Journal of Information Systems and Informatics
Vol. 7, No. 3, September 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i3.1154 Published By DRPM-UBD

Bibliometric Analysis of Cybersecurity Research Trends in Bangladeshi Educational Institutions (2020-2025)

Khadija Sharmin

Department of Management Information Systems, Begum Rokeya University, Rangpur, Bangladesh
E-mail: khadijasharmin@mis.brur.ac.bd; ORCID iD: 0009-0008-0814-0442

Abstract

This study provides a bibliometric analysis of cybersecurity research in Bangladeshi educational institutions from 2020 to mid-2025. Using data from the Scopus database and tools like R and VOSviewer, the results show a steady increase in research output, from 23 publications in 2020 to 77 in 2024, with projections for continued growth in 2025. Key research areas include network security, machine learning, deep learning, and blockchain technologies. Rajshahi University of Engineering and Technology has been a leading institution, with Md. Alamgir Hossain (State University of Bangladesh) being a prominent contributor, publishing 15 articles and accumulating 358 citations. International collaborations have enhanced Bangladesh's global standing in cybersecurity. These findings highlight Bangladesh's increasing role in cybersecurity research, with implications for addressing local challenges and strengthening national cybersecurity resilience.

Keywords: Cybersecurity, Bibliometric Analysis, Research Trends, Bangladesh, Network Security.

1. INTRODUCTION

The rapid advancement and integration of Artificial Intelligence (AI) into digital systems have transformed the cybersecurity landscape, introducing both unprecedented opportunities and novel threats. In this era, cybersecurity research is more critical than ever to ensure the security, privacy, and resilience of digital infrastructure [1]. As Bangladesh undergoes rapid digital transformation, the nation is increasingly vulnerable to cyber threats that jeopardize its critical infrastructure, confidential data, and overall national security [2], [3], [4]. One notable example of this vulnerability was the 2016 Bangladesh Bank heist, in which cybercriminals exploited vulnerabilities in the international financial system to steal $81 million, highlighting the severe risks posed by cyberattacks on financial institutions [5]. This attack, which targeted Bangladesh's central bank, illustrates how critical national assets can be at risk, emphasizing the need for strong cybersecurity defenses. Research shows that public awareness and technical preparedness in cybersecurity remain insufficient, leaving the nation vulnerable to attacks on both government and private sectors [6]. As educational institutions increasingly digitize their operations and data, they become prominent targets for cyberattacks [7].

Therefore, fostering strong and continuous cybersecurity research within Bangladeshi universities is essential—not only to develop technical solutions and frameworks tailored to local needs but also to cultivate a skilled workforce and a culture of cyber awareness [7], [8]. The more research activity occurs in these institutions, the more Bangladesh will benefit. Universities can generate knowledge, train experts, and drive innovation in cybersecurity, all of which are critical for building national resilience and supporting the country's ambitions for a secure digital future [4], [7], [8]. Academic research can inform national policy, improve incident response, and facilitate collaboration between government, industry, and international partners, ensuring that Bangladesh stays ahead of evolving cyber threats [2], [3], [9].

However, prior research is often limited by a narrow focus on awareness or technology adoption, small sample sizes, and a lack of systematic, data-driven mapping of research trends and collaboration networks within Bangladeshi educational institutions [5], [10]. No previous study has comprehensively mapped the scholarly landscape of cybersecurity research in Bangladeshi educational institutions using bibliometric methods. There is a clear gap in understanding the evolution of research themes, author influence, institutional contributions, and international collaborations [10]. Moreover, while global studies have examined cybersecurity research trends, they often overlook the contributions and challenges specific to South Asian nations like Bangladesh [11], [12]. Existing bibliometric studies often focus on broader cybersecurity issues or technologies, leaving the regional context of South Asian countries unexplored [11]. The limited attention to Bangladesh's unique challenges and contributions highlights the need for a more localized, data-driven approach to understanding cybersecurity research within this context.

This study addresses these gaps by providing the first bibliometric analysis of cybersecurity research trends, leading journals, influential authors, and collaborations within Bangladeshi educational institutions from 2020 to mid-2025. While global studies have contributed valuable insights, they often fail to capture the specific needs and challenges faced by countries like Bangladesh, where cybersecurity research is still in its nascent stages [11]. By systematically analyzing publication patterns, citation networks, and thematic evolution, this research offers a novel, data-driven perspective. This study also seeks to fill this gap by conducting a bibliometric analysis of cybersecurity research in Bangladeshi institutions, focusing on publications from 2020 to mid-2025.

2. RESEARCH METHODOLOGY

2.1. Data source and Search strategy

This study employed a bibliometric methodology to systematically analyze cybersecurity-related research within Bangladeshi educational institutions. Bibliometric analysis involves the quantitative evaluation of academic literature, enabling researchers to identify publication trends, influential works, and collaboration networks. Bibliometric methods, often known as "analysis," are increasingly widely used in research evaluation, particularly in scientific and practical disciplines [13], [14], [15], [16]. The scholarly literature for this bibliometric study was gathered from the world- renowned online library database "SCOPUS” on May 26, 2025.

This study retrieved a total of 340 items based on the search query shown in Table 1. Following exclusions, 302 (Table 2) papers were selected for bibliometric analysis in the current study. The study just utilized the terms “Cybersecurity” OR “Information Security” OR “Network Security” OR “Data Protection” OR “Cyber Threats” OR “Cyber Attacks” OR “Digital Security” OR “Cyber Risk Management” and “Educational Institutions in Bangladesh” OR “Bangladeshi Universities” OR “Bangladeshi Schools” OR “Higher Education in Bangladesh” OR “Bangladeshi Colleges” OR “Academic Institutions in Bangladesh” OR “Education Sector in Bangladesh” exploring several keyword combinations in order to thoroughly address certain elements. Applying inclusion and exclusion criteria led to the identification of 302 research publications as unique and relevant; 38 publications were subsequently eliminated from the study. To enhance the reliability of data collection, duplicate records were removed, and only English-language, peer-reviewed articles, reviews, and conference papers were retained**.** Articles from predatory journals or irrelevant domains were excluded. To reduce bias from author self-citations, citation analysis was cross-verified, and no author was allowed to contribute more than 10% of total citations analyzed. Data validation was ensured by manually screening titles, abstracts, and keywords to confirm relevance.

Table 1. Search results of publications.

Keywords	Results
KEY ((“Cybersecurity” OR “Information Security” OR “Network Security” OR “Data Protection” OR “Cyber Threats” OR “Cyber Attacks” OR “Digital Security” OR “Cyber Risk Management”) AND (“Educational Institutions in	340 articles

Keywords	Results
Bangladesh" OR "Bangladeshi Universities" OR "Bangladeshi Schools" OR "Higher Education in Bangladesh" OR "Bangladeshi Colleges" OR "Academic Institutions in Bangladesh" OR "Education Sector in Bangladesh"))	

Table 2. Filtered and refined results of publications.

