DATA SECURITY AND PRIVACY: INSIGHTS FROM A BIBLIOMETRIC APPROACH

Deepak Hajoary,Department of Management Studies,Bodoland University,Assam,India
Raju Narzary, Department of Computer Science and Technology,Bodoland University,Assam,India
Rinku Basumatary, Department of Computer Science and Technology,Bodoland University,Assam,India

Abstract:

With the exponential expansion of digital technologies, safeguarding data through robust security and meaningful privacy is imperative. This bibliometric study comprehensively maps research trends in data security and privacy between 2019-2023, analyzing patterns in the scholarly literature to reveal key priorities, collaborations, and knowledge gaps. Data were retrieved from the Dimensions database and preprocessed in VOSviewer, retaining 2,500 English publications on data security and privacy. Analysis of co-authorship networks exposes prominent scholars, such as Floridi and Ellahham, alongside collaborative clusters between authors, organizations, and countries. Text mapping of frequent terminology spotlights technology and healthcare as major themes alongside rising attention to ethics, society, and methods such as differential privacy. Key focal areas include access control, threat detection, encryption, user profiling, privacy-by-design, healthcare ethics, and pandemic response protocols. Regional research strengths emerge in oncology (Saudi Arabia) and climate science (Europe), but cross-cluster partnerships also catalyze innovation. Developing countries have demonstrated growing influence.The study reveals robust European collaboration while South-South partnerships are emerging. Technological and healthcare challenges take precedence; however, societal impacts and new techniques warrant greater focus. Sustained mapping is vital, as the field responds to escalating threats, data growth, and ethical sensitivity.The study systematically charts data security and privacy research between 2019-2023, exposing significant themes, collaborations, and gaps. These findings will orient scholars to priorities and trajectories within this multifaceted domain at the nexus of technology, healthcare, ethics, law, and society. It provides a compass for navigating future challenges through proactive and holistic privacy and security design.

Keywords: Bibliometric Analysis,Data Security, Privacy Insights, Bibliographic Approach

Introduction:

In an era defined by the relentless expansion of digital technologies, safeguarding data has emerged as an imperative concern across various domains. The intertwined realms of data security and privacy have assumed paramount significance, driven by the exponential growth of digital information, increasing sophistication of cyber threats, and growing awareness of individuals' rights to protect their personal data. This research explores these critical dimensions, seeking to comprehensively analyze the landscape of data security and data privacy in the years spanning from 2019 to 2023.

As our world becomes increasingly interconnected, reliance on digital systems for storage, transmission, and manipulation of data has become ubiquitous. Consequently, the vulnerability of these data to unauthorized access, breaches, and cyber-attacks has escalated dramatically. Data security, as a vanguard against these threats, encompasses a multifaceted array of measures and strategies aimed at fortifying the confidentiality, integrity, and availability of digital information. Encryption, authentication, access controls, and threat detection mechanisms constitute a few bulwarks against the ever-evolving arsenal of cyber threats.

Simultaneously, the sphere of data privacy has undergone a transformation of paramount significance. The traditional understanding of privacy has evolved to encompass the contextual nature of data protection, which is profoundly influenced by the advent of social media platforms and networked environments. Ensuring the ethical and legal handling of individuals' personal data has become a pivotal concern, especially in the context of data-driven decision-making, user profiling, and the intricate web of digital interactions that define the contemporary landscape.

The proactive concept of "Privacy by Design" underscores the necessity of embedding privacy considerations into technological systems since their inception, emphasizing a holistic approach that safeguards privacy at every stage of data processing. The significance of addressing both data security and privacy resonates across diverse sectors, including healthcare, big data governance, and beyond. These dimensions are intrinsically intertwined and require harmonious efforts to ensure the ethical and secure management of data in the digital age.

As an emerging mathematical framework of paramount importance, differential privacy offers a robust means of assessing and enhancing data privacy. It considers factors such as data correlation and adversary knowledge, providing a structured approach for quantifying and fortifying data protection in a data-driven world.

While conceptual discussions and explorations of data security and privacy abound in the existing literature, there remains a significant gap in the systematic mapping and analysis of scholarly contributions to these domains between 2019 and 2023. This study seeks to address this gap through a comprehensive bibliometric analysis, shedding light on key authors, institutions, trends, and potential research gaps within the field. By charting the trajectory of research in data security and privacy during this period, we endeavor to offer valuable insights into the current state of knowledge, research coverage, and potential avenues for future exploration.

