



International Journal of Information Technology, Research and Applications (IJITRA)

Jane Wanjiru Njuki, Stephen Kahara Wanjau (2026). Securing the Open Frontier: A Bibliometric and Thematic Analysis of Research on Open-Source Enterprise Resource Planning (ERP) Software Security, Issue 5(3), 63-78.

ISSN: 2583-5343

DOI:10.59461/ijitra.v5i3.240

The online version of this article can be found at:
<https://www.ijitra.com/index.php/ijitra/issue/archive>

Published by:
PRISMA Publications

IJITRA is an Open Access publication. It may be read, copied, and distributed free of charge according to the conditions of the Creative Commons Attribution 4.0 International license.

International Journal of Information Technology, Research and Applications (IJITRA) is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.



<https://www.prismapublications.com/>

Journal homepage: <https://ijitra.com>

Securing the Open Frontier: A Bibliometric and Thematic Analysis of Research on Open-Source Enterprise Resource Planning (ERP) Software Security

Jane Wanjiru Njuki¹, Stephen Kahara Wanjau²

¹Department of Information Technology, ²Department of Computer Science, Murang'a University of Technology, Murang'a, Kenya

Article Info

Article history:

Received July 16, 2026

Revised August 30, 2026

Accepted September 10, 2026

Keywords:

Open-Source software; enterprise resource planning; ERP security; bibliometric analysis; thematic analysis; software security engineering.

ABSTRACT

Open-Source enterprise resource planning (ERP) systems provide organizations with flexible, customizable and potentially cost-effective alternatives to proprietary ERP platforms. However, their increasing deployment in mission-critical organizational environments introduces significant security challenges involving authentication, authorization, software vulnerabilities, privacy, configuration, maintenance, governance and third-party components. In addition, their community-driven development model, exposed source code, and heterogeneous deployment environments raise distinctive risk management concerns that remain fragmented across the literature. This study conducted a bibliometric and thematic analysis of the research landscape on OS-ERP security, drawing on a curated Scopus-derived citation corpus (n = 40 documents, 2007–2026) retrieved through Harzing's Publish or Perish. After deduplication and relevance screening, documents were classified into nine thematic clusters spanning security and access control, resilience and cloud infrastructure, adoption and risk, ERP selection methods, implementation case studies, and architectural transformation. Descriptive bibliometrics including annual output, document type, citation impact, and lead-author productivity were computed, and thematic co-occurrence in titles was used to trace the field's intellectual structure and evolution across four time period. Results show that security-specific scholarship (17.5% of the corpus) remains a minority relative to adoption and implementation studies (over half of the corpus), that citation impact is concentrated in a small set of foundational access-control and risk papers, and that thematic emphasis has shifted since 2019 toward multi-criteria selection methods and architectural modernization (microservices, IoT integration) rather than deep security engineering. The discussion situates these findings against the broader open-source software (OSS) security literature and identifies a persistent gap between the demonstrated adoption benefits of OS-ERP and the comparatively immature body of empirical security research addressing it. The paper concludes with recommendations for practitioners, researchers, and OS-ERP community maintainers, and proposes a future research agenda centred on empirical security benchmarking, secure-by-design ERP architectures, and longitudinal vulnerability studies.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Jane Wanjiru Njuki, Stephen Kahara Wanjau (2026). *Securing the Open Frontier: A Bibliometric and Thematic Analysis of Research on Open-Source Enterprise Resource Planning (ERP) Software Security*, Issue 5(3), 63-78.

Jane Wanjiru Njuki
Department of Information Technology,
Murang'a University of Technology,
Murang'a, Kenya

1 INTRODUCTION

Enterprise resource planning systems (ERP) have evolved from integrated transaction-processing applications into digitally connected platforms. These systems integrate organisation's core business processes including finance, procurement, inventory, human resources, and customer relations into a single data and process backbone (Mahraz, 2018). Historically dominated by proprietary vendors such as SAP, Oracle, and Microsoft Dynamics, the ERP market has, over the past two decades, seen a steady rise of Open-source alternatives, including Odoo, ERPNext, Apache OFBiz, Dolibarr, and the SlapOS/ERP5 ecosystem (Mladenova, 2020). In addition, Free and Open-source ERP (FOS-ERP) (Almorsy et al., 2012) is attractive to organizations which are resource-constrained because it eliminates licensing costs, enables source-level customisation, and avoids vendor lock-in.

This openness, however, is a double-edged sword. Publicly available source code lowers the barrier for attackers to discover vulnerabilities, community-driven maintenance can produce inconsistent patch cadences, and the customisation flexibility that organizations value often results in insecure default configurations, weak access-control implementations, and unmanaged plugin ecosystems (Almorsy et al., 2012). ERP systems consolidate an organisation's most sensitive operational and financial data, hence, a security failure in an OS-ERP deployment can have organisation-wide consequences ranging from data breaches to supply-chain disruption. Despite this risk profile, security has historically been a secondary concern in OS-ERP research relative to adoption, cost-benefit, and implementation studies.

This study addresses that imbalance by systematically mapping the existing scholarly literature on OS-ERP security using bibliometric and thematic analysis techniques (Linnenluecke et al., 2020). Bibliometric analysis complements conventional systematic reviews by quantifying the structure, productivity, visibility, and thematic development of a research field. Science mapping methods can reveal research growth, influential publications, sources, authors, and thematic signals at scale. The bibliometric framework, for example, formalises bibliometric workflows around data collection, performance analysis, and science mapping (Xiao et al., 2022). The present study applies this general logic to the supplied citation exports, with particular attention to the difference between database-level indicators and record-level citation distributions.

Specifically, the study pursues three objectives: (1) to characterise the volume, growth trajectory, and document-type composition of research addressing open-source ERP and its security dimension; (2) to identify the thematic clusters into which this literature falls and to quantify their relative emphasis and citation impact; and (3) to trace how thematic emphasis has evolved over time, in order to identify emerging and neglected research directions.

The remainder of this paper is organised as follows. Section 2 reviews related bibliometric and security-focused studies on open-source software and ERP systems. Section 3 details the corpus construction, cleaning, and analytical methodology. Section 4 presents descriptive and thematic results supported by tables and visualisations. Section 5 discusses the findings in relation to the wider OSS security literature. Section 6 concludes with recommendations for practitioners and researchers, and Section 7 outlines a future research agenda.

2 Related Work

Prior work has examined open-source ERP adoption and implementation, including the relevance of cost, flexibility, and SME requirements, while security-focused studies have identified factors such as outdated software, excessive access rights, inadequate training, non-compliance, weak authentication, and unauthorised software as indicators requiring explicit security controls. These strands suggest that ERP security research sits at the intersection of enterprise information systems, software engineering, cloud security, data governance, and emerging digital technologies. Therefore, research relevant to this study intersects three broader streams: (a) open-source software (OSS) security research, (b) ERP adoption and implementation research, with particular attention to SMEs, and (c) bibliometric methodology applied to information-systems and software-engineering literatures.

2.1 Open-Source Software Security

A well-established body of work argues that the transparency of open-source software (OSS) source code is simultaneously a security asset ("many eyes" peer review) and a liability (adversaries can study the code as easily as defenders). Within

the corpus analysed here, this tension surfaces in studies of model-driven security engineering applied at runtime (Almorsy, 2012; Almorsy et al., 2012), in access-control frameworks designed for cross-domain delegation (Alam et al., 2011), and in empirical work linking code-change patterns to the introduction of vulnerabilities (Parthiban & Nataraj, 2019). Related infrastructure-level security work addresses resilience in open-source cloud platforms and in the SlapOS open-source ERP-hosting environment specifically, while outlier-based intrusion detection (Abdelkhalek et al., 2019a) has been proposed as a generic protective mechanism applicable to enterprise software stacks (Iraqi & El Bakkali, 2019). These contributions, while not always ERP-specific, establish the methodological and conceptual vocabulary such as threat modelling, access control, intrusion detection, and resilience engineering that OS-ERP security research subsequently draws upon.

