https://doi.org/10.58086/t0n3-0y36

SECURITY AND RISK IN SOFTWARE DEVELOPMENT PROJECTS: A BIBLIOMETRIC REVIEW

Francisco Conceição[1]✉, **Mário Dias Lousã**[1,2], **José Carlos Morais**[1,3]

[1] Instituto Superior Politécnico Gaya (ISPGAYA), Portugal.
[2] Insight - Piaget Research Center for Ecological Human Developement, Portugal.
[3] CEOS.PP, ISCAP, Polytechnic of Porto, Portugal.
✉ Corresponding authors**:** ispg2024100498@ispgaya.pt

Abstract

Security analysis is increasingly central to software development as organizations face rising cyber risk and regulatory pressure. Although extensive research exists on cyber risk assessment, secure software development, and security requirements, the literature remains fragmented at the project level. This study presents a bibliometric analysis of research published between 2015 and 2026, using data retrieved exclusively from The Lens and structured through a PRISMA-guided workflow. Only journal and conference publications addressing security analysis within software development projects were retained, while studies focused solely on isolated technical vulnerabilities or non-project contexts were excluded, resulting in a final dataset of 1,008 documents. The dataset was analyzed using descriptive bibliometrics, collaboration and geographical analysis, field-of-study classification, keyword co-occurrence, co-citation, and bibliographic coupling, supported by VOSviewer. Results show sustained growth after 2019 and strong dominance of computer science and software engineering. Influential contributions cluster around secure SDLC frameworks, ISO/NIST standards, requirement decomposition, and emerging quantitative risk models. Despite this consolidation, the analysis reveals persistent gaps, including weak integration between cyber risk assessment and requirements engineering, limited project-level operationalization of security attributes, and a scarcity of approaches tailored to small and medium-sized enterprises (SMEs). These findings highlight the need for integrated, requirement-driven security analysis frameworks that bridge technical and organizational perspectives within software development projects.

Keywords: SMEs, Software projects, Cyber risk assessment, Requirements engineering, Bibliometric Analysis.

1. Introduction

SMEs are key drivers of economic growth and innovation but remain highly vulnerable to cyber threats. Many lack the financial resources, cybersecurity expertise, and organizational maturity needed to implement robust security and risk-management practices (Brown & Thorpe, 2023). As operations increasingly rely on internally developed software, new projects introduce significant risk when integration points, dependencies, and data flows are not systematically assessed. These pathways may create new attack surfaces, alter trust boundaries, or expose sensitive information, making project-level risk assessment a critical yet often neglected aspect of SME cybersecurity governance.

Academic interest in cyber risk assessment, secure software development life cycles (SDLC), requirements engineering, and security-aware requirement decomposition have expanded, yet research remains fragmented, particularly in SME-focused studies. Evidence shows that many SMEs underestimate cyber threats and deprioritize risk management due to limited resources and cybersecurity literacy (Rizvi et al., 2023). This has produced a persistent gap between high-level governance frameworks and the operational realities of SMEs developing software under technical, organizational, and regulatory constraints.

No existing framework integrates three elements in a manner tailored to SMEs: systematic requirement decomposition, structured mapping of security attributes such as confidentiality, integrity, and availability (CIA), and quantitative project-level risk scoring, including in regulatory contexts such as the EU Cyber Resilience Act (CRA). Current approaches address only fragments of this problem. SDLC standards encourage early security integration but offer little guidance for requirement-level analysis. Requirements engineering models provide decomposition structures but rarely incorporate security attributes systematically. Quantitative risk methods often operate at the organizational level or demand resources unrealistic for SMEs. Although some studies propose lightweight or SME-oriented approaches (El-Hajj et al., 2024), these typically lack requirement-level structuring and rigorous CIA-based analysis. As a result, SMEs lack systematic tools to evaluate the cyber-risk impact of new software components before integration.

These limitations create a clear need to examine how research in this domain has evolved, including which frameworks dominate, how risk assessment and requirements engineering interact, and which gaps persist.

This study responds through a bibliometric analysis of literature published between 2015 and 2026. It charts thematic evolution, identifies influential frameworks and research communities, visualizes conceptual clusters (secure SDLC, requirement decomposition, CIA mapping, and SME governance), and highlights structural gaps motivating the development of an integrated cyber-risk assessment framework for internal SME software projects. By quantifying scientific output and mapping the field's intellectual structure, the study contributes to academic understanding and supports the development of practically adoptable risk-assessment approaches.