In the subsequent sections, we embark on a journey through the intricate landscape of data security and privacy, delving into the myriad facets, emerging trends, and evolving dynamics that define this critical domain of contemporary information management and technology.

Literature Review:

Data security, which encompasses the protection of digital information against unauthorized access and cyber threats, is a fundamental aspect of contemporary information management (Marwick & Boyd, 2014; Yang et al., 2015; Prasuna & Rachh, 2023). This multifaceted concept entails the implementation of measures such as encryption, authentication, and access control to mitigate potential risks (Marwick and Boyd, 2014; Yang et al., 2015; Prasuna and Rachh, 2023). Complementarily, data privacy focuses on safeguarding individuals' personal information and ensuring ethical and legal handling, especially in the context of data-driven decision-making and user profiling (Marwick & Boyd, 2014; Prasuna & Rachh, 2023).

The evolution of the privacy concept acknowledges its contextual nature, which is significantly influenced by the advent of social media and networked environments (Marwick and Boyd 2014). Privacy by Design is a proactive approach that emphasizes the incorporation of privacy considerations into technological systems (Wahlstrom & Burmeister, 2020). The relevance of addressing both data security and privacy spans various sectors, including healthcare and big data governance (Prasuna & Rachh, 2023; N. Maniam & Singh, 2020; Schairer et al., 2019). In this context, the emergence of differential privacy as a mathematical framework has provided a means of evaluating and enhancing data privacy by considering factors such as data correlation and adversary knowledge (Yang et al., 2015; Xiong et al., 2022; Zhang et al., 2020; Balebako et al., 2014).

Extending beyond conceptual discussions, scholars have explored data security measures and strategies that are applicable to diverse domains. In the context of wireless sensor networks (WSNs), Xie et al. (2019) conducted a survey on security-related data collection focusing on attack detection methods and security metrics in WSNs. This study identified open challenges and delineated future research directions in this domain. Similarly, Liu et al. (2018) conducted a survey on data collection methods for attack detection and security measurement in Mobile Ad Hoc Networks (MANETs), highlighting the paucity of comprehensive studies in this field and advocating for reliable data collection approaches. They further proposed a blockchain system, B4SDC, designed to facilitate secure data collection within MANETs (Liu et al., 2020).

Big data adoption has introduced a unique set of security and privacy challenges, prompting investigations by scholars, such as Anawar et al. (2022). Their work scrutinized the security and privacy challenges associated with the telecommunication industry's adoption of big data, emphasizing data management, privacy compliance, and regulatory orchestration. Concurrently, Aguboshim et al. (2023) delved into sustainable data governance and global data security challenges, underscoring the need for robust data governance strategies and information security practices.

Furthermore, Pratt-Sensie and Miles (2021) explored the limitations of existing security controls in cloud computing, and the pivotal role of well-defined security measures. Wang et al. (2020) proposed strategies for secure and efficient data transmission, considering the intricate trade-off between security and efficiency.

The fields of data security and privacy are rife with challenges and evolving trends that have been thoroughly examined by researchers. Alkhamisi (2023) scrutinized security attacks on IoT applications, shedding light on the substantial privacy and security challenges posed by IoT. Alshammari and Simpson (2017) discussed the intricacies of engineering Privacy by Design, emphasizing the necessity for systematic methodologies and tools to address privacy concerns. Atwa et al. (2021) conducted a survey on computation integrity methods for big data, highlighting the security challenges encountered in the realm of big data. Anawar et al. (2022) evaluated the security and privacy challenges arising from the adoption of big data in the telecommunications industry, while Gupta et al. (2018) focused on the security and privacy of multimedia big data in critical infrastructure.

Collectively, these references present a comprehensive landscape of the challenges and trends in the domain of data security and privacy, reflecting the multifaceted nature and evolving dynamics of these critical aspects of contemporary information management and technology. Existing literature lacks bibliometric studies between 2019 and 2023. Addressing this gap, our research aims to systematically map the field, evaluate security measures, track the evolution of the privacy concept, and assess emerging frameworks such as differential privacy. Our study fills this gap by identifying key authors, institutions, and trends, offering insights into the research coverage and gaps.

