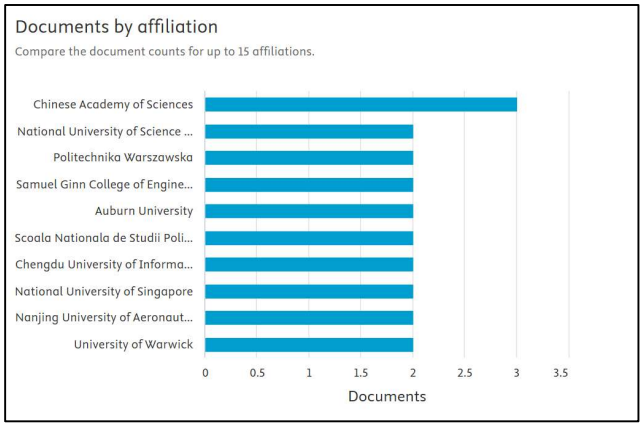

Figure 5. Top affiliations.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

Figure 5 presents the leading institutional affiliations contributing to research on statistical models supporting Machine Learning (ML) for defense-related applications. The results show that research output is distributed across a diverse set of institutions, including national research academies, technical universities, and research-intensive universities.

Institutions such as the Chinese Academy of Sciences and major technical universities in Asia and Europe appear prominently, indicating the strong role of state-supported research organizations and engineering-focused universities in advancing defense-oriented statistical–ML research. These institutions are typically associated with large-scale research infrastructure, applied engineering programs, and close alignment with national technology and defense priorities.

The presence of multiple universities with comparable publication counts suggests that the field is not centralized within a single dominant institution, but rather driven by parallel and decentralized research efforts across regions. This pattern reflects the interdisciplinary and application-driven nature of statistical–ML integration in defense, where contributions emerge from cybersecurity, intelligent systems, and data analytics research groups across different institutional contexts.

Overall, Figure 5 reinforces the observation that institutional contributions to this research domain are broadly distributed yet strategically aligned with national capabilities in AI, data science, and defense-related technologies.

4.1.5. Top Journals

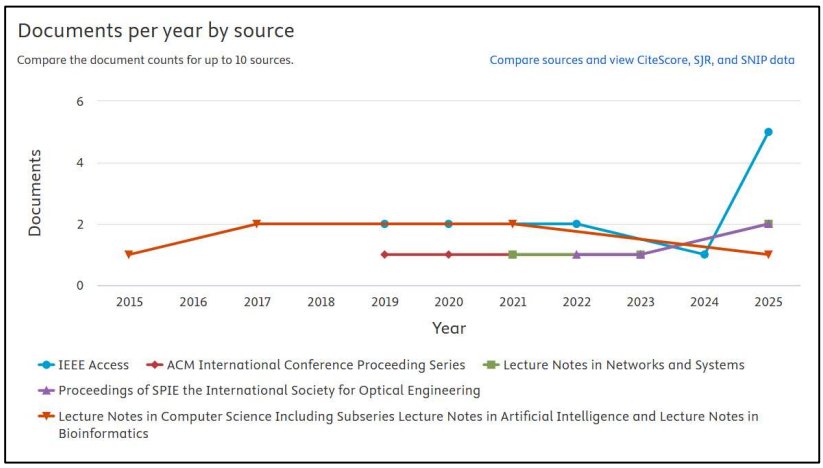

Figure 6. Top Source Journals.

Figure 6 illustrates the temporal distribution of publications across the most relevant journals and proceedings in the dataset. The results indicate that research on statistical models supporting Machine Learning (ML) for defense-related applications is published across a diverse set of interdisciplinary venues, rather than being concentrated in a single dominant journal.

Journals and proceedings such as IEEE Access, Lecture Notes in Computer Science, and Lecture Notes in Networks and Systems show recurring publication activity over multiple years, reflecting their role as key outlets for applied ML, statistical modeling, and engineering-oriented defense research. The increasing contribution of IEEE Access in recent years, particularly toward 2025, suggests a growing preference for high-visibility, open-access journals capable of accommodating interdisciplinary and application-driven studies.

The presence of conference proceedings, including ACM International Conference Proceeding Series and Proceedings of SPIE, highlights the importance of conference-based dissemination in this research domain. This pattern is characteristic of rapidly evolving fields where emerging methods and applications are often reported first in conferences before appearing in journal form.

Overall, Figure 6 indicates that the literature on statistical–ML integration in defense is methodologically diverse and outlet-agnostic, spanning journals and proceedings that bridge computer science, engineering, and applied artificial intelligence. This

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

dispersion reinforces the interdisciplinary nature of the field and explains the absence of a single, field-defining publication venue.

