Asia Pacific Academy of Science Pte. Ltd.

*Metaverse* 2026, 7(3), m260017.
https://doi.org/10.54517/m260017

Article

# Mapping the Evolution of Cybersecurity and Machine Learning Research: Implications for Securing Metaverse Environments

**Nanik Ramini[1], Agus Rahayu[1], Disman Disman[1,*], Dyah Purwaningrum[1], Juliana Juliana[1,*], Asep Miftahuddin[1], Reynaldi Dimas Fhadjrin[2], Mohammed Azim[3]**

[1] Universitas Pendidikan Indonesia, Bandung, Indonesia
[2] Institut Teknologi Bandung, Bandung, Indonesia
[3] James Cook University, Queeslands, Australia
*** Corresponding author:** Disman Disman, disman@upi.edu and Juliana Juliana, julian@upi.edu

**CITATION**

Ramini N, Rahayu A, Disman D, et al. Mapping the Evolution of Cybersecurity and Machine Learning Research: Implications for Securing Metaverse Environments. Metaverse. 2026; 7(3): m260017. https://doi.org/10.54517/m260017

**ARTICLE INFO**

Received: 12 June 2026
Accepted: 12 August 2026
Available online: 18 September 2026



**Abstract:** The rapid expansion of immersive and interconnected digital technologies has intensified cybersecurity challenges and increased the demand for adaptive, intelligence-driven protection. This study systematically maps the intellectual structure, thematic evolution, and research maturity of cybersecurity, machine learning, and metaverse-related research. A total of 359 English-language journal articles indexed in Scopus and published between 2020 and 2026 were selected using the PRISMA-BiB protocol and analyzed using Biblioshiny through annual scientific production, three-field plot, word frequency over time, trend topic, co-occurrence network, and thematic map analyses. Publication output grew rapidly after 2023 and peaked in 2025. The co-occurrence network identified four interconnected clusters: core cybersecurity and intelligent threat detection; artificial intelligence, blockchain, privacy, and secure metaverse technologies; digital twin and cyber-physical infrastructure security; and smart energy and critical infrastructure security. The thematic map positions cybersecurity, network security, and virtual reality as Motor Themes, whereas artificial intelligence, machine learning, digital twins, anomaly detection, blockchain, and the Internet of Things occupy transitional or emerging positions. Synthesizing these findings, this study proposes a relational conceptual framework positioning metaverse cybersecurity as a layered dependency structure rather than a set of parallel research areas. Four testable propositions specify how infrastructure resilience conditions intelligent detection, detection capability extends through cyber-physical integration, integration supplies the data foundation for decentralized trust, and trust governance mediates the translation of technical capability into ecosystem trustworthiness. This developmental asymmetry indicates that the principal bottleneck in securing metaverse ecosystems lies not in detection capability but in the integration and governance layers.

**Keywords:** Cybersecurity; Machine learning; Artificial intelligence; Bibliometric analysis; Science mapping; Metaverse; Virtual reality; Digital twin; Blockchain security; Biblioshiny

## 1. Introduction

The rapid digitalization of economic, financial, governmental, industrial, social, and immersive systems has fundamentally reshaped the global cybersecurity landscape. Cloud computing, e-commerce, mobile financial services, artificial intelligence, the Internet of Things, blockchain, digital twins, and metaverse-based environments have created new opportunities for innovation while simultaneously expanding the attack surface available to cybercriminals [1,2]. Metaverse ecosystems are characterized by persistent virtual environments, immersive interactions, identity continuity, interoperability, and decentralized transactions [3,4]. These characteristics

introduce security risks involving avatars, digital identities, virtual assets, smart contracts, biometric data, spatial interactions, and cross-platform communication that extend beyond conventional online systems [5–7].

Machine learning and artificial intelligence have become central technological capabilities in contemporary cybersecurity. Rule-based and signature-based mechanisms remain useful for detecting known threats; however, their effectiveness is increasingly limited when confronting adaptive, large-scale, and previously unseen attacks. Machine learning, deep learning, predictive analytics, anomaly detection, and automated decision-making enable security systems to identify complex patterns, classify malicious activities, detect fraudulent behavior, and support real-time responses [8–13]. These capabilities are especially relevant to metaverse environments, where multimodal behavioral data, immersive interactions, virtual transactions, digital twins, and interconnected devices require adaptive and privacy-aware security mechanisms [5–7].

Research at the intersection of cybersecurity and machine learning has expanded rapidly, particularly after 2020, alongside the acceleration of cloud adoption, digital transactions, remote interaction, and AI-enabled services. Existing studies have examined intrusion detection, phishing, malware classification, cyber fraud, anti-money laundering, forensic accounting, blockchain security, identity protection, and network monitoring [14–18]. The scope of research has also broadened to digital trust, platform governance, privacy, organizational resilience, ethical accountability, and human-centered security. This transition is highly relevant to metaverse research because secure immersive environments depend not only on technical detection capabilities but also on identity governance, decentralized trust, infrastructure resilience, regulatory oversight, and user protection [4–7].

Bibliometric analysis provides a systematic and reproducible method for examining the intellectual development of rapidly evolving research domains. Performance analysis and science-mapping techniques allow researchers to evaluate publication growth, relationships among cited references, authors, and keywords, thematic evolution, conceptual structures, and research maturity [19–25]. Previous bibliometric studies have investigated specific areas such as cybersecurity governance, cybercrime prevention, intrusion detection, blockchain security, AI-enabled threat detection, cloud-AI-data center human capital ecosystems, and emerging service sectors including halal tourism development [18,26–28]. However, limited attention has been devoted to systematically mapping how these areas converge with virtual reality, extended reality, augmented reality, avatars, digital identities, immersive environments, virtual worlds, digital twins, and blockchain-enabled metaverse infrastructures.

The fragmentation of existing literature creates an important conceptual and methodological gap. Cybersecurity, machine learning, financial crime, blockchain, cyber-physical systems, and immersive technologies are frequently examined as separate knowledge domains, restricting the understanding of how their intellectual and thematic structures collectively shape metaverse security[18,26,29]. A broader bibliometric synthesis is required to explain the emergence of AI-driven cybersecurity, the growing relevance of blockchain and federated learning, the role of digital twins and network security, and the relationship between intelligent threat detection and immersive-platform protection. Such integration is essential because metaverse ecosystems simultaneously depend on artificial intelligence, decentralized infrastructures, virtual identities, connected devices, behavioral data, and human interaction [5–7].

This study systematically maps and analyzes the intellectual structure, thematic evolution, and developmental maturity of research at the intersection of cybersecurity, machine learning, and metaverse-related technologies. A PRISMA-BiB machine learning, and metaverse related technologies. A PRISMA-BiB compliant selection process produced a final dataset of 359 Scopus-indexed articles, which were analyzed exclusively using Biblioshiny. The analytical procedures comprise annual scientific production, Three-Field Plot Analysis, Words Frequency Over Time Analysis, Trend Topics Analysis, Co-occurrence Network Synthesis, and Thematic Map Analysis. The study positions metaverse security as a central analytical domain and examines how AI-enabled detection, blockchain security, digital identity protection, virtual reality, digital twins, cyber-physical resilience, privacy, and governance con-tribute to the development of trustworthy metaverse ecosystems.

## 2. Literature Review

The rapid advancement of digital technologies has positioned cybersecurity as a strategic multidisciplinary field of contemporary research. The growing dependence of organizations, governments, individuals, and virtual communities on cloud computing, the Internet of Things, blockchain, digital twins, and immersive platforms has expanded the cyber-attack surface and increased the complexity of digital threats. Cybersecurity risks now extend beyond the confidentiality, integrity, and availability of information to include organizational resilience, platform accountability, transaction security, digital identity protection, privacy, regulatory governance, human behavior, and trust within immersive digital environments [1,2].

Machine learning and artificial intelligence have emerged as transformative technologies for strengthening cybersecurity through predictive analytics, intelligent automation, and adaptive threat detection [8–13]. Applications such as deep learning, fraud detection, intrusion detection, anomaly detection, forensic accounting, anti-money laundering analytics, and phishing detection enable security systems to identify hidden patterns, process large-scale data streams, detect suspicious activities, and respond to evolving threats more effectively. Their relevance is particularly significant in metaverse environments, where virtual reality, extended reality, augmented reality, avatars, biometric interfaces, digital identities, virtual transactions, digital twins, and decentralized assets generate persistent and highly sensitive data that may be exposed to impersonation, privacy breaches, immersive phishing, smart contract exploitation, and virtual asset fraud [5–7].

The convergence of cybersecurity, machine learning, and metaverse-enabling technologies has generated a rapidly expanding yet fragmented body of knowledge. Existing studies predominantly examine technical threat detection, financial fraud, digital identity, blockchain security, biometric privacy, and immersive interaction risks as separate research domains, providing a limited understanding of how these themes are intellectually connected and have evolved within the broader metaverse cybersecurity ecosystem [30]. This section reviews the development of cybersecurity and machine learning research, examines metaverse-specific security and privacy challenges, compares previous bibliometric studies, and identifies the theoretical, methodological, and thematic gaps that motivate a more comprehensive science-mapping analysis.

### 2.1. Cybersecurity, Machine Learning, and Metaverse Security

Cybersecurity encompasses the protection of digital systems, networks, applications, data, and information assets from unauthorized access, malicious

activities, and cyberattacks. Conventional cybersecurity mechanisms have largely relied on rule-based controls and signature-based detection, which remain effective for known threats but are less capable of responding to rapidly evolving and previously unseen attack patterns. This limitation becomes particularly significant in metaverse environments, where virtual identities, avatars, digital assets, blockchain transactions, smart contracts, extended reality devices, and immersive interactions create interconnected attack surfaces that combine technical, behavioral, financial, and privacy-related vulnerabilities [5–7].

Machine learning provides an adaptive and data-driven approach to these challenges by learning from historical observations, identifying hidden patterns, and detecting anomalous or suspicious activities without depending exclusively on predefined rules. In financial and transactional contexts, machine learning supports fraud detection, anti-money laundering, and the identification of abnormal transaction patterns [14–17]. In network and platform security, supervised, unsupervised, and deep-learning techniques assist in detecting intrusions, malware, phishing, identity misuse, and abnormal user behavior. These approaches extend to e-commerce and online retail environments and multimodal detection of toxic and fraudulent speech in scam confrontation scenarios [31,32]. Deep learning further extends these capabilities by processing complex and high-dimensional data, including text, speech, images, biometric signals, spatial interactions, and behavioral information, which are increasingly relevant to immersive digital ecosystems [8–13].