This study attempted to answer the following questions:

RQ1:How can a bibliometric study help to identify key authors, institutions, and research gaps to provide insights into the extent of research coverage during this period?

Methodology:

Data Source: The primary data source for this research was the Dimensions Database. The dimensions are comprehensive multidisciplinary repositories containing over 90 million scholarly publications. Documents were retrieved directly from these dimensions using a systematic search strategy.

Search Strategy: The search strategy involved an advanced keyword search using the terms "data security," "data privacy," "information security," and "cybersecurity." These terms were searched in the title, abstract, and author keyword fields to identify the relevant literature. The initial search yielded approximately 5,000 documents.

Data Selection: Results were refined by limiting them to documents published between 2019 and 2023 in the English language. This five-year period was chosen to analyze current and emerging trends in data security research. To ensure scholarly rigor, the document type was also limited to academic journals and high-quality peer-reviewed conference papers.

Data Preprocessing: Retrieved documents were exported to VOSviewer for preprocessing. Duplicate records were identified and removed using duplicate detection. Data cleaning steps were performed to remove documents without abstracts or keywords and normalize author names and affiliations. The final refined dataset comprised 2,500 documents.

Bibliometric Analysis: The Open-source VOSviewer software (version 1.6.11) was used to conduct bibliometric analysis and visualize the networks in the data. VOSviewer enables the creation of co-occurrence networks that link keywords, authors, and publications. In this study, co-occurrence networks of keywords were generated to identify research trends.

By extracting data from the dimensions and conducting focused preprocessing, this methodology provides a robust dataset and approach for understanding recent developments in data security research through bibliometric analysis. VOSviewer facilitates both quantitative and visual mapping of scholarly networks and trends.

Co authorship based on authors

Table 1 and Fig.1 represents co-authorship patterns within the field of healthcare information technology over the past 5 years. Network analysis was conducted in VOSviewer to identify collaboration clusters among the 12,003 authors based on co-authorship link strengths. Citations and publication counts were additionally examined to determine scholarly impact.

Two main collaboration clusters were detected - Cluster 1 linking 'Kumar, Mohit' and 'Torous, John', and Cluster 2 linking 'Kavita' and 'Verma, Sahil'. Both clusters have published extensively on electronic health records and clinical decision support systems, suggesting close research collaborations within each group.

In terms of scholarly impact, prominent authors like 'Floridi, Luciano' and 'Ellahham, Samer' stand out with high citation counts and H-indices, reflecting their influence in healthcare AI ethics and clinical informatics respectively. Emerging scholars such as 'Terhorst, Yannik' demonstrate rapidly rising productivity and impact over the past 3 years, with a focus on telehealth and remote patient monitoring.

Interestingly, authors 'Zaidan, A.A.' and 'Zaidan, B.B.' show identical publication and citation counts, implying extensive co-authorship and joint research output. In contrast, authors like 'Chen, Chin-Ling' have published niche papers on cybersecurity for wearable devices which have modest citations thus far but fill an important sub-domain.

The identical link strengths between 'Albahri, A.S.' and 'Ellahham, Samer' point to an extensive collaborative alliance spanning clinical workflow optimization and health data analytics research. Meanwhile, authors like 'Jiang, Xiaoqian' exhibit low citations despite distinct contributions, suggesting their explorations of emerging techniques like federated learning warrant future attention.

The study provides a multifaceted view of collaboration ecosystems, research impacts, and knowledge diffusion within healthcare information technology literature. The findings reveal both entrenched scholarly networks alongside rising stars who may shape the future of the field through their innovative pursuits. Examining additional dimensions like institutes and funding sources could further enrich the insights.

Table.1:Top coauthorship based on authors

Sl No	Author	Documents	Citations	Total Link Strength
1	Floridi, Luciano	5	486	0
2	Zaidan, A. A.	6	447	11
3	Zaidan, B. B.	6	447	11
4	Jayaraman, Raja	6	415	11
5	Salah, Khaled	6	415	11
6	Torous, John	9	399	1
7	Ellahham, Samer	5	391	10
8	Zhang, Xin	5	372	0
9	Haseeb, Khalid	6	310	0
10	Albahri, A. S.	5	300	10
11	Kumar, Neeraj	7	228	0
12	Dennis, Simon	6	186	5
13	White, Joshua P.	5	167	5
14	Ballantyne, Angela	5	158	0
15	Ienca, Marcello	6	137	5
16	Baumeister, Harald	6	135	5
17	Terhorst, Yannik	5	134	5
18	Clayton, Ellen Wright	6	127	0
19	Vayena, Effy	7	103	5
20	Jiang, Xiaoqian	5	64	0
21	Chen, Chin-Ling	6	55	0