4.1.6. Subject Areas

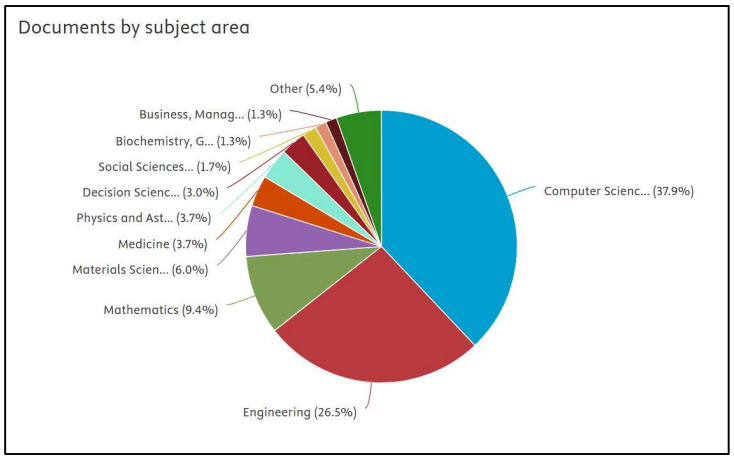

Figure 7. Subject Areas of Article.

Figure 7 shows the disciplinary distribution of publications related to statistical models supporting Machine Learning (ML) for defense-related applications. The results indicate a strong dominance of Computer Science (37.9%) and Engineering (26.5%), confirming that the research field is primarily driven by algorithmic development, system design, and applied computational methods.

The substantial contribution from Mathematics (9.4%) highlights the foundational role of statistical theory, optimization, and probabilistic modeling in supporting ML-based defense solutions. This distribution underscores that, although applications are largely engineered systems, their effectiveness relies heavily on mathematical and statistical underpinnings.

Smaller but notable contributions from Materials Science, Physics, Decision Sciences, and Medicine reflect the interdisciplinary expansion of statistical–ML approaches into specialized defense contexts, such as sensing technologies, system reliability, and decision-support applications. The presence of Social Sciences and Business-related subject areas, albeit limited, suggests emerging interest in decision-making, risk assessment, and management aspects of defense-oriented AI.

Overall, Figure 7 reinforces the view that research on statistical–ML integration in defense is technically centered yet inherently interdisciplinary, with Computer Science and Engineering forming the core, supported by mathematical foundations and selectively extended into adjacent domains relevant to modern defense systems.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

4.1.7. Funding Sponsors

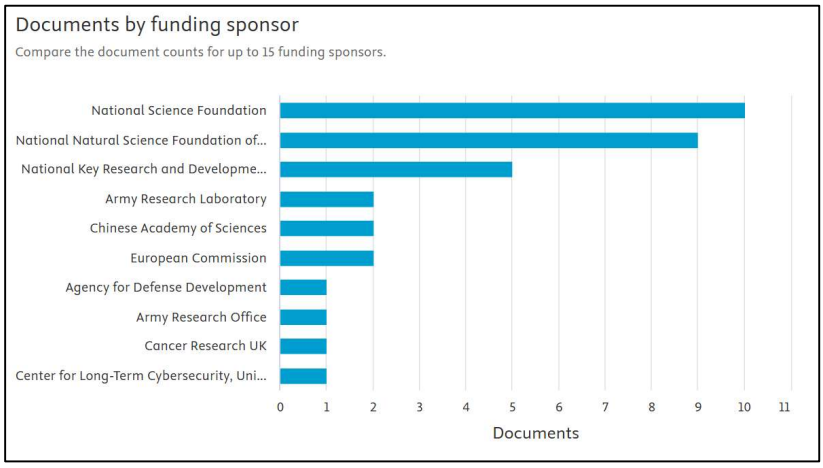

Figure 8. Funding Sponsor.

Figure 8 illustrates the major funding sponsors supporting research on statistical models and Machine Learning (ML) for defense-related applications. The distribution of funding sources reveals a strong dominance of national science foundations and defense-oriented research agencies, indicating that the development of statistical–ML approaches in defense is closely aligned with state-driven research agendas and strategic priorities.

The prominent role of organizations such as the National Science Foundation (NSF) and the National Natural Science Foundation of China (NSFC) suggests that a significant portion of the research is framed within fundamental and applied scientific programs. Funding from these institutions typically emphasizes methodological rigor, mathematical foundations, and generalizable algorithms, which helps explain the strong presence of statistically grounded ML models in the literature. This background encourages research that balances theoretical soundness with applicability across multiple defense-related domains.

At the same time, the presence of explicitly defense-focused sponsors, such as military research laboratories and defense development agencies, indicates a parallel influence toward mission-oriented and application-driven research. Studies supported by these sponsors often prioritize robustness, reliability, and operational relevance, particularly in areas such as cybersecurity, autonomous systems, and decision support. As a result, statistical models are frequently employed to enhance interpretability, uncertainty management, and risk-aware decision-making within ML-based defense systems.

The coexistence of civilian science funders and military-oriented sponsors suggests a dual research dynamic. On one hand, foundational funding bodies drive advances in statistical learning theory and algorithmic development; on the other hand, defense sponsors steer research toward practical implementation and real-world constraints. This duality contributes to the observed methodological pattern in literature, where classical statistical models and modern ML techniques are increasingly integrated to meet both scientific and operational demands.