Keywords	Results
KEY (("Cybersecurity" OR "Information Security" OR "Network Security" OR "Data Protection" OR "Cyber Threats" OR "Cyber Attacks" OR "Digital Security" OR "Cyber Risk Management") AND ("Educational Institutions in Bangladesh" OR "Bangladeshi Universities" OR "Bangladeshi Schools" OR "Higher Education in Bangladesh" OR "Bangladeshi Colleges" OR "Academic Institutions in Bangladesh" OR "Education Sector in Bangladesh"))	302 Articles

2.2. Research Protocol

The research protocol followed a systematic approach, as illustrated in Figure 1. In the first step (Figure 1), a keyword selection process was carried out to define the search terms. In the searching process the fields like title, abstract and keywords are considered. The study focused on literature from the renowned database SCOPUS, collected on May 26, 2025, covering 340 relevant publications from various disciplines. Figure 1: Overview of the Bibliometric Research Process.

1) Keyword Definition: Terms related to cybersecurity and Bangladeshi education were defined based on prior literature and refined iteratively.
2) Database Search: SCOPUS was searched using Boolean operators applied to title, abstract, and keyword fields.
3) Initial Screening: A total of 340 results were obtained.
4) Inclusion/Exclusion: Documents such as working papers, white papers, non-English content, and duplicates were excluded.

5) Data Cleaning: Duplicate entries and irrelevant papers were removed. Author affiliations were normalized to group variants (e.g., "Dhaka Univ." and "University of Dhaka").
6) Final Selection: 302 articles were retained after applying the criteria.
7) Analysis: Bibliometric tools (e.g., VOSviewer, Biblioshiny) were used to explore publication trends, citation networks, and collaborative patterns. This tool allows to extract citation patterns, collaboration networks, and keyword co-occurrence data from the selected articles. VOSviewer was used to create visual representations of co-authorship networks and citation clusters. Both R and VOSviewer provided complementary insights, allowing for a comprehensive understanding of the data, from quantitative metrics to visual network structures. These tools are essential for transforming raw bibliometric data into actionable insights, making the methodology more accessible and transparent.

This protocol ensures transparency, reproducibility, and consistency in the analysis. The dataset consisted of 302 research articles authored by 1090 individuals. Only 9 were single-authored papers, confirming a strong collaborative trend. The global co-authorship rate was found to be 68.21%, suggesting significant international and inter-institutional collaboration.

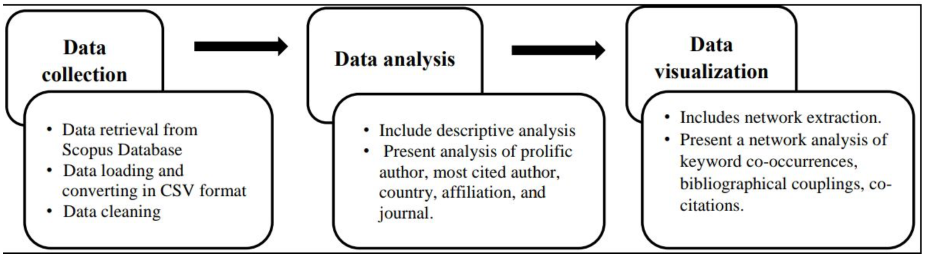
Data collection
Data retrieval from Scopus Database
Data loading and converting in CSV format
Data cleaning
Data analysis
Include descriptive analysis
Present analysis of prolific author, most cited author, country, affiliation, and journal.
Data visualization
Includes network extraction.
Present a network analysis of keyword co-occurrences, bibliographical couplings, co-citations.

Figure 1. Searching, inclusion and exclusion criteria of the collected articles

2.3. Type of Document

The data presented in Table 3 reveals significant insights into the publication patterns in the field of cybersecurity research within Bangladeshi educational institutions. All the collected documents are scholarly articles, which are considered the most reliable and authoritative sources of academic information. These articles, primarily peer-reviewed, ensure a high level of credibility, which is essential for the validity of research in cybersecurity. Articles offer detailed methodologies, results, and discussions, making them a crucial resource for understanding the complex nature of cybersecurity challenges and solutions.

Table 3 highlights a substantial number of articles collected over the 2020-2024 period, emphasizing their importance in the Bangladeshi cybersecurity research landscape. Articles are typically more comprehensive than other types of documents, such as conference papers or books, due to their thorough peer-review process. This process ensures the scholarly rigor required for advancing knowledge in the field of cybersecurity. Furthermore, journal articles in cybersecurity are often cited extensively, reflecting their academic impact and influence.

In the context of Bangladeshi educational institutions, the dominance of articles in the dataset suggests that researchers prefer to disseminate their findings through peer-reviewed journals. This preference underscores the importance of journal articles in providing validated information that informs both theoretical advancements and practical applications in cybersecurity. The articles' prominence in this dataset also signals the growing importance of robust academic research in addressing cybersecurity challenges in the educational sector. This data is crucial for mapping the evolution of cybersecurity research and understanding how Bangladeshi institutions contribute to global cybersecurity knowledge.

Table 3. Main Information about the collected articles of cybersecurity research in Bangladeshi Educational Institutions

Main Information	**Explanation**	**No.**
Timespan	Period of Time	2020:2025
Documents	Total Number of Articles	302
Sources (Journals, Books, etc.)	The frequency distribution of sources	182
Annual Growth Rate	No of Publication Growth per year (%)	20.73
Document Average Age	Mean Publication Age since Release	2
Average Citation	Per Doc Citation	19.72
Authors Keywords	Total Number of Keywords	1182
Authors	No. Of total authors	1090
Authors of single authored articles	Number of single authors per article	9
International Co-authorship (%)	Percent of international co-publication	68.21
Article	Document Type	302