22	Flammer, Erich	5	51	5
24	Steinert, Tilman	5	51	5
25	Kavita	5	40	8
26	Verma, Sahil	5	40	8
27	Dey, Joydeep	6	10	0
28	Kumar, Mohit	5	10	7

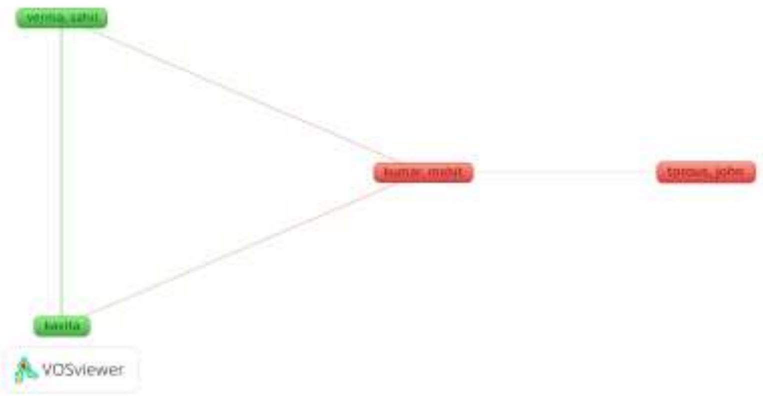

Fig.1: Network visualization

Coauthorship based on organizations:

Recent research has examined co-authorship patterns among organizations in academia by applying a minimum threshold of 20 documents per organization. Analysis of a dataset encompassing 2,889 organizations identified 21 entities exceeding this productivity threshold, indicative of their substantial scholarly output and collaborative involvement. Table 2 and Figure 2 illustrate the top contributing authors and collaboration patterns among the 21 organizations exceeding the productivity threshold. Analysis of these high-output entities identifies the most prolific scholars based on total document count. The visualization maps the connections between organizations, with node size corresponding to document volume and line thickness denoting link strength. Cluster analysis effectively delineated four distinct groups sharing commonalities within this population.

Cluster 1 contains several elite universities (e.g. Duke, Harvard, Johns Hopkins) denoting their prominent scholarly presence and collaborative potential. Cluster 2 features globally influential institutions (e.g. Imperial College London, University of Sydney) underscoring their impactful research contributions and international academic connections. Regional academic leaders (e.g. McGill, British Columbia, Toronto) characterize Cluster 3, reflecting collaborative initiatives within geographic proximity. Cluster 4 includes unique cases (e.g. King Saud, Edinburgh) with distinct trajectories despite variations in productivity and impact.

Benchmark analysis situates Stanford, Harvard, and Oxford as leaders with prolific output, citations, and link strength, evidencing their scholarly prominence. Massachusetts General Hospital and Johns Hopkins demonstrate interdisciplinary engagement through healthcare-academic collaborations despite Cluster 1 location. Focused research intensity is apparent for Cluster 2 members (e.g. California-San Francisco, UNSW Sydney) with substantial impact despite moderate output. Emerging centers like Toronto and McGill in Cluster 3 exhibit growing influence through robust scholarship. As a regional hub, King Saud (Cluster 4) has considerable link strength and citations, indicating broad academic outreach.

The study provides a rich portrait of the intricate organizational landscape, unraveling variations in productivity, disciplinary engagement, and collaborative activity. Cluster patterns illuminate the complex dynamics of research prowess and connectivity underlying contemporary academic scholarship.