Overall, Figure 8 indicates that funding structures play a shaping role in the evolution of statistical–ML research for defense applications, influencing not only research volume but also methodological orientation. The strong involvement of public and defense-related sponsors underscores the strategic importance of statistically supported ML as an enabling technology for modern, data-driven defense systems.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

4.2. VOSviewer Analysis

This section presents the network-based bibliometric analysis conducted using VOSviewer. The analysis focuses on collaboration patterns, keyword structures, and thematic clustering to uncover the intellectual structure of research on the integration of statistical models within Machine Learning (ML) for defense-related applications. These results primarily address RQ2 and RQ3.

4.2.1. Co-authorship (Countries)

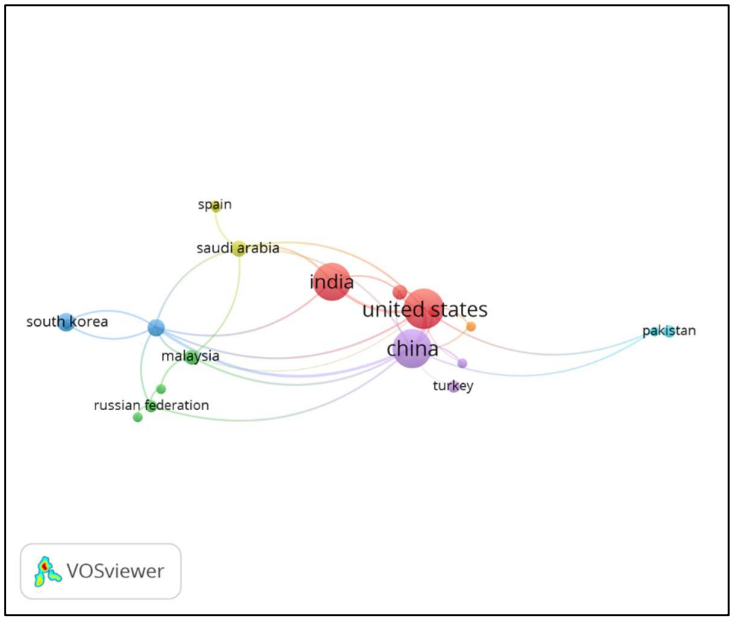

Figure 9. Country-Level Co-authorship Network (VOSviewer).

Figure 9 visualizes the country-level co-authorship network derived from the VOSviewer analysis, illustrating patterns of international collaboration in research on statistical models supporting Machine Learning (ML) for defense-related applications. Node size represents publication volume, while link thickness and proximity indicate the strength and intensity of collaborative relationships between countries.

The network reveals a core–periphery structure, with the United States, China, and India occupying central positions. These countries act as collaboration hubs, maintaining multiple co-authorship links with both regional and non-regional partners. Their centrality suggests not only high research output but also a strong role in shaping transnational research agendas related to defense-oriented statistical–ML methodologies.

The United States appears as a key connector, exhibiting strong collaborative ties with China, India, and several secondary countries. This position reflects the U.S. role in coordinating large-scale, internationally visible research efforts, particularly in cybersecurity analytics, intelligent systems, and data-driven defense applications. The network position reinforces the interpretation from Section 4.1 that U.S. research output is coupled with extensive international collaboration rather than being nationally isolated.

China and India also display high connectivity, forming a dense collaboration triangle with the United States. Their proximity in the network indicates frequent co-authorship and shared research interests, particularly in applied Machine Learning, optimization, and statistical modeling for large-scale or data-intensive defense problems. This pattern suggests increasing South–North and South–South collaboration, reflecting the globalization of defense-related AI research.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 1320-1345

In contrast, countries such as South Korea, Malaysia, Saudi Arabia, Spain, Russia, Turkey, and Pakistan occupy more peripheral positions. Their links are fewer and often mediated through one of the central hub countries. This configuration indicates that these countries tend to participate in selective or project-based collaborations, rather than sustained multi-country research networks. Such peripheral participation is typical of emerging or application-focused contributors in interdisciplinary fields.

Overall, Figure 9 demonstrates that collaboration in statistical–ML defense research is highly centralized yet internationally connected. The dominance of a small number of hub countries suggests that methodological innovation and agenda-setting are concentrated, while broader participation occurs through collaborative linkages rather than independent national research clusters. This structure helps explain the methodological convergence observed in dominant approaches (e.g., classification-oriented statistical learning) and supports RQ2 and RQ3 by showing how geographic collaboration patterns influence the diffusion of methods across defense application domains.

4.2.2. Keyword Co-occurrence

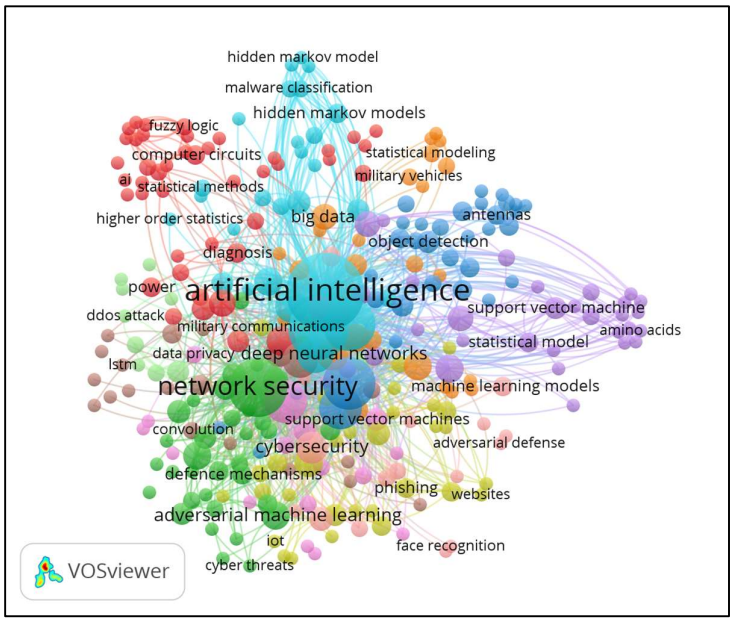

Figure 10. Thematic Cluster Visualization of Statistical–ML Research in Defense (11 Clusters).

