Trends in security research: a text mining-based meta analysis of the literature

Siri Chandana Marrapu, *Missouri University of Science and Technology, and scmrbr@mst.edu*
Ganesh Panja, *Missouri University of Science and Technology, and gp829@mst.edu*
Vishesha Bitla, *Missouri University of Science and Technology, and vbgfn@mst.edu*
Wen-Bin Yu, *Missouri University of Science and Technology, and yuwen@umsystem.edu*

Abstract

The rapid evolution of technology has heightened the need for robust security frameworks to protect sensitive information. As cyber threats become increasingly sophisticated, academic research plays a pivotal role in addressing these challenges by developing innovative solutions. This project, which focuses on uncovering patterns and insights within scholarly articles on security and cyberattacks, is of significant importance to the cybersecurity field. By utilizing text mining to analyze 314 research papers from leading journals published between 1970 and 2024, we aim to identify historical developments, emerging topics, and the contributions of publishers to the field of study. The results of this study not only provide a roadmap for navigating the vast security literature but also offer valuable insights that can inform future research and contribute to the advancement of cybersecurity knowledge.

Keywords: text mining, cybersecurity, security research, meta analysis, journals and publishers, trends in cyber security, SAS enterprise miner.

Introduction

The rapid evolution of technology has heightened the need for robust security frameworks to protect sensitive information. As cyber threats become increasingly sophisticated, academic research plays a pivotal role in addressing these challenges by developing innovative solutions. This project aims to uncover patterns and insights within scholarly articles on security and cyberattacks. Text mining, a subset of data mining, enables the analysis of unstructured textual data, transforming it into structured formats for pattern recognition, clustering, and topic viewing. Using SAS Enterprise, we analyzed a collection of 314 research papers published by leading journals between 1970 and 2024. The primary objective was to identify historical trends, concept links, significant contributions, and emerging topics in cybersecurity research.

This study not only sheds light on the evolution of the field of security research but also addresses the challenges inherent in data collection and clustering. The findings, which are expected to aid future researchers in efficiently navigating the vast landscape of security literature and leveraging text-mining tools to extract meaningful insights, are of significant importance in the field of cybersecurity. Cybersecurity research is crucial for keeping us updated on the rapidly evolving tech world, including emerging cyber threats, and for being proactive in maintaining businesses away from risks and vulnerabilities. (The Royal Society, n.d.) This helps in creating a more trusted digital environment.

Cybersecurity research also leads us to develop innovative solutions like secure communications (public key cryptography), (US National Science Foundation, n.d.) methods that detect software threats (Devo, 2023) and vulnerabilities, privacy securing techniques like federated learning, and making customers aware of the privacy and security of the devices they use in day-to-day life.

It improves threat detection and response capabilities. (Riskrecon by Master Card, 2023) Researchers investigate malware, analyze incident reports, and develop strategies to mitigate risks associated with malware. This research also helps to address and minimize human-related risks. A significant amount of research on cyberattacks also contributes to the development of more secure cryptographic algorithms, protocols, and systems. (Hennick, 2023) It also contributes to workforce development by supporting educational programs that expand the cybersecurity talent. By continually advancing knowledge and developing new solutions, cybersecurity research plays a vital role in protecting digital infrastructure, maintaining secure supply chains, and safeguarding personal data in our increasingly connected world.

Research Methodology

In this project, we have followed the structure outlined in Figure 1 as our Research Methodology. We began by collecting research papers related to cybersecurity, network security, and security issues in digital spaces from 1970 to 2024. An Excel spreadsheet is prepared with a list of the papers. This file undergoes text mining, where SAS Enterprise Miner, a data mining tool, extracts and analyzes the targeted column (the text column of the research paper, here). SAS identifies essential information and features within the provided text. Furthermore, we gained valuable insights and implications from the features, clusters, and topics generated by SAS. In this project, we identified some important and interesting trends among publishers and years. These trends can help us understand how we have evolved from security-related research over the years, in which publishers played a significant role in publishing security-related research.
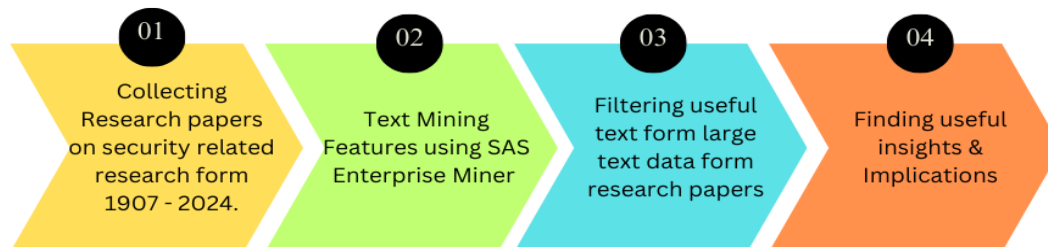