2. Key Concepts and Terms

This section introduces and clarifies the core concepts and terms that underpin the bibliometric analysis presented in this paper. While these concepts are now widely used, their interpretation and operationalization have evolved over time and vary across different research traditions.

2.1 Security Analysis

Security analysis refers to the systematic evaluation of security concerns across the software lifecycle, including requirements, design, implementation, and governance. Earlier approaches treated security as a late technical activity, whereas recent research frames it as a methodological and decision-oriented process shaping architecture and project outcomes (Assal & Chiasson, 2019; Granata, 2024).

2.2 Cyber Risk Assessment

Cyber risk assessment involves identifying and evaluating threats, vulnerabilities, and impacts affecting software systems and development processes. Contemporary studies emphasize design-time and requirements-level analysis, as early decisions strongly influence exposure and mitigation costs (El Amin et al., 2024; Radanliev et al., 2020).

2.3 Requirements Engineering

Requirements engineering concerns the elicitation, analysis, specification, and management of project requirements and is increasingly viewed as a key entry point for integrating security (Quiñones et al., 2018). Existing approaches include goal-oriented, threat-driven, risk-based, and compliance-focused perspectives, contributing to conceptual fragmentation.

2.4 Secure Software Development Lifecycle (SDLC)

Secure SDLC approaches integrate security activities across development phases, supporting earlier risk identification, improved team coordination, and resilience to supply chain threats (McGraw, 2019; Myrbakken & Colomo-Palacios, 2017).

3. Research Questions

This study is guided by a set of research questions designed to map, structure, and interpret the scientific landscape surrounding security analysis within software development.

RQ1: How has the scientific production on cyber risk assessment for software development evolved over time?

Examines how scientific production on cyber risk assessment for software development has evolved over time. Analyzing publication trends provides Insight into the maturation of the field, the emergence of methodological turning points and the influence of regulatory or technological shifts, allowing assessment of whether the domain is expanding, stabilizing or fragmenting.

RQ2: Which authors and institutions have most influenced this research domain?

Investigates which authors and institutions have exerted the greatest influence on this research domain. By analyzing authorship patterns, collaboration networks, and institutional concentration, the study identifies intellectual centers, assesses the coherence of the research community, and explores how academic and industrial environments shape methodological development.

RQ3: Which countries contribute most to research on cyber risk assessment in software development?

Focuses on the geographical distribution of scientific output, identifying the countries that contribute most to research on cyber risk assessment in software development. This analysis highlights regional asymmetries, centers of scientific activity, and the influence of national contexts, while also assessing the field's degree of internationalization.

RQ4: Which cyber risk assessment frameworks, requirement decomposition models, and disciplinary domains dominate the literature on security analysis in software development?

Examine the dominant cyber risk assessment frameworks, requirement decomposition models, and disciplinary domains underpinning literature. It explores how security analysis is framed across academic fields and the extent to which existing approaches integrate or separate risk analysis, requirements engineering, and security attribute mapping.

RQ5: How do keywords cluster conceptually to reveal core themes?

Analyze keyword clustering to reveal core conceptual themes and their interrelationships.

4. Bibliometric Methodology

This study applies the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Figure 1) guidelines to ensure transparency and replicability. While PRISMA was designed for systematic reviews, its framework effectively documents identification, screening, eligibility, and inclusion in bibliometric research. The methodology also incorporates co-citation, bibliographic coupling, and keyword co-occurrence analyses.

4.1 Databases Used

The bibliographic dataset was retrieved exclusively from The Lens, which aggregates metadata from major sources such as CrossRef, PubMed and Microsoft Academic Graph and provides standardized records suitable for bibliometric analysis. Using a single source ensured consistency, reduced duplication, and preserved comparability across retrieved records.

The bibliographic search was conducted in The Lens on 20 December 2025. Bibliometric network construction and visualization were performed using VOSviewer (version 1.6.20), which supported co-authorship, co-citation, bibliographic coupling, and keyword co-occurrence analyses. Data cleaning, filtering, and descriptive statistical analysis were carried out prior to network generation to ensure the consistency and reliability of the bibliographic records.