Metaverse security requires the integration of machine learning with broader governance, privacy, identity-management, and platform-accountability mechanisms. Users may interact through avatars, exchange virtual assets, conduct immersive commerce, access blockchain-based services, and generate persistent behavioral and biometric data, thereby increasing exposure to identity theft, avatar impersonation, immersive phishing, social engineering, virtual asset fraud, smart-contract exploitation, and privacy leakage from extended-reality devices [3–7]. Digital literacy also constitutes a complementary human capital capability because it strengthens users ability to evaluate digital information, use technology responsibly, and adapt to increasingly complex technology-driven environments [33]. These conditions indicate that machine learning-based cybersecurity should not be treated merely as an extension of conventional digital security, but as a foundational capability for building trustworthy, resilient, and accountable metaverse ecosystems [34].

## 2.2. Bibliometric Studies in Cybersecurity and Metaverse

The rapid expansion of research on cybersecurity, digital security, machine learning, and metaverse technologies has generated an increasingly interdisciplinary body of literature in computer science, information systems, finance, governance, public policy, and social sciences. Bibliometric analysis provides a systematic and reproducible approach to examine publication growth, citation structures, collaboration patterns, keyword relationships, intellectual structures, and thematic evolution [19–25]. Its application is particularly relevant to rapidly developing fields in which concepts such as cybercrime, cyber fraud, artificial intelligence, deep learning, fraud detection, intrusion detection, anomaly detection, forensic accounting, anti-money laundering, financial fraud, and phishing evolve across multiple disciplines and application contexts. Unlike conventional narrative reviews, bibliometric and science-mapping methods enable researchers to identify influential contributors, emerging research clusters, and changes in a field's conceptual structure over time [35,36]. Longitudinal bibliometric mapping across extended observation

periods has proven particularly effective in revealing how research priorities within a domain shift in response to technological and institutional change [36].

Bibliometric methods have increasingly been applied to specific cybersecurity domains, including cybercrime prevention, intrusion and anomaly detection, AI-based threat detection, blockchain security, privacy protection, financial fraud analytics, and cybersecurity governance [18,26,37]. Metaverse-related research has simultaneously expanded across virtual reality, augmented reality, extended reality, avatars, digital identities, immersive environments, virtual worlds, digital twins, and blockchain-enabled infrastructures [3–7]. These technologies create a substantial overlap between cybersecurity and machine learning because immersive and decentralized ecosystems require adaptive mechanisms for identity verification, behavioral monitoring, fraud detection, phishing prevention, virtual asset protection, and secure digital transactions. Bibliometric mapping can reveal how established cybersecurity knowledge and intelligent analytical methods are being extended to address the distinctive risks of metaverse environments.

Existing bibliometric studies nevertheless tend to examine cybersecurity, machine learning, financial crime, blockchain, or immersive technologies as separate research domains. Many studies emphasize publication productivity and citation performance while providing limited analysis of thematic evolution, research maturity, and the relationships among AI-driven detection, forensic accountability, anti-money laundering, digital identity, blockchain security, human behavior, and immersive interaction risks [38–41]. Therefore, a more comprehensive science-mapping approach is required to position metaverse security as a central analytical domain and explain how technological, financial, behavioral, governance, and virtual-environment dimensions collectively shape the development of contemporary cybersecurity research.

### 2.3. Research Gap and Conceptual Positioning

Research on cybersecurity and machine learning has expanded substantially over the past decade; however, important conceptual and methodological gaps remain. Previous studies have predominantly examined specific applications, including intrusion detection, malware classification, phishing detection, anomaly detection, financial fraud analytics, anti-money laundering, forensic accounting, and blockchain security [30,42–45]. These contributions offer valuable insights into individual security challenges but provide a limited understanding of the broader intellectual structure connecting cybersecurity, intelligent threat detection, digital identity, immersive technologies, governance, behavioral security, financial protection, and metaverse-specific risk. This fragmentation is particularly significant because metaverse ecosystems integrate virtual reality, augmented reality, extended reality, avatars, digital twins, virtual assets, blockchain infrastructures, and persistent user interactions within interconnected digital environments [46–48].

Existing reviews and bibliometric studies have generally treated cybersecurity, machine learning, financial crime, blockchain and immersive technologies as separate knowledge domains. Limited attention has been devoted to systematically mapping their intersection while simultaneously incorporating AI-driven threat detection, cyber fraud, identity protection, immersive phishing, decentralized transaction security, virtual-world governance, human-centered safeguards, and forensic accountability [18,26]. This separation restricts previous research from explaining how established cybersecurity capabilities are being adapted to the distinctive technical, be-havioral, financial, ethical, privacy, and governance challenges associated with metaverse

environments. Therefore, a comprehensive analytical perspective is required to position metaverse security as a central research domain rather than a secondary interpretative extension of general cybersecurity scholarship.

This study employs a Biblioshiny-based bibliometric and science-mapping approach to analyze an expanded dataset of 359 Scopus-indexed articles retrieved through an integrated search strategy encompassing cybersecurity, machine learning, artificial intelligence, and metaverse-enabling technologies. This approach follows established practice in which cluster-based bibliometric mapping is used to derive integrated development strategies within fragmented research domains [49]. Metaverse cybersecurity is conceptually positioned as a multidisciplinary knowledge ecosystem in which machine learning and artificial intelligence provide adaptive detection, prediction, and analytical capabilities, while digital identity governance, blockchain security, fraud prevention, forensic accountability, digital commerce protection, privacy safeguards, human behavior, and immersive-platform governance constitute interdependent security dimensions. This conceptual positioning provides a foundation for examining the intellectual structure, thematic evolution, research maturity, and emerging directions of metaverse cybersecurity research.

## 3. Methods

This study employs a quantitative bibliometric research design to examine the intellectual structure, thematic evolution, and research maturity of the intersection between cybersecurity, machine learning, and metaverse-related scholarship. Bibliometric analysis was selected because it enables a systematic and reproducible assessment of scientific production, conceptual relationships, thematic patterns, and emerging research directions within a rapidly expanding interdisciplinary domain [19–25]. The analysis was conducted using Biblioshiny on an expanded dataset of 359 Scopus-indexed articles retrieved through an integrated search strategy covering cybersecurity, machine learning, artificial intelligence, and metaverse-enabling technologies. Performance analysis and science mapping techniques were applied to evaluate annual scientific production, source–author–keyword relationships, keyword development over time, trend topics, co-occurrence structures, and thematic maturity. Metaverse security is positioned as a central analytical domain rather than merely an interpretative lens, thereby strengthening the alignment between the dataset, analytical procedures, and the study's theoretical contribution.

### 3.1. Research Design

This study adopted a bibliometric design that integrates performance analysis and science mapping to examine the development of cybersecurity, machine learning, and metaverse research. Performance analysis was applied to assess publication growth, scientific productivity, and keyword frequency, and science-mapping techniques were used to investigate conceptual relationships, thematic structures, and the developmental maturity of the field. All analyses and visualizations were conducted using Biblioshiny, a web-based interface of the Bibliometrix package in R that supports reproducible bibliometric data processing, statistical analysis, and graphical mapping [22–25]. The analytical procedures included annual scientific production, three-field plot analysis, word-frequency development over time, trend topics, keyword co-occurrence networks, and thematic mapping, thereby ensuring methodological consistency across the study.

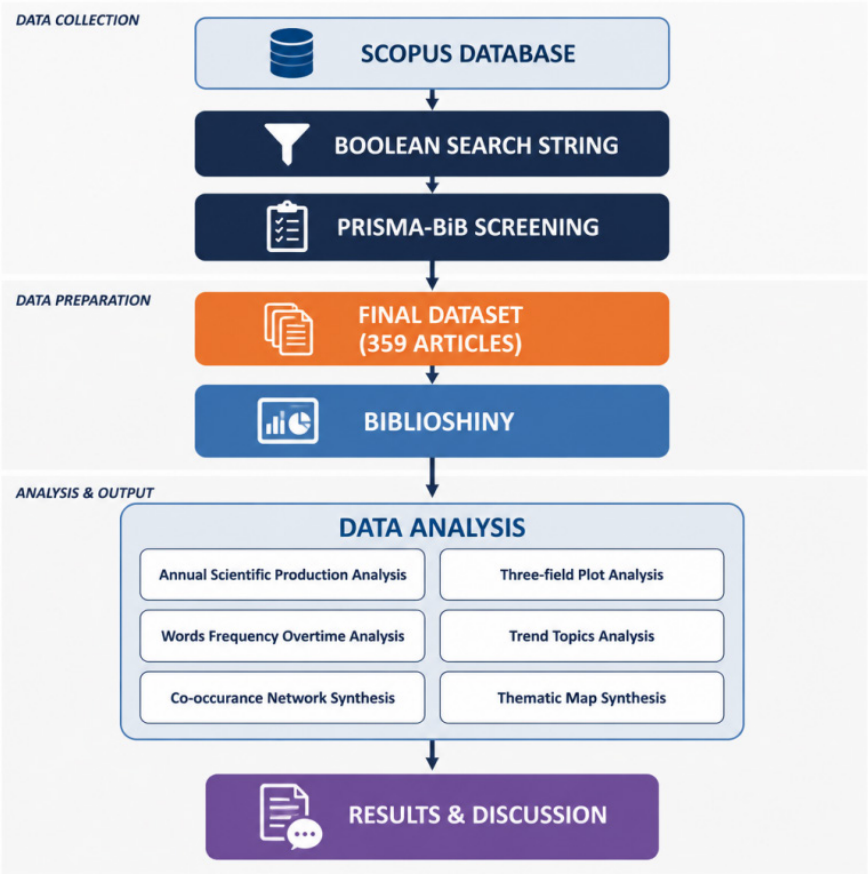


**Figure 1.** Research Framework of the Bibliometric Analysis

**Figure 1** presents the research framework adopted in this study, beginning with data retrieval from the Scopus database through a structured Boolean search strategy, followed by eligibility screening using the PRISMA-BiB protocol. The screening process yielded a final dataset of 359 articles, which were analyzed entirely in Biblioshiny to ensure methodological consistency across performance analysis and science mapping. The analytical procedures comprised annual scientific production, three-field plot analysis, word-frequency development over time, trend topics, keyword co-occurrence networks, and thematic mapping. This framework places metaverse security within the core analytical scope of the study by examining how cybersecurity, machine learning, artificial intelligence, digital identity, blockchain security, immersive environments, and related technologies are interconnected within the evolving research domain.