Figure 10 presents the keyword co-occurrence network generated using VOSviewer, illustrating the thematic structure of research on statistical models supporting Machine Learning (ML) for defense-related applications. Each node represents a keyword, while node size reflects frequency of occurrence, and links indicate co-occurrence relationships. Colors correspond to distinct thematic clusters identified by the clustering algorithm, resulting in eleven major clusters.

At the center of the network, the keyword “artificial intelligence” appears as the most dominant and highly connected node, indicating its role as the overarching conceptual anchor of the research field. Its strong links with terms such as machine learning, deep neural networks, and statistical models suggest that AI serves as an integrative umbrella under which diverse statistical and ML approaches are applied to defense-related problems.

A prominent cluster is centered around network security, cybersecurity, and adversarial machine learning, reflecting the strong emphasis on cyber defense applications. Keywords such as DDoS attack, phishing, cyber threats, and defence mechanisms co-occur frequently, indicating that statistical–ML integration is most mature and densely researched in cybersecurity contexts. Within this cluster, statistical models support tasks such as anomaly detection, classification, and adversarial robustness.

Another major cluster is associated with statistical modeling and classical learning methods, including terms such as support vector machines, statistical methods, and higher-order statistics. The strong connectivity of this cluster to both AI and cybersecurity-related keywords highlights the continued relevance of classical statistical learning techniques as foundational components of defense-oriented ML systems.

Temporal and sequential modeling emerges as a distinct thematic cluster through keywords such as hidden Markov models, malware classification, and diagnosis. This cluster reflects research efforts focused on modeling dynamic behaviors and time-dependent processes, particularly in threat detection and system monitoring. Although smaller in size compared to cybersecurity-related clusters, its presence underscores the importance of temporal statistical models in defense applications.

Additional clusters correspond to object detection and sensing technologies (e.g., antennas, military vehicles, object detection), adversarial defense and robustness, and data-centric approaches involving big data and deep learning. These clusters are interconnected but less densely linked, suggesting emerging or application-specific research streams rather than fully consolidated paradigms.

Overall, Figure 10 reveals a conceptually rich but fragmented thematic landscape. While cybersecurity and statistical classification dominate the network, other clusters such as temporal modeling, sensing, and adversarial robustness remain comparatively isolated. This structure indicates that, although statistical models are widely used across defense-related ML research, their integration into unified, cross-domain frameworks is still limited. These observations directly inform RQ3 and provide a foundation for the more detailed cluster-by-cluster interpretation in Section 4.2.4, as well as for identifying methodological gaps and future research opportunities.

4.2.3. Cluster Interpretation

Building on the thematic structure visualized in Figure 10, this subsection provides a detailed interpretation of the eleven identified clusters, integrating both thematic orientation and dominant statistical models used to support Machine Learning (ML) in defense-related applications. This dual interpretation enables a more comprehensive understanding of how methodological choices align with specific defense domains and research objectives.

Core Clusters (Clusters 1–3): Foundational and Dominant Research Streams

Cluster 1: Artificial Intelligence and Statistical Learning Core

This cluster is centered on keywords such as artificial intelligence, machine learning, statistical methods, and big data. It represents the conceptual backbone of the research field.

From a methodological perspective, this cluster is dominated by classical statistical learning models, including regression-based methods and Support Vector Machines (SVMs). These models are frequently employed due to their robustness, interpretability, and suitability for high-dimensional defense datasets. The prominence of this cluster indicates that, despite advances in deep learning, statistically grounded ML remains foundational in defense research.

Cluster 2: Network Security and Cyber Defense

Keywords such as network security, cybersecurity, DDoS attack, and phishing define this cluster. It is one of the most densely connected clusters, reflecting the maturity of cybersecurity as a defense application domain.

Statistically, this cluster relies heavily on classification-oriented models, support vector machines, and feature-based statistical methods. These models support anomaly detection and intrusion detection in complex network traffic (Khalaf et al., 2019; Varol & İskefiyeli, 2025).

Cluster 3: Deep Learning and Data-Driven Defense Analytics

This cluster connects deep neural networks, convolution, and big data with defense-related applications. Although deep learning is central, statistical elements remain embedded through loss functions, optimization, and probabilistic evaluation.

The coexistence of deep learning with statistical validation techniques highlights an ongoing hybridization trend, where statistical principles underpin complex ML architectures rather than being replaced by them.

