Microwave Review
July 2026, Vol. 32, No. 1, pp. 34-43
DOI: 10.18485/mtts_mr.2026.32.1.6

Mapping the Research Landscape of Smart Metering Infrastructure Security: A Bibliometric Analysis of Trends, Themes, and Future Directions

Anu Sathyajith Mathew, Axel Sikora

Abstract – **The Smart Metering Infrastructure is a critical component of modern power grids. It faces escalating cybersecurity threats that could potentially jeopardise grid stability, consumer privacy, and utility operations. This study presents a bibliometric analysis of 1889 peer-reviewed publications from Scopus and IEEE Xplore from 2015 till 2025 to systematically map the security research landscape for the Smart Metering Infrastructure. Using keyword co-occurrence network analysis and the Walktrap clustering algorithm, five dominant research themes were identified: Smart metering Network Architecture and Infrastructure, Real-Time Monitoring and Data Systems, Intrusion Detection and Threat Analytics, Authentication and Access Control, and Homomorphic and Differential Privacy. Temporal analysis reveals that intrusion detection exhibits the highest growth rate (335.7%), followed by privacy-preserving techniques (167.5%), reflecting intensified focus on machine learning-based threat detection and regulatory-driven privacy requirements. Emerging topics include federated learning, adversarial machine learning, and quantum-resistant cryptography, while generic encryption approaches show decline. These findings provide researchers with a structured understanding of the field's evolution and promising future research directions.**

Keywords – **Smart Metering Infrastructure, Advanced Metering Infrastructure, AMI Security, Cybersecurity, Bibliometric Analysis, Privacy Preservation, Intrusion Detection, Authentication, Machine Learning, Blockchain**

I. INTRODUCTION

The modernization of electrical grids has established Smart Metering Infrastructure (SMI) as a critical component of smart grid systems worldwide. SMI integrates smart meters, communication networks, and meter data management systems (MDMS) to enable bidirectional data exchange between utilities and consumers [1]. This infrastructure supports essential grid functions including real-time consumption monitoring, dynamic pricing, demand response programs, outage detection, and integration of distributed energy resources [2]. The connectivity that enables these capabilities also exposes AMI to a broad spectrum of cybersecurity threats [3].

Article history: Received December 05, 2025; Accepted March 26, 2026. This paper is an expanded version of the article "State of the Art in Smart Metering Infrastructure Security: A Keyword Co-Occurrence Analysis," presented at 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies, Ohrid, North Macedonia, June 26 – 28, 2025. [DOI: 10.1109/ICEST66328.2025.11098305].

Anu Sathyajith Mathew and Axel Sikora are with the Institute of Reliable Embedded Systems and Communication Electronics, Offenburg University of Applied Sciences, 77652 Offenburg, Germany.
E-mail: anu.mathew@hs-offenburg.de, axel.sikora@hs-offenburg.de

The attack surface of SMI spans multiple domains. At the device level, smart meters capture fine-grained consumption data, often at 15-minute intervals, revealing occupancy patterns, daily routines, and appliance usage. This granularity raises significant privacy concerns[4] [5]. At the network level, communication links connecting millions of endpoints to utility control centres remain susceptible to eavesdropping, data manipulation, and denial-of-service attacks[6]. The consequences extend beyond data breaches. The cyberattacks on Ukraine's power grid demonstrated that adversaries could exploit such vulnerabilities to cause widespread physical disruption [7].

The research community has devoted considerable effort to SMI security, producing a substantial literature on cryptographic protocols, authentication mechanisms, intrusion detection systems, privacy-preserving data aggregation, and secure communication architectures [8], [9], [10], [11]. The rapid expansion and interdisciplinary nature of this research have dispersed knowledge across computer science, electrical engineering, and information security venues. This fragmentation creates challenges for researchers seeking to assess the current state of the field, distinguish mature themes from emerging directions, and identify gaps requiring further investigation.

Bibliometric analysis provides a systematic approach to address this challenge. Through quantitative examination of publication metadata, including keywords, authorship, citations, and venues, bibliometric methods map the intellectual structure of research domains, trace their evolution, and identify emerging frontiers. This study uses bibliometric analysis with the Bibliometrix R package and wake algorithm to examine SMI cybersecurity research published between 2015 and 2025 [12], [13]. Focusing on this period captures the latest developments and changing threats in smart metering infrastructure. The following research questions were addressed:

RQ1: What are the publication trends and growth patterns in SMI cybersecurity research?
RQ2: What are the dominant research themes, and how are they organized into thematic clusters?
RQ3: How has the thematic focus of the field evolved over the study period?
RQ4: What geographic patterns characterize research contribution and collaboration?

The remainder of this paper is organized as follows. Section II provides background on SMI architecture and associated security challenges. Section III reviews notable cyberattacks targeting smart grid infrastructure. Section IV examines related work, including prior bibliometric studies and systematic reviews. Section V describes the research methodology, covering data collection, preprocessing, and analytical techniques.

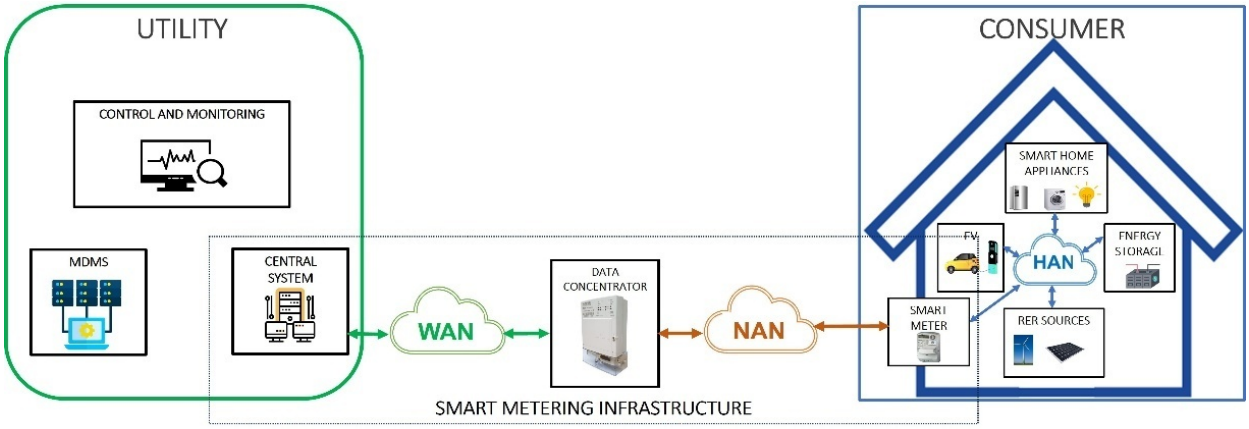

Fig. 1. Smart Metering Infrastructure.