4.2 Dynamic Anonymization Algorithm

The search strategy was developed iteratively to balance conceptual breadth and thematic precision. Exploratory searches were used to refine terminology and boundaries and to ensure coverage of research on security analysis in software projects. The final query reflects the convergence of three domains: cyber-risk assessment, security-aware requirements engineering and software development life cycles, and was applied in The Lens to retrieve publications framing security as a methodological component of software projects:

(("cyber risk assessment" AND "software development") OR ("software requirements" AND "security" AND "risk") OR ("risk assessment" AND "software project"))

To reflect contemporary developments in cybersecurity governance, secure software engineering, and regulations such as NIS2 and the CRA, the search was limited to publications from 2015 to 2026. This timeframe captures both the early emergence of requirement-level security models and the later shift toward integrated risk-aware development practices. All records were exported in structured bibliographic format for screening and refinement through the PRISMA workflow.

4.3 PRISMA Workflow - Inclusion/Exclusion Criteria

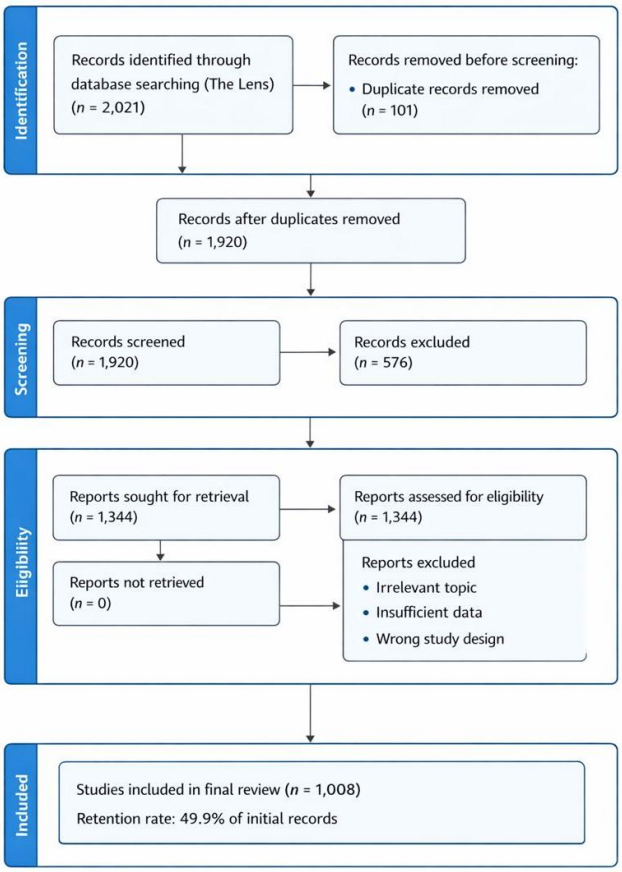

Fig 1. PRISMA flow diagram illustrating the study selection process
Source: Authors' elaboration based on PRISMA statement (no date).

Identification

The identification stage aimed to capture the broadest possible set of publications relevant to the security analysis of software projects. A comprehensive search was conducted exclusively in The Lens using the final, refined query designed to capture the intersection of cyber risk assessment, security-oriented requirements engineering, and software project contexts.

This search returned 2,021 records, representing a wide range of disciplinary perspectives. Prior to screening, 101 duplicate records were identified and removed based on metadata comparison, resulting in 1,920 unique records entering the screening phase.

Screening

The screening stage focused on eliminating records that were clearly outside the scope of the study without requiring detailed conceptual analysis. Titles and abstracts of the 1,920 records were reviewed to assess basic relevance and completeness. During this phase, 576

records were excluded because they did not address security analysis in software development contexts, lacked sufficient descriptive information, or fell outside academic literature.

Technical reports, editorial notes, white papers, and unreviewed preprints were also excluded at this stage. The screening process ensured that the remaining corpus was both methodologically credible and thematically aligned with the study's objectives, leaving 1,344 records.

Eligibility

The eligibility stage assessed the 1,344 publications that passed screening by reviewing abstracts, keywords, and full texts to determine substantive contributions to software-project security analysis. Studies were considered eligible if they proposed or applied frameworks, models, or methods supporting structured security evaluation within software development life cycles.

Publications focusing mainly on isolated vulnerabilities, penetration testing, or narrow threat enumeration, as well as those limited to high-level organizational governance without project-level methodology, were excluded. As a result, 336 studies were removed due to thematic irrelevance, insufficient methodological contribution, or unsuitable design.

Inclusion

The final dataset comprises 1,008 publications, corresponding to a retention rate of 49.9% of the initially identified records. These studies form the empirical basis for all subsequent bibliometric analyses.