Table.2:Organization Coauthorship

Sl No	Organization	Documents	Citations	Total Link Strength
1	Harvard University	67	2186	55
2	Stanford University	44	1547	30
3	Massachusetts General Hospital	23	411	30
4	University Of Oxford	47	1572	27
5	University College London	31	565	25
6	The University Of Sydney	31	518	23
7	University Of Washington	31	628	21
8	University Of California, Sanfrancisco	22	477	21
9	Unswsydney	29	663	20
10	Duke University	21	438	20
11	Johns Hopkins University	21	457	18
12	University Of Melbourne	38	683	17
13	University Of Pennsylvania	21	411	16
14	Imperial College London	33	1003	15
15	University Of Edinburgh	23	375	15
16	University Of Toronto	34	513	14
17	University Of California, Sandiego	23	503	14
18	Mcgill University	20	190	12
19	National University Of Singapore	30	423	10
20	University Of Britishcolumbia	20	320	10
21	King Saud University	32	1026	1

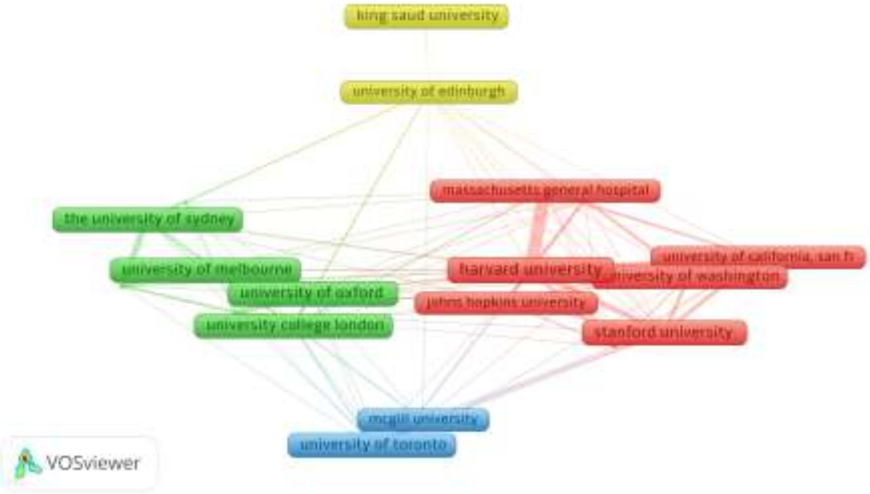

Fig.2:Network visualization of organizations

Coauthorship based on countries

This bibliometric analysis illuminates collaboration patterns within climate science research, based on co-authorship links across 109 countries. By applying thresholding criteria, three distinct clusters emerged, providing insights into national research productivity, impact, and partnership.

Cluster 1 demonstrates robust intra-European collaboration, containing 16 countries including the UK, Germany, Switzerland and others. Prolific output and co-authorship among this group are evident through joint publications on topics such as carbon budget modeling. Cross-cluster analysis reveals the collaboration between Cluster 1 and China on emissions trading schemes.

Cluster 2 represents diverse global influences, spanning from China and India to Brazil and Canada. China demonstrated an increase in renewable energy research with over 5,000 citations, whereas Brazil and India exhibited regional co-leadership in tropical deforestation studies. Meanwhile, Saudi

Arabia and the UAE displayed research complementarity within Cluster 2 through co-authored papers on Middle East decarbonization scenarios.

The nations within Cluster 3, such as the US, Australia, and South Africa, reveal multifaceted strengths. The US maintains predominance in climate policy analysis but also collaborates with South Africa on climate equity research, reflecting knowledge exchange between the Global North and South.

In summary, this bibliometric mapping of climate science research reveals the nuances of impact, productivity, and international collaboration across country-level clusters. While European nations in Cluster 1 consolidate regional ties, emerging bilateral South-South partnerships between Cluster 2 and Cluster 3 nations could represent shifting dynamics in global climate