Section VI presents result on publication trends, thematic clusters, temporal evolution, and geographic distribution. Section VII discusses findings and their implications. Section VIII concludes the paper.

II. Background

A smart grid is an intelligent framework integrating various elements within the energy landscape, such as power generation, transmission, distribution and consumption [14]. The control and automation processes across the entire electricity sector are coupled with modern communication technologies and coordinated efficiently in smart grids [14] [15]. NIST [16] identifies Distribution, Transmission, Bulk Generation, Service Providers, Operations, Markets and Customers as the major domains of a Smart Grid Information System. An intelligent smart metering system is at the core of these energy grids [15].

Smart metering infrastructure, also referred to as advanced metering infrastructure (AMI), is a comprehensive system that includes smart metering devices, communication networks, and data management systems. These help in monitoring and managing energy consumption in a more efficient and granular manner. They can include features like automatic two-way metering and billing, demand response capabilities, detection and restoration services for power outages, distributed control features, data storage capabilities, fault identification and diagnosis, seamless end-to-end communication, digital interface displays, various communication options, and the potential to function as an Internet of Things (IoT) device[17].

In [18], a comparative analysis is conducted on the smart metering infrastructure and regulatory frameworks in France, Germany, and Switzerland. However, the focus of this paper is to seek a more generalised approach to the overall architecture of the SMI system (Fig: 1). The key components of a smart metering system include a smart meter, data concentrator unit, data management system (MDMS), and communication networks.

1. Smart Meter: Smart meters are electronic devices that replace traditional analogue meters. They measure and record energy consumption (electricity, gas, water) automatically with greater accuracy and in real-time. They are equipped with communication interfaces to transmit consumption data to data collection points, through wired or wireless networks [19].
2. Data Concentrator Unit: The data concentrator performs collection and management of data sourced from different smart meters. Additionally, the DCU facilitates the transmission of specific or comprehensive data acquired from utility or customer smart meters to the intended consumers. By consolidating communication and management tasks for a set of smart meters into a single device, data concentrators streamline the process of gathering information, organising communications, and consequently reduce overall operational costs [14].
3. Meter Data Management System (MDMS): The MDMS is responsible for the storage and management of the data that is generated in a smart metering infrastructure. Furthermore, this data is analysed so that meaningful inferences can be drawn about electricity consumption and power quality, and it facilitates dynamic pricing and load forecasting [19].
4. Communication Networks: The interconnection of various elements within the smart metering infrastructure is facilitated through these communication networks. Within the smart grid framework, diverse communication technologies and architectures may be utilised. When selecting a specific communication protocol or technology for smart metering infrastructure applications, factors such as latency, reliability, scalability, and security are crucial considerations[17] .

There are three different types of communication networks in SMI. While specific names for these networks may vary across countries, this discussion aims to provide a general overview, without using country-specific terminology:

- Wide Area Network (WAN): The Wide Area Network (WAN) connects the local data concentrator, such as a smart meter gateway [19], to the central data centre of utility companies. This long-distance network enables essential tasks such as remote meter reading, firmware updates, and the aggregation of usage data on a larger scale [10][15].
- Home Area Network (HAN): The Home Area Network (HAN) functions as a localised communication network within homes or buildings, facilitating seamless interaction between smart meters and in-home devices. Through

HAN, consumers gain the ability to monitor and control their energy consumption with smart appliances, thermostats, and other connected devices. This network empowers users to make informed decisions about their energy usage, promoting greater efficiency and awareness on an individual household level [10].

- Neighbourhood Area Network (NAN): Operating at an intermediate level, the Neighbourhood Area Network (NAN) bridges the gap between individual HANs within a specific neighbourhood or cluster of homes and the broader utility network. NAN connects multiple smart meters to a local data concentrator, allowing for the aggregation of data before transmission to the utility's central system through the WAN. This localised network optimises communication efficiency, reducing the load on the wider infrastructure and enhancing the overall performance of smart metering systems within a given community[17] .

These components work together to create an integrated and efficient system for managing energy consumption and data.

III. Cyber Security Incidents in Smart Metering

Given the critical role of metering data in billing accuracy, demand response programs, outage management, and grid-balancing operations, any compromise to smart metering systems poses substantial risks to operational continuity, economic integrity, and consumer trust. High-profile cyber incidents over the past decade demonstrate that adversaries are increasingly capable of targeting the energy sector with sophisticated malware, ransomware, and coordinated intrusion campaigns. These attacks have affected utility providers, renewable energy assets, and metering networks, leading to outcomes ranging from localized disruptions to large-scale blackouts and, in severe cases, deliberate sabotage with implications for public safety and national security [20].

As the next-generation power grid continues to expand, integrating millions of smart meters, sensors, communication devices, and automated control systems, the attack surface grows proportionally. Ensuring the resilience of this evolving infrastructure is therefore essential to defend against emerging cyber threats and maintain reliable grid operations. Table 1 provides an overview of notable cybersecurity attacks on energy and metering infrastructures reported from 2007, illustrating the increasing frequency, sophistication, and impact of such events [11], [21],[22].

IV. Related Works

Existing surveys on SMI security have predominantly employed narrative review methodologies with manual categorization of literature. Shokry et al. [9] proposed a layered security framework examining device, network, and application vulnerabilities, while Kim et al. [42] developed detailed taxonomies of attack techniques and defensive countermeasures. Ghiasi et al. [43] traced the evolution of threat landscapes across past, present, and future perspectives.