This curated dataset comprises publications that align security evaluation with software engineering processes, requirement decomposition, architectural considerations, and project-level governance. It provides an empirical foundation for the analyses presented in the subsequent sections. The complete progression from identification to inclusion is visually summarized in the PRISMA flow diagram included in this paper.

4.4 Analysis Procedures

The analytical phase characterized research on security analysis in software development using descriptive and relational bibliometric techniques applied to 1,008 publications extracted and normalized from The Lens.

Temporal analysis examined publication trends (2015–2026), identifying growth, acceleration, and stabilization phases in relation to regulatory and methodological developments. Authorship analysis assessed productivity and collaboration patterns to reveal the field's intellectual structure and concentration of influence.

Disciplinary analysis evaluated the distribution of publications across fields to determine the dominance of technical versus organizational perspectives. Keyword co-occurrence, co-citation, and bibliographic coupling analyses identified dominant themes, intellectual linkages, and structural gaps, forming the empirical basis for the results.

5. Results

This section presents the empirical findings of bibliometric analysis. The results are organized around five research questions, each addressing a distinct aspect of the scholarly landscape on security analysis in software development. Beyond summarizing the evidence, the chapter highlights structural patterns, conceptual orientations, and persistent gaps within the literature.

5.1. RQ1: Evolution of Scientific Output Over Time

The temporal distribution of publications shows (Figure 2) a clear evolution in scientific output between 2015 and 2026. From 2015 to 2018, publication activity remained stable, suggesting an early consolidation phase characterized by consistent research interest and limited methodological diversification.

From 2019 onwards, a pronounced upward trend emerges, peaking between 2021 and 2022. This period represents the highest level of scientific output and reflects a phase of accelerated academic interest. The surge coincides with the wider adoption of SDLCs, growing awareness of software supply chain risks, and the increasing influence of cybersecurity regulation and governance frameworks. This concentration of publications indicates that security analysis in software projects gained strategic relevance within both academic and research communities.

After 2022, publication counts decline but remain above pre-2019 levels, indicating stabilization rather than reduced interest. Lower values for 2025 and 2026 should be interpreted cautiously due to indexing delays.

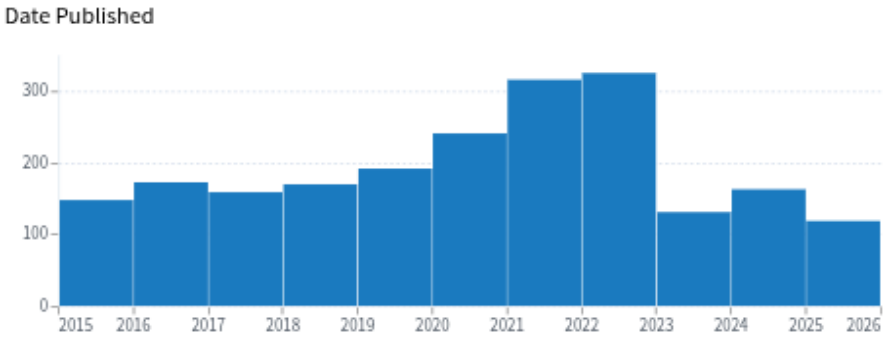

Fig 2. Scientific output on cyber risk assessment and security analysis in software development (2015–2026).
Source: The Lens database (2025).

5.2. RQ2: Influential Authors

The author profile analysis (Figure 2) reveals an uneven distribution of contributions, with a small group of researchers publishing repeatedly while most authors contribute only occasionally. This suggests that the field is influenced by limited core contributors rather than a consolidated research community.

Ruzanna Chitchyan emerges as the most prolific author, reflecting sustained engagement with requirements engineering and security-aware development. Alberto Rodrigues da Silva and Alok Mishra also show notable publication activity at the intersection of software engineering, project management, and security. Authors with two publications further reinforce the presence of limited continuity across the field.

The relatively low number of publications per author highlights the interdisciplinary and fragmented nature of the domain, with contributions often originating from adjacent research areas. This fragmentation aligns with broader bibliometric findings showing weak integration between cyber risk assessment and requirements engineering. Overall, intellectual leadership is present but not yet strongly centralized.