2.2 Open-Source ERP Adoption, Risk, and Implementation

A substantially larger stream of literature addresses why and how organisations predominantly SMEs adopt open-source ERP. This includes interpretive case studies on the organisational risk of mission-critical OSS adoption (Poba-Nzaou et al., 2014), technology organisation environment (TOE) style studies of adoption intention (Fougatsaro, 2009) (Panduwiya et al., 2021), readiness-assessment frameworks (Hidayanto et al., 2013), and numerous configuration and deployment case studies including payroll, accounting, e-commerce, and manufacturing modules implemented via the Accelerated SAP (ASAP) methodology on open-source platforms such as Odoo (Terminanto et al., 2017) (Terminanto et al., 2017, 2019; Terminanto & Hidayanto, 2017a) (Aroba & Abayomi, 2023). Earlier foundational work traced the organisational and strategic case for open-source ERP more broadly (de Carvalho & Johansson, 2011) (Olson et al., 2018) (Johansson & Sudzina, 2009) and its impact on firm performance once adopted (Cereola et al., 2012). A recurring finding across this stream is that OS-ERP adoption decisions are driven primarily by cost, flexibility, and vendor independence, with security emerging if at all as a secondary risk factor considered alongside data migration, staff training, and change-management challenges.

2.3 ERP Selection Methodologies

A distinct and growing cluster applies multi-criteria decision-making (MCDM) techniques such as Fuzzy Analytic Hierarchy Process (AHP), TOPSIS, SHERPA, and WASPAS to help SMEs select among competing open-source ERP packages (Ibrahim et al., 2023) (Ibrahim et al., 2023; Utama et al., 2024), or supporting infrastructure such as database management systems (Gunawan, 2020). While these studies occasionally list "security" or "data protection" as one weighted criterion among many (cost, usability, vendor support, scalability), none in the reviewed corpus treats security as the primary object of investigation, suggesting selection research currently under-weights security relative to functional and economic criteria.

2.4 Bibliometric and Thematic Analysis in Information Systems

Bibliometric methods including citation counting, co-word analysis, and thematic clustering (Linnenluecke et al., 2020; Xiao et al., 2022) are well established for mapping the intellectual structure of information systems sub-fields. Such analyses typically rely on large corpora (hundreds to thousands of records) drawn from Scopus or Web of Science and often incorporate co-citation or bibliographic coupling network analysis. The present study adopts a lighter-weight but methodologically consistent variant of this approach, appropriate to the topic open-source ERP security whose indexed literature is still comparatively small and dispersed across information systems, software-engineering, and security venues. This scarcity is itself a finding in that it indicates that OS-ERP security has not yet consolidated into a recognised sub-field with its own dedicated venues, in contrast to the maturing adoption and implementation literature.

3. Methodology

3.1 Research Design

This study employs a bibliometric and thematic analysis design, combining quantitative descriptive bibliometrics (publication counts, document types, citation counts) with qualitative thematic classification of document titles and subject matter. This mixed approach is appropriate given the moderate corpus size after relevance screening, which precludes large-scale network-based bibliometrics (e.g., co-citation mapping) but supports rigorous descriptive and thematic synthesis.

3.2 Research questions

The analysis is guided by three research questions:

RQ1: What is the temporal, document-type, and citation-impact profile of research related to open-source ERP security?

RQ2: What thematic clusters characterise this literature, and how much attention does security-specific research receive relative to adoption, implementation, and selection research?

RQ3: How has thematic emphasis shifted over time, and what gaps does this reveal for future research?

3.3 Data Source and Retrieval

Bibliographic records were retrieved from the Scopus database using Harzing's Publish or Perish (PoP) software, which queries Scopus and exports standardised citation metadata including author(s), title, source/venue, publication year, DOI, and a Scopus-derived cumulative citation count ("cited by") in Research Information Systems (RIS) format. Five separate PoP export sessions (conducted between 18 August and 5 September 2026) targeting open-source ERP and related security, adoption, and implementation search terms yielded five RIS files comprising 66 raw bibliographic records in total. The five files were as a result of different keyword application in the Scopus retrieval.

3.4 Data Cleaning and Relevance Screening

Raw records were parsed programmatically using Python *rispy* library and subjected to a four-stage cleaning protocol:

i) Deduplication: records were deduplicated using DOI as the primary key, with normalised title-matching as a fallback for records lacking a DOI. This removed 9 duplicate records (66 → 57 unique records), reflecting overlap between the five separate search sessions.

ii) Structural filtering: 12 records lacking any identifiable author and whose titles matched generic proceedings-volume or working-conference naming conventions (e.g., "18th Americas Conference on Information Systems 2012, AMCIS 2012, Volume 4") were excluded as non-analysable placeholder entries exported by Scopus for whole conference volumes rather than individual papers.

iii) Relevance screening: five additional records were excluded as topically irrelevant false positives introduced by the citation-search process: three biomedical articles on cardiac atrial fibrillation (sharing incidental keyword or author-network overlap with the seed searches), one undated trade-press "Note" lacking identifiable authorship, and one systematic review on logistics business-intelligence unrelated to ERP security.

iv) Final corpus: after cleaning, 40 unique, topically relevant documents remained and constitute the analytical corpus for this study.

It is important to note the scope of this exclusion protocol: it removes clear noise and non-analysable placeholders while retaining documents across the full spectrum of OS-ERP related scholarship (security-specific, adoption, implementation, selection, and architecture), so that the relative weight of security research within the broader field can be meaningfully assessed. The corpus is best characterised as a curated citation-network sample rather than an exhaustive systematic-review population; this scope decision and its implications are revisited as a limitation in Section 6.

3.5 Variable Extraction

For each retained record, the following variables were extracted or derived: publication year; source/venue name; lead and co-author names; DOI; and Scopus cumulative citation count (parsed from the PoP "Cited By" annotation field). Because the PoP/Scopus RIS export used for this corpus tagged nearly all records with a generic journal-article reference type irrespective of their true publication form a recognised quirk of Publish or Perish's RIS output document type (journal article, conference paper, book chapter, or book) was reclassified manually using venue-name heuristics: Springer "Lecture Notes" series were coded as book chapters; venues containing "conference", "proceedings", "colloquium", or "symposium" were coded as conference papers; the single monograph-length title was coded as a book; and all remaining records were coded as journal articles. A four-period temporal scheme (2007–2013, 2014–2018, 2019–2023, 2024–2026) was defined post hoc to give approximately balanced bins for trend analysis.

3.6 Thematic Classification

Each document was assigned to exactly one of nine mutually exclusive thematic clusters based on a rule-based keyword classification of its title, subsequently verified by manual review: Security & Access Control; Resilience & Cloud Infrastructure; Software Quality & Engineering Practice; ERP Selection & MCDM (multi-criteria decision-making) Methods; Adoption, Risk & Readiness; Implementation & Configuration Case Studies; Architecture, Infrastructure & Digital Transformation; Performance & Organisational Impact; and Open-Source ERP: General/Strategy. Classification rules and edge-case adjudication (e.g., distinguishing a security-audit case study from a general implementation case study) followed the priority order in which the clusters are listed above, with security and resilience-related keywords taking precedence to avoid under counting security relevant work embedded within broader implementation narratives.