### 3.2. Data Collection and Selection Procedure

The bibliometric dataset was retrieved from the Scopus database because of its broad multidisciplinary coverage, standardized indexing procedures, and comprehensive bibliographic metadata. Data were collected in early 2026 using a structured Boolean query applied to the title, abstract, and keyword fields. The search strategy integrated three interrelated conceptual domains: cybersecurity and digital security; machine learning, artificial intelligence, and intelligent threat-detection applications; and metaverse-enabling technologies, including virtual reality, extended reality, augmented reality, avatars, digital identity, immersive environments, virtual worlds, digital twins, and blockchain security. The complete Boolean search string applied to the Scopus title, abstract, and keyword fields (searched July 2026) was as follows: “TITLE-ABS-KEY ( ( "cybersecurity" OR "cyber security" OR

"cybercrime" OR "cyber fraud" OR "digital security" ) AND ( "machine learning" OR "deep learning" OR "artificial intelligence" OR "fraud detection" OR "intrusion detection" OR "anomaly detection" OR "forensic accounting" OR "anti-money laundering" OR "financial fraud" OR "phishing" ) AND ( "metaverse" OR "virtual reality" OR "extended reality" OR "augmented reality" OR "avatar" OR "digital identity" OR "immersive environment*" OR "virtual world*" OR "digital twin" OR "blockchain security" ) )". This expanded strategy positioned metaverse security within the core dataset and strengthened the alignment between the research scope, analytical design, and reviewer recommendations.

Eligibility criteria were established to maintain the thematic relevance and bibliographic consistency. The search was restricted to English-language journal articles published between 2020 and 2026, while conference papers, book chapters, editorials, notes, and non-English documents were excluded. Records were evaluated according to their substantive relevance to the intersection of cybersecurity, machine learning, and metaverse-related security, rather than on the incidental appearance of isolated search terms.

The PRISMA-BiB protocol was applied to structure the identification, screening, eligibility assessment, and final inclusion stages [25]. The initial Boolean search on the Scopus database, integrating the three conceptual clusters described in Section 3.2, retrieved 1,535 records. Predefined eligibility filters document type (journal article), language (English), and publication year (2020-2026) were then applied at the database level, narrowing the dataset to 364 records. This filtering step reduced the corpus based on bibliographic metadata rather than substantive thematic judgment. Title and abstract screening of these 364 records subsequently identified one duplicate record and four records whose primary research domain (e.g., urban landscape planning, tourism policy, precision agriculture) was substantively unrelated to cybersecurity, machine learning, or metaverse security despite incidental keyword overlap. These five records were excluded, resulting in a final dataset of 359 articles for bibliometric and science-mapping analysis. The complete selection process is presented in **Figure 2**.

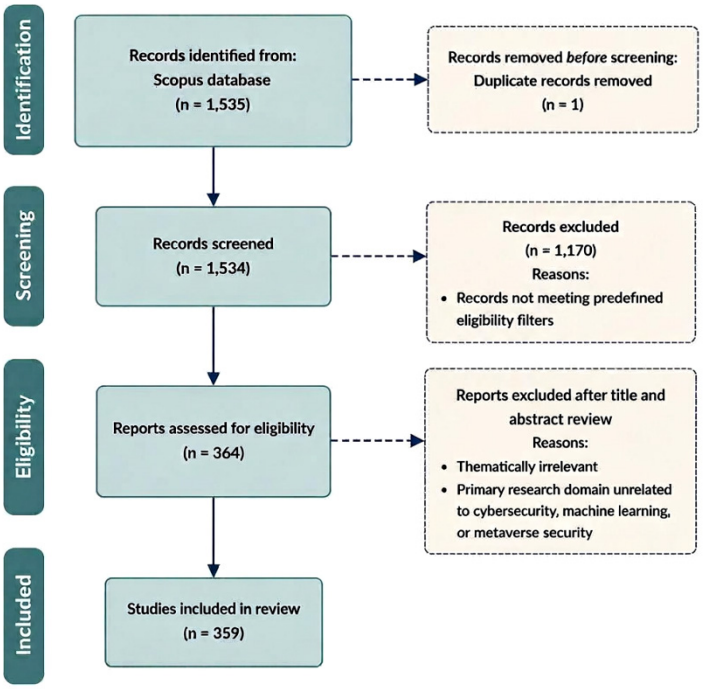


**Figure 2.** PRISMA Flow Diagram

### 3.3. Data Analysis Techniques

The 359 selected publications were analyzed exclusively using Biblioshiny through an integrated combination of performance analysis and science-mapping techniques. Annual Scientific Production Analysis was applied to examine publication growth and the temporal development of the research domain; Three-Field Plot Analysis was used to identify relationships among source journals, authors, and author-defined keywords; Words Frequency Over Time Analysis evaluated changes in the occurrence and prominence of major concepts; Trend Topics Analysis traced the emergence, persistence, and decline of dominant research themes; Co-occurrence Network Synthesis identified conceptual associations and major thematic clusters among keywords; and Thematic Map Analysis Synthesis assessed the relevance and developmental maturity of research themes based on centrality and density. The resulting patterns were interpreted within the integrated scope of cybersecurity, machine learning, and metaverse security to explain the relationships among artificial intelligence, fraud and anomaly detection, digital identity, blockchain security, immersive technologies, governance, privacy, and human-centered security in the emerging virtual ecosystems. These interpretive patterns were further synthesized into a conceptual framework integrating co-occurrence clusters and thematic map maturity stages into a unified model of the metaverse cybersecurity ecosystem.

## 4. Results and discussion

This section presents the results of the bibliometric analysis conducted exclusively in Biblioshiny and examines the intellectual development of research at the intersection of cybersecurity, machine learning, and metaverse-related technologies. The analysis covers publication growth, the relationships among cited references, authors, and keywords, the temporal evolution of research topics, keyword co-occurrence structures, and thematic maturity of research topics. The discussion moves beyond descriptive reporting by interpreting the forces driving the rapid expansion of AI-enabled cybersecurity, the growing relevance of blockchain and privacy-preserving technologies, and the increasing integration of digital twins, virtual reality, network security, and cyber-physical infrastructure within emerging metaverse ecosystems.

The findings are organized into five analytical dimensions: annual scientific production, intellectual structure, topic evolution, thematic clustering, and thematic development. This structure demonstrates how established cybersecurity foundations converge with intelligent detection, decentralized trust, immersive technologies, and infrastructure resilience.

### 4.1. Publication Growth and Scientific Production

**Figure 3** presents the annual scientific production of cybersecurity, machine learning, and metaverse security from 2020 to 2026. Publication output increased from three articles in 2020 to 15 in 2021, 28 in 2022, and 37 in 2023, indicating the gradual consolidation of this interdisciplinary domain. The early growth phase reflects increasing scholarly attention to the convergence of intelligent threat detection, digital security, virtual environments, and decentralized technologies rather than to cybersecurity and machine learning as isolated research areas.

Publication activity accelerated markedly in 2024, reaching 75 articles, as immersive technologies, digital identities, blockchain infrastructures, virtual assets, and artificial intelligence became more closely integrated into emerging Metaverse ecosystems. The expansion of cloud services, digital transactions, extended-reality

platforms, and data-intensive virtual interactions has increased the need for adaptive security mechanisms capable of addressing identity misuse, fraud, privacy leakage, anomalous behavior, and infrastructure vulnerabilities. This development helps explain the rapid growth of AI-driven cybersecurity research and the increasing relevance of blockchain security, governance, and user protection in immersive digital environments [5–7,50–52].

Publication output reached its highest level in 2025, with 123 articles, representing rapid expansion and increased disciplinary maturity. This suggests that metaverse security research has moved beyond an exclusively technical focus toward a broader socio-technical agenda encompassing digital identity governance, virtual asset protection, financial fraud prevention, privacy, platform accountability, human behavior, and regulatory challenges. The decline to 78 articles in 2026 should be interpreted cautiously because the current-year record is likely incomplete owing to publication schedules and Scopus indexing delays rather than indicating a substantive reduction in scholarly interest

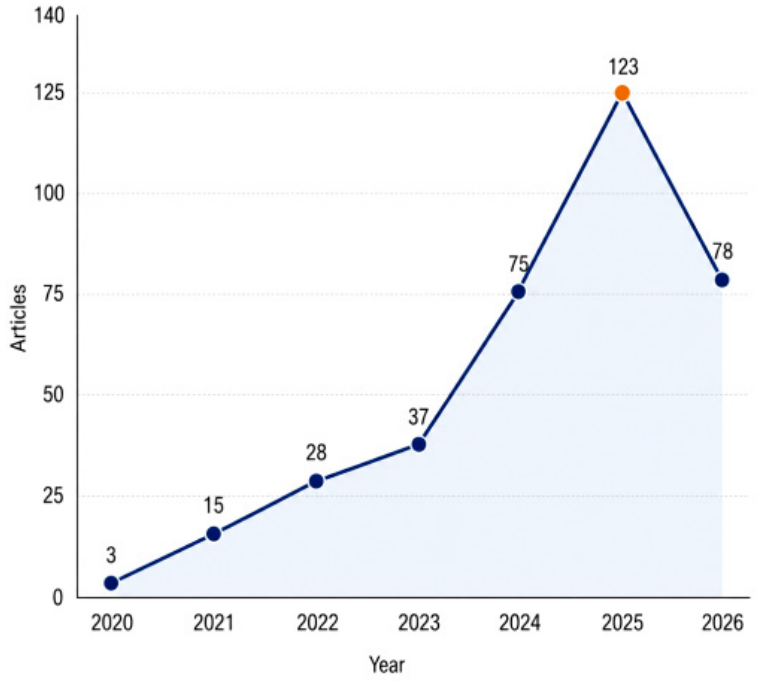


**Figure 3.** Annual Scientific Production

**Figure 3** shows that the intersection of cybersecurity, machine learning, and metaverse-related technologies has developed into a rapidly expanding research domain, particularly since 2024. Publication growth alone does not reveal how knowledge is distributed across journals, authors, and research themes. The following section examines these relationships through a Three-Field Plot Analysis to identify the principal contributors and conceptual linkages shaping the field.