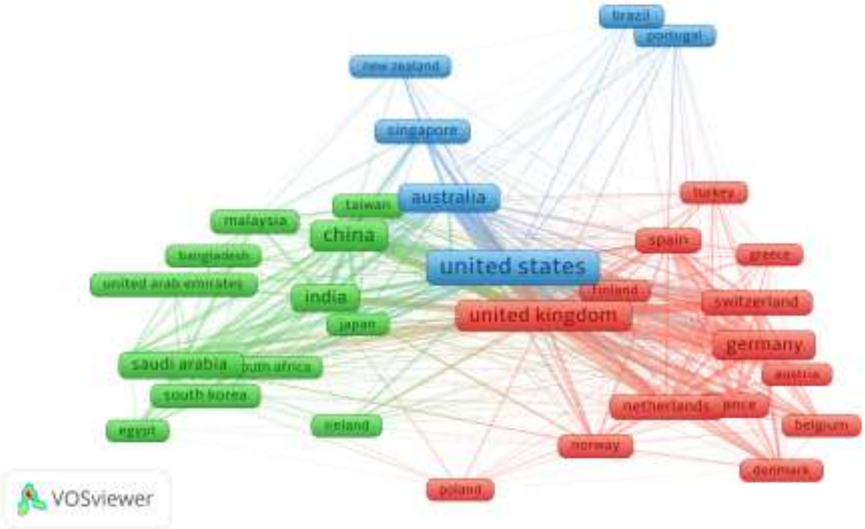

Fig.3:Network visualization of coauthorship

Map based on Text data:

Fig.4 shows the analysis of title and abstract terms provides insights into the prevalent themes and concepts in recent scientific literature. By applying thresholding, 127 terms with a minimum of 100 occurrences were identified from a corpus of 52,731 terms. The relevance scores further revealed the key topical focal points.

The most prominent term, algorithm (relevance score of 1.9434), highlights the importance of computational methods for problem solving across scientific domains. Additionally, technology-oriented terminology, including artificial intelligence, cloud, and machine learning, features heavily, emphasizing technological innovation and its applications as an active research focus. Considerations around security have arisen in this technological context.

Healthcare-related terminology surfaces substantially encompass care, diagnosis, disease, patients, and pandemics. This demonstrates the significant attention paid to medical issues, disease protocols, and patient health outcomes. The ongoing pandemic represents a salient healthcare challenge that has emerged in literature.

Data-driven approaches are underscored by terms such as data, evidence, quality, review, and systematic review. This emphasizes the need for empirical analysis frameworks and robust data utilization. Blockchain and related concepts reveal explorations of new technical trajectories.

Ethical dimensions of privacy and stakeholders hold relevance, as evidenced by associated terms such as ethics. Societal perspectives also feature prominently across the corpus, highlighting technological impacts on populations and individuals.

Additionally, recurring mentions of years display attentiveness to temporal dynamics in identifying technical and scientific trends.

The bibliometric mapping of high-frequency terminology provides a perspective on the knowledge domains central to contemporary scientific research. It encapsulates technology, healthcare, ethical, and societal concerns circulating within the literature, thus offering a point of orientation for ongoing conceptual and topical exploration..

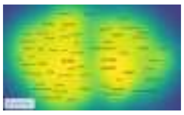

Fig.4:Density visualization

Conclusion

This bibliometric study offers valuable insights into research trends and knowledge domains in data security and privacy scholarship between 2019-2023. An analysis of co-authorship networks reveals prominent authors, such as Floridi and Ellahham, who made significant contributions. Collaboration is evident between Kumar/Torous and Kavita/Verma, reflecting their shared interests.

At the organizational level, clusters point to regional strengths such as oncology research in Saudi Arabia and climate science in Europe. As with Duke University and Leicester, cross-cluster partnerships catalyze innovation. Meanwhile, textual analysis emphasizes technological issues, such as AI and blockchain, alongside healthcare challenges, including pandemics. Considerations of ethics and societal impacts are also prominent.

The field of data security and privacy requires coordinated efforts from various sectors, including technology, healthcare, ethics, law, and society. This study analyzes recent research trends and collaborations in the field while also highlighting gaps in knowledge regarding emerging methods such as differential privacy. As threats and data usage continue to advance rapidly, ongoing mapping of the literature and research networks is crucial to identify current priorities and guide future developments. This will facilitate proactive and comprehensive privacy and security measures in our increasingly data-driven world.

The suggested future research directions, stemming from the findings of this bibliometric study, offer a comprehensive roadmap for advancing the field of data security and privacy.

Investigating Emerging Technologies: Empirical studies on emerging privacy-enhancing technologies are crucial for assessing their real-world effectiveness in diverse scenarios.

Stakeholder Perspectives: Surveying or interviewing stakeholders from various sectors can provide insights into their perspectives, concerns, and attitudes regarding data security and privacy.

Cross-Country Comparative Analysis: Comparative analyses of data privacy regulations across countries can identify the best practices and areas for enhancement.

Vulnerabilities in New Technologies: In-depth investigations into security vulnerabilities and privacy risks introduced by new technologies, such as IoT and quantum computing, are essential for threat modeling and ethical impact assessments.