TABLE 1
Cyber security attacks

Cyber Security Attacks	Year
Stuxnet Worm attack on Iranian nuclear power station **[23]**	2007
Energy firms in North America and Europe **[24]**	2014
Electrical power station in Ivano-Frankivsk-Ukraine - Spear-phishing and a 'Black Energy' Trojan horse to delete data, destroy hard disks, and control infected computers. Also, DoS attack on the phone numbers of companies running the power station **[25]**	2015
The U.S., Saudi Arabia and South Korea (energy and petrochemicals) - Malware through targeted spear-phishing emails sent to employees- APT33**[22]**	2017
Schneiden Electric's Triconex safety instrumented system targeted by modifying in-memory firmware to add malicious functionality allowing an attacker to read/modify memory contents and execute custom code **[26]**	2017
Targeted emails by hackers to steal the credentials and cyberattack on SCADA systems at Wolf Creek nuclear unit in US **[27]**	2017
High volume network reconnaissance activity targeting Industrialized control systems by US and UK-based electric utility companies **[21]**	2017
Detection of issues on Entergy Corporation's corporate network, affecting internal IT network and some employee devices **[28]**	2018
Cyberattack on Latitude Technologies, provider of electronic data-sharing between pipeline companies, gas producer, and utility customers **[29]**	2018
Multi-stage intrusion campaign that staged malware, conducted spear phishing, and gained remote access into energy sector networks on multiple US-based electric utilities.**[30]**	2018
Cyberattacks targeted North American Electric Reliability Corporation power grids by exploiting a firewall vulnerability at a vendor, enabling attackers to trigger device reboots. **[32]**	2019
Supply chain attack through Solar Winds Orion System by hacker group known as Nobelium **[32]**	2020
Targeted intrusion activity to increase the infrastructure usage on Electric grid operators in India **[21]**	2020
LineStar Integrity Services data breach by ransomware attack**[33]**	2021
Unauthorized access to customers' personal details in Npower app data breach **[34]**	2021
Ransomware attack on Australian utility company CS energy **[35]**	2021
Cyber security incident affecting UK multi-utility infrastructure and services provider Fulcrum **[36]**	2022
Data breach in Italy's energy agency Gestore dei Servizi Energetici SpA **[37]**	2022
DDoS cyber-attack on Lithuania's state-owned energy group Ignitis **[38]**	2022
Ransomware attack and data leakage in Greece's largest natural gas supplier DESFA by Ragnar Locker **[39]**	2022
FrostyGoop ICS malware attack on Ukrainian heating infrastructure **[20]**	2023-2024
Coordinated breach of 22 Danish energy companies; attackers accessed ICS and forced sites into island mode **[40]**	2023
MOVEit supply-chain breach impacting multiple US utilities **[41]**	2025

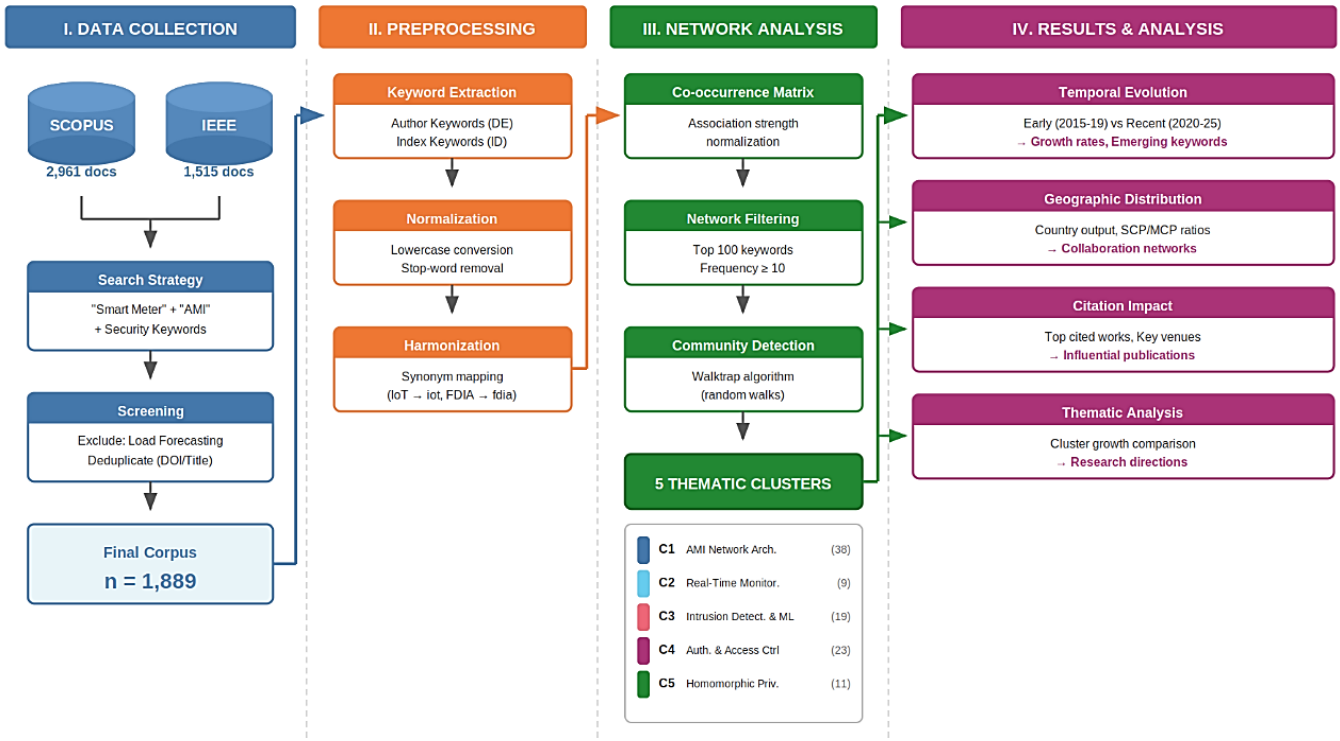

Fig. 2. Research Methodology

These surveys provide valuable conceptual frameworks but rely on subjective thematic groupings that may reflect author perspectives rather than objective patterns in literature.

Domain-specific reviews have examined aspects of SMI security in depth. Husnoo et al. [44] comprehensively analysed false data injection attack methodologies and detection techniques for active distribution systems. Leszczyna [45] evaluated coverage and gaps across cybersecurity standards applicable to smart grids, providing guidance for regulatory compliance. Ghosal and Conti [10] systematically compared key management protocols across efficiency, scalability, and security criteria. While these focused reviews offer depth, they do not reveal cross-domain relationships or quantify relative research attention across topics.

