CYBERSECURITY IN CLOUD COMPUTING: AN ANALYSIS OF KEY CHALLENGES

Alberta Ingriana[1]

[1]Management Department, Faculty of Business and Management, Universitas Dinamika Bangsa, Jambi, Indonesia

E-mail: [1]) alberta@unama.ac.id

ABSTRACT

This study conducts a systematic literature review (SLR) to analyze cybersecurity challenges in cloud computing, aiming to consolidate fragmented knowledge and identify emerging trends. Utilizing the PRISMA framework, 48 academic and industry publications from 2018 to 2025 were reviewed. Thematic coding identified five core issues: data breaches, cloud misconfigurations, insecure APIs, insider threats, and compliance challenges. To complement the qualitative synthesis, bibliometric analysis using VOSviewer was performed, generating keyword co-occurrence networks, temporal overlay visualizations, and density maps. The findings indicate a shift in research focus from purely technical solutions to integrated, strategic frameworks involving AI, machine learning, and enterprise policy alignment. Clusters of research activity were observed around intrusion detection, risk management, IoT integration, and cloud governance. Despite technological advances, challenges persist due to inconsistent implementation and a lack of standardization across deployment models. This review contributes to the scholarly and practical discourse by highlighting knowledge gaps and proposing future research directions, including the development of holistic, cross-domain security frameworks.

Keywords: ***AI, Cloud Computing, Cybersecurity, Risk Management, VOSviewer***

1. INTRODUCTION

Cloud computing has emerged as a cornerstone of modern digital transformation, enabling organizations to optimize their operations by leveraging scalable, flexible, and cost-effective IT infrastructures. Its rapid adoption across diverse sectors ranging from healthcare and education to finance and manufacturing has fundamentally altered how organizations store, access, and manage data. These cloud-based platforms provide ubiquitous access to computing resources and services, shifting the paradigm from traditional on-premise systems to distributed, service-oriented architectures. The growing reliance on cloud environments underscores the need to understand not only their operational advantages but also the complex security risks that accompany their implementation. As businesses increasingly integrate cloud technologies into their core operations, ensuring the confidentiality, integrity, and availability of critical data has become a paramount concern.

While the cloud offers numerous benefits, it simultaneously introduces unique cybersecurity challenges that distinguish it from conventional IT environments. Traditional security frameworks often fall short in addressing the fluid and distributed nature of cloud-based systems. In particular, the multi-tenant architecture of public clouds—where multiple customers share the same infrastructure—creates potential vulnerabilities for data breaches, unauthorized access, and crosstenant attacks. These threats are compounded by issues such as lack of visibility into third-party cloud providers, insufficient user access control mechanisms, and insecure application programming interfaces (APIs). Moreover, the ease of provisioning resources in the cloud, while advantageous for agility, often leads to configuration errors and shadow IT practices, further elevating the risk landscape. Studies have noted that misconfigured cloud storage remains a leading cause of data exposure incidents (Yacelga et al., 2023; Rodriguez-Barboza et al., 2024), signaling a persistent gap in cybersecurity practices within cloud-based ecosystems.

The dynamic and rapidly evolving nature of cybersecurity threats in cloud computing environments has necessitated the exploration of advanced technologies and methodologies to enhance protection mechanisms. Increasingly, machine learning (ML) and artificial intelligence (AI) are being employed to develop adaptive security models capable of identifying and mitigating threats in real time. These intelligent systems enable more proactive and predictive security measures, such as anomaly detection, behavioral analysis, and automated response protocols. As highlighted in recent literature, such integration of AI into cloud security frameworks enhances the resilience of systems against zero-day attacks, advanced persistent threats, and insider risks (Alzoubi et al., 2024; Sohal et al., 2018). Furthermore, these technologies offer the ability to scale with the size and complexity of cloud environments, allowing organizations to maintain robust defenses without compromising performance or user experience. The convergence of cloud computing and AI-based cybersecurity not only marks a technological advancement but also represents a strategic imperative for futureproofing digital infrastructures.

Despite these promising developments, the cybersecurity landscape in cloud computing remains fragmented, with inconsistent implementations and a lack of standardized best practices. Organizations often struggle to assess which security frameworks, tools, and techniques are most effective or appropriate for their specific cloud configurations. This complexity is intensified by the diversity of cloud deployment models—public, private, hybrid, and multi-cloud—each of which presents distinct security challenges and policy considerations. As a result, the body of academic and industry research on cloud cybersecurity has grown substantially in recent years, producing a rich yet dispersed field of knowledge. However, the sheer volume of this research, combined with varying methodological approaches and terminological inconsistencies, makes it difficult to extract a coherent understanding of the current state of the field.