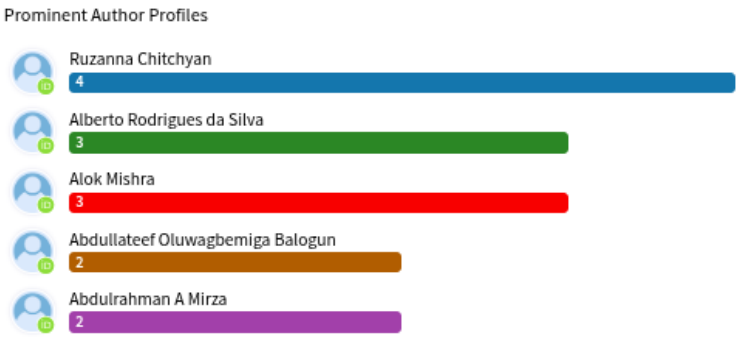

Fig 3. Prominent author profiles in research on cyber risk assessment and security analysis in software development (2015–2026).
Source: The Lens database (2025).

5.3. RQ 3: Geographical Distribution of Scientific Output

Scientific output is geographically concentrated in a small number of countries, producing an uneven global research landscape. Activity is strongest in North America, Western Europe, and parts of the Asia–Pacific region, with limited contributions from Africa, much of South America, and the Middle East (Figure 4).

The United States leads with 197 publications, reflecting strong academic infrastructure, sustained investment in cybersecurity, and close collaboration between academia, industry, and government. The United Kingdom follows with 134 publications, supported by a mature research ecosystem and a regulatory environment emphasizing cybersecurity governance. China contributes 111 publications, representing the largest output in the Asia–Pacific region and signaling a growing strategic emphasis on software security, primarily through technically oriented research.

Within Europe, Germany (72) demonstrates notable activity, often aligned with engineering-driven and standards-based approaches. Brazil (50) emerges as a key contributor in South America. India (61) and Australia (51) further reinforce Asia–Pacific representation.

Overall, dominant frameworks and methodologies are shaped mainly within technologically advanced economies.

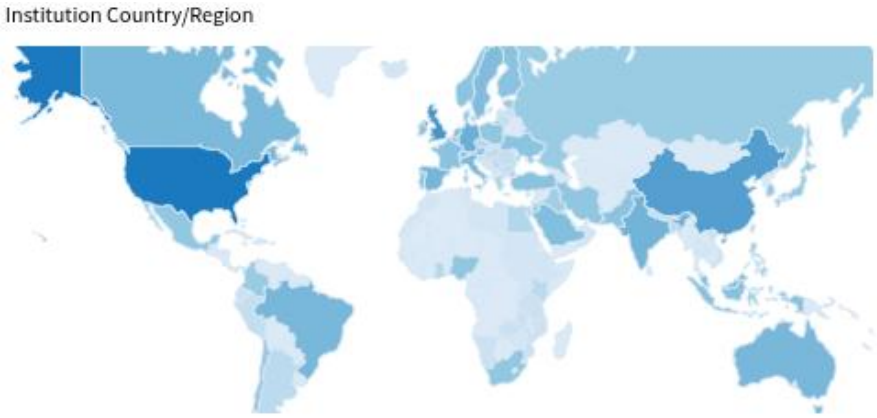

Fig 4. Global research output on cyber risk assessment in software development (2015–2026)
Source: The Lens database (2025).

5.4. RQ4: Dominant Frameworks, Conceptual Foundations and Disciplinary Origins

Literature converges around a limited set of influential frameworks. The NIST Secure Software Development Framework (SP 800-218) is a central reference, particularly in work addressing secure development practices and organizational governance. ISO/IEC 27034 and ISO/IEC 27005 also feature prominently, providing governance-oriented guidance and risk assessment structures often operationalized through threat–likelihood–impact models.

Within requirements engineering, decomposition-oriented approaches such as the Requirements Abstraction Model support analysis of how security requirements propagate across artefacts, and architectural layers, frequently structured around CIA. A smaller body of work explores quantitative risk assessment models inspired by FAIR, introducing probabilistic reasoning and scoring mechanisms that remain only partially integrated into software engineering practice.

To contextualize these frameworks, a field-of-study analysis was conducted. Computer Science dominates the dataset (Figure 5), framing security analysis primarily as a technical problem grounded in modelling, and computational reasoning. Software Engineering and Engineering provide secondary contributions, supporting secure SDLC practices and requirement decomposition, but largely retain a technical focus. Business and Information Systems fields contribute relatively little, suggesting underrepresentation of organizational and managerial perspectives and helping explain the scarcity of SME-oriented frameworks.