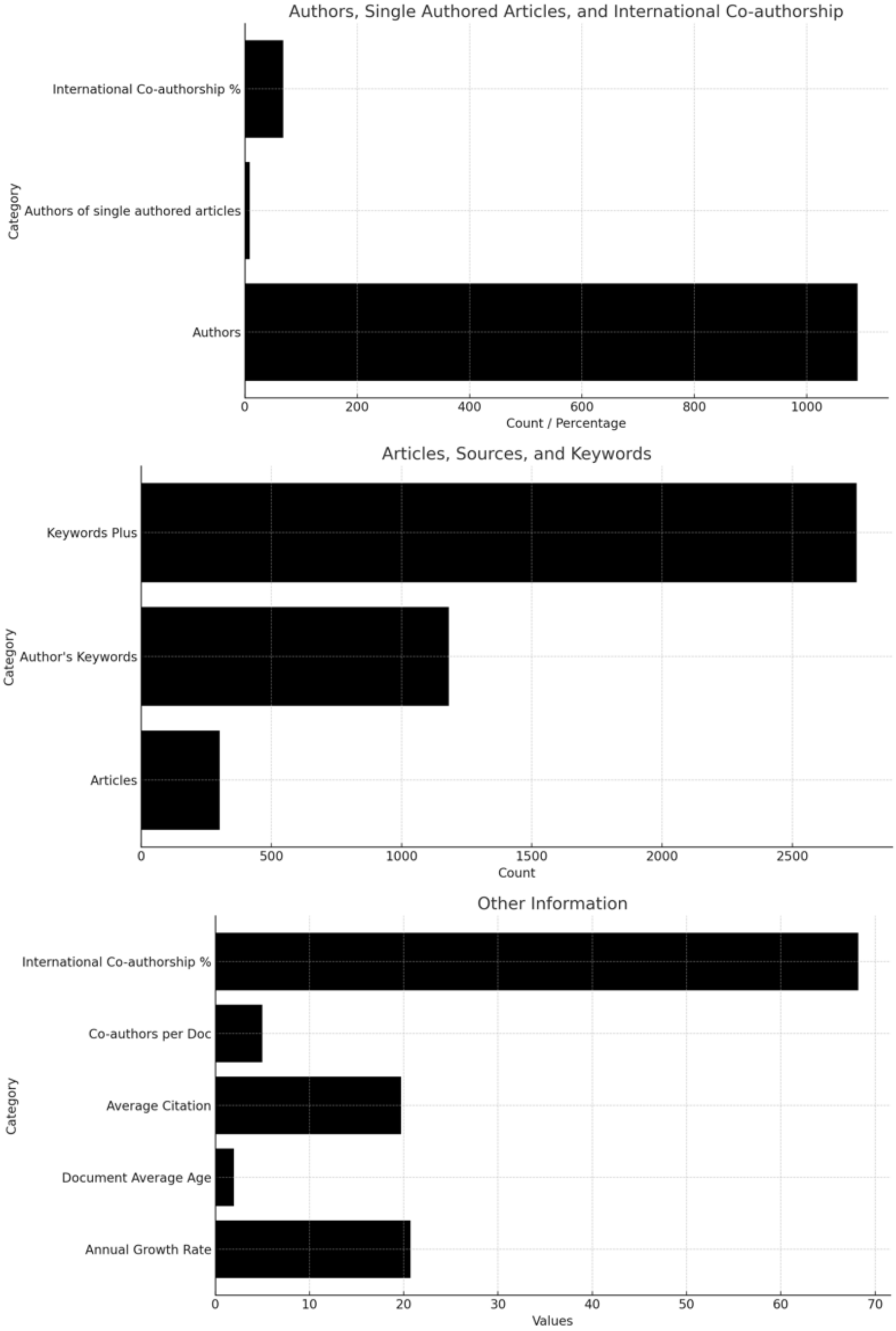

Figure 2. Main information about the collected articles of artificial intelligence in information systems

The detailed information for the selected articles is shown in Table 3. A total of 302 research articles were produced by 1090 authors who contributed to various aspects of cybersecurity research in Bangladeshi educational institutions. Of these, only 9 authors wrote single-authored papers, with the bulk of the research being the result of collaborative efforts. Additionally, the global rate of co-authorship in cybersecurity research stands at 68.21%, underscoring the international collaboration involved, reflecting the cooperative nature of addressing cybersecurity issues.

2.4. Methodological Limitations

Despite the robustness of bibliometric methods, this study acknowledges several limitations:

1) Quantitative Focus: Bibliometric analysis emphasizes quantitative indicators (e.g., citation counts), which may overlook the qualitative depth of publications.
2) Database Bias: The study relies solely on SCOPUS, potentially missing relevant works indexed elsewhere.
3) Author and Institutional Bias: Highly cited authors or institutions may dominate the network, affecting diversity.
4) Self-Citation Risk: Despite attempts to control it, some self-citation bias may persist.

Future studies may benefit from integrating content analysis or qualitative methods to enrich the bibliometric findings.

2.5. Bibliometric Analysis

This study employed the R programming language and the VOSviewer Bibliometrix package for analysis and visualization, tools that can be incorporated into a comprehensive data analysis workflow [17], [18], [19]. R is used to analyze yearly production, citations, co-citations, and co-authorships with tools like Bibliometrix. On the other hand, VOSviewer helps visualize networks like term co-occurrence and bibliographic coupling through clustering and density mapping. For data collection, information was retrieved from the Scopus database, then converted into CSV format. The data was analyzed to provide details like key authors, journals, countries, and affiliations. In the final step, the data was visualized using network analysis. The settings for VOSviewer included using fractional counting and limiting the number of authors per document to 25.

3. RESULTS AND DISCUSSION

3.1. Analysis of yearly Research Volume

The period from 2020 to 2025 shows a consistent increase in cybersecurity research within Bangladeshi educational institutions, as shown in Figure 3. In 2020, 23 articles were published, marking the beginning of focused research activity in this area. The number of publications rose to 42 in 2021, reflecting an expanding interest in cybersecurity. The growth continued in 2022, with 43 articles published, indicating sustained academic engagement. The number of publications saw a significant rise in 2023, with 58 articles, signaling a surge in research output. In 2024, the number of publications peaked at 77, indicating a substantial increase in academic attention to the subject. As of May 25, 2025, 59 articles have already been published, and this number is expected to rise, potentially exceeding the total publications of 2024 by the end of the year.

This bibliometric analysis illustrates the growing importance of cybersecurity research in Bangladeshi educational institutions from 2020 to 2025, with a continuing upward trajectory in research output. The data for 2025, showing 59 articles in the first five months, suggests a continued and accelerating interest in the field.

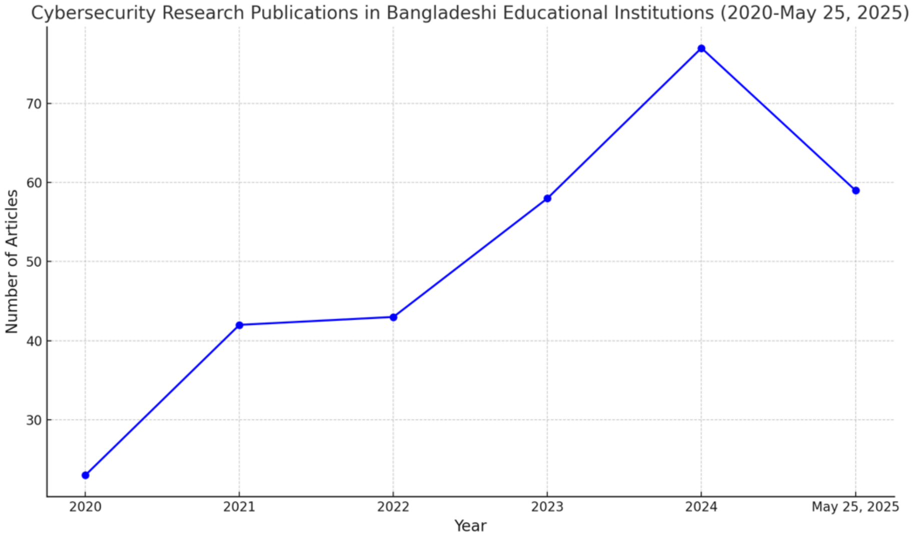

Figure 3. Yearly research volume of Cybersecurity in Bangladeshi Educational Institutions

3.2. Authors who are highly productive and influential

By analyzing the data in Table 4, we can identify the authors who have made the most significant contributions to the field of cybersecurity. Md. Alamgir Hossain (State University of Bangladesh) and Md. Rashidul Islam (Rajshahi University of Engineering and Technology) are two of the most influential authors in the field of cybersecurity in Bangladesh. Md. Alamgir Hossain has published 15 articles in the cybersecurity domain and holds an h-index of 9, with a total of 358 citations across his body of work. Although his citation count is relatively moderate, his consistent publication in cybersecurity positions him as one of the key contributors in this field in Bangladesh. On the other hand, Md. Rashidul Islam has also contributed 15 articles in cybersecurity, and with an h-index of 12, he has accumulated 517 citations. His higher h-index and citation count reflect his growing influence and recognition in the cybersecurity community, indicating a slightly higher impact than Hossain in the field.