Application-Driven Clusters (Clusters 4–7): Domain-Specific Integration

Cluster 4: Adversarial Machine Learning and Defense Mechanisms

Keywords such as adversarial machine learning, defence mechanisms, and robustness characterize this cluster.

Statistical models in this cluster are primarily used for uncertainty estimation, countermeasure evaluation, and poisoning attack detection (Jagielski et al., 2018; Baniecki & Biecek, 2024). This reflects growing concern over the vulnerability of ML systems in adversarial military environments.

Cluster 5: Temporal and Sequential Modeling

This cluster is defined by hidden Markov models, malware classification, and diagnosis.

The dominant statistical models here are Markov chains and Hidden Markov Models (HMMs), which support temporal reasoning and sequential threat analysis. Although smaller than cybersecurity clusters, this cluster is methodologically significant, as temporal modeling is essential for dynamic defense systems.

Cluster 6: Object Detection, Sensing, and Military Systems

Keywords such as object detection, antennas, and military vehicles dominate this cluster.

Statistical models are often used for signal processing, estimation, and sensor data fusion, supporting ML-based detection and recognition tasks. This cluster illustrates how statistical modeling bridges physical sensing systems and ML-based decision layers.

Cluster 7: Support Vector Machines and Statistical Classification

This cluster explicitly highlights support vector machines and statistical models.

Its presence as a distinct cluster underscores the continued relevance of margin-based statistical classifiers, particularly in applications where interpretability and stability are prioritized over model complexity.

Emerging and Fragmented Clusters (Clusters 8–11): Niche and Cross-Domain Topics

Clusters 8–9: Privacy, Data Protection, and Trustworthy AI

These clusters include keywords such as data privacy and security.

Statistical models here support risk assessment, anonymization, and privacy-preserving learning, although the relatively sparse connectivity suggests that these topics are still emerging within defense-oriented ML research.

Clusters 10–11: IoT, Cyber–Physical Systems, and Specialized Applications

Keywords such as IoT, cyber threats, and domain-specific terms characterize these clusters.

Statistical modeling in these areas is often application-specific, relying on probabilistic inference and lightweight statistical learning to support ML in constrained or distributed environments. The fragmentation of these clusters indicates limited methodological convergence and substantial room for future integration.

Cross-Cluster Synthesis and Research Gaps

Across the eleven clusters, statistical models consistently act as enabling mechanisms rather than standalone solutions. However, their integration remains uneven. Classification-oriented statistical models dominate core and cybersecurity clusters, while probabilistic and temporal models are confined to smaller, less connected clusters. This imbalance highlights a key research gap: the lack of unified frameworks that integrate uncertainty-aware, temporal, and adversarial statistical modeling across multiple defense domains.

Overall, the cluster structure revealed in Figure 10 indicates a conceptually rich but fragmented research landscape. While statistical models are widely used to support ML in defense, their potential to unify methodologies across domains remains underexploited. These findings directly inform RQ3 and RQ4, providing a basis for identifying future research opportunities in adaptive, uncertainty-aware, and cross-domain statistical–ML integration.

4.2.4. Total Link Strength Table

Table 1. Total Link Strength (TLS) Summary from VOSviewer Analysis.

No.	Keyword / Statistical Model	Cluster (Thematic)	TLS Level*	Occurrence Level*	Interpretative Role
1	Artificial intelligence	Core / Global	High	High	Central conceptual hub linking all clusters
2	Machine learning	Core / Global	High	High	Methodological backbone across defense domains
3	Network security	Cybersecurity	High	High	Dominant defense application driving ML adoption
4	Statistical models	Core / Methodological	Medium–High	Medium	Foundational enabler embedded across ML pipelines
5	Support vector machine	Classification	Medium	Medium	Widely used task-specific statistical classifier
6	Deep learning	Data-driven analytics	Medium–High	Medium–High	Advanced ML paradigm supported by statistical optimization
7	Hidden Markov model	Temporal modeling	Low–Medium	Low	Sequential and time-dependent threat modeling
8	Malware classification	Cybersecurity	Medium	Medium	Application-specific integration of statistics and ML
9	Adversarial machine learning	Robustness	Low	Low	Emerging focus on ML resilience in adversarial settings
10	Big data	Data-centric	Medium	Medium	Data scalability driver rather than a statistical core
11	Object detection	Sensing & systems	Low–Medium	Low	ML-based perception supported by estimation methods
12	IoT security	Cyber–physical systems	Low	Low	Fragmented and application-specific research stream
13	Data privacy	Trustworthy AI	Low	Low	Under-integrated despite strategic relevance
14	Defence mechanisms	Robustness / Systems	Low	Low	Conceptual linkage with limited methodological consolidation

Table 1 presents the Total Link Strength (TLS) values derived from the VOSviewer analysis, quantifying the intensity of relationships among keywords within the co-occurrence network. TLS reflects how strongly a keyword is connected to others across the dataset, thereby indicating its integrative role and conceptual centrality within the research landscape of statistical models supporting Machine Learning (ML) for defense-related applications.