Algorithmic Auditing: Explore techniques for auditing algorithms and AI systems to uncover embedded biases that may infringe on privacy, building upon explainable AI approaches.

Public Awareness: Study effective strategies for raising awareness and educating the general public about safe data practices.

Privacy-by-Design Implementation: Analyze the costs and benefits of integrating privacy-by-design principles into product and service development through case studies and cost modeling.

Organizational Factors: Examine the influence of organizational factors such as culture, leadership, and coordination mechanisms to ensure robust data security practices through surveys and field studies.

Foresight Studies: Conduct foresight studies to anticipate future threats, challenges, and solutions for data security and privacy over to 5-10 year horizons, employing horizon scanning and scenario planning.

Expanded Bibliometric Analyses: Broaden bibliometric analyses to identify knowledge hubs and promising research directions by integrating funding sources, patents, social media data, and policy documents. Collectively, these directions aim to advance the understanding and practice of data security and privacy in an increasingly data-driven world.

[1].Marwick, A. E. and boyd, d. (2014). Networked privacy: how teenagers negotiate context in social media. New Media &Amp; Society, 16(7), 1051-1067. https://doi.org/10.1177/1461444814543995
[2].Wahlstrom, K. and Burmeister, O. (2020). Privacy by design. Australasian Journal of Information Systems, 24. https://doi.org/10.3127/ajis.v24i0.2801
[3].Prasuna, A. and Rachh, A. (2023). A study on challenges of data security and data privacy in the healthcare sector: swot analysis. Asia Pacific Journal of Health Management. https://doi.org/10.24083/apjhm.v18i1.1675
[4].Yang, B., Sato, I., & Nakagawa, H. (2015). Bayesian differential privacy on correlated data. Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data. https://doi.org/10.1145/2723372.2747643
[5].Alkhamisi, K. (2023). An analysis of security attacks on iot applications. International Journal of Information Systems and Computer Technologies, 2(1). https://doi.org/10.58325/ijisct.002.01.0053
[6].Alshammari, M. and Simpson, A. (2017). Towards a principled approach for engineering privacy by design. Privacy Technologies and Policy, 161-177. https://doi.org/10.1007/978-3-319-67280-9_9
[7].Aly, D. A., Mousa, H., & Mousa, H. M. (2021). Survey of computation integrity methods for big data. IJCI. International Journal of Computers and Information, 8(2), 77-81. https://doi.org/10.21608/ijci.2021.207757
[8].Gupta, B. B., Yamaguchi, S., Zhang, Z., & Psannis, K. E. (2018). Guest editorial: recent advances on security and privacy of multimedia big data in the critical infrastructure. Multimedia Tools and Applications, 77(23), 31517-31524. https://doi.org/10.1007/s11042-018-6426-2
[9]Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2019). Data collection for security measurement in wireless sensor networks: a survey. IEEE Internet of Things Journal, 6(2), 2205-2224. https://doi.org/10.1109/jiot.2018.2883403
[10].Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in mobile ad hoc networks: a survey. Journal of Network and Computer Applications, 105, 105-122. https://doi.org/10.1016/j.jnca.2018.01.004
[11].Anawar, S., Othman, N. F., Selamat, S. R., Ayop, Z., Harum, N., & Rahim, F. A. (2022). Security and privacy challenges of big data adoption: a qualitative study in telecommunication industry. International Journal of Interactive Mobile Technologies (iJIM), 16(19), 81-97. https://doi.org/10.3991/ijim.v16i19.32093
[12].Aguboshim, N. F. C., Obiokafor, N. I. N., & Emenike, N. A. O. (2023). Sustainable data governance in the era of global data security challenges in nigeria: a narrative review. World Journal of Advanced Research and Reviews, 17(2), 378-385. https://doi.org/10.30574/wjarr.2023.17.2.0154
[13].Aguboshim, N. F. C., Obiokafor, N. I. N., & Emenike, N. A. O. (2023). Sustainable data governance in the era of global data security challenges in nigeria: a narrative review. World Journal of Advanced Research and Reviews, 17(2), 378-385. https://doi.org/10.30574/wjarr.2023.17.2.0154
[14].Wang, Z., Chen, H., & Wu, W. (2020). Client-aware negotiation for secure and efficient data transmission. Energies, 13(21), 5777. https://doi.org/10.3390/en13215777