However, quantitative bibliometric analysis of smart grid security remains limited. Sakhnini et al. [46] analysed and reported publication trends, journal and author distributions, and a keyword heat-map. Their findings demonstrated exponential growth in the field and identified computational efficiency and false positive minimization as primary detection concerns. That study did not identify thematic clusters or quantify growth rates across research themes. Our conference paper [47] introduced network-based analysis using VOSviewer on 549 Scopus documents, producing preliminary cluster visualizations. That work did not include temporal analysis, growth rate quantification, or IEEE Xplore coverage. To extend previous research, this study draws on literature from both databases, applies the Bibliometrix R tool [12] along with Walktrap [13] algorithm for cluster detection, compares findings across different time periods, and systematically identifies future research directions based on bibliometric trends.

V. METHODOLOGY

This section describes the research methodology employed for the bibliometric analysis, encompassing data collection, preprocessing, network construction, clustering, and temporal analysis. A detailed illustration of the methodology adopted in this study is presented in Figure 2. Each stage is described below.

A. Data Sources and Search Strategy

Over the past decade, the security of smart metering infrastructure has been extensively explored in academic research, as evidenced by numerous systematic surveys and domain-specific analyses [9], [10], [43], [44], [48].

To assemble a comprehensive and representative body of literature, we conducted systematic searches across two prominent academic databases: Scopus and IEEE Xplore, both of which are recognised as key resources for peer-reviewed research in engineering, computing, and cybersecurity domains. The search strategies were informed by terminology prevalent in leading surveys, ensuring alignment with established research in the field. For IEEE Xplore, the query was structured as follows:

- Query: ("smart meter" OR "smart metering" OR "advanced metering infrastructure" OR "AMI" OR "smart metering infrastructure") AND (security OR cybersecurity OR "cyber attack" OR "intrusion detection" OR "anomaly detection" OR authentication OR encryption OR cryptography OR "data protection" OR privacy) NOT ("load forecasting" OR "demand prediction" OR "energy forecasting" OR optimisation OR "power quality" OR "load management")

- Results: 1,515 documents

For Scopus, we implemented a similarly targeted search that included:

- Query: TITLE-ABS-KEY (("smart meter" OR "smart metering" OR "advanced metering infrastructure" OR AMI) AND ("cybersecurity" OR "cyber attack" OR "intrusion detection" OR "anomaly detection" OR authentication OR encryption OR cryptography OR privacy OR "data protection")) AND NOT TITLE-ABS-KEY ("load forecasting" OR "demand prediction" OR "energy forecasting" OR optimisation OR "power quality" OR "load management" OR "fault detection" OR "defect detection" OR "computer vision" OR "image detection") AND PUBYEAR > 2014 AND PUBYEAR < 2025
- Results: 2,961 documents

These queries were intentionally designed to focus on cybersecurity and privacy aspects of smart metering infrastructure, while rigorously excluding literature centred on unrelated topics such as load forecasting, demand prediction, energy optimisation, power quality, load management, and fault or defect detection.

Then conference proceedings and similar materials were filtered using the advanced filtering options available within Scopus and IEEE Xplore to ensure relevance. Only English-language journal articles and conference papers published between 2015 and 2025 were considered. After the initial database search, an additional manual screening of results was conducted to eliminate papers that were not genuinely related to the subject matter. This process ensured that the resulting corpus was both highly relevant and representative of the current state of research in SMI security. The final corpus comprised **1,889 unique documents**.

B. Keyword Preprocessing

Author keywords and index terms were extracted for co-occurrence analysis. The combined set contained 4,246 unique author keywords and 8,262 index terms. Keywords underwent the following normalization steps:

1. **Case normalization**: All keywords were converted to lowercase.
2. **Character cleaning**: Non-alphabetic characters were removed except hyphens in compound terms.
3. **Stop term removal**: Generic English stop words and domain-specific high-frequency but low-semantic tokens were excluded. These decisions align with vocabulary and terminology patterns noted in SMI literature[9] [49], [18], [11] and the NIST Smart Grid framework [16].
4. **Synonym harmonization**: A synonym dictionary mapped common variants to consistent forms:
   - "internet of things" → "iot"
   - "cyber-security", "cyber security" → "cybersecurity"
   - "false data injection attack" → "fdia"
   - "intrusion detection system" → "ids"

   Such harmonization improves co-occurrence analysis by reducing lexical fragmentation.

C. Network Construction

A keyword co-occurrence network was constructed to represent the conceptual structure of the research domain. In this network, nodes represent keywords and edges represent co-occurrence relationships between keywords appearing together in the same document. Edge weights were normalized using association strength [50] to account for differences in keyword frequency. The network was filtered to include the top 100 keywords by occurrence frequency, ensuring sufficient representation while maintaining analytical tractability. Keywords appearing in fewer than 10 documents were excluded to remove noise from infrequent terms.

D. Clustering Algorithm

Community detection was performed using the Walktrap algorithm [13] which identifies densely connected groups of nodes through random walk analysis. The algorithm operates on the principle that random walks tend to remain within densely connected communities, with transitions between communities being less frequent. The Walktrap algorithm was selected over alternatives such as Louvain and Leiden due to its stability across multiple runs and suitability for weighted networks of moderate size.

E. Temporal Analysis

To examine thematic evolution, the corpus was divided into two periods: early, 2015-2019, and recent, 2020-2025, For each keyword, occurrence frequencies were calculated separately for each period, enabling computation of growth rates as the percentage change from early to recent period. Keywords appearing only in the recent period were classified as emerging terms. Cluster-level growth rates were computed by aggregating keyword frequencies within each cluster.

F. Citation and Geographic Analysis

Citation analysis examined the distribution of citations across documents to identify highly influential works. The top-cited documents were extracted and categorized by thematic focus to understand which research directions achieved greatest impact.

Geographic analysis mapped author affiliations to countries, calculating publication counts and distinguishing single-country publications (SCP) from multiple-country publications (MCP). The international collaboration rate was computed as the MCP ratio for each country.

VI. RESULTS

This section presents the bibliometric findings organized according to the five research questions outlined in Section I. The analysis covers publication trends, thematic clusters, temporal dynamics, geographic distribution, and influential works.