Based on the h-index, total citations (TC), and number of publications (NP) in the cybersecurity domain, it was determined that Iqbal H. Sarker (Edith Cowan University, Australia) is also one of the leading authors in the field, with the highest h-index of 48 and a total of 17,999 citations. While his total citations reflect his broader body of work across multiple research areas, his 10 publications focused on cybersecurity have contributed to his prominence in the field. This highlights his exceptional impact and extensive recognition within cybersecurity, along with his broader academic influence. Md. Shahadat Hossain (University of Chittagong, Bangladesh) follows closely with an h-index of 45 and 6,165 citations from his cumulative body of work across various research domains, including cybersecurity. His contributions in cybersecurity, reflected through his 10 publications in the field, further solidify his impact.

Table 4: Top productive and contributing authors of Cybersecurity Research in Bangladesh

Rank	Author	Affiliation	Country	h-index	TC	NP
1	HOSSAIN MA (Md. Alamgir Hossain)	State University of Bangladesh	Bangladesh	9	358	15
2	ISLAM MR (Md. Rashidul Islam)	Rajshahi University of Engineering and Technology	Bangladesh	12	517	15
3	RAHMAN MA (Md. Atiqur Rahman)	East West University Dhaka	Bangladesh	13	450	13

Rank	Author	Affiliation	Country	h-index	TC	NP
4	RAHMAN A. (Anichur Rahman)	National Institute of Textile Engineering and Research, Const. of DU	Bangladesh	27	2649	12
5	ISLAM MS (Md. Saiful Islam)	Bangladesh University of Engineering and Technology	Bangladesh	19	2423	11
6	HOSSAIN MS (Mohammad Shahadat Hossain)	University of Chittagong	Bangladesh	45	6165	10
7	SARKER IH (Iqbal H. Sarker)	Edith Cowan University (ECU)	Australia	48	17999	10
8	ANWAR A. (Adnan Anwar)	Deakin University	Australia	40	5205	7
9	FARUQUI N (Nuruzzaman Faruqui)	Daffodil International University	Bangladesh	16	770	7
10	ISLAM MM (Md. Manowarul Islam)	Jagannath University	Bangladesh	21	2133	7

Additionally, the analysis of the collaboration network (Figure 4) provides deeper insights into the relationships between these authors and their co-authors in cybersecurity. The size of each node corresponds to the number of publications in cybersecurity, while the edges between the nodes represent the level of collaboration among the authors [20]. The red cluster is the most prominent and represents a highly productive and influential group. It includes Hossain MA, Islam MR, Rahman MA, and Islam MS, who have worked together on a significant number of cybersecurity publications. Their central position in this cluster and their high citation counts reflect their leadership in the field. Hossain MA plays a pivotal role in driving research in this area, as shown by his extensive collaborative work and high citation impact.

In the orange cluster, we see the collaboration between Rahman A and Rahman MA, indicating another tightly knit research group. Despite being slightly smaller, this cluster shows how these researchers have contributed to advancing cybersecurity, highlighting their significant work in the field. The purple cluster, which includes authors like Uddin MA and Islam MM, is a smaller, more specialized group. These authors, while having fewer publications and citations compared to the central figures in the red and orange clusters, still play an important role in contributing to more focused areas of cybersecurity research. Finally, the green cluster with authors like Faruqui N, Barros A, and Vhaidzzaman M, represents a niche group of researchers, showcasing the diversity of topics and expertise within cybersecurity.

Figure 4 illustrates a network of highly interconnected researchers, with Hossain MA, Islam MR, and Rahman MA at the core. These authors dominate the field not only due to their individual research productivity but also because of their strong collaborative efforts. The red cluster's prominence indicates their significant contributions to the cybersecurity domain, further emphasized by their extensive publications and broader citation impact.

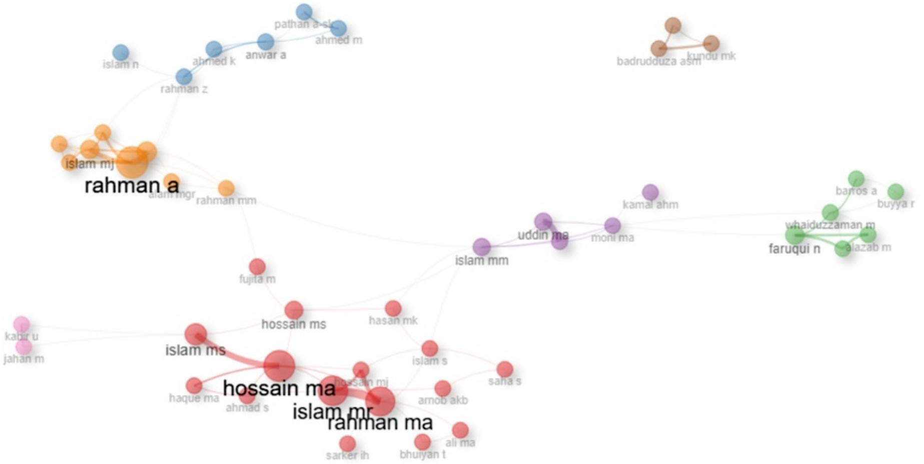

Figure 4. Cluster of author's collaboration in Cybersecurity Research in Bangladesh.

3.3. Major journals for the published articles

A comprehensive list of reputable journals has been compiled that regularly publish scholarly articles in the field of cybersecurity. According to the analysis, IEEE ACCESS stands out as the leading journal, contributing 31 publications, making up 47.7% of the total publications in the dataset. Other significant sources include ELECTRONICS (SWITZERLAND) with 5 publications (7.7%) and SENSORS with 7 publications (10.8%). Additionally, COMPUTERS, MATERIALS AND CONTINUA contributed 4 publications (6.2%) while CYBERSECURITY, ENERGIES, and IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS each contributed 3 publications (4.6%). Other journals like SECURITY AND COMMUNICATION NETWORKS, WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, and ALGORITHMS made smaller contributions, reflecting their specialized focus within cybersecurity. Figure 5 represents the exact distribution of publications across these sources, with IEEE ACCESS being the most prominent journal, accounting for nearly half of the total publications in this area.