3.7 Analytical Techniques

Descriptive statistics (frequency counts, means, maxima) were computed for each variable using Python (pandas-equivalent CSV processing). Citation-impact analysis compared total and mean citations across thematic clusters and identified the top-cited documents overall. Temporal-thematic evolution was analysed by cross-tabulating cluster membership against the four-period temporal scheme. All visualisations were produced using Matplotlib.

4 4. Results

4.1 Descriptive Overview

The final corpus comprises 40 documents published between 2007 and 2026, collectively accumulating 282 recorded citations (mean = 7.05 citations per document; median = 3). Conference papers are the dominant document type ($n = 20$, 50%), followed by journal articles ($n = 14$, 35%), book chapters ($n = 5$, 12.5%), and one book (2.5%) as shown in Figure 1. This distribution is consistent with a still-maturing applied research area in which conference venues (software engineering, information systems, and industry-oriented colloquia) serve as the primary dissemination channel, ahead of slower-cycle journal publication.

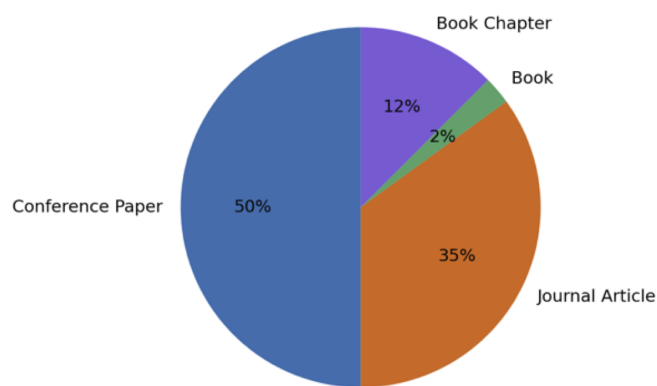


Figure 1: Document-type composition of the corpus.

Annual output shows an uneven but persistent publication pattern rather than a single sharp growth curve. An early cluster around 2009–2013 coincides with the initial academic interest in free/open-source ERP (FOS-ERP) as a distinct research object, followed by a second, more security- and selection-oriented resurgence from 2019 onward, including a notable peak in 2023 ($n = 6$).

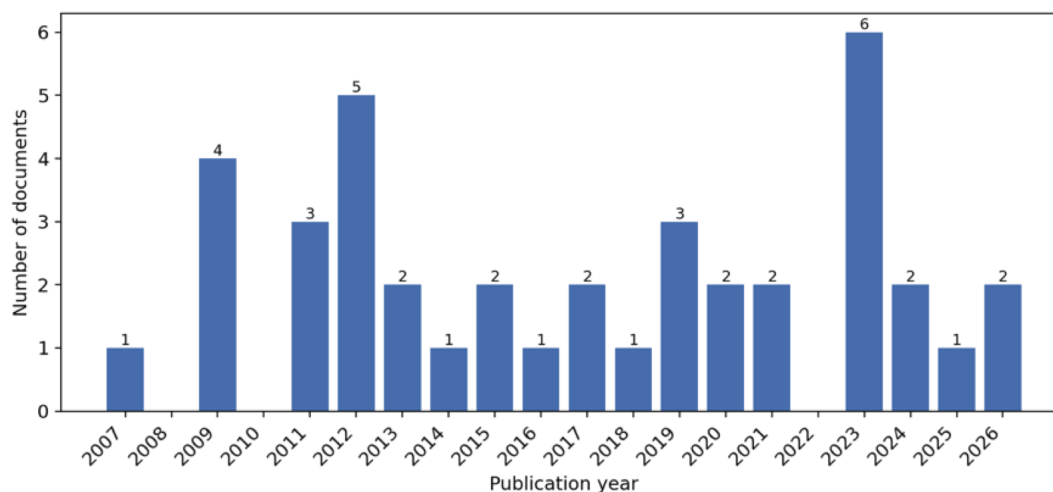


Figure 2: Annual distribution of publications in the corpus (2007–2026).

4.2 Thematic Distribution

Classifying the corpus into nine thematic clusters (Table 1, Figure 3) shows that Implementation & Configuration Case Studies form the largest cluster ($n = 10$, 25%), followed by Security & Access Control ($n = 7$, 17.5%) and the General/Strategy cluster ($n = 7$, 17.5%). ERP Selection & MCDM Methods contains five documents (12.5%) and Adoption, Risk & Readiness contains four (10%). The remaining clusters include Architecture/Infrastructure, Resilience & Cloud Infrastructure, Performance & Organisational Impact, and Software Quality & Engineering Practice which are comparatively small with three, two, one, and one documents respectively.

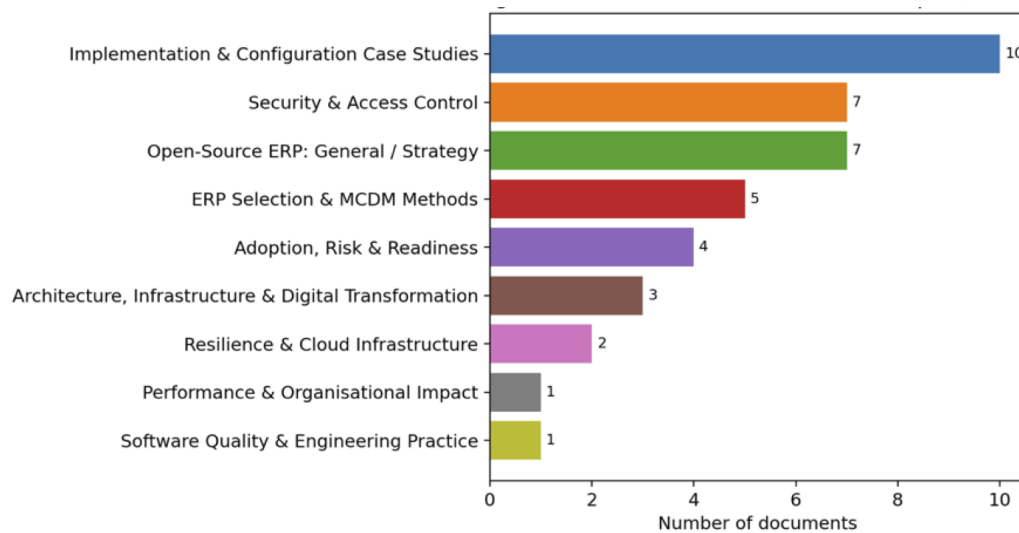


Figure 3: Thematic distribution of the corpus ($n = 40$).

Table 1 summarises citation and cluster-size statistics. Notably, Security & Access Control—despite being only the second-largest cluster by document count—ranks among the higher-impact clusters by total citations, driven substantially by two highly cited foundational papers on access-control delegation and model-driven runtime security engineering (see Section 4.3).

Table 1: Corpus composition and citation impact by thematic cluster.