A. *Publication Trends and Corpus Overview (RQ1)*

The final corpus comprises 1,889 documents published between 2015 and 2025, drawn from 492 sources and authored by 5,326 researchers. Conference papers and journal articles account for nearly equal shares of the literature, with 1,076 conference papers and 1,012 journal articles, alongside 115 book chapters and 65 review articles. The average document receives 17.93 citations, indicating moderate scholarly attention across the field.

Publication volume increased from 133 documents in 2015 to a peak of 258 documents in 2023, representing a 94% increase over the decade. The period from 2015 to 2019 produced 547 documents, while 2020 to 2025 contributed 1,340 documents, reflecting a 145% increase in the recent period. Annual output stabilized between 247 and 258 documents from 2022 to 2024, suggesting the field has reached a mature and sustained research trajectory. The 2025 figure of 192 documents represents partial-year data.

Citation patterns reveal a temporal lag consistent with scholarly publishing norms. Documents from 2018 and 2019 achieve the highest average citations per document at 35.81 and 35.44 respectively, while more recent publications from 2023 and 2024 average 11.15 and 5.65 citations respectively, reflecting their shorter exposure to the academic community.

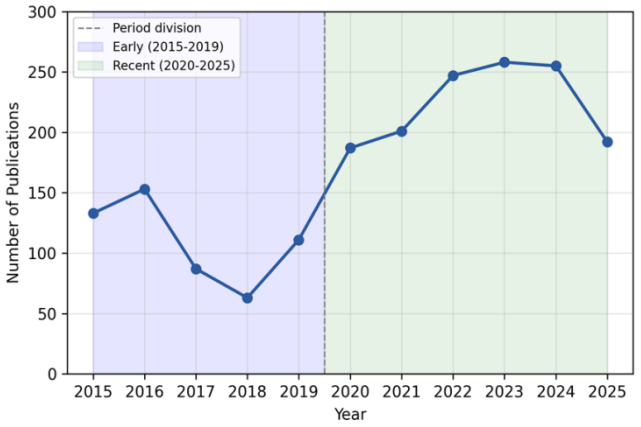

Fig. 3. Annual publication output in SMI cybersecurity research (2015-2025).

B. *Thematic Structure and Research Clusters (RQ2)*

Application of the Walktrap community detection algorithm to the keyword co-occurrence network identified five distinct research clusters. Table 2 summarizes each cluster's composition and network characteristics.

Cluster 1 (SMI Network Architecture) contains 38 keywords with the highest average degree (51.95), indicating strong interconnection with other themes. This cluster encompasses foundational infrastructure concepts. Cluster 3 (Intrusion Detection) groups 19 keywords cantered on detection methodologies, reflecting adoption of data-driven security. The co-occurrence of machine learning, deep learning, and anomaly detection reflects methodological convergence noted in recent surveys [42].

TABLE 2
TOPICS AND KEYWORDS

Cluster	Major Topic	Keywords	Top Keywords	Avg Degree
1	SMI Network Architecture & Infrastructure	38	ami, smart power grids, network security, cybersecurity	51.95
2	Real-Time Monitoring & Data Systems	9	encryption, energy consumption, real-time systems, monitoring	29.33
3	Intrusion Detection & Threat Analytics	19	anomaly detection, cyber attack, machine learning, deep learning	48.84
4	Authentication & Access Control	23	authentication, privacy, security, cryptography, key management	50.30
5	Homomorphic & Differential Privacy	11	privacy preserving, data aggregation, homomorphic encryption	48.27

Cluster 4 (Authentication & Access Control) contains 23 keywords related to authentication protocols. Cluster 5 (Homomorphic & Differential Privacy) represents specialized privacy-preserving techniques with 11 keywords but high average degree (48.27), indicating dense conceptual connections. These privacy themes align with concerns raised by Leszczyna [45] regarding smart grid data protection requirements. Cluster 2 (Real-Time Monitoring) is smallest with 9 keywords and lowest average degree (29.33).

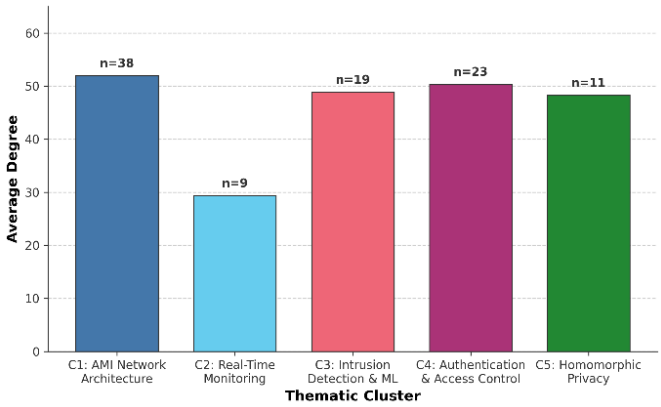

Fig. 4. Average network degree by cluster, with keyword counts (n)

C. *Temporal Evolution and Emerging Themes (RQ3)*

Comparison of keyword frequencies between periods reveals substantial shifts in research priorities. Table 3 presents growth rates for each thematic cluster.

TABLE 3
TOPIC GROWTH RATES

Cluster	Early	Recent	Δ	Rate%	Status
AMI Network Architecture	1,319	2,733	+1,414	107.2	Rapid
Real-Time Monitoring	270	281	+11	4.1	Stable
Intrusion Detection	384	1,673	+1,289	335.7	Rapid
Authentication & Access	1,231	1,814	+583	47.4	Growing
Homomorphic & Differential	320	856	+536	167.5	Rapid

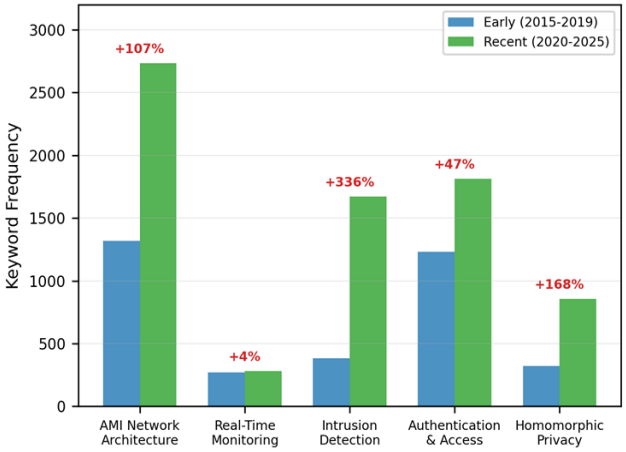

Fig. 5. Average network degree by cluster, with keyword counts (n)

The Intrusion Detection cluster exhibits the highest growth rate at 335.7%, expanding from 384 to 1,673 keyword occurrences. This trajectory reflects accelerating interest in ML-based threat detection, consistent with trends identified by Ghiasi et al. [43]. The Homomorphic & Differential Privacy cluster grew 167.5%, indicating rising attention to mathematical privacy guarantees beyond conventional encryption.
Table 4 includes keyword growth rates.