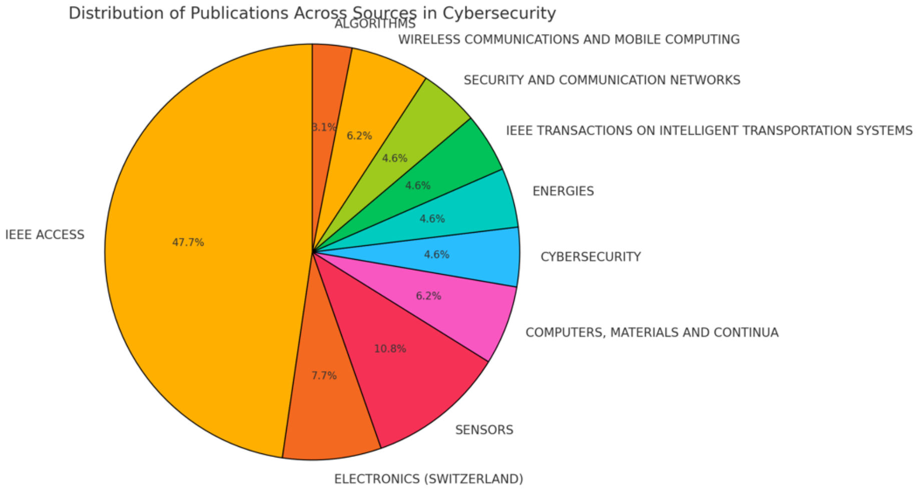

Figure 5. Top 10 journals for the published articles of Cybersecurity Research in Bangladesh

3.4. Country-specific analysis of the articles

The country rankings in Table 5 were generated using R programming (Bibliometrics package), which analyzes the total number of publications contributed by each country. According to the analysis, Bangladesh holds the top position, followed by Australia, Malaysia, USA, and Saudi Arabia, based on their respective publication counts over the years. This ranking highlights Bangladesh as the leading country in terms of total articles published, with Australia and Malaysia contributing significantly as well. Bangladesh saw a sharp increase in publications, with a steady rise in the number of articles published from 2020 to 2025, reflecting its growing research output in recent years. Australia also shows consistent growth, maintaining a strong presence in the field. Meanwhile, Saudi Arabia and USA, though ranked lower, exhibit steady contributions to the overall research landscape in this domain.

Table 5. Top 5 highest productive countries of the articles of Cybersecurity

Rank	Country	Total Articles
1	Bangladesh	2308
2	Australia	392
3	Malaysia	242
4	USA	196
5	Saudi Arabia	169

Subsequently, the collaboration network shown in Figure 6, highlights the global connections between countries in the domain of artificial intelligence in information systems. Bangladesh stands at the center of the network with the largest node, indicating its dominant position and significant number of publications in the field. The red-colored nodes represent countries with strong collaborative ties, while the blue-colored nodes signify countries with fewer or weaker collaborations. The network shows dense linkages between Bangladesh and other countries like Australia, Malaysia, Saudi Arabia, India, and Pakistan, reflecting high levels of academic and research partnerships. The thickness of the edges between nodes indicates the strength of these collaborations, with thicker lines representing more frequent co-authored publications. Countries like Rwanda, Indonesia, Kenya, and South Africa, represented by smaller blue nodes, form more isolated clusters with fewer connections, indicating lower levels of collaboration in the field. On the other hand, countries like Germany, USA, Italy, and France also appear in the red cluster, though their collaborative intensity with Bangladesh is somewhat less compared to countries like Malaysia and Saudi Arabia. This network provides a visual representation of the global collaborative landscape in artificial intelligence research within information systems, highlighting Bangladesh's central role in fostering international academic partnerships.

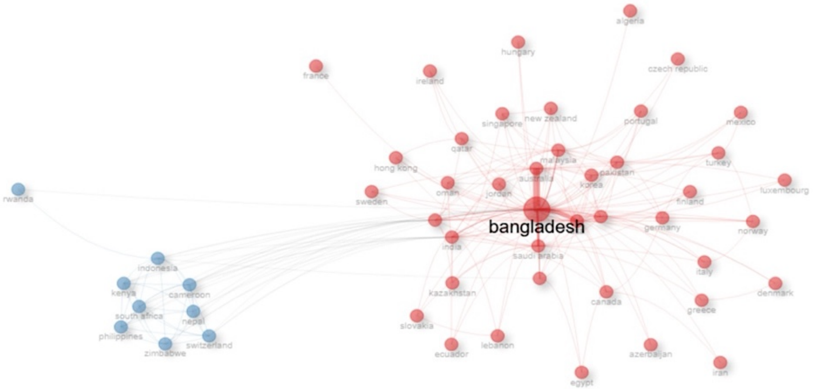

Figure 6. Cluster of collaborative countries of the articles of Cybersecurity Research

3.5. Analysis of affiliations of the authors

This analysis identifies the foremost academic institutions contributing to cybersecurity research in Bangladesh. Table 6 outlines the top affiliations, highlighting those whose faculty have made substantial contributions through their publications. Rajshahi University of Engineering and Technology leads the ranking with 59 articles, demonstrating its dominant position in the field of cybersecurity research. Following closely, Daffodil International Univers**ity** ranks second with 34 articles, further emphasizing its significant role in advancing cybersecurity studies in the country. University of Dhaka ranks third, with 32 articles, reflecting its longstanding commitment to cybersecurity research. Other notable institutions, including Khulna University of Engineering and Technology and United International University, also contribute notably to the field, securing the fourth and fifth positions with 31 and 29 articles, respectively. These findings highlight the growing academic interest and output in cybersecurity research across Bangladesh, with these universities making critical contributions to the development and enhancement of the field.

Table 6. Top 5 highest productive affiliations of cybersecurity research in Bangladesh

Rank	Affiliation	Articles
1	Rajshahi University of Engineering and Technology	59
2	Daffodil International University	34
3	University Of Dhaka	32
4	Khulna University of Engineering and Technology	31
5	United International University	29

Institutional collaboration plays a crucial role in advancing cybersecurity research within Bangladeshi educational institutions. A bibliometric analysis of the relevant literature highlights that partnerships between academic institutions are central to driving progress in the field. In Figure 7, the collaboration network reveals multiple clusters of institutions, each demonstrating varying levels of collaboration. The largest cluster, represented in Red, includes prominent institutions like Rajshahi University of Engineering and Technology and Bangladesh University of Engineering and Technology (BUET), indicating the highest frequency of collaboration within this group. Other smaller clusters represent universities like Jahangirnagar University, Daffodil International University, and Mawlana Bhashani Science and Technology University, each contributing to specialized areas of cybersecurity research. This network underscores the growing importance of collaborative efforts among Bangladeshi academic institutions in advancing cybersecurity knowledge.