This systematic literature review addresses that gap by consolidating and synthesizing existing studies on cybersecurity in cloud computing to provide a comprehensive and structured overview of the field. The central problem that motivates this review is the lack of an integrative perspective on how cybersecurity challenges in cloud environments are being addressed through different strategies, technologies, and frameworks. Existing reviews often focus on narrow aspects—such as intrusion detection systems or data encryption—without situating these discussions within the broader context of evolving threat landscapes and organizational needs. Furthermore, many prior studies are limited by selective literature coverage, absence of reproducible methodologies, or lack of theoretical grounding. Consequently, practitioners and researchers alike face difficulties in navigating the fragmented literature to derive actionable insights or identify future research directions.

Conducting this systematic review is justified on both practical and scholarly grounds. From a practical standpoint, organizations need evidence-based guidance to select and implement effective security measures tailored to their cloud environments. Understanding the effectiveness, applicability, and limitations of various cybersecurity approaches can directly inform decisionmaking processes, policy development, and risk management strategies. From a scholarly perspective, a systematic synthesis of the literature provides a valuable knowledge base that identifies research trends, methodological gaps, and emergent themes. Such a synthesis not only advances theoretical understanding but also supports the development of new frameworks and research agendas aimed at improving cybersecurity outcomes in cloud settings. By adhering to rigorous review protocols and transparent criteria, this review contributes to elevating the methodological quality of the field and enhancing the reliability of its knowledge base.

The specific objectives of this systematic literature review are threefold. First, it seeks to categorize and critically analyze the primary cybersecurity challenges faced in cloud computing environments, considering different deployment and service models. Second, it aims to evaluate the range of solutions proposed in the literature, including both traditional and emerging technologies such as AI and ML, in order to assess their effectiveness and limitations. Third, this review identifies key research gaps and proposes directions for future investigations that can contribute to developing more resilient and adaptive security paradigms. These objectives are framed by the following research questions: (1) What are the major cybersecurity threats and vulnerabilities associated with cloud computing? (2) What technological and organizational measures have been proposed or implemented to mitigate these risks? (3) What are the current limitations in the field, and how can future research address these challenges?

The scope of this review is deliberately focused to ensure depth and analytical clarity. It includes peer-reviewed academic articles, conference proceedings, and high-quality industry reports published between 2018 and 2025, which align with the most recent advancements and discussions in cloud cybersecurity. Literature that addresses generic cybersecurity issues not explicitly related to cloud computing is excluded to maintain thematic coherence. Similarly, studies limited to legal or policy dimensions without technological analysis are not considered in the primary synthesis, though they may be referenced where relevant. The review encompasses multiple cloud service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—to capture the breadth of security concerns across different operational layers. It also considers various deployment models to account for organizational diversity in cloud adoption.

The potential contributions of this systematic review are both theoretical and practical. Theoretically, it enriches the academic discourse by providing a consolidated framework for understanding the intersections between cloud computing and cybersecurity. It highlights methodological trends and conceptual developments, contributing to the formation of a more coherent and cumulative body of knowledge. Practically, the review offers actionable insights for IT professionals, system architects, and decision-makers tasked with securing cloud infrastructures. By comparing the relative strengths and weaknesses of different security solutions, the review aids in identifying best practices and guiding strategic investments in cybersecurity. Additionally, it informs educators and curriculum developers about the essential competencies and knowledge areas needed to train future cybersecurity professionals.

2. RESEARCH METHOD

This study employs a systematic literature review (SLR) design to synthesize the current academic discourse on cybersecurity challenges in cloud computing. By following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, the review process ensures methodological rigor, transparency, and replicability. Bibliometric analysis using VOSviewer further complements the qualitative synthesis by mapping research trends and thematic structures in the field.

2.1. Research Design

The research adopts a systematic literature review methodology structured according to PRISMA guidelines. This structured approach facilitates an exhaustive and unbiased identification, screening, and synthesis of relevant literature. The combined use of qualitative synthesis and bibliometric techniques provides both depth and breadth in understanding the evolution and direction of research on cloud cybersecurity.

2.2. Research Questions

To maintain a focused review, three guiding research questions were formulated:

1. **RQ1**: What are the main cybersecurity challenges in cloud computing environments?
2. **RQ2**: How have these challenges evolved over time?
3. **RQ3**: What solutions and mitigation strategies have been proposed in the literature?

These questions frame the entire review process, from search strategy to data analysis.

2.3. Data Sources and Search Strategy

To capture high-quality and comprehensive academic contributions, the literature search was conducted across five major databases: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar. These databases were selected based on their relevance and coverage of technical and interdisciplinary publications in computer science and cybersecurity.