TABLE 4
KEYWORD GROWTH RATES

Keyword	Early	Recent	Δ	Status
machine learning	21	245	+224	Growing
blockchain	50	265	+215	Growing
cybersecurity	66	278	+212	Growing
anomaly detection	52	221	+169	Growing
deep learning	17	121	+104	Growing
federated learning	0	93	+93	New
fdia	10	87	+77	Growing
differential privacy	34	104	+70	Growing

At the individual keyword level, machine learning shows the largest increase (21→245). Federated learning appeared in 93 recent documents as a new paradigm for privacy-preserving collaborative training. Adversarial machine learning, GANs, and quantum computing each emerged as new topics. The decline of generic encryption (59 → 28) suggests shift toward specialized cryptographic techniques, corroborating observations by Ghosal and Conti [9] on authentication protocol evolution.

D. Geographic Distribution and Collaboration (RQ4)

Research output concentrates in Asia, with China contributing 353 documents (25.5%) and India 224 documents (16.2%). The USA follows with 110 documents (7.9%). Table 5 presents contributing countries and collaboration patterns.
International collaboration rates vary substantially. The UK exhibits the highest rate at 52.9%, with over half of publications involving international co-authors. India and Iran show lower rates (14.7% and 13.3%). The overall international co-authorship rate stands at 27.1%. Citation impact does not correlate directly with volume: Iran achieves 59.67 average citations despite ranking eighth in output, while China averages 17.55.

TABLE 5
CITATION ANALYSIS- GEOGRAPHIC PERSPECTIVE

Country	Pubs	SCP	MCP	Collab%
China	353	254	99	28.0
India	224	191	33	14.7
USA	110	77	33	30.0
United Kingdom	51	24	27	52.9
South Korea	50	29	21	42.0
Australia	45	28	17	37.8
Canada	41	24	17	41.5
Iran	30	26	4	13.3

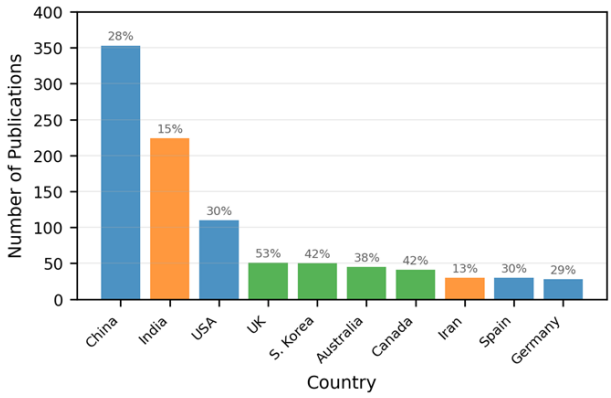

Figure 6. Geographic distribution with international collaboration rates (%)

VII. DISCUSSION

The bibliometric analysis reveals a maturing field characterized by accelerating ML-based security interest, geographic concentration in Asia, and thematic pivot from infrastructure toward detection and privacy-preserving techniques.

A. Field Maturation and Sustained Growth

The cumulative growth in the number of publications indicates that SMI cybersecurity has transitioned from emerging specialty to established subfield. The balance between confer-

ence papers and journal articles reflects a healthy publication ecosystem where preliminary findings develop into archival contributions.

The high average citation count (17.93) indicates sustained scholarly attention, driven by increasing real-world smart meter deployment and corresponding security concerns. The finding that 2018-2019 publications achieve highest per-document citations aligns with typical citation accumulation windows in engineering fields.

B. Thematic Shifts Toward Machine Learning

The 335.7% growth in Intrusion Detection represents the dominant recent trend. This shift reflects broader ML adoption across cybersecurity, but the magnitude in SMI context likely stems from unique smart meter data characteristics: high dimensionality, temporal regularity, and consumption patterns enabling anomaly-based detection. Similar trends were noted by Kim et al. [40] in their analysis of smart grid defense mechanisms.

The emergence of specific architectures (CNNs, LSTMs, GANs) indicates methodological sophistication beyond generic ML approaches. Federated learning's appearance in 93 documents addresses a fundamental tension: need for large training datasets versus privacy constraints limiting data centralization. This enables collaborative model training without raw data sharing, particularly suited to utility contexts.

The emergence of adversarial machine learning signals growing awareness that ML-based detectors themselves become attack surfaces. Adversarial examples crafted to evade detection represent second-generation threats the field is beginning to address.

C. Evolution of Privacy Research

The 167.5% growth in Homomorphic & Differential Privacy indicates shift from generic encryption toward mathematically rigorous frameworks providing formal guarantees. Homomorphic encryption enables computation on encrypted data, allowing utilities to perform billing and analytics without accessing plaintext records. Differential privacy provides quantifiable privacy loss bounds.

The relative decline of generic encryption does not indicate abandonment but rather diversification into specialized applications. This evolution aligns with privacy requirements documented in smart grid standards [43] and authentication protocol surveys [10].

D. Geographic Implications

The concentration in China and India (41.7% combined) reflects aggressive smart grid deployment programs. China's State Grid Corporation operates the world's largest smart meter network, providing both motivation and data access. The disparity in international collaboration rates carries implications for knowledge transfer and security standardization. Countries with high collaboration rates may achieve faster integration of international best practices, while domestically focused communities risk developing solutions misaligned with global standards. The absence of correlation between publication volume and citation impact indicates research quality is not geographically determined.