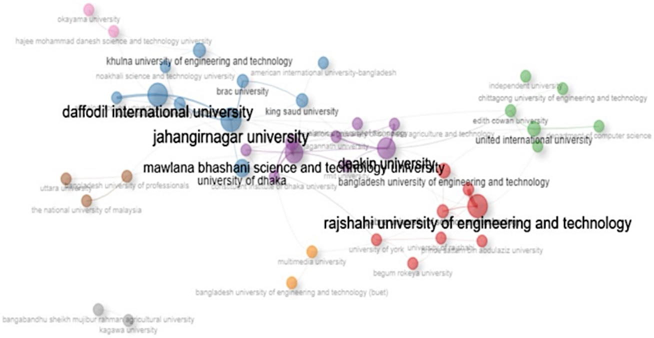
okayama university
hajee mohammad danesh science and technology university
khulna university of engineering and technology
american international university-bangladesh
noakhali science and technology university
brac university
independent university
chittagong university of engineering and technology
daffodil international university
king saud university
edith cowan university
jahangirnagar university
agriculture and technology
united international university
department of computer science
jagannath university
mawlana bhashani science and technology university
deakin university
uttara university
bangladesh university of professionals
university of dhaka
constituent institute of dhaka university
rmit university
bangladesh university of engineering and technology
the national university of malaysia
rajshahi university of engineering and technology
university of york
university of rajshahi
prince sattam bin abdulaziz university
multimedia university
begum rokeya university
bangladesh university of engineering and technology (buet)
bangabandhu sheikh mujibur rahman agricultural university
kagawa university

Figure 7. Institutional collaboration of the articles of cybersecurity research in Bangladeshi Educational Institutions

3.6. Keyword Analysis

In creating the word cloud presented in the figure, certain commonly used keywords such as "cybersecurity" and "network security" were deliberately excluded from the analysis, as they appeared frequently in the initial search criteria and article extractions. To ensure clarity and avoid redundancy, overlapping terms were also omitted. The resulting word cloud, depicted in Figure 8, emphasizes the most prevalent keywords associated with network security, derived from a thorough examination of cybersecurity literature. The terms highlighted in the word cloud represent key research topics in the field, including deep learning, machine learning, intrusion detection, and blockchain, among others. These keywords not only illustrate the core areas of focus within network security research but also reflect the prevailing trends and evolving directions in the domain.

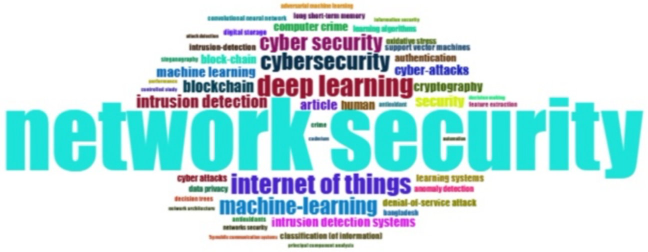

Figure 8. Top 25 author keywords of the articles of Cybersecurity in Bangladeshi Educational Institutions

3.7. Citation analysis of the articles

Citation analysis in this study evaluates how frequently specific articles are referenced in other academic works. Table 7 presents the top 10 papers based on total citations. The paper ranked 1st leads with 472 citations and a high normalized

TC of 7.76, indicating its significant and sustained impact in the field. The normalized total citations (Normalized TC) metric adjusts for the length of time an article has been published, providing a fair comparison between articles published in different years. It allows us to assess the relative impact of newer papers, which have had less time to accumulate citations. Papers with higher normalized TC values, such as the 1st ranked paper, show that these articles are being cited at a relatively higher rate, signaling their ongoing relevance and importance in the field. Other notable contributions, such as the papers ranked 2nd and 3rd, also demonstrate significant citation activity, though they have slightly lower normalized citation rates. The analysis suggests that while some papers have garnered considerable attention, there are still emerging areas in the field that require more in-depth exploration and research engagement.

Table 7. Top papers based on citation measure of cybersecurity research in Bangladesh

Rank	Paper	Total Citations (TC)	TC per Year	Normalized TC
1	[21]	472	78.67	7.76
2	[22]	253	42.17	4.16
3	[23]	214	71.33	9.22
4	[24]	170	42.50	6.36
5	[25]	168	33.60	4.79
6	[26]	166	55.33	7.15
7	[27]	156	31.20	4.45
8	[28]	133	26.60	3.79
9	[29]	116	23.20	3.31
10	[30]	105	35.00	4.52

3.8. Most frequent words bibliometrics

This section provides a bibliometric analysis of the most frequent words occurring in cybersecurity research. Figure 9 illustrates the frequency of words that appear most often across academic papers in this field. The term "cybersecurity" stands out as the most frequent, occurring 35 times, followed by terms like "machine learning" (32 occurrences) and "deep learning" (26 occurrences). Other notable terms include "blockchain", "security", and "intrusion detection system", which highlight key themes and research areas within the cybersecurity domain. This analysis sheds light on the focal points of current cybersecurity studies and reflects the growing importance of technologies like machine learning and blockchain in enhancing security measures.

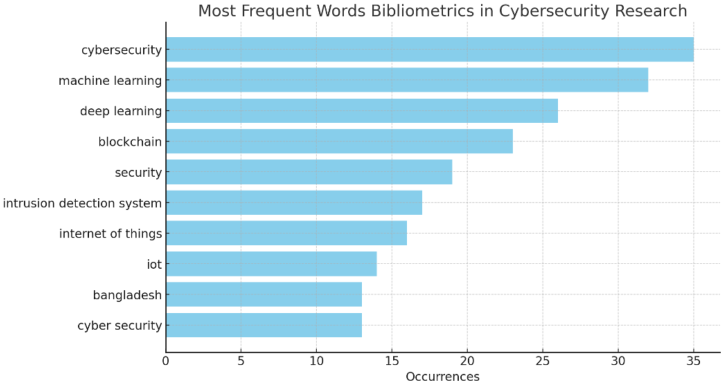

Figure: 9. Most Frequent Words Bibliometrics in Cybersecurity Research

3.9. Key topics trends in cybersecurity research

The distribution of key topics in cybersecurity research was analyzed by calculating the frequency of each term across the gathered research articles, with the results visualized in the tree map shown in the figure. Network security, deep learning, and machine learning are the most prominent topics in current cybersecurity research, indicating a strong emphasis on these areas. Other frequently discussed terms include intrusion detection, cybersecurity, data privacy, and blockchain, reflecting growing interest in securing systems, protecting data, and leveraging advanced technologies like AI in cybersecurity.

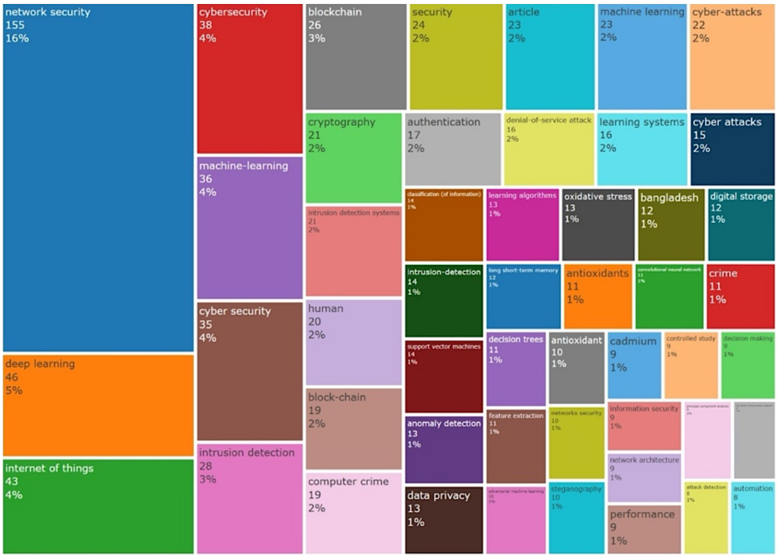

Figure 10. Trending topics on the field of cybersecurity research in Bangladeshi Educational Institutions

3.2 Discussion

This research delves into the trends, impacts, and evolution of scholarly work within this interdisciplinary field through the lens of bibliometric analysis. By examining academic publications, citation patterns, and collaborative efforts, the study aims to identify influential works, leading authors, and the key thematic areas driving the research landscape. The bibliometric approach provides valuable insights into the structure of the field, highlighting how research has evolved over time. Additionally, it helps to uncover emerging topics, trends in author collaboration, and the overall impact of key publications. Through this methodology, the study offers a comprehensive understanding of the major contributions, shifts in focus, and the dynamic nature of this domain.