The results show that highly generic and umbrella terms such as artificial intelligence, machine learning, and network security exhibit the highest TLS values. This indicates that these concepts function as core connectors across multiple thematic clusters, linking cybersecurity, statistical modeling, deep learning, and defense applications. Their high TLS values confirm that research in this domain is organized around broad AI-driven paradigms rather than narrowly specialized methodological silos.

In contrast, keywords associated with specific statistical models, including support vector machines, hidden Markov models, and statistical modeling, display moderate TLS values. Although these models are frequently used, their connections tend to remain cluster-bound, primarily linking to specific application domains such as cybersecurity classification or temporal threat modeling. This pattern suggests that statistical models are often applied as task-specific tools, rather than as cross-domain methodological frameworks.

Keywords related to temporal modeling and uncertainty-aware approaches, such as hidden Markov models and probabilistic inference, generally show lower TLS values compared to classification-oriented terms. This indicates that, while temporally aware and probabilistic models are conceptually important, they are less integrated into the broader ML-defense research network. Their limited connectivity reinforces earlier observations of methodological fragmentation and underutilization of uncertainty-aware statistical approaches.

Emerging topics, including adversarial machine learning, data privacy, and IoT-related security, tend to exhibit low TLS values, reflecting their nascent or niche status within the literature. These topics often appear at the periphery of the network, with weaker links to dominant statistical–ML paradigms. While this suggests limited current integration, it also highlights significant opportunities for future research, particularly in developing unified statistical–ML frameworks that address robustness, trust, and distributed defense environments.

Overall, the TLS analysis provides quantitative evidence of a hierarchical conceptual structure within the field. Broad AI and cybersecurity concepts serve as highly connected hubs, while specific statistical models and emerging defense challenges remain comparatively isolated. This imbalance underscores a critical research gap: the need to elevate statistical models, especially probabilistic and temporal approaches from supporting roles to integrative components capable of bridging multiple defense application domains.

By revealing which concepts are central and which remain peripheral, Table S4 directly informs RQ2, RQ3, and RQ4, offering a data-driven basis for identifying dominant methodologies, structural fragmentation, and future research directions in statistical–ML integration for defense applications.

4.3. Research Questions and Answers

This subsection synthesizes the bibliometric results, network analyses, thematic cluster interpretation (Section 4.2.4), and Total Link Strength (TLS) analysis (Table S4) to explicitly address the four research questions (RQ1–RQ4). The answers presented below reflect the consolidated evidence derived from Scopus metadata, VOSviewer mappings, and cross-cluster synthesis.

RQ1: What are the publication trends over the last ten years concerning research on the integration of statistical models within Machine Learning approaches for defense-related applications?

The analysis demonstrates a clear and sustained growth in publications over the last decade, with a marked acceleration in the most recent years. Early studies were relatively sparse and focused on exploratory applications of classical statistical learning methods in specific defense contexts. From the late 2010s onward, publication volume increased steadily, reflecting the broader diffusion of Machine Learning across defense-related research. The sharp rise observed after 2023 indicates a maturation phase, in which statistically supported ML approaches are increasingly recognized as strategically important for cybersecurity,

autonomous systems, and data-driven defense analytics. These trends confirm that research interest in statistical–ML integration has shifted from isolated experimentation toward a more established and rapidly expanding domain.

RQ2: Which statistical models are most frequently employed to support Machine Learning algorithms in defense-related research?

The results indicate that **classification-oriented statistical models** dominate the literature. Margin-based classifiers, particularly Support Vector Machines, and regression-based methods appear most frequently across clusters, especially within cybersecurity and detection-oriented applications. The TLS analysis (Table S4) further shows that these models achieve moderate connectivity but remain largely confined to specific application clusters. In contrast, **probabilistic and temporal statistical models**, such as Bayesian approaches and Hidden Markov Models, exhibit lower TLS values, indicating limited cross-domain integration despite their theoretical relevance. This imbalance suggests that statistical models are predominantly used as task-specific enablers rather than as unifying methodological frameworks.

RQ3: In which specific defense domains do statistical models contribute most significantly to Machine Learning-based solutions?

Statistical models contribute most significantly in **cybersecurity and network defense**, which form the most densely connected thematic clusters. In these domains, statistical learning supports intrusion detection, malware classification, and anomaly detection tasks. Additional contributions are observed in **temporal threat analysis, autonomous and sensing systems, and system monitoring**, where statistical models facilitate sequential reasoning, estimation, and signal processing. However, cluster-level analysis reveals that these contributions are domain-specific, with limited methodological transfer across clusters. This pattern highlights the application-driven nature of statistical–ML integration in current defense research.

RQ4: What are the key challenges in integrating statistical models with Machine Learning in military environments, and what research opportunities and future directions have been identified?

The combined cluster interpretation and TLS analysis identify several key challenges. First, there is a strong reliance on deterministic, classification-focused models, with insufficient emphasis on uncertainty-aware and probabilistic reasoning. Second, temporal statistical models remain weakly connected to other research clusters, limiting their impact on adaptive and intelligence-driven defense systems. Third, emerging themes such as adversarial robustness, privacy, and cyber–physical security exhibit low connectivity, indicating fragmentation and early-stage development. These challenges point to clear research opportunities, including the development of **integrated statistical–ML frameworks** that explicitly incorporate uncertainty modeling, temporal dynamics, and cross-domain generalization. Addressing these gaps is essential for advancing robust, trustworthy, and operationally relevant AI systems in military environments.