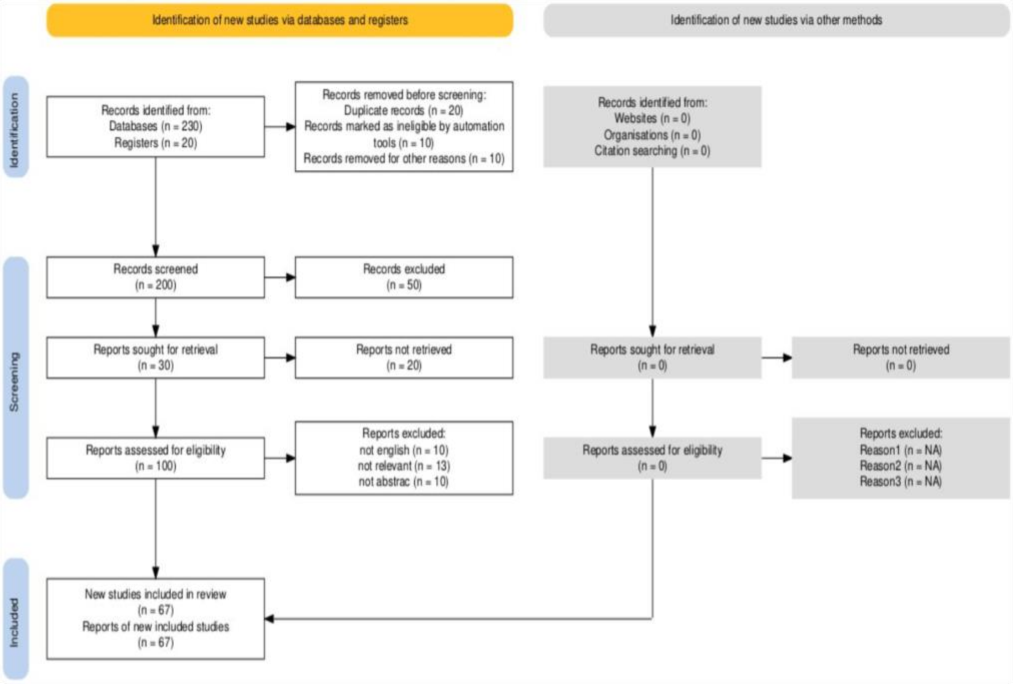
Identification of new studies via databases and registers
Identification of new studies via other methods
Identification
Screening
Included
Records identified from:
Databases (n = 230)
Registers (n = 20)
Records removed before screening:
Duplicate records (n = 20)
Records marked as ineligible by automation tools (n = 10)
Records removed for other reasons (n = 10)
Records identified from:
Websites (n = 0)
Organisations (n = 0)
Citation searching (n = 0)
Records screened
(n = 200)
Records excluded
(n = 50)
Reports sought for retrieval
(n = 30)
Reports not retrieved
(n = 20)
Reports sought for retrieval
(n = 0)
Reports not retrieved
(n = 0)
Reports assessed for eligibility
(n = 100)
Reports excluded:
not english (n = 10)
not relevant (n = 13)
not abstrac (n = 10)
Reports assessed for eligibility
(n = 0)
Reports excluded:
Reason1 (n = NA)
Reason2 (n = NA)
Reason3 (n = NA)
New studies included in review
(n = 67)
Reports of new included studies
(n = 67)

Figure 1. PRISMA Flow Diagram

2.4. Data Extraction and Coding Procedure

A structured data extraction protocol was employed using Microsoft Excel. Each included article was assessed based on the following elements: publication year, author(s), title, methodology, study focus, identified cybersecurity challenges, proposed mitigation strategies, and relevant findings.

A thematic coding approach was then applied. Codes were grouped into major cybersecurity issues including: Data breaches, Cloud misconfigurations, Insecure APIs, Insider threats, and Compliance issues. These themes were iteratively refined to ensure comprehensive coverage and reduce overlap.

2.5. Quality Assessment and Reliability

To ensure methodological rigor, a quality appraisal checklist based on the Mixed Methods Appraisal Tool (MMAT) was adapted. Each study was assessed independently by two reviewers on dimensions such as clarity of research objectives, appropriateness of methodology, data integrity, and relevance to the research questions. Disagreements were resolved through discussion or by involving a third reviewer.

2.8. Bibliometric and Visual Analysis

To augment the thematic synthesis, bibliometric analysis was conducted using **VOSviewer**. This analysis focused on:

1. Keyword co-occurrence: to map thematic foci in cybersecurity literature.
2. Author collaboration networks: to identify influential researchers and institutions.
3. Temporal overlay visualization: to trace the evolution of research themes from 2013 to 2024.

3. RESULTS AND DISCUSSION

This section presents the findings of the systematic literature review, structured thematically and supported by bibliometric analysis using VOSviewer. The goal is to identify key cybersecurity challenges, thematic trends, and proposed solutions as observed across the selected body of literature.