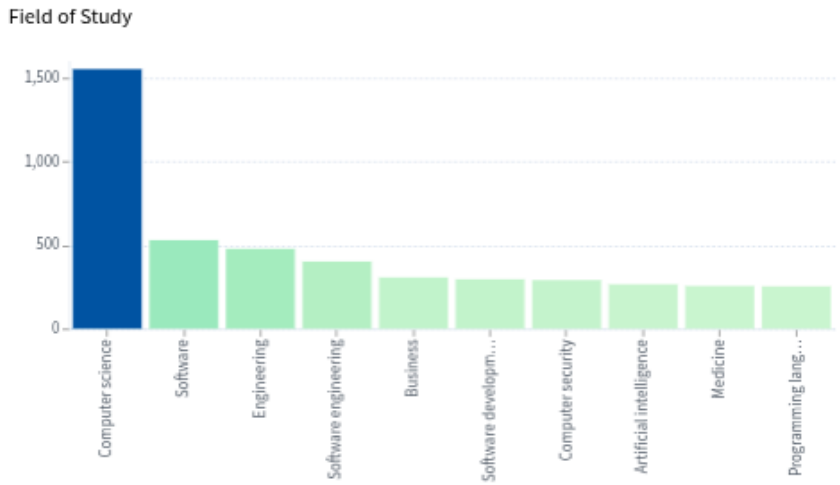

Fig 5. Dominant academic fields in security analysis research for software development projects (2015–2026).
Source: The Lens database (2025).

5.5. RQ5: Keyword Cluster Analysis

The keyword co-occurrence network (Figure 6) reveals a conceptually fragmented but moderately interconnected field. Distinct color clusters represent coherent thematic orientations, with link density indicating conceptual proximity and node position reflecting interaction across themes. Central nodes such as system, model, requirement, and risk act as bridges between clusters, while peripheral nodes represent specialized strands.

Red Cluster: System-Centered and Information-Oriented Security

The red cluster centers on system, security, data, information, application, and technology, reflecting a system-centric perspective focused on protecting information assets and architectures. Its strong internal connectivity suggests a mature research tradition rooted in computer science, though its separation from project- and requirement-oriented terms indicates limited integration with development processes.

Green Cluster: Project, Risk, and Development Lifecycle Orientation

The green cluster groups risk, project, software development, model, and technique, representing research that situates security within software projects and development life cycles. While it emphasizes decision-oriented and process-aware analysis, its limited overlap with system-level concepts suggests abstraction from concrete security attributes.