Thematic Cluster	n	Total Citations	Mean Citations/Doc	Max Citations
Implementation & Configuration Case Studies	10	45	4.5	12
Security & Access Control	7	76	10.9	38
Open-Source ERP: General / Strategy	7	38	5.4	26
ERP Selection & MCDM Methods	5	9	1.8	3
Adoption, Risk & Readiness	4	54	13.5	31
Architecture, Infrastructure & Digital Transformation	3	13	4.3	12
Resilience & Cloud Infrastructure	2	18	9	13
Performance & Organisational Impact	1	29	29	29
Software Quality & Engineering Practice	1	0	0	0

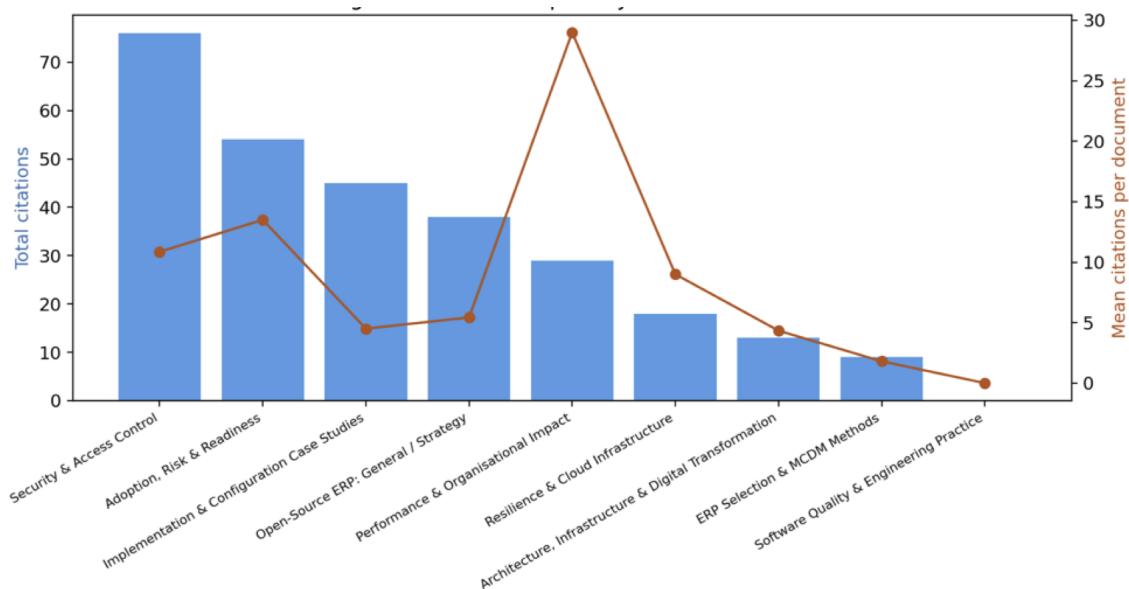


Figure 4: Citation impact (total and mean per document) by thematic cluster.

4.3 Citation Impact: Most-Cited Documents

The ten most-cited documents in the corpus as illustrated in Figure 5 and Table 2 are dominated by two categories: general-purpose security/access-control research subsequently adopted by the ERP and enterprise-systems community (e.g., a cross-domain access-control delegation framework, Alam (Alam et al., 2011), and a model-driven runtime security-engineering approach, Almorsy (Almorsy, 2012), and organisational studies of OSS/ERP adoption risk and readiness Poba-Nzaou (Poba-Nzaou et al., 2014) and Cereola (Cereola et al., 2012). The single most-cited document in the corpus is Alam's (2011) scalable, lightweight cross-domain access-control and delegation framework with 38 citations, followed by Poba-Nzaou's (2014) interpretive case study on the risk of adopting mission-critical OSS applications with 31 citations and Cereola's (2012) study of top-management-team impact on firm performance in SMEs adopting commercial open-source ERP with 29 citations. Other highly cited works include the foundational strategy text on free and open-source ERP by Carvalho, 2011 with 26 citations, an ERP implementation-readiness framework by Hidayanto, 2013 with 17 citations, and Suciu's (2012) open-source cloud-resilience solution with 13 citations.

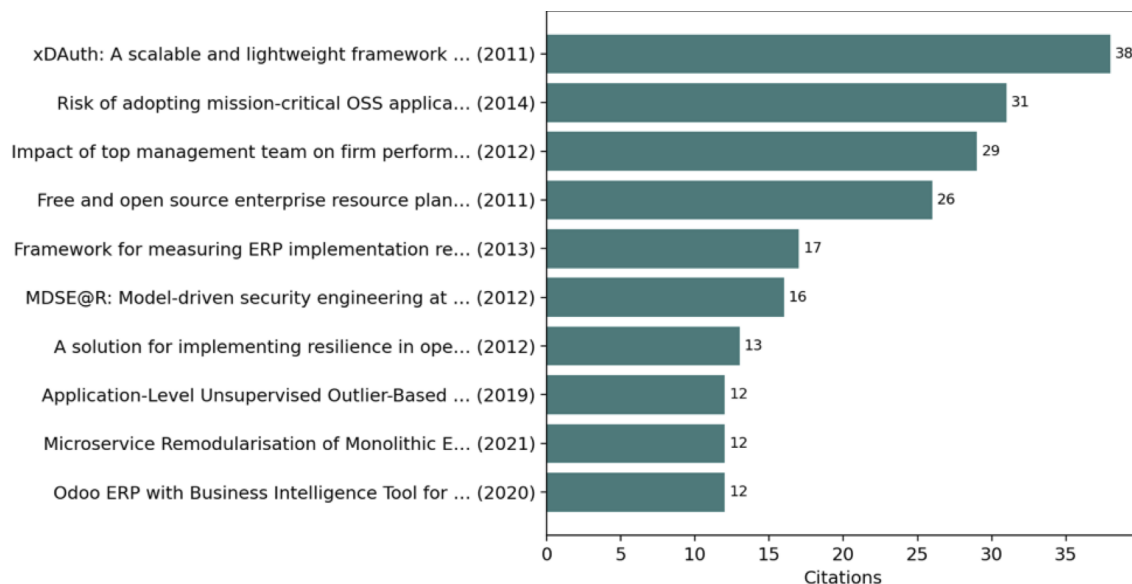


Figure 5: Ten most-cited documents in the corpus.

Table 2 document ranking ranging from 1 to 15, year of publication, title, the lead author, type and number of citations.

Table 2: Fifteen most-cited documents in the corpus.

Rank	Year	Title	Lead Author	Type	Citations
1	2011	xDAuth: A scalable and lightweight framework for cross domain access control and delegation	Alam, M.	Conference Paper	38
2	2014	Risk of adopting mission-critical OSS applications: An interpretive case study	Poba-Nzaou, P.	Journal Article	31
3	2012	Impact of top management team on firm performance in small and medium-sized enterprises adopting commercial open-source enterprise resource planning	Cereola, S.J.	Journal Article	29
4	2011	Free and Open-Source enterprise resource planning: Systems and strategies	Carvalho, R.A. de	Book	26
5	2013	Framework for measuring ERP implementation readiness in small and medium enterprise (SME): A case study in software developer company	Hidayanto, A.N.	Journal Article	17
6	2012	MDSE@R: Model-driven security engineering at runtime	Almorsy, M.	Book Chapter	16
7	2012	A solution for implementing resilience in Open-Source cloud platforms	Suciu, G.	Conference Paper	13
8	2019	Application-Level Unsupervised Outlier-Based Intrusion Detection and Prevention	Iraqi, O.	Journal Article	12
9	2021	Microservice Remodularisation of Monolithic Enterprise Systems for Embedding in Industrial IoT Networks	Alwis, A.A.C. De	Book Chapter	12
10	2020	Odoo ERP with Business Intelligence Tool for a Small-Medium Enterprise: A Scenario Case Study	Wu, J.Y.	Conference Paper	12
11	2023	An Enterprise Resource Planning (ERP) SAP Implementation Case Study in South Africa Small Medium Enterprise Sectors	Aroba, O.J.	Book Chapter	10
12	2017	Identifying characteristics and configurations in Open-Source ERP in accounting using ASAP: A case study on SME	Terminanto, A.	Conference Paper	7
13	2023	Performance evaluation of ERP based to ISO/IEC 25010:2011 quality model (a case study)	Panduwiyasa, H.	Conference Paper	7
14	2012	Practical solutions for resilience in SlapOS	Courteaud, R.	Conference Paper	5
15	2016	Comparative analysis of Open-Source ERP softwares for small and medium enterprises	Bajaj, S.	Conference Paper	5