## 4.2. Intellectual Structure of the Research Field

A Three-Field Plot Analysis was conducted in Biblioshiny to examine the relationships among cited references, influential authors, and merged author keywords within the cybersecurity–machine learning–metaverse research domain. The visualization indicates that the field is structured through the interaction of established cybersecurity knowledge, AI-driven analytical methods, and metaverse-enabling technologies. This configuration demonstrates that contemporary metaverse security

research draws upon multiple intellectual foundations, including network protection, cyber-physical systems, digital twins, blockchain infrastructures, the Internet of Things, and immersive virtual environments.

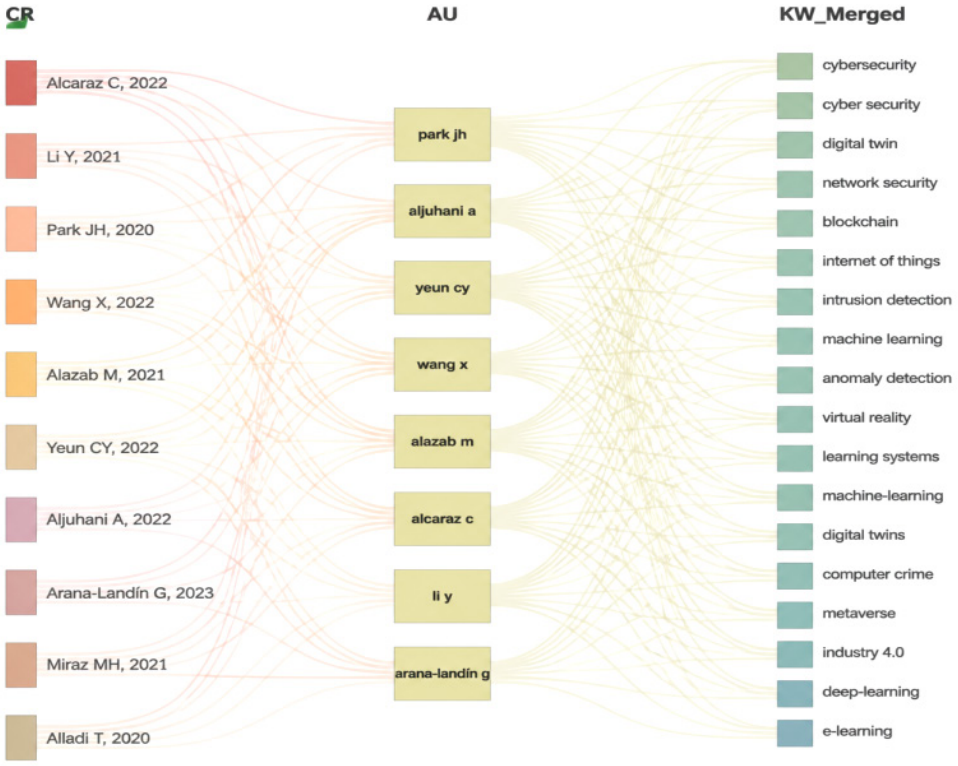


**Figure 4.** Intellectual Structure of Cybersecurity and Machine Learning Research: A Three-Field Plot Analysis

**Figure 4** illustrates the linkages among cited references (CR), authors (AU), and merged keywords (KW_Merged). Authors such as Park J. H., Aljuhani A., Yeun C. Y., Wang X., Alazab M., and Alcaraz C. are connected to recurring concepts including cybersecurity, cyber security, digital twin, network security, blockchain, the Internet of Things, intrusion detection, machine learning, anomaly detection, virtual reality, deep learning, and the metaverse. The density of these connections indicates that knowledge production is concentrated around the convergence of intelligent threat detection and the technological infrastructures that support immersive, interconnected, and decentralized digital environments.

The author–keyword relationships reveal a major intellectual stream centered on AI-enabled cybersecurity. Machine learning, deep learning, intrusion detection, anomaly detection, and network security form a closely connected group that reflects the growing demand for adaptive mechanisms capable of identifying evolving threats across large-scale heterogeneous digital systems. The prominence of these themes suggests that algorithmic detection has become a foundational capability for monitoring suspicious behavior, protecting networked environments, and supporting real-time security responses on metaverse-related platforms.

The prominence of digital twin, the Internet of Things, Industry 4.0, blockchain, virtual reality, and metaverse-related keywords reveals a second intellectual stream focused on cyber-physical and immersive infrastructures. Digital twins and IoT technologies extend security concerns from conventional information systems to continuously connected physical–virtual environments, whereas blockchain and

virtual reality introduce additional challenges involving decentralized transactions, asset integrity, platform interoperability, and immersive interactions. These linkages show that metaverse security is embedded directly within the analyzed knowledge structure rather than being treated solely as a contextual interpretation of general cybersecurity findings [53].

The Three-Field Plot demonstrates that the intellectual structure of the field is shaped by the convergence of intelligent cyber-threat detection, cyber-physical infrastructure protection, and immersive digital ecosystem security. This convergence strengthens the conceptual positioning of metaverse cybersecurity as a multidisciplinary research domain and provides a basis for examining the evolution of its principal themes over time [54].

### 4.3. Evolution of Research Topics

The evolution of keyword frequencies provides a temporal perspective on how the cybersecurity–machine learning–metaverse research domain developed between 2020 and 2026. **Figure 5** shows that *cybersecurity* and *cyber security* remained the most frequently occurring terms throughout the observation period, reaching approximately 160 and 130 cumulative occurrences, respectively by 2026. *Network security* also demonstrated sustained growth, whereas *artificial intelligence*, *digital twin*, and *machine learning* increased markedly after 2023. This pattern indicates a shift from conventional network protection approaches to intelligent, adaptive, and data-driven security frameworks capable of addressing increasingly complex digital threats.

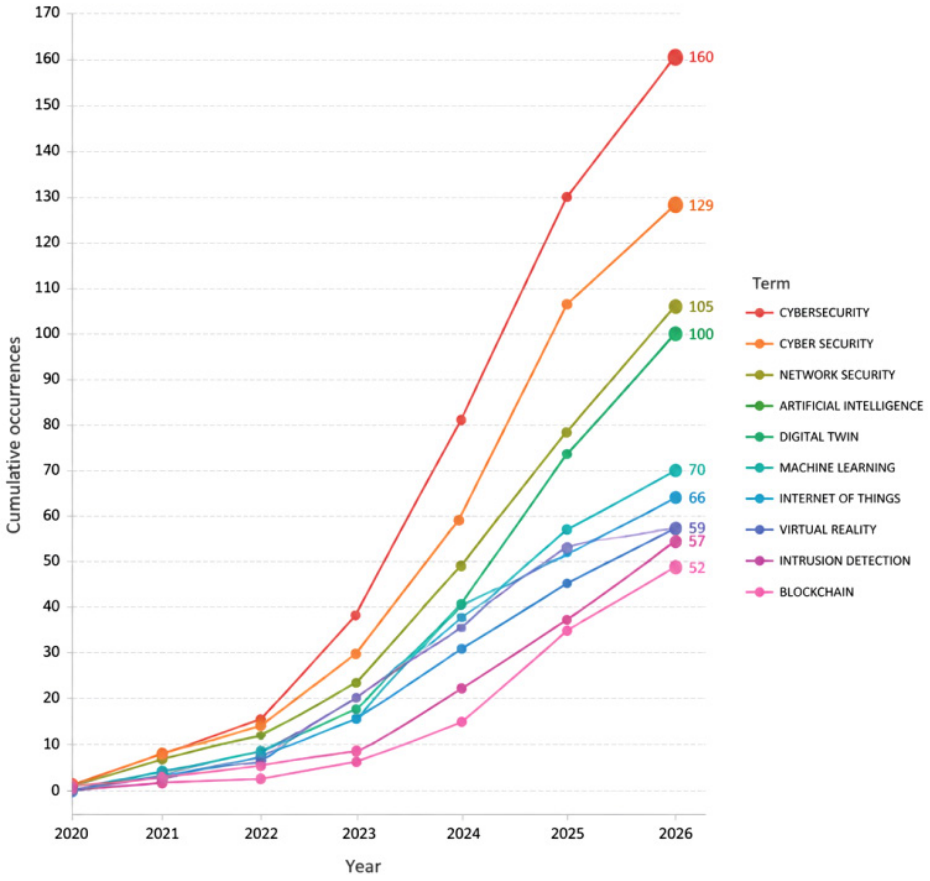


**Figure 5.** Words Frequency Over Time

The growing prominence of *digital twin, Internet of Things*, *virtual reality*,

*intrusion detection*, and *blockchain* reveals the increasing integration of cybersecurity with the technological foundations of metaverse ecosystems. The sharp acceleration of these terms after 2024 reflects the expanding scholarly attention to interconnected physical–virtual systems, immersive interactions, decentralized infrastructures, and real-time threat monitoring. These developments demonstrate that metaverse security is becoming embedded within the broader evolution of cybersecurity research through the convergence of AI-enabled detection, virtual-environment protection, digital identity assurance, and blockchain-based trust mechanisms [5–7].

The cumulative keyword patterns presented in **Figure 5** provide an overview of long-term thematic growth, but they do not indicate the specific periods in which particular topics emerged, peaked, or gained scholarly prominence. Therefore, Trend Topics Analysis was conducted in Biblioshiny to examine the temporal progression of established and emerging research areas within the cybersecurity–machine learning–metaverse domain. **Figure 6** shows a transition from foundational infrastructure-oriented topics toward intelligent, privacy-aware, and decentralized security approaches.