E. Implications of Emerging Keywords

Quantum computing's appearance (15 documents) signals early preparation for post-quantum cryptography. Current SMI protocols rely on assumptions vulnerable to quantum algorithms. While practical quantum computers remain years away, the 10-20 year smart meter lifespan creates urgency for quantum-resistant protocol development.

Blockchain's growth (50 → 265) positions it among largest increases. Applications span peer-to-peer energy trading, decentralized identity management, and tamper-evident audit logging. Sustainability depends on resolution of scalability and energy consumption concerns.

VIII. CONCLUSION

This study presented a bibliometric analysis of 1,889 SMI cybersecurity documents (2015-2025) from Scopus and IEEE Xplore. The analysis employed keyword co-occurrence networks with Walktrap community detection [13] to identify thematic clusters and compared keyword frequencies across early (2015-2019) and recent (2020-2025) periods.

Five principal findings emerged. First, SMI cybersecurity research has matured into a sustained subfield, with annual output stabilizing at ~250 documents. The corpus demonstrates balanced contributions from conferences and journals. Second, the thematic structure comprises five clusters: SMI Network Architecture, Real-Time Monitoring, Intrusion Detection, Authentication & Access Control, and Homomorphic & Differential Privacy.

Third, the field has undergone pronounced methodological shift toward ML-based security. The Intrusion Detection cluster grew 335.7%, driven by deep learning adoption and emerging techniques including federated learning and adversarial ML. Fourth, privacy research evolved from generic encryption toward mathematically rigorous frameworks with 167.5% growth in homomorphic and differential privacy techniques.

Fifth, research output concentrates in Asia, with China and India contributing 41.7% of corresponding authorships. International collaboration rates vary from 52.9% (UK) to 13.3% (Iran), suggesting uneven integration into global knowledge networks.

The bibliometric trends suggest priority directions: adversarial robustness evaluation and model interpretability for ML-based detection; federated learning protocols for cross-utility collaboration; bridging analytics research and operational deployment; and post-quantum cryptographic protocols for long-lifespan SMI systems.

As smart metering infrastructure expands globally, security challenges will intensify. Bibliometric analysis indicates that while researchers are actively tackling these challenges, ongoing efforts to implement theoretical breakthroughs into practical, real-world SMI security measures are crucial to achieving robust and privacy-aware smart metering systems.

REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G. P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," in *IEEE Trans. Ind. Inform.*, vol. 7, no. 4, pp. 529–539, Nov. 2011, DOI: 10.1109/TII.2011.2166794

[2] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," in *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019, DOI: 10.1109/TSG.2018.2818167

[3] W. Wang and Z. Lu, "Cyber Security in the Smart Grid: Survey and Challenges," in *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013, DOI: 10.1016/j.comnet.2012.12.017

[4] D. Radovanovic, A. Unterweger, G. Eibl, D. Engel, and J. Reichl, "How Unique is Weekly Smart Meter Data?," in *Energy Informatics*, vol. 5, no. S1, p. 13, Sept. 2022, DOI: 10.1186/s42162-022-00205-8

[5] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, May 2009, DOI: 10.1109/MSP.2009.76

[6] J. M. Nambundo, O. De Souza Martins Gomes, A. D. De Souza, and R. C. S. Machado, "Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review," in *Energies*, vol. 18, no. 6, p. 1445, Mar. 2025, DOI: 10.3390/en18061445

[7] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," SANS Industrial Control Systems, 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/analysis-cyber-attack-ukrainian-power-grid-36235

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012, DOI: 10.1109/SURV.2012.010912.00035

[9] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic Survey of Advanced Metering Infrastructure Security: Vulnerabilities, Attacks, Countermeasures, and Future Vision," in *Future Generation Computer Systems*, vol. 136, pp. 358–377, Nov. 2022, DOI: 10.1016/j.future.2022.06.013

[10] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019, DOI: 10.1109/COMST.2019.2907650

[11] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," *in IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019, DOI: 10.1109/COMST.2019.2899354

[12] M. Aria and C. Cuccurullo, "Bibliometrix : An R-tool for Comprehensive Science Mapping Analysis," *Journal of Informetrics*, vol. 11, no. 4, pp. 959–975, Nov. 2017, DOI: 10.1016/j.joi.2017.08.007

[13] P. Pons and M. Latapy, "Computing Communities in Large Networks Using Random Walks," *Computer and Information Sciences - ISCIS 2005*, Berlin Heidelberg, 2005, pp. 284–293, vol. 3733, DOI: 10.1007/11569596_31

[14] N. S. Suresh, N. S. Padmavathy, S. A. Daniel, and R. Kappagantu, "Smart Grid Implementations and Feasibilities," in *Integration of Renewable Energy Sources with Smart Grid*, 1st edition, Wiley, 2021, pp. 327–346. DOI: 10.1002/9781119751908.ch15

[15] Bundesministerium für Wirtschaft und Energie, "Was Sind Eigentlich 'Smart Grids'?" [Online]. Available: https://energiewende.bundeswirtschaftsministerium.de/EWD/Redaktion/Newsletter/2019/05/Meldung/direkt-erklaert.html

[16] National Institute of Standards and Technology (NIST), "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 1108R2, Feb. 2012. [Online]. Available: https://www.nist.gov/system/files/documents/smartgrid/NIST_Framework_Release_2-0_corr.pdf

[17] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication Network Requirements for Major Smart Grid Applications in HAN, NAN and WAN," in *Computer Networks*, vol. 67, pp. 74–88, July 2014, DOI: 10.1016/j.comnet.2014.03.029

[18] I. Rigoev and A. Sikora, "Security Aspects of Smart Meter Infrastructures," *Smart Meters*, vol. 97, Springer, 2023, pp. 77–154. DOI: 10.1007/978-3-031-27556-2_5

[19] IBM, "What are Smart Meters?" 2025. [Online]. Available: https://www.ibm.com/topics/smart-meter

[20] D. Abraham, S. H. Houmb, and L. Erdodi, "Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation," in *Applied Sciences*, vol. 15, no. 17, p. 9233, Aug. 2025, DOI: 10.3390/app15179233

[21] S. G. C. Insights, *Energy Security Sentinel™*., 2022

[22] K. Susantha, D. Lu, and X. Wang, "Lessons Learned from Previous Cyberattacks on Energy Systems – Global and Australian Context," in *2023 IEEE International Future Energy Electronics Conference (IFEEC)*, Sydney, Australia: IEEE, Nov. 2023, pp. 550–554. DOI: 10.1109/IFEEC58486.2023.10458537.