4.4 Temporal Evolution of Thematic Emphasis

Cross-tabulating thematic cluster against the four-period temporal scheme is illustrated in Figure 6 which reveals a clear shift in the field's centre of gravity. In the earliest period (2007–2013, n = 17 documents), the General/Strategy cluster dominates

the research by Fougatsaro (Fougatsaro, 2009) Carvalho(de Carvalho & Johansson, 2011), Stefanou (Almorsy et al., 2012), reflecting foundational conceptual work defining FOS-ERP as a research object, alongside an early wave of Security & Access Control publications by Alam in 2011, Stojanovic in 2011 and Almorsy in 2012. The middle period (2014–2018, $n = 7$) is dominated by Implementation & Configuration Case Studies by Terminanto(Terminanto & Hidayanto, 2017b) , 2017, 2018; Tang, 2015). The most recent full period (2019–2023, $n = 14$) shows the emergence of ERP Selection & MCDM Methods by Ibrahim (Ibrahim et al., 2023) and Utama (Utama et al., 2024) alongside continued implementation case-study work by Wu (Wu & Chen, 2020), Aroba (Aroba & Abayomi, 2023), and Panduwiyasa [] and a renewed Security & Access Control presence by Iraqi (Iraqi & El Bakkali, 2019), Abdelkhalek(Abelkhalek et al., 2019b) and Gómez (Gómez et al., 2021), The earliest documents of the newest period (2024–2026, $n = 5$) are so far dominated by Architecture/Infrastructure by Ram, 2024, Manasia, 2026 and Selection-methods research with Utama et al., 2025 and Abreu, 2026, with comparatively less new security-specific output beyond Bibi(Bibi, 2024) an observation returned to in the Discussion. Ram, Manasia, Utama and Abreu were among the papers retrieved through the Scopus in the Publish or Perish platform, however their full articles were not retrieved for in-depth analysis.

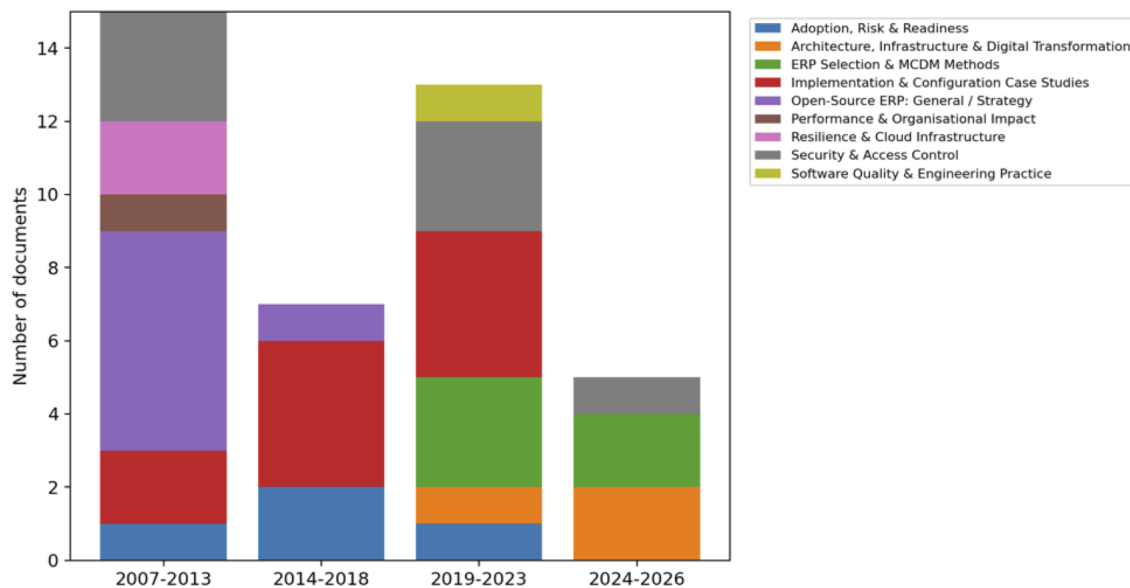


Figure 6 : Evolution of thematic emphasis across four publication periods.

4.5 Productivity and Source Distribution

Author productivity in the corpus was highly dispersed with only two lead authors contributing more than one document for instance a maximum of four documents from Terminanto, 2017, 2017, 2018, 2019, associated with a coherent stream of ASAP-methodology implementation case studies, and two from Panduwiyasa both in 2023. In addition, the great majority of lead authors numbering 34 of 36 distinct lead authors appear only once. This pattern, combined with 36 distinct publication venues across 40 documents, is characteristic of an emergent, pre-paradigmatic research area that has not yet consolidated around a small set of core authors or dedicated journals/conferences reinforcing the thematic evidence that OS-ERP security is not yet a mature, self-referential sub-field.

5 Discussion

5.1 A Security Minority Within a Broader Adoption-Oriented Field

The central empirical finding of this study is quantitative indicating only 17.5% of the corpus that is 7 of 40 documents is classifiable as directly addressing security or access control (Alam, 2011; Almorsy, 2012; Stojanovic, 2011; Abdelkhalek, 2019; Iraqi, 2019; Gómez, 2021; Bibi, 2024), compared with nearly half the corpus when Implementation, Adoption/Risk, and Selection clusters are combined accounting for 19 of 40 documents which is 47.5%. This imbalance mirrors a broader pattern documented in the OSS security literature, where functional, economic, and adoption considerations (Poba-Nzaou, 2014; Cereola, 2012) typically precede security as a research priority until high-profile incidents shift attention. For OS-ERP

specifically, the concentration of sensitive organisational data within a single integrated platform arguably warrants earlier and more sustained security attention than the current literature reflects.

5.2 Citation Impact Reflects Cross-Fertilisation, Not ERP-Native Security Research

A striking pattern in the citation-impact results (Section 4.3) is that the highest-cited "security" documents in the corpus are not ERP-native security studies but general-purpose access-control and security-engineering contributions (cross-domain access-control delegation, Alam, 2011; model-driven runtime security engineering, Almorsy, 2012) that have been picked up by the broader enterprise-systems community. This suggests that OS-ERP security research to date has been more a downstream consumer of general software-security methodology than a generator of ERP-specific security theory, architectures, or benchmarks. The most highly cited genuinely ERP-focused security contribution in the corpus Poba-Nzaou's (2014) interpretive case study on the organisational risk of adopting mission-critical OSS frames security primarily as an organisational-risk factor rather than a technical one, further underscoring the relative scarcity of deep technical security research (e.g., vulnerability analysis, penetration testing, or formal security verification) specific to open-source ERP codebases. Even the most technically detailed ERP-security contributions in the corpus such as an ISO 27001 implementation in an educational OS-ERP deployment (Bibi, 2024) and a security-audit case study in an industrial e-health OS-ERP system (Gómez, 2021) remain single-organisation case studies rather than generalisable technical benchmarks.