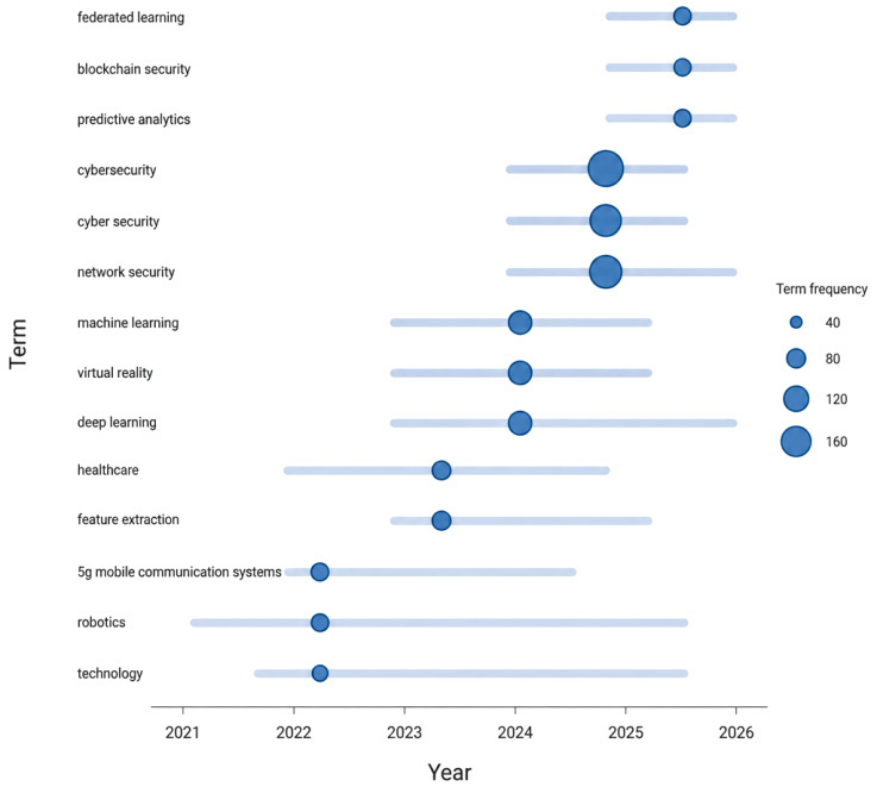


**Figure 6.** Trend Topics

Research activity during the earlier period was associated with technology, robotics, 5G mobile communication systems, healthcare, and feature extraction. These topics reflect the development of connected infrastructures and data processing capabilities that later supported more advanced cybersecurity applications. The emergence of machine learning, deep learning, and virtual reality around 2023–2024 indicates a shift toward intelligent threat detection and the protection of increasingly immersive and data-intensive environments [55].

Cybersecurity, cyber security, and network security have become the most prominent themes around 2025, as indicated by their larger bubbles and sustained temporal presence. Their prominence reflects the growing need to protect cloud-

based services, interconnected devices, virtual platforms, and digital transactions from increasingly adaptive threats. The simultaneous development of machine learning, deep learning, and virtual reality demonstrates that algorithmic security and immersive-environment protection have become closely interconnected research priorities [5–7,32].

Federated learning, blockchain security, and predictive analytics appear as the most recent topics in 2026, signalling an emerging focus on privacy-preserving intelligence, decentralized trust, and proactive threat anticipation. These themes are particularly relevant to metaverse ecosystems because secure virtual environments require distributed data processing, resilient blockchain infrastructures, transaction integrity, and predictive monitoring without excessive exposure of sensitive behavioral and biometric information. Therefore, the trend analysis confirms that metaverse-related security has become embedded within the thematic evolution of the field rather than remaining an external interpretative perspective.

### 4.4. Thematic Clusters in Cybersecurity and Machine Learning Research

A keyword co-occurrence network analysis was conducted using Biblioshiny to examine the conceptual structure of research at the intersection of cybersecurity, machine learning, and metaverse-related technologies. Co-occurrence analysis identifies relationships among frequently associated keywords and reveals how individual research topics are organized into broader thematic domains. Closely connected terms form distinct clusters that represent the principal technological, infrastructural, and security-oriented knowledge areas in the field.

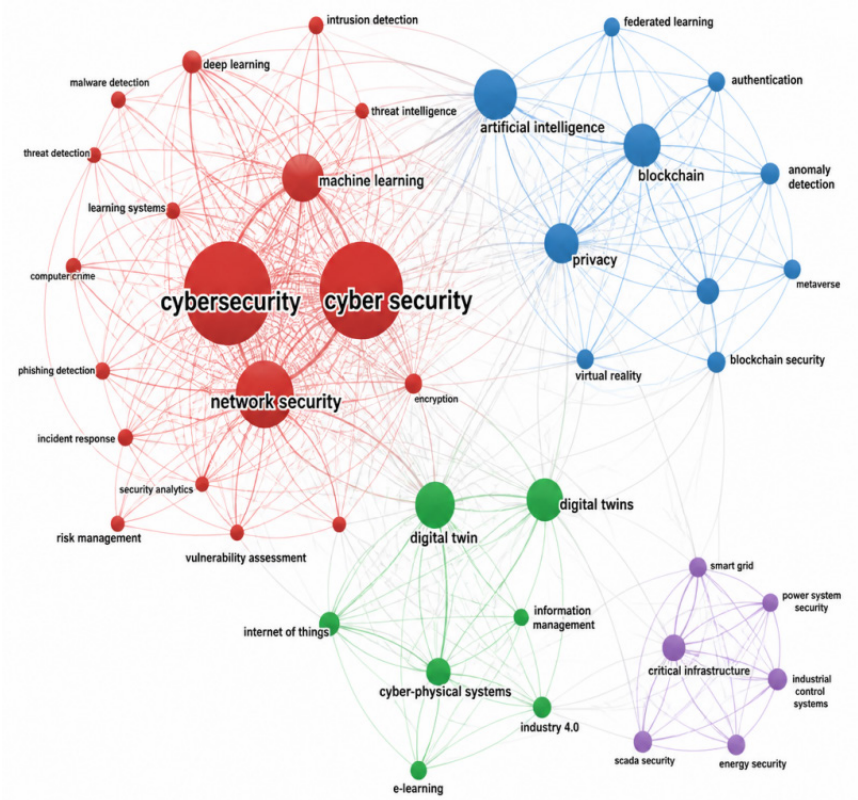


**Figure 7.** Co-occurance Network

**Figure 7** reveals four distinct but closely interconnected clusters. The red cluster is dominated by *cybersecurity*, *cyber security,* and *network security*, confirming their position as the principal conceptual anchors of the literature. The blue cluster reflects

the growing integration of artificial intelligence, blockchain, privacy, authentication, anomaly detection, and metaverse-related technology. The green cluster represents cyber-physical and digital infrastructure themes, including digital twins, connected systems, and information management, whereas the smaller purple cluster indicates a more specialized application domain. Extensive cross-cluster linkages demonstrate that contemporary security research increasingly combines intelligent threat detection, decentralized trust, immersive technologies, and infrastructure resilience.

The network structure positions metaverse security within the core conceptual architecture of the field rather than as an external interpretative dimension. The close relationships among cybersecurity, machine learning, blockchain security, virtual environments, digital twins, and network protection indicate that secure metaverse ecosystems require integrated technical and governance mechanisms. This configuration provides the basis for interpreting the four thematic clusters in greater detail and identifying the principal research directions shaping the development of metaverse cybersecurity.

a) Cluster 1: Core Cybersecurity and Intelligent Threat Detection

The red cluster is centered on *cybersecurity*, *cyber security*, *network security*, *machine learning*, *deep learning*, and intrusion-related concepts. Its dense internal structure indicates that intelligent threat detection remains the principal knowledge core of the field, driven by the need to identify increasingly adaptive attacks across interconnected networks and digital platforms. Within metaverse environments, this cluster supports real-time monitoring, anomaly recognition, identity protection, and detection of malicious activities across virtual interaction, transaction, and communication layers.

b) Cluster 2: AI, Blockchain, Privacy, and Secure Metaverse Technologies

The blue cluster brings together artificial intelligence, blockchain, blockchain security, authentication, privacy, anomaly detection, federated learning, and metaverse-related technologies. This configuration reflects the growing scholarly attention to decentralized trust, privacy-preserving analytics, and secure identity management in distributed digital environments. Its relevance to metaverse security lies in its ability to protect sensitive behavioral and biometric data, verify avatars and digital identities, secure virtual assets, and enable intelligent monitoring without exposing users' personal information.

c) Cluster 3: Digital Twin and Cyber-Physical Infrastructure Security

The green cluster is associated with digital twins, cyber-physical systems, connected devices, edge computing, embedded technologies and information management. These themes represent the convergence of physical and virtual infrastructures, where security incidents can propagate between real-world systems and their digital representations. Metaverse ecosystems increasingly depend on such infrastructures to support persistent simulation, spatial interaction, and real-time data exchange, making resilience, interoperability, and secure data synchronization central research concerns.

d) Cluster 4: Smart Energy and Specialized Critical Infrastructure Security

The smaller purple cluster represents a more specialized domain related to smart grids, energy systems, and critical infrastructure security. Its peripheral position suggests a narrower but technically mature research area that remains connected to the broader cybersecurity and cyber-physical systems literature. This cluster is relevant to future metaverse ecosystems because large-scale immersive platforms depend on reliable computing, communication, and energy infrastructures, the disruption of

which could affect virtual services, digital economies, and interconnected physical environments.

These findings extend previous bibliometric investigations of cybersecurity and artificial intelligence. Ali et al. [50] similarly identified AI/ML integration, privacy, and identity verification as dominant themes in a bibliometric analysis of ASEAN cybersecurity research, corroborating the centrality of Clusters 1 and 2 in the present study. However, their regionally bounded corpus did not capture the digital twin and cyber-physical infrastructure dimensions (Cluster 3) or the smart energy and critical infrastructure dimensions (Cluster 4) observed here, suggesting that the global and metaverse-integrated search strategy of the present study captures a broader and more technologically diversified knowledge structure than region-specific analyses. This divergence highlights the added analytical value of explicitly incorporating metaverse-enabling technologies into search and classification strategies.

### 4.5. Thematic Development and Research Maturity

The co-occurrence network reveals major thematic domains but does not fully capture their developmental status. A thematic map analysis was conducted to evaluate their relative importance and maturity levels. The thematic map classifies research themes according to centrality, which reflects relevance and influence, and density, which represents internal development and conceptual maturity.