[23] Wikipedia contributors, "Stuxnet — Wikipedia, The Free Encyclopedia." 2024. [Online]. Available: https://en.wikipedia.org/wiki/Stuxnet

[24] Symantec, "Dragonfly Threat Against Western Energy Suppliers." 2014. [Online]. Available: https://docs.broadcom.com/doc/dragonfly

[25] J. Don, "Lessons Learned from a Forensic Analysis of The Ukrainian Power Grid Cyberattack." 2017. [Online]. Available: https://blog.isa.org/lessons-learned-forensic-analysis

[26] B. Johnson, "Attackers Deploy new ICS Attack Framework 'Triton.'" 2017. [Online]. Available: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton

[27] M. H. M.A, "Hackers Targeting US Nuclear Power Plants, Report Finds" 2017. [Online]. Available: https://www.linkedin.com/pulse/hackers-targeting-us-nuclear-power-plants-report-finds-hamdan-mba/

[28] R. Walton, "Malware Found in Entergy's corporate Network Raises MISO Alert." 2018. [Online]. Available: https://www.utilitydive.com/news/malware-found-in-entergys-corporate-network-raises-miso-alert/516681/

[29] C. Krauss, "Cyberattack Shows Vulnerability of Gas Pipeline Network." 2018. [Online]. Available: https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html

[30] CISA, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." 2018. [Online]. Available: https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical

[31] S. Coble, "REvil Claims Responsibility for Invenergy Hack." 2021. [Online]. Available: https://www.infosecurity-magazine.com/news/revil-claims-responsibility-for/

[32] R. Goswami, "SEC sues SolarWinds over Massive Cyberattack." 2023. [Online]. Available: https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html

[33] F. Sanders, "Hacker leaks 70GB of Data From Pipeline Operator — Ransomware." 2021. [Online]. Available:

https://www.techtimes.com/articles/261201/20210608/hacker-leaked-70gb-data-dark-web-ransomware-attack-linestart.htm
[34] M. Brignall, “Npower Withdraws Mobile App After Hackers Steal Personal Details.” 2021. [Online]. Available: https://www.theguardian.com/business/2021/feb/27/npower-mobile-app-hackers-personal-details
[35] J. Menn, “Ransomware Attack on Australian Utility Claimed by Russian-Speaking Criminals.” 2021. [Online]. Available: https://www.reuters.com/
[36] H. Edwardes-Evans, “UK Utility Services Provider Fulcrum Alerts Market to Cyber Incident.” 2022. [Online]. Available: https://www.spglobal.com/commodityinsights/
[37] B. News, “Italy’s Energy Agency Suffered Malware Attack.” 2022. [Online]. Available: https://www.bloomberg.com/news/articles/2022-08-29/italy-s-energy-agency-suffered-malware-attack-halted-it-systems
[38] A. Meehan, “Lithuanian Energy Firm Disrupted by DDoS Attack.” 2022. [Online]. Available: https://www.infosecurity-magazine.com/news/lithuanian-energy-ddos-attack/
[39] M. Gooding, “Ragnar Locker Ransomware Hits Greek gas Supplier DESFA.” 2022. [Online]. Available: https://techmonitor.ai/technology/cybersecurity/desfa-cyberattack-ragnar-locker-ransomware
[40] Cybersecurity Review, “Denmark Energy Cyber Attack Highlights Infrastructure Security Gaps.” [Online]. Available: https://www.cybersecurity-review.com/denmark-energy-cyber-attack-highlights-infrastructure-security-gaps/
[41] R. Dosumu, “MOVEit Data Breach: A Case Study in Zero-Day Exploits and Organizational Cybersecurity Preparedness,” 2025, DOI: 10.13140/RG.2.2.17029.26081.
[42] Y. Kim, S. Hakak, and A. Ghorbani, “Smart Grid Security: Attacks and Defence Techniques,” *IET Smart Grid*, vol. 6, no. 2, pp. 103–123, Apr. 2023, DOI: 10.1049/stg2.12090
[43] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, “A Comprehensive Review Of Cyber-Attacks And Defense Mechanisms For Improving Security In Smart Grid Energy Systems: Past, Present And Future,” *Electric Power Systems Research*, vol. 215, p. 108975, Feb. 2023, DOI: 10.1016/j.epsr.2022.108975
[44] M. A. Husnoo, A. Anwar, N. Hosseinzadeh, S. N. Islam, A. N. Mahmood, and R. Doss, “False Data Injection Threats in Active Distribution Systems: A Comprehensive Survey,” 2021, *arXiv*. DOI: 10.48550/ARXIV.2111.14251
[45] R. Leszczyna, “A Review of Standards With Cybersecurity Requirements for Smart Grid,” *Computers & Security*, vol. 77, pp. 262–276, Aug. 2018, DOI: 10.1016/j.cose.2018.03.011
[46] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey,” *Internet Things*, vol. 14, p. 100111, June 2021, DOI: 10.1016/j.iot.2019.100111
[47] A. S. Mathew and A. Sikora, “State of the Art in Smart Metering Infrastructure Security: A Keyword Co-Occurrence Analysis,” *60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, Ohrid, North Macedonia: IEEE, June 2025, pp. 1–6. DOI: 10.1109/ICEST66328.2025.11098305.
[48] P. O. Ajiboye, K. O.-B. O. Agyekum, and E. A. Frimpong, “Privacy and Security of Advanced Metering Infrastructure (AMI) Data and Network: A Comprehensive Review,” *Journal of Engineering and Applied Science*, vol. 71, no. 1, p. 91, Dec. 2024, DOI: 10.1186/s44147-024-00422-w
[49] C.-C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021, DOI: 10.1109/TSG.2020.3010230
[50] N. J. Van Eck and L. Waltman, “Software Survey: Vosviewer, a Computer Program for Bibliometric Mapping,” *Scientometrics*, vol. 84, no. 2, pp. 523–538, Aug. 2010, DOI: 10.1007/s11192-009-0146-3