01	02	03	04
Collecting Research papers on security related research form 1907 - 2024.	Text Mining Features using SAS Enterprise Miner	Filtering useful text form large text data form research papers	Finding useful insights & Implications

Figure 1. Research Methodology

Data Exploration

An Excel spreadsheet is prepared for the same with the columns of Title of the research paper, respective hyperlink (for future reference), Authors, Number of authors, Year published, Name of Journal, Name of Conference, and Name of the Conference Series if applicable, Other research categories like books, chapters, etc.; Publisher of the work, and the Text of the research paper. The text of the research paper is compiled according to the cell limit in Excel. We primarily included essential segments of the research papers in the order of importance: Abstract, Introduction, Conclusions, Discussion, and Methodology, as

the entire paper's text does not fit into one cell. We successfully collected 314 research papers from various publishers between 1970 and 2024. Figure 2 shows a brief picture of the Excel spreadsheet we have made.

Title	Link	Authors	Year	Number of Authors	Journal Name	Conference Name	Conference Series	Others (Books, Theses, Dissertations, Patents, preprints, White papers, Technical Reports, etc.)	Publisher	Text
Scalable secure one-to-many group communication using dual encryption Author links open overlay panel	Scalable secure	L.R. Dondeti, S. Mukherjee, A. Samal	2000	3	Computer Communications				Elsevier	Multicasting is a scalable solution for group communication. Whereas secure unicast is a well-understood problem, scalable secure multicast poses several unique security problems, namely
Secure distributed storage and retrieval	Secure distributed storage	Garay, Juan A., Rosario Gennaro, Charanjit Jutla, Tal Rabin	2000	5	Theoritical Computer Science				Elsevier	In his well-known Information Dispersal Algorithm paper, Rabin showed a way to distribute information in pieces among servers in such a way that
Security of remotely operated robotic telescopes	Remotely operated Telescopes	Peter J. Surrey, Dorothy Muecke-Herzberg	2000	2		Astronomical Telescopes and Instrumentation 2000 conference	Advanced Global Communications Technologies for Astronomy		SPIE Digital Library	A robotic telescope is both a complex system with many potential modes of failure, and an attractive target for computer criminals. The paper describes a
Supporting reconfigurable security policies for mobile programs	Supporting security policies	Hashii, B, S Malabarba, R Pandey, M Bishop.	2000	5	Computer Networks				Elsevier	Programming models that support code migration have gained prominence, mainly due to a widespread shift from stand-alone to distributed applications. Although appealing in terms of
Mathematical Models of Computer Security	Models of computer sec	Peter Y. A. Ryan	2001	1		Foundations of Security Analysis and Design (FOSAD 2000)	Lecture Notes in Computer Science (LNCS)		Springer	In this chapter I present a process algebraic approach to the modelling of security properties and policies. I will concentrate on the concept of secrecy, also known as
The Role of Trust Management in Distributed Systems Security	Role of Trust Management in DDos security	Matt Blaze, Joan Feigenbaum, John Ioannidis, Angelos D. Keromytis	2001	4				Secure Internet Programming	Springer	Abstract. Existing authorization mechanisms fail to provide powerful and robust tools for handling security at the scale necessary for today's
Computer security impaired by legitimate users	Comp Sec	Besnard, Denis, Budi Arief.	2003	3	Computers & Security				Elsevier	Computer security has traditionally been assessed from a technical point of view. Another way to assess it is by investigating the role played by legitimate users of systems in impairing the level

Figure 2. Picture of a Spreadsheet containing datapoints, research papers collected, through their categories.

Text Mining Process

SAS Enterprise Miner is a data mining tool used to analyze large amounts of textual data and identify patterns within it. Starting with the File Import node, which takes the data file as input, we have uploaded our Excel file. In this node, we edited the variables and columns, selecting the Text column as the text variable and the Publisher and Year columns as targets. Next, the Text Parsing node is connected; this breaks down large text into terms. These terms assign weights to each term based on its frequency of use in the text. Next, the Text Filter node filters the terms by dropping unwanted terms that are assigned less weight. Next comes the Text Cluster node, which is the most crucial part of the model. Singular Value Decomposition (SVD) helps us to manage the dimensions of the term document frequency. A lower SVD yields informative text that is mined, while a higher SVD provides a more comprehensive summary. This helps group similar terms and clustering, which enables us to find unique patterns and insights within the text. The text Topic node provides the topics of the clusters, helping to align them with specific topics. This process enables us to derive practical implications from extensive, unstructured textual data. Figure 3 is a snapshot of our model in SAS Enterprise Miner.
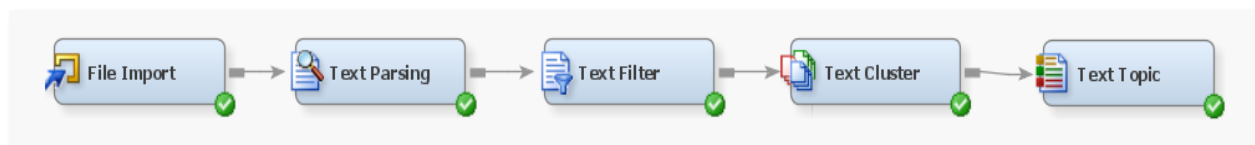
Figure 3. Model in SAS Enterprise Miner