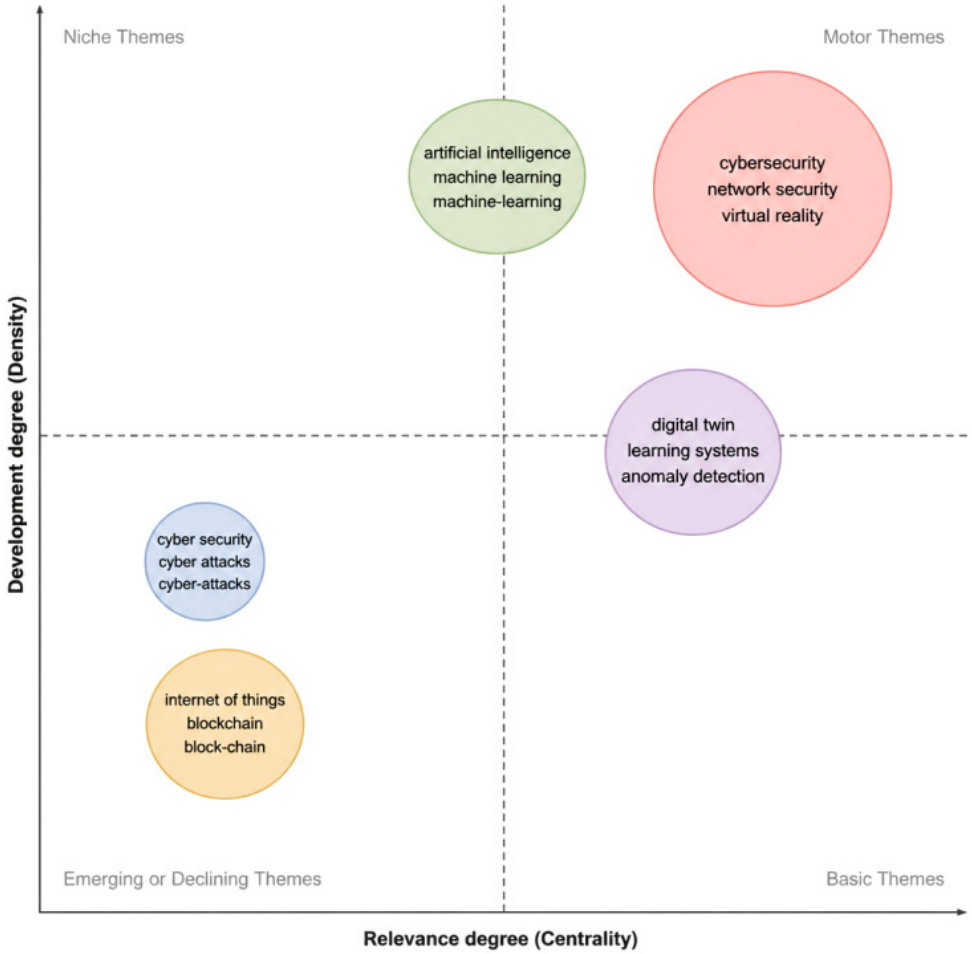


**Figure 8.** Thematic Map

**Figure 8** classifies the themes into four quadrants: Motor Themes, Niche Themes, Basic Themes, and Emerging or Declining Themes. The map shows that

*cybersecurity*, *network security*, and *virtual reality* occupy the Motor Themes quadrant, indicating that these topics are both highly relevant and comparatively well-developed. Their joint positioning demonstrates that immersive-environment protection is closely integrated with established cybersecurity and network-security research.

The cluster comprising *artificial intelligence*, *machine learning*, and *machine-learning* appears near the boundary between Niche and Motor Themes. This position suggests strong internal development and increasing field-wide relevance, although the cluster has not yet achieved the same level of centrality as the core cybersecurity themes. Its location reflects the growing role of intelligent detection, predictive analytics, and automated response in securing avatars, digital identities, behavioral data, virtual transactions, and immersive platforms.

The positioning of artificial intelligence and machine learning near the Motor Themes boundary also reflects a discernible temporal shift in the field's intellectual maturity. Kim [37] characterized artificial intelligence as an emerging rather than central influence on information security research by analyzing an earlier publication window. The present analysis, incorporating publications through 2026, indicates that this cluster has since advanced toward a more central and developmentally mature position, consistent with the broader trajectory of AI-driven security research documented in recent scientometric work [17,18].

The themes *of digital twin*, *learning systems*, and *anomaly detection* are positioned close to the boundary between Motor and Basic Themes. Their high centrality indicates strong relevance, whereas their moderate density suggests that their internal theoretical and methodological development remains in progress. These themes represent an important transitional area in which cyber-physical simulation, adaptive learning, and real-time anomaly recognition are increasingly applied to interconnected physical–virtual and metaverse environments.

The clusters containing *cyber security*, *cyberattacks*, and *cyber-attacks*, together with *Internet of Things*, *blockchain*, and *block-chain*, appear in the Emerging or Declining Themes quadrant. Their position should not be automatically interpreted as evidence of declining importance because emerging and declining topics occupy the same quadrant. The continuing expansion of metaverse infrastructures suggests that these themes are undergoing conceptual transition toward blockchain security, decentralized identity, IoT-enabled immersive systems, and integrated cyber-risk management.

The thematic configuration confirms that metaverse cybersecurity is developing through the convergence of mature security foundations and emerging intelligent, decentralized, and cyber-physical technologies. The prominence of virtual reality within the Motor Themes quadrant and the strategic positioning of AI, digital twins, anomaly detection, blockchain, and IoT demonstrate that metaverse security has become an integral component of the field’s intellectual development, rather than a secondary interpretative extension.

### 4.6. Relational Conceptual Framework of the Metaverse Cybersecurity Ecosystem

Synthesizing the co-occurrence clusters presented in **Figure 7** and the thematic map findings presented in **Figure 8, Figure 9** proposes a conceptual framework positioning metaverse cybersecurity as an integrated, multidisciplinary knowledge ecosystem rather than as four disconnected research areas. The framework advances beyond descriptive classification by specifying the directional relationships through

which each cluster conditions, extends, or governs the others. The ordering of these relationships is derived empirically from the developmental positions established in the thematic map analysis, and is formalised through four propositions.

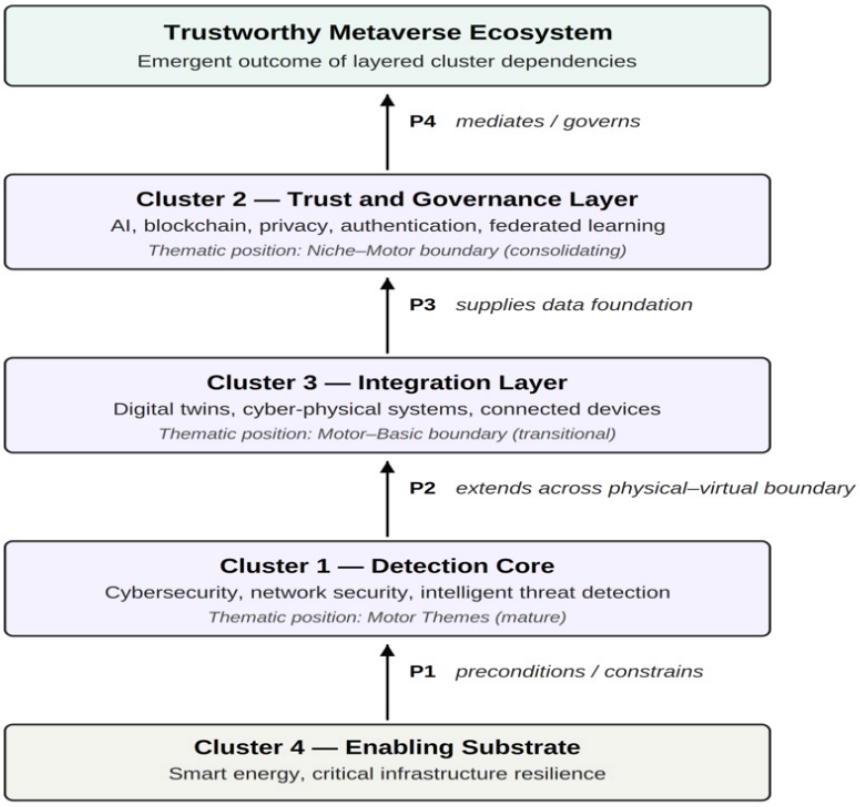


**Figure 9.** Relational Conceptual Framework of the Metaverse Cybersecurity Ecosystem

The smart energy and critical infrastructure cluster occupies the lowest position in the framework, functioning as an enabling substrate. Its peripheral location within the co-occurrence network reflects a narrow thematic scope rather than limited importance, since intelligent detection mechanisms cannot operate without reliable computing, communication, and energy infrastructures. Large-scale immersive platforms depend on persistent computational availability, and disruption at this level propagates upward through every higher-order security capability. This dependency is expressed in the first proposition. P1: infrastructure and energy resilience operates as a boundary condition for metaverse cybersecurity, such that the effectiveness of all higher-order security capabilities is constrained by the reliability of the underlying computational and energy substrate.

The core cybersecurity and intelligent threat-detection cluster occupies the Motor Themes quadrant and constitutes the generative capability layer of the framework. Its high centrality and high density confirm that intelligent detection remains the most developmentally mature component of the field. However, detection capability developed for conventional network environments does not transfer automatically to immersive contexts, where security incidents may originate in virtual interactions yet manifest in connected physical systems. The digital twin and cyber-physical infrastructure cluster provides the mechanism through which detection is extended across this boundary. This relationship is expressed in the second proposition. P2: the security value of intelligent threat detection in metaverse environments is contingent upon its extension through cyber-physical integration mechanisms, since

detection confined to virtual layers alone cannot secure ecosystems in which incidents propagate between physical systems and their digital representations.

The digital twin and cyber-physical infrastructure cluster occupies the boundary between Motor and Basic Themes, functioning as the connective layer of the framework. Its transitional position is theoretically meaningful rather than incidental, because this layer generates the continuous behavioural, spatial, and transactional data streams upon which decentralised trust mechanisms operate. Identity verification, anomaly recognition, and privacy-preserving analytics all require the persistent data foundation that cyber-physical integration supplies. This dependency is expressed in the third proposition. P3: cyber-physical integration supplies the data foundation upon which decentralised trust and privacy-preserving governance mechanisms depend, such that the developmental maturity of the trust and governance layer is partially conditioned by advances in cyber-physical integration.