3.1 Bibliometric Analysis Results

The bibliometric visualization using VOSviewer offers a comprehensive view of keyword co-occurrence patterns within the selected articles. Three types of network visualizations were generated: cluster network, temporal overlay, and density map, which reveal the intellectual structure, research trends over time, and thematic concentrations in the literature. The **first visualization** (Figure 2) presents a **keyword co-occurrence network**, where nodes represent keywords and edges indicate the frequency of their co-occurrence. Keywords like *detection*, *risk*, *iot*, *platform*, *vulnerability*, and *strategy* dominate the network, indicating their centrality in the discourse. The clusters identified include:

1. **Red Cluster**: Focuses on *vulnerability*, *risk*, *strategy*, *platform*, and *landscape*, highlighting research concerned with identifying threat landscapes and developing mitigation frameworks.
2. **Blue Cluster**: Centers around *intrusion detection system*, *traffic*, and *algorithm*, representing works on technical detection mechanisms and efficiency.
3. **Green Cluster**: Emphasizes *iot*, *trend*, *industry*, and *blockchain*, which points to emerging technologies integrated into cloud security.
4. **Purple Cluster**: Includes *cloud computing security*, *machine learning*, and *sensor*, reflecting studies that incorporate AI and data-driven methods.
5. **Yellow Cluster**: Connected to *enterprise*, *innovation*, and *interoperability*, denoting works that explore cloud integration in organizational systems and its security implications.

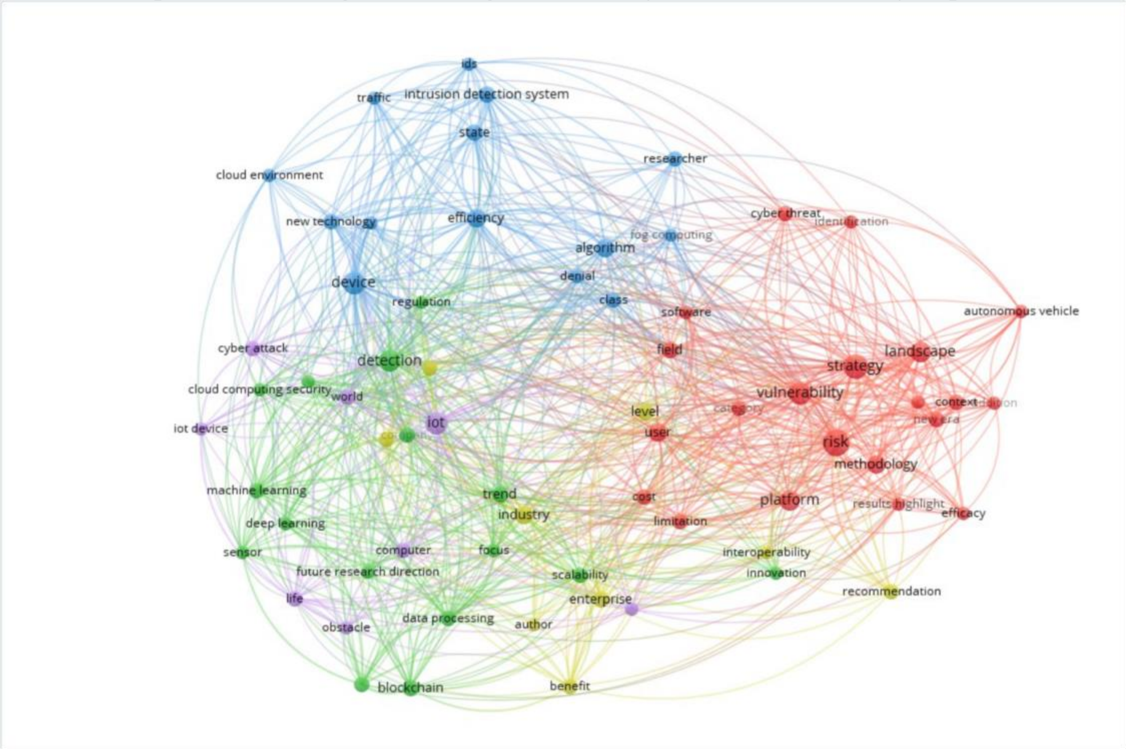

Figure 2. VOSviewer Keyword Co-occurrence Network

(Source: Authors' own visualization based on the selected 48 articles.)

The second visualization (Figure 3) shows a temporal overlay map, which reflects how topics have evolved between 2021 and 2024. Earlier studies (dark blue) focused on foundational themes such as *intrusion detection*, *device*, and *cloud environment*. Over time, there has been a shift toward more complex and strategic themes (yellow), including *vulnerability*, *risk*, *platform*, *strategy*, and *autonomous vehicles*. This shift suggests a growing interest in the strategic management of cloud cybersecurity rather than purely technical interventions.