The period from 2020 to 2025 demonstrates a notable and consistent increase in cybersecurity research within Bangladeshi educational institutions. Publications rose from 23 articles in 2020 to 77 in 2024, reflecting growing academic attention. With 59 articles already published by May 2025, this upward trajectory indicates a continued surge in interest and research output, suggesting an ongoing acceleration in the field. The research suggests that Md. Alamgir Hossain (State University of Bangladesh) and Md. Rashidul Islam (Rajshahi University of Engineering and Technology) both stand out with 15 publications each in the field of cybersecurity in Bangladeshi educational institutions. On the other hand, Iqbal H. Sarker stands out as the most influential author in the field of cybersecurity in Bangladeshi educational institutions with the highest h-index of 48 and a total of 17,999 citations. According to the analysis, a total of 302 papers were published from 182 journals that were considered significant. IEEE ACCESS leads in cybersecurity publications, followed by ELECTRONICS and SENSORS. Other journals like COMPUTERS, MATERIALS AND CONTINUA, and CYBERSECURITY also contribute significantly to the cybersecurity research in Bangladeshi educational institutions.

Bangladesh's cybersecurity research is particularly influenced by its local context, with a growing need to address national infrastructure vulnerabilities, particularly in critical sectors such as banking, finance, and government. The local context has driven research toward practical, region-specific challenges, such as securing financial transactions and protecting government databases from cyber threats. This research trajectory reflects the increasing recognition of cybersecurity as essential for national security and resilience, especially after high-profile cyber incidents like the Bangladesh Bank cyber heist.

Bangladesh occupies a central position in the network, represented by the largest node, highlighting its leading role and substantial number of publications in cybersecurity research and international collaborations. This study reveals that

Rajshahi University of Engineering and Technology has established itself as the leading Bangladeshi educational institution in the field of cybersecurity research. In the citation analysis, there is a higher number of citations between journals such as "Journal of Big Data," "Symmetry", "Mobile Networks and Applications" etc. Iqbal H. Sarker is the most influential author with highest citations among the top 10 most cited authors in this domain.

The study also highlights key topics in cybersecurity research, with network security, deep learning, and machine learning being the most prominent areas of focus. Additionally, there is a growing interest in intrusion detection, cybersecurity, data privacy, and blockchain, reflecting the increasing importance of securing systems, protecting data, and leveraging advanced technologies like AI in the cybersecurity domain.

When compared to other South Asian countries like India and Pakistan, Bangladesh’s cybersecurity research is still developing. While countries like India have heavily invested in cybersecurity research as part of their national digital security initiatives, Bangladesh's focus remains more region-specific, addressing local vulnerabilities and infrastructure needs. However, Bangladesh's increasing academic output and international collaboration signal its growing role in the global cybersecurity landscape.

This study highlights distinctive trends when compared to research in related fields such as machine learning (ML) and data science. While ML research primarily focuses on algorithmic advancements and is often driven by tech giants, and data science emphasizes the application of big data with strong industry involvement, cybersecurity research in Bangladesh has a unique emphasis on addressing local challenges and enhancing national security frameworks. The findings suggest opportunities for fostering global collaboration and learning from related fields, which could lead to innovative solutions in cybersecurity, benefiting both organizational security and societal resilience [20].

This bibliometric analysis focuses solely on cybersecurity research within Bangladeshi educational institutions, which limits the scope by not considering research from other regions or sectors. It relies on a single database (e.g., Scopus), which may limit the comprehensiveness of the findings. Additionally, there is a potential language bias, and the use of citation-based metrics may not fully capture the dynamic nature of cybersecurity research, nor does it account for qualitative insights. While the study provides valuable insights into the volume of research conducted, it does not delve into the specific content or nature of the research itself, which could offer a deeper understanding of the themes and practical applications being explored. Additionally, the analysis is based on up-to-date information, which makes it difficult to fully compare past trends with the current trajectory. Future research should broaden the scope to include a more comprehensive analysis of the research themes, methodologies, and findings. Incorporating data from a wider range of institutions, including global collaborations, and conducting longitudinal studies will enable a more robust comparison of trends over time.

4. CONCLUSION

This study makes a significant contribution to the existing body of knowledge on cybersecurity research within Bangladeshi educational institutions. As digital threats evolve, the importance of cybersecurity research becomes ever more critical in securing national and global digital infrastructures. This bibliometric analysis offers a comprehensive overview of the trends, influential publications, key authors, and research themes that are shaping the cybersecurity research landscape in Bangladesh. The findings indicate a clear upward trajectory in research output from 2020 to 2025, highlighting a growing academic focus on cybersecurity issues which is one of the most important things for the country to be taken care of especially after significant cybersecurity incidents such as the 2016 Bangladesh Bank cyber heist. In this incident, hackers managed to steal $81 million from the central bank's account, highlighting vulnerabilities in Bangladesh's financial systems and the critical need for robust cybersecurity measures. This breach not only exposed the weaknesses in the country's financial infrastructure but also underscored the urgent need for advanced cybersecurity research to protect against such sophisticated attacks. By mapping citation patterns and identifying prominent journals, this study provides a detailed understanding of the most influential publications and the significant contributors to the field. Topics such as network security, deep learning, machine learning, data privacy, and blockchain are increasingly prevalent in the research, signaling a broader interest in advanced technologies and their applications in cybersecurity. The results also provide valuable insights for shaping national cybersecurity policy, directing research funding, and enhancing digital resilience in educational and governmental institutions.

Cybersecurity research can play a vital role in helping Bangladesh safeguard its digital assets and infrastructure. By focusing on emerging threats, enhancing the detection of cyber-attacks, and developing advanced security protocols, cybersecurity research can strengthen the country's defenses. Areas such as network security, fraud detection, and the application of artificial intelligence in cybersecurity can contribute to building more resilient systems that can better detect, prevent, and respond to cyber threats, reducing the likelihood of similar incidents in the future. As Bangladesh continues to digitalize its economy, investment in cybersecurity research will be crucial in preventing future cybercrimes and ensuring the stability of its financial and governmental institutions. However, this study is limited by its reliance on the SCOPUS database, which may exclude relevant studies from other sources. Future research could benefit from incorporating additional databases and mixed-method approaches, including qualitative assessments, to capture a broader and deeper understanding of the cybersecurity landscape.