V. CONCEPTUAL AND DEEP LITERATURE SYNTHESIS

This section synthesizes the bibliometric findings, thematic cluster interpretation (Section 4.2.4), and Total Link Strength (TLS) analysis (Section 4.2.5) to develop a higher-level conceptual understanding of how statistical models support Machine Learning (ML) in defense-related applications. Rather than reiterating results, this section integrates empirical evidence to identify structural patterns, conceptual relationships, and research gaps that inform theory-building and future research directions.

5.1. Thematic Clusters and Conceptual Structure

The eleven thematic clusters identified through VOSviewer analysis reveal a conceptually rich yet fragmented research landscape. Core clusters centered on artificial intelligence, machine learning, and cybersecurity exhibit dense internal connectivity and high TLS values, indicating methodological maturity and strong integration. These clusters predominantly employ classification-oriented statistical models, such as Support Vector Machines and regression-based approaches, which function as reliable enablers for detection and decision-making tasks in defense contexts.

In contrast, application-driven clusters related to temporal modeling, sensing systems, and cyber–physical security demonstrate weaker inter-cluster connectivity. Although these clusters address strategically important defense challenges, their statistical

models are often developed and applied in isolation. This separation suggests that thematic specialization has outpaced methodological integration, limiting the transferability and scalability of statistical–ML solutions across defense domains.

5.2. Conceptual Relationships among Statistical Models and ML Paradigms

Across clusters, statistical models primarily function as supporting components embedded within ML pipelines rather than as unifying conceptual frameworks. High TLS values associated with generic AI and ML concepts indicate strong convergence at the paradigm level, whereas moderate-to-low TLS values for specific statistical models reveal limited cross-cluster diffusion.

Classification-focused statistical learning dominates the conceptual core, while probabilistic and temporal models remain peripheral. This pattern indicates that uncertainty modeling and sequential reasoning despite being theoretically well suited to military environments have not been systematically integrated into mainstream defense-oriented ML research. Consequently, existing conceptual relationships favor performance-driven learning over uncertainty-aware and adaptive modeling.

5.3. Research Gaps and Emerging Themes

The synthesis highlights several cross-cutting research gaps. First, there is a structural imbalance between widely adopted deterministic classifiers and underutilized probabilistic and temporal statistical models. Second, emerging themes such as adversarial robustness, data privacy, and cyber–physical system security exhibit low TLS values, indicating early-stage development and weak integration with core methodological frameworks.

These gaps suggest that future research should prioritize integrative approaches that bridge thematic clusters rather than deepen isolated application silos. In particular, combining probabilistic inference, temporal modeling, and Machine Learning within unified architectures represents a significant opportunity to enhance robustness, adaptability, and trustworthiness in defense systems.

5.4. Implications for Theory and Defense-Oriented AI Research

From a theoretical perspective, the findings indicate that existing defense-oriented ML research relies on a narrow subset of statistical models, constraining conceptual diversity and theoretical advancement. Elevating statistical models from auxiliary tools to central components of ML system design is essential for capturing the uncertainty, risk, and dynamic behavior inherent in military environments.

Practically, this synthesis underscores the need for defense AI research to move toward cross-domain methodological integration. By leveraging statistical models as conceptual bridges across application areas, future research can contribute to the development of more robust, explainable, and operationally relevant ML-based defense systems.

VI. CONCLUSION

6.1. Summary of Findings

This study employed a hybrid Systematic Literature Review (SLR) and bibliometric approach to investigate the role of statistical models in supporting Machine Learning (ML) for defense-related applications. Based on a Scopus dataset of 130 publications, the findings reveal a sustained increase in research activity over the past decade, with a pronounced acceleration in recent years. Bibliometric indicators and network-based analyses demonstrate that research efforts are concentrated in cybersecurity, network defense, and data-driven defense analytics, while thematic clustering uncovers a diverse yet fragmented intellectual structure.

From a methodological standpoint, classification-oriented statistical models particularly Support Vector Machines and regression-based approaches dominate the literature and underpin multiple core clusters. In contrast, probabilistic and temporal statistical models, such as Bayesian methods and Hidden Markov Models, exhibit lower levels of integration across clusters. The Total Link Strength (TLS) analysis provides quantitative evidence that many statistically relevant models remain confined to specific applications rather than functioning as cross-domain integrative frameworks.

6.2. Theoretical Implications

The findings suggest that existing defense-oriented ML research is theoretically constrained by its reliance on a limited subset of statistical modeling paradigms. While statistical principles implicitly support most ML systems, explicit uncertainty-aware and temporally adaptive statistical models are underrepresented. This limits the capacity of current theoretical frameworks to fully address the uncertainty, adversarial behavior, and dynamic conditions inherent in military environments.

By repositioning statistical models from auxiliary tools to central components of ML system design, future research can advance theoretical foundations for trustworthy, adaptive, and risk-aware defense AI. In particular, integrating probabilistic reasoning and temporal modeling into ML architectures represents a critical step toward more realistic and robust theoretical models.