The overlay visualization map generated using VOSviewer illustrates the thematic structure and keyword co-occurrence in the literature related to [your research topic, e.g., "IoT security" or "digital marketing strategies"]. The network is divided into several color-coded clusters, each representing a distinct thematic area. For instance, the red cluster is centered around keywords such as "strategy," "vulnerability," "risk," and "platform," indicating a strong focus on risk management and strategic planning. The blue cluster highlights terms like "intrusion detection system (IDS)," "algorithm," and "device," reflecting a technical emphasis on detection mechanisms and computational approaches. The green cluster, which includes "blockchain," "enterprise," and "trend," suggests an intersection between emerging technologies and industrial application. Meanwhile, the purple and yellow clusters encompass topics like "IoT," "machine learning," and "cloud computing security," emphasizing technological integration and future research directions. The dense interconnections among nodes signify a high level of interdisciplinarity and interrelation among concepts, illustrating the complex and interconnected nature of current research in the field. This visualization aids in identifying dominant research themes, emerging trends, and potential gaps in the literature.

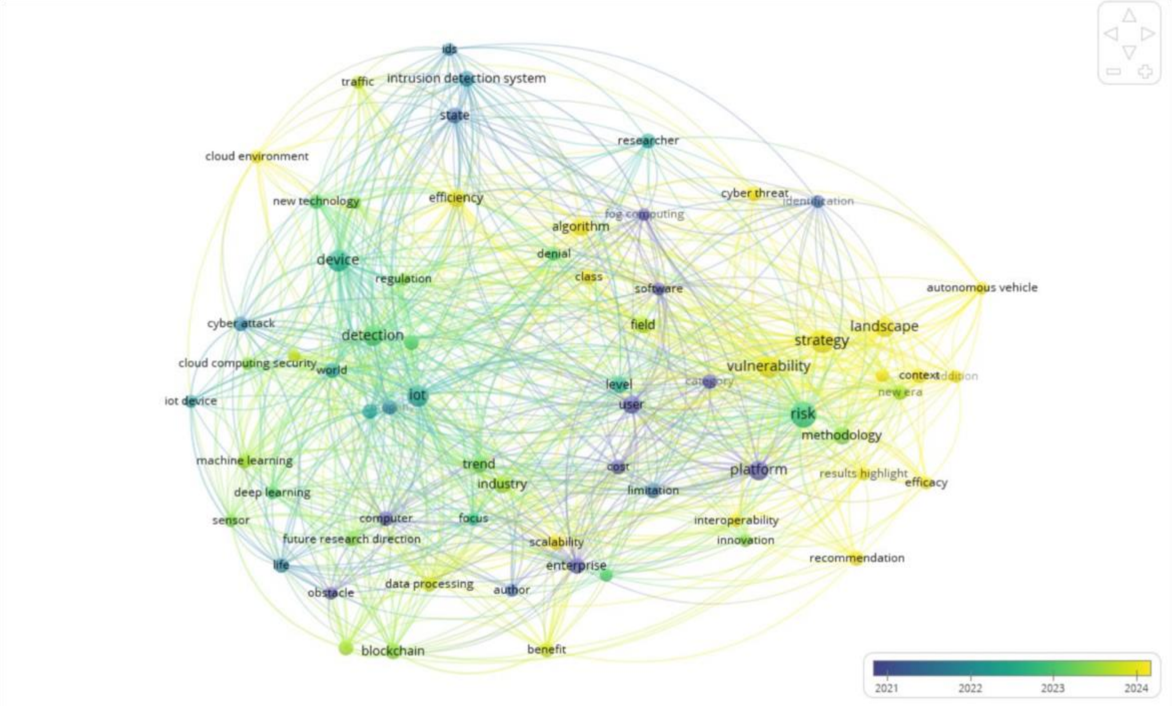

Figure 3. VOSviewer Temporal Overlay Visualization

The third visualization (Figure 4) is a density map that highlights the most intensively studied keywords. Brighter yellow zones (e.g., *iot*, *detection*, *vulnerability*, *risk*) represent frequent and highly interconnected terms, suggesting concentrated research activity in these domains.

The overlay visualization map generated using VOSviewer illustrates the temporal evolution of key themes within the analyzed literature, with color gradients representing the average publication year of keywords (from dark blue for earlier years to yellow for more recent ones). The visualization reveals that earlier studies (2021–2022) predominantly focused on technical aspects such as "intrusion detection system," "deep learning," "machine learning," and "cloud computing security," as indicated by their darker hues. In contrast, more recent research trends (2023–2024), shown in yellow, emphasize broader strategic and emerging themes like "strategy," "vulnerability," "autonomous vehicle," "landscape," and "recommendation." The presence of terms such as "blockchain," "enterprise," and "platform" in green shades reflects a transition phase where research began integrating technological innovation with practical implementation and risk considerations. This temporal shift demonstrates how the field is progressing from foundational technical development toward applied research, strategic frameworks, and real-world deployment, thereby offering insights into evolving priorities and future research directions.