5.3 The Rise of Selection Methods as a Missed Opportunity for Security Criteria

The growth of MCDM-based ERP selection research since 2019 (Fuzzy AHP, TOPSIS: Ibrahim, 2023; Utama et al., 2025; SHERPA/WASPAS: Paz, 2023; industry 4.0 strategic selection: Abreu, 2026) represents a methodologically sophisticated and growing sub-stream. However, review of the corpus's selection-methods documents shows that security is, at best, one minor weighted criterion among many (cost, functionality, vendor support, ease of use), rather than a first-class decision dimension with its own sub-criteria (e.g., patch cadence, CVE history, access-control granularity, encryption support). This represents a concrete, addressable gap: existing MCDM frameworks could be extended relatively easily to formally incorporate security posture as a weighted selection criterion for SMEs choosing among open-source ERP platforms.

5.4 Architectural Modernisation Introduces New, Under-Studied Attack Surfaces

The emergence of microservice re-modularisation and IoT-network integration research (Alwis, 2021) in the most recent period signals that open-source ERP systems are increasingly being decomposed into distributed, network-exposed architectures. This architectural shift—while beneficial for scalability and Industry 4.0 integration (Manasia, 2026; Ram, 2024)—introduces new attack surfaces (inter-service communication, API gateways, IoT-device trust boundaries) that are not addressed by the access-control and resilience research conducted in the earlier, more monolithic era of OS-ERP deployment (e.g., SlapOS-style cloud resilience, Courteaud, 2012; Suciu, 2012). The corpus contains no documents that examine security specifically in the context of microservice-based or IoT-integrated open-source ERP, representing a timely gap given the direction of architectural travel signalled by Alwis (2021).

5.5 Limitations

This study has several limitations. First, the corpus ($n = 40$) is a curated citation-network sample retrieved via a specific set of Publish or Perish search sessions rather than an exhaustive systematic-review population constructed via a fully documented multi-database Boolean search strategy (e.g., PRISMA); as such, the volumetric findings should be interpreted as indicative of relative emphasis within the retrieved sample rather than as a definitive census of the entire OS-ERP security literature. Second, thematic classification was performed at the level of document titles using a rule-based keyword approach (manually verified), which, absent full-text or abstract screening, may occasionally misclassify documents whose title does not fully reflect their content. Third, Scopus-derived citation counts are a single, time-bound impact proxy and do not capture qualitative influence, altmetric attention, or grey-literature/community impact (e.g., GitHub issue discussions, security advisories) that may be particularly relevant for open-source software research. Fourth, the exclusion of unauthored, proceedings-volume placeholder records, while methodologically necessary, means the study does not capture every individual paper that may have appeared within those conference volumes. Fifth, because most source records were exported with a uniform generic reference type, document-type classification relied on a manual venue-name heuristic rather than publisher-asserted metadata, which may occasionally misclassify borderline cases (e.g., extended conference papers republished as journal articles).

6 Conclusion and Recommendations

This bibliometric and thematic analysis of 40 Scopus-indexed documents demonstrates that research explicitly addressing the security of open-source ERP systems remains a minority strand within a broader, more adoption and implementation-oriented literature. Citation impact in the security space is driven largely by general-purpose security-engineering contributions rather than ERP-native technical security research, and recent thematic growth has favoured selection methodologies and architectural modernisation over deep security investigation even as that architectural modernisation (microservices, IoT integration) plausibly expands the attack surface these systems present.

6.1 Recommendations for Practitioners

1. SMEs and organisations evaluating open-source ERP platforms should treat security posture (patch cadence, CVE history, access-control granularity, encryption capabilities) as an explicit, weighted criterion in vendor/platform selection not an afterthought to cost and functionality.
2. Organisations deploying OS-ERP should institute independent security audits (as demonstrated in the limited case-study literature on industrial e-health OS-ERP deployments) rather than relying solely on community-maintained default configurations.
3. IT decision-makers should map their OS-ERP architecture (monolithic vs. microservice/IoT-integrated) explicitly to a corresponding threat model, since the security assumptions of earlier monolithic deployments do not transfer cleanly to newer distributed architectures.

6.2 Recommendations for Researchers

1. Prioritise ERP-native technical security research (vulnerability analysis, penetration testing, formal verification of access-control implementations) rather than continuing to rely primarily on imported, general-purpose security frameworks.
2. Extend existing MCDM-based ERP-selection frameworks (Fuzzy AHP, TOPSIS, SHERPA, WASPAS) to formally incorporate multi-dimensional security criteria, enabling security-aware platform selection for SMEs.
3. Pursue longitudinal and comparative studies that track the security posture of major OS-ERP projects (Odoo, ERPNext, Apache OFBiz, Dolibarr) over time, analogous to established OSS vulnerability-lifecycle research in other software domains.

6.3 Recommendations for Open-Source ERP Communities and Maintainers

1. Publish structured, machine-readable security advisories and maintain public CVE-style disclosure records to enable exactly the kind of empirical security research this analysis finds lacking.
2. Provide reference-secure default configurations and automated security-hardening tooling, given the evidence that SME adopters often lack dedicated security expertise at deployment time.

7 Future Work

Building on the gaps identified in Sections 5 and 6, five priority directions are proposed for future research:

1. Empirical security benchmarking: systematic vulnerability assessment and penetration testing across major open-source ERP platforms, published as comparable, repeatable benchmarks.
2. Security-aware selection frameworks: extension of existing Fuzzy AHP/TOPSIS/SHERPA/WASPAS ERP-selection models with explicit, validated security sub-criteria and weighting schemes.
3. Secure architectures for distributed OS-ERP: dedicated security research on microservice-based and IoT-integrated open-source ERP deployments, including API-gateway security, service-to-service authentication, and IoT-device trust management.

4. Longitudinal vulnerability-lifecycle studies: tracking of disclosed vulnerabilities, patch latency, and community responsiveness across major OS-ERP projects over multi-year windows, following established methodologies from OSS security research.
5. Expanded, systematic corpus construction: a full PRISMA-style systematic review across multiple databases (Scopus, Web of Science, IEEE Xplore, ACM Digital Library) with abstract/full-text screening, to validate and extend the thematic structure identified in this exploratory analysis, ideally supplemented with co-citation and bibliographic-coupling network analysis once a larger corpus is assembled.