6.3. Practical Implications

From a practical perspective, the dominance of deterministic classifiers reflects a focus on performance-driven solutions, often at the expense of uncertainty representation and interpretability. For defense practitioners and system designers, incorporating statistical models that explicitly quantify uncertainty and temporal dynamics can enhance robustness, situational awareness, and decision confidence in operational settings.

The observed fragmentation across application domains also highlights opportunities for cross-domain integration. Developing unified statistical–ML frameworks applicable to cybersecurity, autonomous systems, and sensing platforms may improve interoperability, scalability, and efficiency in defense technology development.

6.4. Limitations

This study has several limitations. First, the analysis is limited to publications indexed in the Scopus database, which may exclude relevant studies from other sources or classified defense research. Second, bibliometric and network analyses depend on the quality and completeness of metadata, which may be affected by inconsistencies in author affiliations, keywords, or funding disclosures. Third, the study focuses on published literature and does not directly evaluate the operational performance of the identified models in real-world military systems.

6.5. Future Research Directions

Future research should prioritize the development of integrative statistical–ML approaches that address the identified gaps. Greater emphasis is needed on probabilistic modeling, uncertainty quantification, and temporal reasoning within ML-based defense systems. Additionally, research efforts should explore cross-cluster integration, linking cybersecurity, cyber–physical systems, and autonomous platforms through shared statistical–ML frameworks.

Further studies may extend this work by incorporating additional bibliographic databases, conducting longitudinal citation analyses, or empirically validating hybrid statistical–ML models in realistic defense scenarios. Such efforts would strengthen the evidence base for developing robust, trustworthy, and operationally relevant AI systems in military environments.

REFERENCES

[1] Baniecki, H., & Biecek, P. (2024). Adversarial attacks and defenses in explainable artificial intelligence: A survey. Information Fusion, 108, Article 102303. https://doi.org/10.1016/j.inffus.2024.102303

[2] Chander, R., & Kumaravelan, G. (2021). Machine learning techniques for intrusion detection systems: A statistical perspective. *International Journal of Information Security Science*, 10(2), 45–58.

[3] Duy, P. T., Minh, V. Q., Dang, B. T. H., Son, N. D. H., Quyen, N. H., & Pham, V.-H. (2024). A study on adversarial sample resistance and defense mechanism for multimodal learning-based phishing website detection. IEEE Access, 12, 11450–11465. https://doi.org/10.1109/ACCESS.2024.3436812

[4] El Othmani, O., Mosbah, A., Yahyaoui, A., & Bouaicha, A. (2023). AI-driven automated analysis systems: Integrating statistical and machine learning models. *Journal of Imaging*, 9(11), Article 373.

[5] Ghosh, S., Kumar, V., & Roy, K. (2025). Statistical learning approaches for intelligent security analytics. *Molecular Informatics*, 44(5–6).

[6] Imran, M., Afzal, M. T., & Qadir, M. A. (2016). Malware classification using dynamic features and Hidden Markov Model. Journal of Intelligent & Fuzzy Systems, 31(2), 837–847. https://doi.org/10.3233/JIFS-169015

[7] Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In Proceedings - IEEE Symposium on Security and Privacy (pp. 19–35). IEEE. https://doi.org/10.1109/SP.2018.00057

[8] Jia, Y., Zhong, F., Alrawais, A., Gong, B., & Cheng, X. (2020). FlowGuard: An intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet of Things Journal, 7(10), 9552–9562. https://doi.org/10.1109/JIOT.2020.2993782

[9] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691–51713. https://doi.org/10.1109/ACCESS.2019.2908998

[10] Kolsur, S., & Hosmani, S. (2018). Artificial intelligence-based cybersecurity frameworks: A statistical learning perspective. *International Journal of Security and Networks*, 13(2), 89–101.

[11] Kumar, V., Das, A. K., & Sinha, D. (2021). Machine learning and statistical models for intelligent defense systems. *Advances in Intelligent Systems and Computing*, 999, 279–294.

[12] Mahesh Kumar, S. V., & Parvathi, S. U. (2024). Machine learning and statistical techniques for cyber–physical system security. *Lecture Notes in Networks and Systems*, 341–352.

[13] Nallakaruppan, M., Ramesh, R., & Subramanian, S. (2024). Statistical feature learning for network security applications. *Journal of Information Security and Applications*, 78, 103504.

[14] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, Article n71. https://doi.org/10.1136/bmj.n71

[15] Pawełczyk, M. Ł., & Wojtyra, M. (2020). Real world object detection dataset for quadcopter unmanned aerial vehicle detection. IEEE Access, 8, 174394–174409. https://doi.org/10.1109/ACCESS.2020.3026192

[16] van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

[17] Varol, M., & İskefiyeli, M. (2016). An intrusion detection system for critical infrastructure using machine learning and statistical analysis. *Engineering Applications of Artificial Intelligence*, 56, 34–45.

[18] Varol, M., & İskefiyeli, M. (2025). An intrusion detection system for critical infrastructures: Modbus approach. Engineering Applications of Artificial Intelligence, 162, Article 112410. https://doi.org/10.1016/j.engappai.2025.112410