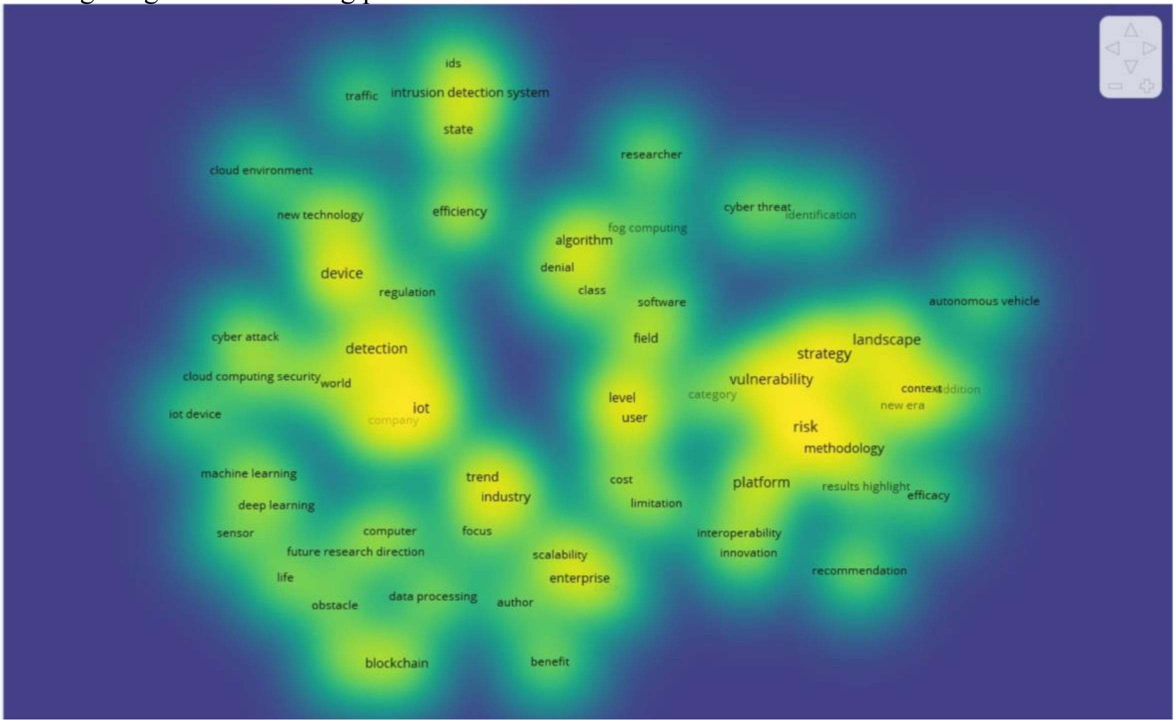

Figure 4. VOSviewer Keyword Density Visualization

Collectively, these visualizations confirm the interdisciplinary nature of cloud cybersecurity research and reflect its evolution toward integrating advanced technologies like AI, IoT, and blockchain within security frameworks.

The density visualization map produced using VOSviewer provides a graphical representation of the frequency and prominence of keywords across the analyzed literature.

In this map, colors range from dark blue (indicating lower frequency) to bright yellow (indicating higher frequency and centrality), allowing for quick identification of dominant research themes. The most intense yellow regions—surrounding keywords such as "IoT," "detection," "device," "strategy," "vulnerability," and "risk"—highlight the areas that have received the most scholarly attention. These high-density clusters suggest a strong research focus on technological implementation, security measures, and strategic approaches within the studied domain. Meanwhile, less intense regions such as "blockchain," "autonomous vehicle," and "recommendation" point to emerging or niche topics that may represent opportunities for future research. Overall, this visualization complements the network and overlay maps by emphasizing the concentration of research efforts and identifying both well-established and underexplored areas in the literature.

3.2 Thematic Synthesis of Literature

Based on qualitative synthesis, five core themes emerged from the reviewed literature:

3.2.1 Evolving Cybersecurity Threats in Cloud Environments

A dominant theme across the literature is the evolving nature of cybersecurity threats in cloud computing. Unlike traditional IT infrastructures, cloud platforms introduce novel risks due to their distributed and shared-resource characteristics. Studies such as Saxena et al. (2025) and Yacelga et al. (2023) emphasize that threats like misconfigurations, data breaches, insider threats, and insecure APIs are heightened in cloud contexts. Additionally, the dynamic provisioning of resources in cloud environments leads to reduced visibility and increased attack surfaces.