REFERENCES

[1] C. Y. Chen, W. Quan, N. Cheng, S. Yu, J. H. Lee, G. M. Perez, … S. Shieh, "IEEE Access special section editorial: Artificial intelligence in cybersecurity," *IEEE Access*, vol. 8, pp. 163329-163333, 2020.

[2] T. H. Chowdhury, N. Parvez, S. S. Urmi, and K. A. Taher, "Cybersecurity Challenges and Policy Options for Bangladesh," in *2021 Int. Conf. on Information and Communication Technology for Sustainable Development (ICICT4SD)*, Feb. 2021, pp. 472-476.

[3] M. R. Uddin, "The National Cybersecurity Strategy of Bangladesh: A Critical Analysis," *J. Int. Affairs*, vol. 21, no. 1, 2017.

[4] M. M. M. Rahaman, "Recent advancement of cyber security: Challenges and future trends in Bangladesh," *Saudi J. Eng. Technol.*, vol. 7, no. 6, pp. 278-289, 2022.

[5] A. Al Mamun, J. B. Ibrahim, and S. M. Mostofa, "Cyber security awareness in Bangladesh: an overview of challenges and strategies," *Int. J. Comp. Sci. Informat. Technol. Res.*, vol. 9, no. 1, pp. 88-94, 2021.

[6] M. Tasnim, M. Tasnim, S. Laila, T. Tabassum, and S. Al Haque, "Determining cybersecurity awareness and human-cyber behaviour in Bangladeshi women: Addressing factors, risks and overcoming knowledge disparities," Ph.D. dissertation, BRAC Univ., 2025.

[7] A. S. Sikder, "Cybersecurity Framework for Ensuring Confidentiality, Integrity, and Availability of University Management Systems in Bangladesh," *Int. J. Imminent Sci. Technol.*, vol. 1, no. 1, pp. 17-39, Nov. 2023. DOI: 10.70774/IJIST.V1I1.4

[8] R. U. Azad, S. Tasmim, and M. Atikuzzaman, "Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework," *Glob. Knowl. Mem. Commun.*, 2025. DOI: 10.1108/gkmc-05-2024-0319

[9] A. S. Sikder and M. R. Islam, "Enhancing Cyber-Resilience within Bangladesh's Legal Framework: Evaluating Preparedness and Mitigation Strategies against Technologically-Driven Threats," *Int. J. Imminent Sci. Technol.*, vol. 1, no. 1, pp. 40-57, 2023.

[10] D. P. Khurana, "Mapping the Cybersecurity Research: A Comprehensive Bibliometric Analysis," SSRN, 2024.

[11] S. Pradip, K. Sarker, and R. Z. Khan, "Cybersecurity Considerations for Smart Bangladesh: Challenges and Solutions," *Asian J. Res. Comput. Sci.*, vol. 17, no. 6, pp. 145-156, Apr. 2024. DOI: 10.9734/AJRCOS/2024/V17I6464

[12] M. Best, L. Krumov, and I. C. Bacivarov, "Cyber Security in Banking Sector," *Int. J. Inf. Secur. Cybercrime*, vol. 8, no. 2, Dec. 2019.

[13] O. Ellegaard and J. A. Wallin, "The bibliometric analysis of scholarly production: How great is the impact?," *Scientometrics*, vol. 105, no. 3, pp. 1809-1831, Dec. 2015. DOI: 10.1007/S11192-015-1645-Z

[14] I. Passas, "Bibliometric Analysis: The Main Steps," *Encyclopedia*, vol. 4, no. 2, pp. 1014-1025, Jun. 2024. DOI: 10.3390/ENCYCLOPEDIA4020065

[15] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285-296, Sep. 2021. DOI: 10.1016/J.JBUSRES.2021.04.070

[16] P. Ahmad, J. A. Asif, M. K. Alam, and J. Slots, "A bibliometric analysis of Periodontology 2000," *Periodontol. 2000*, vol. 82, no. 1, pp. 286-297, Feb. 2020. DOI: 10.1111/PRD.12328

[17] J. M. Merigó and J. B. Yang, "A bibliometric analysis of operations research and management science," *Omega*, vol. 27, no. 1, pp. 71-100, 2017. DOI: 10.1016/j.omega.2016.12.004 IDEAS/RePEc+1

[18] S. Büyükkidik, "A Bibliometric Analysis: A Tutorial for the Bibliometrix Package in R Using IRT Literature," *J. Meas. Eval. Educ. Psychol.*, vol. 13, no. 3, pp. 164-193, Sep. 2022. DOI: 10.21031/EPOD.1069307

[19] K. Ragazou, I. Passas, A. Garefalakis, E. Galariotis, and C. Zopounidis, "Big Data Analytics Applications in Information Management Driving Operational Efficiencies and Decision-Making: Mapping the Field of Knowledge with Bibliometric Analysis Using R," *Big Data Cogn. Comput.*, vol. 7, no. 1, p. 13, Jan. 2023. DOI: 10.3390/BDCC7010013

[20] Y. Gao et al., "Global trends and future prospects of e-waste research: a bibliometric analysis," *Environ. Sci. Pollut. Res.*, vol. 26, no. 17, pp. 17809-17820, Jun. 2019. DOI: 10.1007/S11356-019-05071-8

[21] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, pp. 1-29, Dec. 2020. DOI: 10.1186/S40537-020-00318-5

[22] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model," *Symmetry*, vol. 12, no. 5, p. 754, May 2020. DOI: 10.3390/SYM12050754

[23] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 296-312, Feb. 2023. DOI: 10.1007/S11036-022-01937-3

[24] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," *Cybersecurity*, vol. 5, no. 1, pp. 1-22, Dec. 2022. DOI: 10.1186/S42400-021-00103-8

[25] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," *IEEE Access*, vol. 9, pp. 50961-50981, 2021. DOI: 10.1109/ACCESS.2021.3067331

[26] M. A. Talukder et al., "A dependable hybrid machine learning model for network intrusion detection," *J. Inf. Secur. Appl.*, vol. 72, p. 103405, Feb. 2023. DOI: 10.1016/J.JISA.2022.103405

[27] I. H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1-16, May 2021. DOI: 10.1007/S42979-021-00535-6

[28] A. Rahman et al., "SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT," *IEEE Access*, vol. 9, pp. 28361-28376, 2021. DOI: 10.1109/ACCESS.2021.3058244

[29] N. Islam, F. Farhin, I. Sultana, M. S. Kaiser, M. Mahmud, … G. H. Cho, "Towards machine learning based intrusion detection in IoT networks," *Comput. Mater. Contin.*, vol. 69, no. 2, pp. 1801-1821, 2021.

[30] M. N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F. M. Bui, and S. M. Ibrahim, "Federated Machine Learning for Detection of Skin Diseases and Enhancement of Internet of Medical Things (IoMT) Security," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 835-841, Feb. 2023. DOI: 10.1109/JBHI.2022.3149288