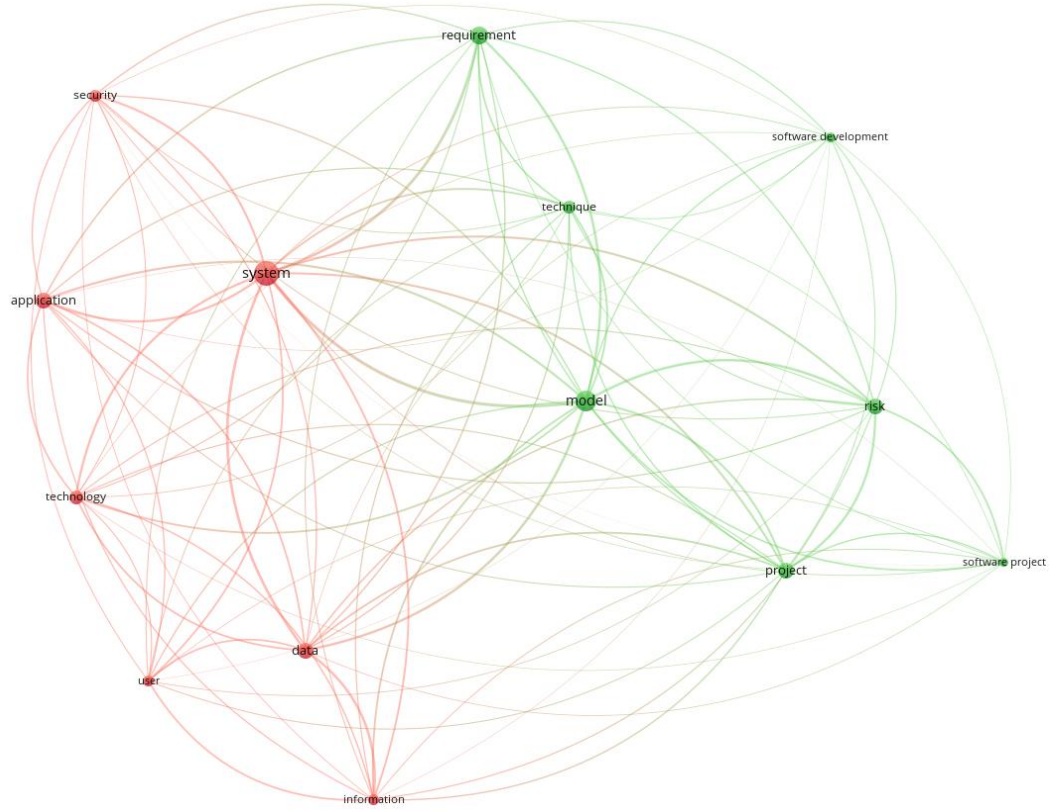

Fig 6.Conceptual structure of security analysis research in software development projects (2015–2026)
Source: VOSviewer (2025).

Light Green Cluster: Requirements and Methodological Abstraction

The light green cluster focuses on requirement, model, and technique, acting as a conceptual bridge between system and project perspectives. Although the requirement appears as a highly connected node, the relative sparsity of this cluster indicates that requirement-driven security analysis remains underdeveloped.

Synthesis of Cluster Roles

Taken together, the clusters reveal three partially aligned perspectives: system-centric security, project- and risk-oriented analysis, and requirements-based abstraction. While conceptual bridges exist, persistent fragmentation confirms the absence of cohesive frameworks integrating system-level attributes, requirement decomposition, and project-level risk evaluation.

6. Results

6.1. Trends Emerging from the Bibliometric Analysis

The bibliometric analysis shows rapid growth after 2019 followed by stabilization, indicating a shift from exploratory research to methodological consolidation. This is reflected in increasing reliance on secure SDLC guidance and standards-based frameworks, alongside a gradual rise in quantitative and model-driven risk assessment. Research remains geographically concentrated in countries with mature software and cybersecurity ecosystems, which shape dominant methodological perspectives.

The field is still led by computer science and software engineering, reinforcing a technical framing of security analysis, while organizational and socio-technical perspectives remain marginal. Thematic patterns indicate a gradual shift from system- and information-centered security towards project- and requirements-oriented approaches, although integration across these strands remains limited.

These findings align with earlier bibliometric studies reporting strong post-2018 growth, increasing dependence on secure SDLC frameworks, and persistent separation between technical security research and project-level decision processes (Khan et al., 2020; Williams et al., 2025). Compared with broader software-security reviews, this study also identifies a stronger emphasis on governance-oriented standards (ISO/NIST) and weaker integration of requirements engineering and quantitative risk modelling.

6.2. Literature Gaps with Direct Implications

Despite this consolidation, the literature shows persistent structural gaps with theoretical and practical implications. Cyber risk assessment and requirements engineering remain weakly integrated, so security requirements are often defined without explicit links to prioritized risk, limiting project-level usefulness. Security attributes from the CIA triad are widely referenced but rarely operationalized in analytical models supporting structured evaluation across decomposed requirements or development artifacts.

Many approaches also remain anchored at the organizational or governance level, providing strategic guidance but little operational support for software projects, especially in early

lifecycle phases where design trade-offs are critical. In addition, SME constraints are seldom treated as design assumptions, with frameworks often presuming expertise and tooling unrealistic for resource-constrained organizations.

Similar gaps are reported in previous bibliometric and systematic reviews, which highlight the dominance of technically focused approaches and limited integration of organizational constraints and early-phase requirements analysis (Khan et al., 2020; Leppänen et al., 2022). Their recurrence across independent studies suggests this fragmentation is structural rather than dataset specific.

6.3. How These Gaps Justify New Research

These gaps justify further research on project-level frameworks integrating cyber risk assessment with requirements engineering. Requirement-driven approaches combining systematic decomposition, CIA mapping, and structured risk scoring provide a basis for consistent prioritization and traceability across software artifacts (Fathabadi et al., 2024; Jiang et al., 2023).

This integration is particularly important for SMEs, where security measures must be feasible under resource constraints and growing regulatory pressure. Future frameworks should therefore prioritize lightweight design, tool support, and automation.

Recent studies also highlight the potential of emerging technologies, especially artificial intelligence for automated threat modelling, and risk prediction, and DevSecOps pipelines for continuous assessment and compliance verification (Bedoya et al., 2024). Together, these directions enable scalable, requirement-centered, and resource-efficient security analysis for modern software projects.