References

- [1] Abdelkhalek, M., Jamil, A. M., & Ben Othmane, L. (2019a). Identification of the impacts of code changes on the security of software. *Proceedings - International Computer Software and Applications Conference*, 2(2), 569–574. <https://doi.org/10.1109/COMPSAC.2019.10268>
- [2] Abdelkhalek, M., Jamil, A. M., & Ben Othmane, L. (2019b). Identification of the impacts of code changes on the security of software. *Proceedings - International Computer Software and Applications Conference*, 2(2), 569–574. <https://doi.org/10.1109/COMPSAC.2019.10268>
- [3] Alam, M., Zhang, X., Khan, K. H., & Ali, G. (2011). xDAuth: A scalable and lightweight framework for cross domain access control and delegation. *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*, 31–40. <https://doi.org/10.1145/1998441.1998447>
- [4] Almorsy, M. (2012). MDSE@R: Model-driven security engineering at runtime. *Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 7672(Query date: 2026-08-18 16:11:18), 279–295. https://doi.org/10.1007/978-3-642-35362-8_22
- [5] Almorsy, M., Suciu, G., Courteaud, R., Bibi, S., Gunawan, A., Ram, S. S. H., Stefanou, C. J., Carstea, C., Kontsevoi, B., & Abreu, A. L. I. (2012). SMEs and FOS-ERP Systems: Risks and Opportunities. *18th Americas Conference on Information Systems 2012 Amcis 2012*, 4(Query date: 2026-08-18 16:11:18), 632–636. <https://doi.org/10.1109/ICC-ROBINS60238.2024.10534001>
- [6] Aroba, O. J., & Abayomi, A. (2023). An implementation of SAP enterprise resource planning—A case study of the South African revenue services and taxation sectors. *Cogent Social Sciences*, 9(1). <https://doi.org/10.1080/23311886.2023.2228060>
- [7] Bibi, S. (2024). Implementing ISO 27001 Security Measures in Educational Open-Source ERP Systems. *Proceedings 2024 14th International Conference on Software Technology and Engineering Icste 2024*, (Query date: 2026-08-18 16:11:18), 35–39. <https://doi.org/10.1109/ICSTE63875.2024.00014>
- [8] Cereola, S. J., Wier, B., & Norman, C. S. (2012). Impact of top management team on firm performance in small and medium-sized enterprises adopting commercial open-source enterprise resource planning. *Behaviour and Information Technology*, 31(9), 889–907. <https://doi.org/10.1080/0144929X.2010.528029>
- [9] de Carvalho, R. A., & Johansson, B. (2011). Free and open source enterprise resource planning: Systems and strategies. *Free and Open Source Enterprise Resource Planning: Systems and Strategies*, 1–227. <https://doi.org/10.4018/978-1-61350-486-4>
- [10] Fougatsaro, V. G. (2009). The power of Open-Source ERP. *Proceedings of the 1st International Conference on Manufacturing Engineering Quality and Production Systems Meqaps 09*. 1–79.
- [11] Gómez, J., Olivero, M., García-García, J. A., & Escalona, M. J. (2021). A Practical Experience Applying Security Audit Techniques in an Industrial e-Health System Which Uses an Open Source ERP. *International Conference on Web Information Systems and Technologies, WEBIST - Proceedings*, 2021-Octob(Webist), 482–489. <https://doi.org/10.5220/0010714500003058>
- [12] Gunawan, A. (2020). Selection of open source database management for system development using analytic hierarchy process method in PT. XYZ. *Proceedings of 2020 International Conference on Information Management and Technology Icimtech 2020*, (Query date: 2026-08-18 16:11:18), 632–636. <https://doi.org/10.1109/ICIMTech50083.2020.9211121>

- [13] Hidayanto, A. N., Hasibuan, M. A., Handayani, P. W., & Sucahyo, Y. G. (2013). Framework for measuring ERP implementation readiness in small and medium enterprise (SME): A case study in software developer company. *Journal of Computers (Finland)*, 8(7), 1777–1782. <https://doi.org/10.4304/jcp.8.7.1777-1782>
- [14] Ibrahim, M. F., Kurrahman, T., & Utama, D. M. (2023). Open-Source ERP Systems Selection: An Integrated Method based on Fuzzy AHP-TOPSIS. *Journal of Logistics, Informatics and Service Science*, 10(4), 234–249. <https://doi.org/10.33168/JLISS.2023.0416>
- [15] Iraqi, O., & El Bakkali, H. (2019). Application-Level Unsupervised Outlier-Based Intrusion Detection and Prevention. *Security and Communication Networks*, 2019(5). <https://doi.org/10.1155/2019/8368473>
- [16] Johansson, B., & Sudzina, F. (2009). Choosing open source ERP systems: What reasons are there for doing so? *IFIP Advances in Information and Communication Technology*, 299, 143–155. https://doi.org/10.1007/978-3-642-02032-2_14
- [17] Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. *Australian Journal of Management*, 45(2), 175–194. <https://doi.org/10.1177/0312896219877678>
- [18] Mahraz, M. (2018). Implementation and Management of ERP Systems: A. *Ieomsociety.Org*, (2010), 1684–1694. <http://ieomsociety.org/ieom2018/papers/478.pdf>
- [19] Mladenova, T. (2020). Open-source ERP systems: An overview. 2020 International Conference Automatics and Informatics, ICAI 2020 - Proceedings. <https://doi.org/10.1109/ICAI50593.2020.9311331>
- [20] Olson, D. L., Johansson, B., & De Carvalho, R. A. (2018). Open source ERP business model framework. *Robotics and Computer-Integrated Manufacturing*, 50, 30–36. <https://doi.org/10.1016/j.rcim.2015.09.007>
- [21] Panduwiyasa, H., Saputra, M., Azzahra, Z. F., & Aniko, A. R. (2021). Accounting and Smart System: Functional Evaluation of ISO/IEC 25010:2011 Quality Model (a Case Study). *IOP Conference Series: Materials Science and Engineering*, 1092(1), 012065. <https://doi.org/10.1088/1757-899x/1092/1/012065>
- [22] Parthiban, K., & Nataraj, R. V. (2019). An Efficient Architecture to Ensure Data Integrity in ERP Systems. 2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019, 236–241. <https://doi.org/10.1109/ICACCS.2019.8728352>
- [23] Poba-Nzaou, P., Raymond, L., & Fabi, B. (2014). Risk of adopting mission-critical OSS applications: An interpretive case study. *International Journal of Operations and Production Management*, 34(4), 477–512. <https://doi.org/10.1108/IJOPM-03-2012-0117>
- [24] Terminanto, A., & Hidayanto, A. N. (2017a). Identifying characteristics and configurations in open source ERP in accounting using ASAP: A case study on SME. *Proceedings - 2017 International Conference on Soft Computing, Intelligent System and Information Technology: Building Intelligence Through IOT and Big Data, ICSIIT 2017, 2018-Janua*, 227–232. <https://doi.org/10.1109/ICSIIT.2017.47>
- [25] Terminanto, A., & Hidayanto, A. N. (2017b). Identifying characteristics and configurations in open source ERP in accounting using ASAP: A case study on SME. *Proceedings - 2017 International Conference on Soft Computing, Intelligent System and Information Technology: Building Intelligence Through IOT and Big Data, ICSIIT 2017, 2018-Janua*, 227–232. <https://doi.org/10.1109/ICSIIT.2017.47>
- [26] Terminanto, A., Hidayanto, A. N., & Maulana, B. (2019). Development, configuration and implementation open source ERP in manufacturing modul with accelerated Sap method. *International Journal of Management*, 10(3), 77–98. <https://doi.org/10.34218/IJM.10.3.2019.009>
- [27] Terminanto, A., Swantoro, H. A., & Hidayanto, A. N. (2017). Configurations and implementation of payroll system using open source erp: A case study of Koperasi PT Sri. *IOP Conference Series: Materials Science and Engineering*, 277(1). <https://doi.org/10.1088/1757-899X/277/1/012036>
- [28] Utama, D. M., Ibrahim, M. F., & Jabari, A. N. A. A. K. (2024). A Fuzzy Multi-Criteria Approach for Selecting Open-Source ERP Systems in SMEs Using Fuzzy AHP and TOPSIS. *Jurnal Optimasi Sistem Industri*, 23(2), 167–187. <https://doi.org/10.25077/josi.v23.n2.p167-187.2024>
- [29] Wu, J. Y., & Chen, L. T. (2020). Odoo ERP with Business Intelligence Tool for a Small-Medium Enterprise: A Scenario Case Study. *ACM International Conference Proceeding Series*, 323–327. <https://doi.org/10.1145/3377571.3377607>
- [30] Xiao, Z., Qin, Y., Xu, Z., Antucheviciene, J., & Zavadskas, E. K. (2022). The Journal Buildings: A Bibliometric Analysis (2011–2021). *Buildings*, 12(1). <https://doi.org/10.3390/buildings12010037>

Appendix A. Full Corpus Listing (n = 40)

The following table lists all 40 documents retained in the analytical corpus, sorted by publication year, with assigned thematic cluster and citation count.