3.2.2 Strategic Importance of Risk Assessment and Vulnerability Management

Another key focus area is risk and vulnerability management. Literature highlights the need for tailored risk assessment models that consider the heterogeneity of cloud environments. Works by Zheng et al. (2022) and Mercy et al. (2025) suggest that existing risk models often fail to capture the layered complexities of public, private, and hybrid clouds. Effective vulnerability identification tools, supported by automated assessment systems, are increasingly recommended to manage real-time threats.

3.2.3 Emergence of AI and Machine Learning for Threat Detection

AI and machine learning have become crucial in the evolution of cloud security. Sohal et al. (2018) and Alzoubi et al. (2024) demonstrate that ML-based intrusion detection systems can detect anomalies in massive datasets faster and more accurately than rule-based systems. The integration of these technologies not only improves threat detection but also enables predictive analytics, which allows organizations to act before threats materialize.

3.2.4 Security Challenges in IoT and Edge-Cloud Ecosystems

The expansion of IoT devices and their integration with cloud platforms have introduced new challenges. Devices often lack robust security controls, creating potential entry points for cyber-attacks. Studies such as those by Morolong et al. (2023) and Garg et al. (2022) emphasize the need for lightweight encryption protocols and distributed trust mechanisms suitable for constrained devices. The co-occurrence of *iot*, *device*, and *detection* in the bibliometric map supports the thematic prominence of this issue.

3.2.5 Organizational Readiness and Strategic Policy Frameworks

Beyond technical solutions, the literature underscores the role of organizational culture, governance, and policy in effective cloud security. Alatawi (2023) and Albshaier et al. (2024) advocate for integrated strategies that combine technological, human, and procedural controls. The keyword cluster related to *enterprise*, *interoperability*, and *innovation* reflects the growing body of research advocating a holistic security governance model that aligns with business objectives.

3.3 Implications and Research Gaps

The findings suggest that while significant advancements have been made, gaps remain. There is insufficient standardization of security protocols across different cloud providers. Moreover, many studies still focus on isolated technical fixes without integrating broader organizational or policy perspectives.

Future research should explore: cross-domain frameworks that integrate cloud, AI, and regulatory compliance, cloud security in low-resource contexts or developing economies, and longitudinal studies to assess the impact of emerging technologies on cloud security over time.

4. CONCLUSION

Standardized protocols and uneven implementation across cloud models. Through thematic and This systematic literature review presents a comprehensive synthesis of cybersecurity challenges in cloud computing environments, highlighting both persistent vulnerabilities and evolving defense mechanisms. The findings reveal that while technological solutions—such as AI-powered threat detection and machine learning algorithms—offer promising advancements, the security landscape remains fragmented due to a lack of bibliometric analyses, five key research domains were identified: threat evolution, risk assessment, AI integration, IoT security, and strategic policy development. The results underscore the need for more cohesive frameworks that integrate technical, organizational, and regulatory components to achieve resilient cloud security. Furthermore, emerging areas such as edge-cloud ecosystems and AI governance warrant deeper exploration. Future research should focus on cross-domain, adaptable models that accommodate diverse organizational needs and evolving technological landscapes. Practitioners and policymakers can leverage these insights to shape more robust cloud security strategies aligned with both operational goals and compliance requirements.

REFERENCE

Gunawan, G., Utomo, A. S. A., & Benediktus, H. S. (2021). Optimization of shipyard layout with material handling cost as the main parameter using genetic algorithm. *AIP Conference Proceedings*, *2376*(1).

Ingriana, A. (2025). *THE INFLUENCE OF E-TRUST ON CONSUMER PURCHASING BEHAVIOR IN E-COMMERCE*. *1*(3). https://journal.dinamikapublika.id/index.php/Jumder

Ingriana, A., Chondro, J., & Rolando, B. (2024). *TRANSFORMASI DIGITAL MODEL BISNIS KREATIF: PERAN SENTRAL E-COMMERCE DAN INOVASI TEKNOLOGI DI INDONESIA* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/JUMDER

Ingriana, A., Gianina Prajitno, G., & Rolando, B. (2024). *THE UTILIZATION OF AI AND BIG DATA TECHNOLOGY FOR OPTIMIZING DIGITAL MARKETING STRATEGIES* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/IJEBS

Ingriana, A., Hartanti, R., Mulyono, H., & Rolando, B. (2024). Pemberdayaan E-Commerce: Mengidentifikasi Faktor Kunci Dalam Motivasi Pembelian Online. *Jurnal Manajemen Dan Kewirausahaan (JUMAWA)*, *1*(3), 101–110.