The artificial intelligence, blockchain, privacy, and secure metaverse technologies cluster occupies the highest position in the framework because it performs the translation function through which technical capability becomes user-facing trust. Detection mechanisms identify threats, but governance mechanisms determine whether digital identities are verifiable, virtual assets are protected, biometric data remains confidential, and platform accountability is enforceable. Its position at the boundary between Niche and Motor Themes indicates that this translation function is actively consolidating but has not yet reached full maturity. This mediating role is expressed in the fourth proposition. P4: decentralised trust and privacy governance mediate the relationship between technical security capability and ecosystem trustworthiness, such that improvements in detection capability alone do not produce trustworthy metaverse ecosystems in the absence of corresponding governance mechanisms.

Taken together, the framework specifies that metaverse cybersecurity emerges not from any single cluster but from a layered dependency structure in which infrastructure resilience conditions detection capability, detection capability extends through cyber-physical integration, and integration supplies the evidentiary basis for decentralised governance. The developmental positions identified in the thematic map are consistent with this ordering, revealing a systematic asymmetry across the four layers: the detection core is developmentally mature, the integration layer remains transitional, and the governance layer is still consolidating. This asymmetry constitutes the principal diagnostic contribution of the framework, indicating that the current bottleneck in securing metaverse ecosystems lies not in detection capability but in the integration and governance layers through which that capability is translated into trustworthy immersive environments. The four propositions are directly testable and provide a structured foundation for subsequent empirical investigation using platform case studies, practitioner surveys, or incident-based analyses.

## 5. Conclusion

This study provides a comprehensive bibliometric assessment of research at the intersection of cybersecurity, machine learning, and metaverse-related technologies using a PRISMA-BiB-compliant procedure and Biblioshiny-based performance analysis and science-mapping. The expanded search strategy produced a final dataset of 359 Scopus-indexed articles, enabling the examination of annual scientific production, cited reference–author–keyword relationships, keyword development over time, trend topics, co-occurrence structures, and thematic maturity. Metaverse

security was positioned as a central analytical domain through the inclusion of virtual reality, extended reality, augmented reality, avatars, digital identity, immersive environments, virtual worlds, digital twins, and blockchain security.

Research activity increased substantially during the observation period, with particularly rapid growth after 2023 and a publication peak in 2025. The intellectual structure of the field reflects the convergence of established cybersecurity knowledge with machine learning, network protection, digital twins, blockchain, the Internet of Things, and immersive technologies. Temporal analysis further shows a transition from foundational infrastructure-oriented topics toward AI-enabled detection, privacy-preserving intelligence, predictive analytics, decentralized trust, and secure virtual environments.

The co-occurrence network identified four interconnected thematic clusters: core cybersecurity and intelligent threat detection; artificial intelligence, blockchain, privacy, and secure metaverse technologies; digital twin and cyber-physical infrastructure security; and specialized smart energy and critical infrastructure security. The thematic map indicates that cybersecurity, network security, and virtual reality function as well-developed Motor Themes, whereas artificial intelligence and machine learning occupy a transitional position between Niche and Motor Themes. Digital twins, learning systems, and anomaly detection appear between Motor and Basic Themes, whereas blockchain, the Internet of Things, cyberattacks, and related concepts represent emerging or conceptually transitioning areas.

The theoretical contribution of this study lies in the proposed relational conceptual framework, which advances beyond descriptive classification by specifying the directional dependencies among the four thematic clusters. Rather than presenting metaverse cybersecurity as a set of parallel research areas that jointly contribute to a common outcome, the framework identifies a layered dependency structure governed by four propositions. Infrastructure and energy resilience operates as a boundary condition constraining all higher-order security capabilities (P1). Intelligent threat detection, although developmentally the most mature component of the field, delivers security value in immersive contexts only when extended through cyber-physical integration mechanisms (P2). Cyber-physical integration in turn supplies the continuous behavioural, spatial, and transactional data foundation upon which decentralised trust mechanisms depend (P3). Decentralised trust and privacy governance then mediate the translation of technical detection capability into ecosystem trustworthiness, such that advances in detection alone are insufficient to produce trustworthy immersive environments (P4).

The principal diagnostic value of this framework derives from the developmental asymmetry it reveals. The thematic map positions establish that the detection core has achieved Motor Theme status, whereas the integration layer remains at the Motor–Basic boundary and the governance layer continues to consolidate at the Niche–Motor boundary. This ordering indicates that the current constraint on securing metaverse ecosystems is not a deficiency in detection capability but the comparative immaturity of the integration and governance layers through which that capability must be translated into verifiable identity, protected assets, and enforceable platform accountability. This finding carries a direct implication for research prioritisation: continued investment in algorithmic detection performance, while valuable, is unlikely to yield proportionate gains in ecosystem trustworthiness unless matched by corresponding development in cyber-physical integration and decentralised governance mechanisms. The four propositions are formulated to be directly testable

and provide a structured agenda for subsequent empirical validation.

The practical implications are relevant to researchers, policymakers, platform developers, cybersecurity professionals, and digital infrastructure providers. Investment in machine learning-based monitoring, privacy-preserving analytics, blockchain security, identity assurance, and cyber-physical resilience is essential for protecting virtual assets, avatars, behavioral data, immersive transactions, and interconnected infrastructures. The study remains limited by its reliance on English-language Scopus-indexed journal articles and the inability of bibliometric methods to assess the theoretical depth and methodological quality of individual publications. Future research may extend the analysis through additional databases, longitudinal comparisons, content-based reviews, and empirical validation of integrated metaverse cybersecurity frameworks.

Future research should examine how artificial intelligence, machine learning, federated learning, predictive analytics, and anomaly detection can be integrated into metaverse cybersecurity architectures. The priority areas include avatar and digital identity verification, virtual asset protection, immersive phishing detection, blockchain and smart-contract security, privacy-preserving analysis of behavioral and biometric data, and threat mitigation across digital twins, the Internet of Things, and cyber-physical systems. Empirical studies should also investigate human-centered risks, including trust formation, social engineering, security awareness, behavioral manipulation, and user responses to automated security interventions in immersive environments. Empirical validation of the four propositions advanced in this study represents a particularly productive avenue. Proposition P1 may be examined through infrastructure disruption case studies on large-scale immersive platforms; P2 through comparative evaluation of detection architectures operating within virtual-only versus cyber-physically integrated environments; P3 through analyses of how digital twin data availability conditions the performance of privacy-preserving trust mechanisms; and P4 through practitioner surveys or platform-level studies examining whether detection performance predicts user trust independently of governance maturity.

Comparative and interdisciplinary research is required to clarify how regulatory frameworks, platform governance, organizational resilience, ethical principles, and technological infrastructure influence metaverse security across countries, industries, and application contexts. Future studies should develop and empirically validate integrated metaverse cybersecurity frameworks that combine intelligent threat detection, decentralized trust, identity governance, privacy protection, infrastructure resilience, and human oversight. Methodological extensions may incorporate additional bibliographic databases, longitudinal thematic comparisons, systematic content analysis, and mixed-method designs to evaluate the theoretical development, practical effectiveness, and contextual applicability of emerging metaverse security solutions.

**Author contributions:** Conceptualization, NR and AR; methodology, DP; software, AM; validation, JJ, MA, NR; formal analysis, AM and DD; investigation, NR and DP; resources, MA; data curation, NR; writing original draft preparation, NR, DP and RD F; writing review and editing, JJ, MA and RDF; visualization, AM; supervision, JJ; project administration, JJ; funding acquisition, NR, DD, JJ. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Acknowledgment:** This article used DeepL AI Translator as a translation tool from

Indonesian to English, and also used ChatGPT 5.2 to improve content readability and make the language easier to understand. In addition, figures generated by Biblioshiny were subsequently refined using the Gamma App to enhance visual clarity and presentation quality for academic publication.

**Conflicts of interest:** The authors declare no conflicts of interest.

## Reference


1. Ahmad A, Maulana R, Yassir M. Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems. Journal of Information Engineering and Management. 2024, 6:7–11. https://doi.org/10.61992/jiem.v6i1.57.
2. Juneja A, Goswami SS, Mondal S. Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of Technology and Information Education. 2024, 3:1–22. https://doi.org/10.56556/jtie.v3i2.907.
3. Dionisio JDN, Iii WGB, Gilbert R. 3D Virtual worlds and the metaverse. ACM Computing Surveys. 2013, 45:1–38. https://doi.org/10.1145/2480741.2480751.
4. Dwivedi YK, Hughes L, Baabdullah AM, et al. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management. 2022, 66:102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.
5. Wang Y, Su Z, Zhang N, et al. A Survey on Metaverse: Fundamentals, Security, and Privacy. IEEE Communications Surveys & Tutorials. 2023, 25:319–352. https://doi.org/10.1109/comst.2022.3202047.
6. Di Pietro R, Cresci S. Metaverse: Security and Privacy Issues. IEEE Transactions on Privacy, Security and Data Integrity. 2021, p. 281–288. https://doi.org/10.1109/tpsisa52974.2021.00032.
7. Chen Z, Wu J, Gan W, et al. Metaverse Security and Privacy: An Overview. IEEE International Conference on Big Data. 2022, p. 2950–2959. https://doi.org/10.1109/bigdata55660.2022.10021112.
8. Curran K, Curran E, Killen J, et al. The role of generative AI in cyber security. Metaverse. 2024, 5:2796. https://doi.org/10.54517/m.v5i2.2796.
9. Ali B, Shah SI, Sajid L, et al. Design of Intelligent Cyber Defense Frameworks Using Artificial Intelligence for Proactive Threat Detection, Prediction, and Automated Response. Global Research Journal of Natural Sciences. 2026. https://doi.org/10.53762/grjnst.04.01.01.
10. Bibers I, Arreche O, Alayed W, et al. Ensemble-IDS: An Ensemble Learning Framework for Enhancing AI-Based Network Intrusion Detection Tasks. Applied Sciences. 2025, 15:10579. https://doi.org/10.3390/app151910579.
11. Salama MA, Tawfeek RM, Hamdy S, et al. Advances in Ensemble Machine Learning for Network Intrusion Detection Systems: A Comprehensive Review. Benha Journal of Engineering Science and Technology. 2025, 2:117–125. https://doi.org/10.21608/bjest.2025.445861.
12. Sanmorino A, Gustriansyah R, Puspasari S, et al. Improving Threat Detection in Information Security with Ensemble Learning. Applied Cybersecurity & Internet Governance. 2025. https://doi.org/10.60097/acig/210525.
13. Shelke P, Hamalainen T. Analysing Multidimensional Strategies for Cyber Threat Detection in Security Monitoring. European Conference on Cyber Warfare and Security. 2024, 23:780–787. https://doi.org/10.34190/eccws.23.1.2123.
14. Amalan Fernando MR, Shinde J. Strengthening Cybersecurity in Modern Finance: Safeguarding Online Banking and Beyond. International Journal of Scientific Research in Engineering and Management. 2025, 09:1–9. https://doi.org/10.55041/ijsrem43088.
15. Chaturvedi M, Sharma S, Ahmed G. Optimized early financial fraud detection and prevention method to enhance the security. Journal of Information and Optimization Sciences. 2025, 46:359–369. https://doi.org/10.47974/jios-1920.
16. Pan E. Machine Learning in Financial Transaction Fraud Detection and Prevention. Transactions on Economics, Business and Management Research. 2024, 5:243–249. https://doi.org/10.62051/16r3aa10.
17. Razzaq K, Shah M. Advancing Cybersecurity Through Machine Learning: A Scientometric Analysis of Global Research Trends and Influential Contributions. Journal of Cyber Policy. 2025, 5:12. https://doi.org/10.3390/jcp5020012.
18. Razzaq K, Shah M. Emerging Trends in Cybersecurity: Machine Learning as a Game-Changer in Next-Generation Cybersecurity Applications. F1000Research. 2026, 15:276. https://doi.org/10.12688/f1000research.173916.1.