Year	Lead Author	Title	Type	Cluster	Cites
2007	Imtiaz, A.	Collaboration within the tool-and-die manufacturing industry through open-source modular Erp/Crm systems	Journal Article	Open-Source ERP: General / Strategy	4
2009	Metrailler, A.	Agile deployment of Open-Source ERP in SME's	Conference Paper	Implementation & Configuration Case Studies	2
2009	Salmans, B.	Organization size, IT capabilities, and EA perceptions: Dark clouds on the ERP horizon?	Conference Paper	Open-Source ERP: General / Strategy	2
2009	Imtiyan, M.R.	The implementation of ERP software maintenance in Open-Source platforms	Conference Paper	Implementation & Configuration Case Studies	0
2009	Carstea, C.	The power of Open-Source ERP	Conference Paper	Open-Source ERP: General / Strategy	0
2011	Carvalho, R.A. de	Free and Open-Source enterprise resource planning: Systems and strategies	Book	Open-Source ERP: General / Strategy	26
2011	Stojanovic, M.	Security management issues for Open-Source ERP in the NGN environment	Journal Article	Security & Access Control	0
2011	Alam, M.	xDAuth: A scalable and lightweight framework for cross domain access control and delegation	Conference Paper	Security & Access Control	38
2012	Suciu, G.	A solution for implementing resilience in Open-Source cloud platforms	Conference Paper	Resilience & Cloud Infrastructure	13
2012	Cereola, S.J.	Impact of top management team on firm performance in small and medium-sized enterprises adopting commercial open-source enterprise resource planning	Journal Article	Performance & Organisational Impact	29
2012	Almorsy, M.	MDSE@R: Model-driven security engineering at runtime	Book Chapter	Security & Access Control	16
2012	Courteaud, R.	Practical solutions for resilience in SlapOS	Conference Paper	Resilience & Cloud Infrastructure	5
2012	Stefanou, C.J.	SMEs and FOS-ERP Systems: Risks and Opportunities	Journal Article	Open-Source ERP: General / Strategy	1
2013	Johansson, B.	Developing Open-Source ERP systems for SMEs: Is that still of interest?	Book Chapter	Open-Source ERP: General / Strategy	0
2013	Hidayanto, A.N.	Framework for measuring ERP implementation readiness in small and medium enterprise (SME): A case study in software developer company	Journal Article	Adoption, Risk & Readiness	17
2014	Poba-Nzaou, P.	Risk of adopting mission-critical OSS applications: An interpretive case study	Journal Article	Adoption, Risk & Readiness	31
2015	Wölfel, K.	Automated ERP category configuration support for small businesses	Journal Article	Implementation & Configuration Case Studies	1
2015	Tang, N.H.	Open-Source ERP adoption for small-medium enterprises: A case study of Vietnamese firm	Journal Article	Adoption, Risk & Readiness	1
2016	Bajaj, S.	Comparative analysis of Open-Source ERP softwares for small and medium enterprises	Conference Paper	Open-Source ERP: General / Strategy	5

2017	Terminanto, A.	Configurations and implementation of payroll system using Open-Source erp: A case study of Koperasi PT Sri	Conference Paper	Implementation & Configuration Case Studies	2
2017	Terminanto, A.	Identifying characteristics and configurations in Open-Source ERP in accounting using ASAP: A case study on SME	Conference Paper	Implementation & Configuration Case Studies	7
2018	Terminanto, A.	Implementation and configurations Open-Source ERP in ecommerce module (A case study on SME)	Conference Paper	Implementation & Configuration Case Studies	1
2019	Iraqi, O.	Application-Level Unsupervised Outlier-Based Intrusion Detection and Prevention	Journal Article	Security & Access Control	12
2019	Terminanto, A.	Development, configuration and implementation Open-Source ERP in manufacturing modul with accelerated Sap method	Journal Article	Implementation & Configuration Case Studies	3
2019	Abdelkhalek, M.	Identification of the impacts of code changes on the security of software	Conference Paper	Security & Access Control	4
2020	Wu, J.Y.	Odoo ERP with Business Intelligence Tool for a Small-Medium Enterprise: A Scenario Case Study	Conference Paper	Implementation & Configuration Case Studies	12
2020	Gunawan, A.	Selection of Open-Source database management for system development using analytic hierarchy process method in PT. XYZ	Conference Paper	ERP Selection & MCDM Methods	2
2021	Gómez, J.	A Practical Experience Applying Security Audit Techniques in an Industrial e-Health System Which Uses an Open-Source ERP	Conference Paper	Security & Access Control	2
2021	Alwis, A.A.C. De	Microservice Remodularisation of Monolithic Enterprise Systems for Embedding in Industrial IoT Networks	Book Chapter	Architecture, Infrastructure & Digital Transformation	12
2023	Paz, J.V.B. de la	An Approach to Select an Open-Source ERP for SMEs Based on Industry 4.0 and Digitization Considering the SHERPA and WASPAS Methods	Journal Article	ERP Selection & MCDM Methods	1
2023	Aroba, O.J.	An Enterprise Resource Planning (ERP) SAP Implementation Case Study in South Africa Small Medium Enterprise Sectors	Book Chapter	Implementation & Configuration Case Studies	10
2023	Panduwiyasa, H.	Modelling the Adoption of Open-Source Enterprise Resource Planning System in Culinary SMEs	Conference Paper	Adoption, Risk & Readiness	5
2023	Ibrahim, M.F.	Open-Source ERP Systems Selection: An Integrated Method based on Fuzzy AHP-TOPSIS	Journal Article	ERP Selection & MCDM Methods	3
2023	Panduwiyasa, H.	Performance evaluation of ERP based to ISO/IEC 25010:2011 quality model (a case study)	Conference Paper	Implementation & Configuration Case Studies	7
2023	Kontsevoi, B.	Practice of Technical Debt Management with TETRA™ in Terms of Open-Source Project Assessment	Conference Paper	Software Quality & Engineering Practice	0
2024	Bibi, S.	Implementing ISO 27001 Security Measures in Educational Open-Source ERP Systems	Conference Paper	Security & Access Control	4

2024	Ram, S. Sai Haree	Revolutionizing Global IT Supply Chains: A Decentralized Framework for Cost-Effective and Streamlined Operations in Critical Events	Conference Paper	Architecture, Infrastructure & Digital Transformation	1
2025	Utama, D M	A Fuzzy Multi-Criteria Approach for Selecting Open-Source ERP Systems in SMEs Using Fuzzy AHP and TOPSIS	Journal Article	ERP Selection & MCDM Methods	3
2026	Manasia, A.	Revolutionizing Efficiency: The Impact of Business Process Automation on Modern Enterprises	Journal Article	Architecture, Infrastructure & Digital Transformation	0
2026	Abreu, A.L. Infante	Strategy for Selecting an Enterprise Resource Planning System in the Industry 4.0 Project of AICA Pharmaceutical Laboratories	Book Chapter	ERP Selection & MCDM Methods	0