Maha, V. A., Derian Hartono, S., Prajitno, G. G., & Hartanti, R. (2024). *E-COMMERCE LOKAL VS GLOBAL: ANALISIS MODEL BISNIS DAN PREFERENSI KONSUMEN* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/Jumder

Mulyono, H., Hartanti, R., & Rolando, B. (2024). *SUARA KONSUMEN DI ERA DIGITAL: BAGAIMANA REVIEW ONLINE MEMBENTUK PERILAKU KONSUMEN DIGITAL* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/JUMDER

Mulyono, H., Ingriana, A., & Hartanti, R. (2024). *PERSUASIVE COMMUNICATION IN CONTEMPORARY MARKETING: EFFECTIVE APPROACHES AND BUSINESS RESULTS* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/IJEBS

Mulyono, H., & Rolando, B. (2024). Savoring The Success: Cultivating Innovation And Creativity For Indonesian Culinary MSMEs Growth. *Economics and Business Journal (ECBIS)*, *2*(4), 413–428.

Putri, L. W. B., & Setiawan, B. L. T. (2025). *ANALYZING THE STRATEGIC CONTRIBUTION OF SOCIAL MEDIA INFLUENCERS TO E-COMMERCE MARKETING EFFECTIVENESS*. *1*(2). https://journal.dinamikapublika.id/index.php/Jumder

Rahardja, B. V., Rolando, B., Chondro, J., & Laurensia, M. (2024). *MENDORONG PERTUMBUHAN E-COMMERCE: PENGARUH PEMASARAN MEDIA SOSIAL TERHADAP KINERJA PENJUALAN* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/JUMDER

Rolando, B. (2018). *Tingkat Kesiapan Implementasi Smart Governance di Kota Palangka Raya*. UAJY.

Rolando, B. (2024). *CULTURAL ADAPTATION AND AUTOMATED SYSTEMS IN E-COMMERCE COPYWRITING: OPTIMIZING CONVERSION RATES IN THE INDONESIAN MARKET* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/IJEBS

Rolando, B., Chandra, C. K., & Widjaja, A. F. (2025). *TECHNOLOGICAL ADVANCEMENTS AS KEY DRIVERS IN THE TRANSFORMATION OF MODERN E-COMMERCE ECOSYSTEMS*. *1*(2). https://journal.dinamikapublika.id/index.php/Jumder

Rolando, B., & Ingriana, A. (2024). *SUSTAINABLE BUSINESS MODELS IN THE GREEN ENERGY SECTOR: CREATING GREEN JOBS THROUGH RENEWABLE ENERGY TECHNOLOGY INNOVATION* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/IJEBS

Rolando, B., Nur Azizah, F., Karaniya Wigayha, C., Bangsa, D., Jl Jendral Sudirman, J., Jambi Selatan, K., & Jambi, K. (2024). *Pengaruh Viral Marketing Shopee Affiliate, Kualitas Produk, dan Harga Terhadap Minat Beli Konsumen Shopee*. https://doi.org/10.47065/arbitrase.v5i2.2167

Rolando, B., & Wigayha, C. K. (2024). Pengaruh E-Wom Terhadap Keputusan Pembelian Online: Studi Kasus Pada Pelanggan Aplikasi Kopi Kenangan. *Jurnal Manajemen Dan Kewirausahaan (JUMAWA)*, *1*(4), 193–210.

Tan, D. M., & Alexia, K. R. (2025). *THE INFLUENCE OF TIKTOK AFFILIATE CONTENT QUALITY AND CREDIBILITY ON PURCHASE DECISIONS VIA THE YELLOW BASKET FEATURE*. *1*(2). https://journal.dinamikapublika.id/index.php/Jumder

Widjaja, A. F. (2025). *FACTORS INFLUENCING PURCHASE INTENTION IN E-COMMERCE: AN ANALYSIS OF BRAND IMAGE, PRODUCT QUALITY, AND PRICE*. *1*(3). https://journal.dinamikapublika.id/index.php/Jumder

Wigayha, C. K., Rolando, B., & Wijaya, A. J. (2024). *PELUANG BISNIS DALAM INDUSTRI HIJAU DAN ENERGI TERBARUKAN* (Vol. 1, Issue 1). https://journal.dinamikapublika.id/index.php/Jumder

Wigayha, C. K., Rolando, B., & Wijaya, A. J. (2025). *A DEMOGRAPHIC ANALYSIS OF CONSUMER BEHAVIORAL PATTERNS ON DIGITAL E-COMMERCE PLATFORMS. 1*(2). https://journal.dinamikapublika.id/index.php/Jumder

Winata, V., & Arma, O. (2025). *ANALYZING THE EFFECT OF E-WALLET USABILITY ON CUSTOMER RETENTION IN MOBILE PAYMENT APPS. 1*(2). https://journal.dinamikapublika.id/index.php/Jumder

Zahran, A. M. (2025). *THE IMPACT OF MARKETING STRATEGIES ON THE SUCCESS OF THE FAST FASHION INDUSTRY: A SYSTEMATIC REVIEW. 1*(3). https://journal.dinamikapublika.id/index.php/Jumder