19. Albahri OS, Alamoodi AH. Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. Mesopotamian Journal of CyberSecurity. 2023, 2023:158–169. https://doi.org/10.58496/mjcsc/2023/018.
20. Passas I. Bibliometric Analysis: The Main Steps. Encyclopedia. 2024, 4:1014–1025. https://doi.org/10.3390/encyclopedia4020065.
21. Nnodim J, Vitus O, Amarachi IP. A familiar insight into the use of bibliometric terms. Multidisciplinary Journal of Data and Humanities. 2025, 2:65–79. https://doi.org/10.37899/mjdh.v2i2.160.
22. Yıldız M, Karakuş Yılmaz T. Bibliometric Analysis in Scientific Research Using R: A Review of Scopus and Web of Science Databases. Journal of Data Analysis. 2024, 0:31–46. https://doi.org/10.26650/joda.1462396.
23. Kumar R. Bibliometric Analysis: Comprehensive Insights into Tools, Techniques, Applications, and Solutions for Research Excellence. Specialty Engineering and Management Sciences. 2025, 3:45–62. https://doi.org/10.31181/sems31202535k.
24. Shushanyan RA, Ohanyan MJ. HOW TO PERFORM A BIBLIOMETRIC ANALYSIS OF JOURNALS FOR SPECIFIC SCIENTIFIC FIELDS. Proceedings of Metallurgy, Material Science, Mining Engineering. 2021:9–22. https://doi.org/10.53297/18293395-2021.2-9.
25. Ng JY, Liu H, Masood M, et al. Guidance for the reporting of bibliometric analyses: A scoping review. Quantitative Science Studies. 2025, 6:988–1001. https://doi.org/10.1162/qss.a.12.
26. Khan S, Olivia TSL, Khan N, et al. Data Analytic for Cyber Security: A Review of Current Framework Solutions, Challenges and Trends. Emerging Science and Technology Management. 2022, 18:1–6. https://doi.org/10.55549/epstem.1182628.
27. Marlina L, Juliana J, Nasrullah AA, et al. A bibliometric review on halal tourism development. Edelweiss Applied Science and Technology. 2024, 8:8848–8859. https://doi.org/10.55214/25768484.v8i6.3881.
28. Noor R, Rahayu A, Hurriyati R, et al. Human Capital Readiness for Cloud–AI–Data Center Ecosystems: A Bibliometric Review. Human Resources Management and Services. 2026. https://doi.org/10.18282/hrms6018.
29. Sarker SPK, Das R, Hasan R. Integration of Machine Learning and Human Expertise for the Improvement of Cybersecurity: Applications and Challenges. Journal of Engineering Research and Reports. 2024, 26:346–361. https://doi.org/10.9734/jerr/2024/v26i61185.
30. Pooyandeh M, Han K-J, Sohn I. Cybersecurity in the AI-Based Metaverse: A Survey. Applied Sciences. 2022, 12:12993. https://doi.org/10.3390/app122412993.
31. Razzaq K, Shah M, Fattahi M, et al. Empowering machine learning for robust cyber-attack prevention in online retail: an integrative analysis. Humanities and Social Sciences Communications. 2025, 12. https://doi.org/10.1057/s41599-025-04636-y.
32. Gumelar AB, Yuniarno EM, Nugroho A, et al. An Improved Toxic Speech Detection on Multimodal Scam Confrontation Data Using LSTM-Based Deep Learning. International Journal of Intelligent Engineering and Systems. 2024, 17:880–904. https://doi.org/10.22266/ijies2024.1231.67.
33. Iskandar I, Juliana J, Miftahuddin A, et al. Digital Literacy and Academic Productivity: A Human Capital Perspective in Higher Education. Human Resources Management and Services. 2026, 8(1). https://doi.org/10.18282/hrms5793.
34. Thakar H, Thakar D, Pradhan V. Artificial intelligence and machine learning in Metaverse security. CRC Press. 2025, p. 115–143. https://doi.org/10.1201/9781003581659-7.
35. Kamarul Zaman NJF, Ahmi A, Ismail S, et al. Gig economy insights: key trends, influencers and research directions. Global Knowledge, Memory and Communication. 2025. https://doi.org/10.1108/gkmc-07-2024-0456.
36. Ninglasari SY, Himawan MF, Noer LR, et al. Mapping Customer Satisfaction Research in Islamic Banking: A Bibliometric Analysis (1998–2023). Review of Islamic Economics and Finance n.d.. 8(2). https://doi.org/10.17509/rief.v8i2.
37. Kim T-H. A Study on the Influence of Artificial Intelligence Research on the Development of Information Security Research. Asia-Pacific Journal of Convergent Research Interchange. 2021, 7:41–53. https://doi.org/10.47116/apjcri.2021.12.05.
38. Ilić L, Šijan A, Predić B, et al. Research Trends in Artificial Intelligence and Security—Bibliometric Analysis. Electronics. 2024, 13:2288. https://doi.org/10.3390/electronics13122288.
39. Judijanto L, Endrianto E, Vandika AY. Mapping the Cybersecurity Research through Bibliometric Analysis. West Science Information System and Technology. 2024, 2:374–382. https://doi.org/10.58812/wsist.v2i03.1534.
40. Dwivedi R. International journal of information security: a bibliometric study, 2007–2023. International Journal of Information Security. 2024, 23:2159–2187. https://doi.org/10.1007/s10207-024-00840-0.
41. Abu Huson Y, Sierra-García L, Garcia-Benau MA. A bibliometric review of information technology, artificial intelligence,

and blockchain on auditing. Total Quality Management & Business Excellence. 2023:91–113. https://doi.org/10.1080/14783363.2023.2256260.

42. Ahsan M, Nygard KE, Gomes R, et al. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy. 2022, 2:527–555. https://doi.org/10.3390/jcp2030027.
43. Therasa PR, Shanmuganathan M, Bapu BRT, et al. Machine learning models for enhancing cyber security. International Journal of Electronic Security and Digital Forensics. 2024, 16:590–601. https://doi.org/10.1504/ijesdf.2024.140742.
44. Therasa PR, Shanmuganathan M, Tapas Bapu BR, et al. Machine learning models for enhancing cyber security. International Journal of Electronic Security and Digital Forensics. 2024, 1. https://doi.org/10.1504/ijesdf.2024.10057194.
45. Tulsyan R, Shukla P, Singh T, et al. Cyber Security Threat Detection Using Machine Learning. International Journal of Scientific Research in Engineering and Management. 2024, 08:1–6. https://doi.org/10.55041/ijsrem37949.
46. Dohler M, Kim Y-G, Franco MG, et al. Making the MetAverse A Reality: Challenges And Opportunities. IEEE Communications Magazine. 2023, 61:14–15. https://doi.org/10.1109/mcom.2023.10268119.
47. Uddin M, Manickam S, Ullah H, et al. Unveiling the Metaverse: Exploring Emerging Trends, Multifaceted Perspectives, and Future Challenges. IEEE Access. 2023, 11:87087–87103. https://doi.org/10.1109/access.2023.3281303.
48. Lee L-H, Braud T, Zhou PY, et al. All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. Foundations and Trends in Human–Computer Interaction. 2024, 18:100–337. https://doi.org/10.1561/1100000095.
49. Marlina L, Juliana J, Ismail S, et al. Halal industry development strategy: a bibliometric analysis. Journal of Islamic Marketing. 2026, 17:324–348. https://doi.org/10.1108/jima-12-2024-0591.
50. Ali AS, Zaaba ZF, Singh MM, et al. Advancing cybersecurity in ASEAN: current trends, emerging challenges, and opportunities for enhanced resilience. International Journal of Information Security. 2025, 24. https://doi.org/10.1007/s10207-025-01111-2.
51. Btoush E, Kobbaey T, Tamimi H, et al. Machine Learning-Based Cyber Fraud Detection: A Comparative Study of Resampling Methods for Imbalanced Credit Card Data. Applied Sciences. 2026, 16:850. https://doi.org/10.3390/app16020850.
52. Marazqah Btoush EAL, Zhou X, Gururajan R, et al. A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science. 2023, 9:e1278. https://doi.org/10.7717/peerj-cs.1278.
53. Huang Y, Li YJ, Cai Z. Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics. 2023, 6:234–247. https://doi.org/10.26599/bdma.2022.9020047.
54. Radanliev P. Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. Frontiers in Blockchain. 2024, 7. https://doi.org/10.3389/fbloc.2024.1359130.
55. Awadallah A, Eledlebi K, Zemerly MJ, et al. Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities. IEEE Communications Surveys & Tutorials. 2025, 27:1008–1052. https://doi.org/10.1109/comst.2024.3442475.