7. Conclusions

This study shows that research on security analysis in software development has grown steadily and increasingly converges around secure SDLC models and ISO/NIST standards, indicating methodological consolidation. However, risk assessment, requirements engineering, and security attributes remain weakly integrated, and most frameworks operate at the

governance level rather than at the project level. SMEs are particularly underrepresented despite their high-risk exposure.

Overall, the literature still lacks cohesive, project-level frameworks integrating requirement decomposition, security attributes, and structured risk assessment, highlighting the need for lightweight and operational approaches suited to real-world software development constraints.

References

Assal, H., & Chiasson, S. (2018). Security in the software development lifecycle. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)* (pp. 281-296).

Bedoya, M., Palacios, S., Díaz-López, D., Laverde, E., & Nespoli, P. (2024). Enhancing DevSecOps practice with large language models and Security Chaos Engineering. *International Journal of Information Security*, *23*(6), 3765–3788. https://doi.org/10.1007/s10207-024-00909-w

Brown, C., & Thorpe, S. (2023). Towards Developing a formal model for tracking Cyber-Security Investments in Jamaica. In *SoutheastCon 2023*, 883–888.

El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. *Journal of Cybersecurity and Privacy*, *4*(2), 357–381. https://doi.org/10.3390/jcp4020018

El-Hajj, M., & Mirza, Z. A. (2024). ProtectingSmall and Medium Enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics*, *13*(19), 3910. https://doi.org/10.3390/electronics13193910

Fathabadi, A. S., Snook, C., Dghaym, D., Hoang, T. S., Alotaibi, F., & Butler, M. (2025). Systematic hierarchical analysis of requirements for critical systems. *Innovations in Systems and Software Engineering*, *21*(2), 569–593. https://doi.org/10.1007/s11334-024-00551-8

Granata, D., & Rak, M. (2024). Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. *Software Quality Journal*, *32*(1), 125–161. https://doi.org/10.1007/s11219-023-09634-4

Jiang, Y., Jeusfeld, M. A., Ding, J., & Sandahl, E. (2023). Model-based cybersecurity analysis: Extending enterprise modeling to critical infrastructure cybersecurity. *Business & Information Systems Engineering*, *65*(6), 643–676. https://doi.org/10.1007/s12599-023-00811-0

Khan, R., Khan, S., Ilyas, M., & Idris, M. (2020). *The State of the Art on Secure Software Engineering*. 24th International Conference on Evaluation and Assessment in Software Engineering, Pages 487 - 492. https://doi.org/10.1145/3383219.3383290

Leppänen, T., Honkaranta, A., & Costin, A. (2022). Trends for the DevOps security. A systematic literature review. Em *Lecture Notes in Business Information Processing* (pp. 200–217). Springer International Publishing. https://doi.org/10.1007/978-3-031-11510-3_12

McGraw, G. (2019). *Software security: Building security in* (2nd ed.). Addison-Wesley.

Quiñones, D., Rusu, C., & Rusu, V. (2018). A methodology to develop usability/user experience heuristics. *Computer Standards & Interfaces*, *59*, 109–129. https://doi.org/10.1016/j.csi.2018.03.002

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ (Clinical Research Ed.)*, *372*, n71. https://doi.org/10.1136/bmj.n71

PRISMA statement. (no date). PRISMA Statement. Retrieved December 3, 2025, from https://www.prisma-statement.org/

Radanliev, P., De Roure, D., Nurse, J. R. C., et al. (2020). *Cyber risk in IoT systems*. IEEE Access, 8, 125249–125266. https://doi.org/10.20944/PREPRINTS201903.0104.V1

Rizvi, S., Zwerling, T., Thompson, B., Faiola, S., Campbell, S., Fisanick, S., & Hutnick, C. (2023). A modular framework for auditing IoT devices and networks. *Computers & Security*, *132*(103327), 103327. https://doi.org/10.1016/j.cose.2023.103327

Williams, L., Benedetti, G., Hamer, S., Paramitha, R., Rahman, I., Tamanna, M., Tystahl, G., Zahan, N., Morrison, P., Acar, Y., Cukier, M., Kästner, C., Kapravelos, A., Wermke, D., & Enck, W. (2025). *Research Directions in Software Supply Chain Security*. https://doi.org/10.1145/3714464