Results

In this project, we aimed to derive valuable insights and trends from security research papers collected and segregated into different sets, utilizing clustering analysis to provide details on the types of research available in security-related fields within the collected papers. By using Excel, we can identify which publishers contributed the most in specific years and track the growth of the research over the past few decades. Below is Figure 4, which shows the number of publishers over the years from 1970 to 2024. The total represents the number of data points (research papers) we had collected; Springer, IEEE, Elsevier, and ACM made significant contributions towards security research. Over the years, research has increased. While collecting data, we observed that there are fewer papers from the 1970s and 1980s compared to those from 2020, which is understandable given the rapid growth in the digital space.

Publishers	1971-1980	1981-1990	1991-2000	2001-2010	2011-2020	2021-2024	Grand Total
Acadamic Press. Inc.	1						1
ACM	11					3	14
Addison Wesley			1				1
Blue Mark Publishers						1	1
Bon View Publishing Pte Ltd.						1	1
British Columbia Institute of Technology (BCIT)				1			1
CRC Press			2				2
Elsevier	2	5	20	17	27	22	93
Global Mainstream Journal						1	1
IARJSET						1	1
IEEE	9	11	11	7	30	21	89
IET					1		1
IGI Global Publishing						1	1
IJARCCE						1	1
IJCTT						1	1
IOP Publisheing					1		1
IRACST					1		1
Ital Publication						1	1
JAIGS						1	1
MDPI					1	14	15
MECS					1		1
Mesopotamian Journal of Cyber Security						1	1
MIT Libraries			3		1		4
Privolzhsky State University of Telecommunications and Informatics			1				1
Sage Journals					1		1
SAMS /Pearson			1				1
SPIE Digital Library			1				1
Springer	2	22	2	6	16	20	68
State University System of Florida			1				1
Taylor & Francis			1			1	2
Tech Science Press						1	1
Unknown						1	1
USENIX			1				1
Wiley Library						1	1
World Scientific News						1	1
Grand Total	25	38	45	31	80	95	314

Figure 4. Published research through years.

Concept Link Results

Concept Links are also used to know how each concept in the research is connected based on the available data. Let us look at the Concept Linkage of the term "Vulnerability." Figure 5 provides insight into

vulnerability and its explanation in the papers, with known vulnerabilities serving as common targets for threat actors. Cybersecurity threats exploit these vulnerabilities, potentially leading to suspicious activity that signals an impending attack. The process of escalation allows attackers to move within a system to gain more control, often employing sophisticated attack methods. User permission management and addressing vulnerabilities through patches and security measures are key to protecting against exploitation. The digital landscape provides the context for all these concepts, highlighting the environment that needs to be protected and where vulnerabilities can be found and explored. Fig 5 shows the concept linkage tree generated by SAS.
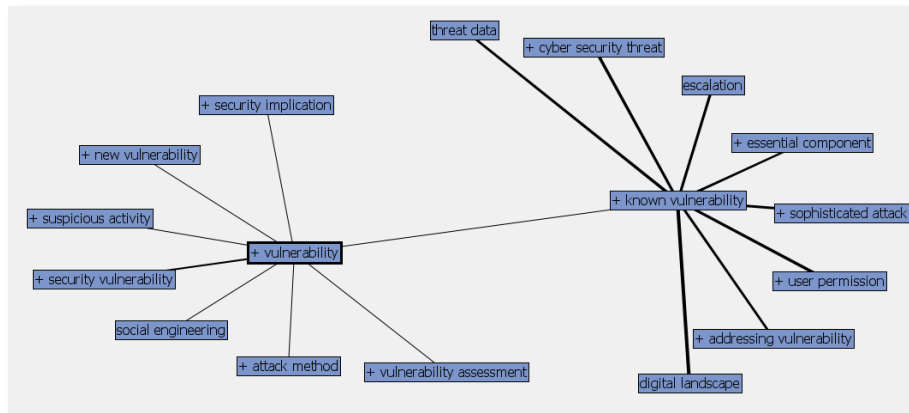
Figure 5. Concept Linkage for "Vulnerability"

Let us look at another term, Concept Linkage, for the term" Cryptography." Cryptography, as the main term, links to ciphers, which are the fundamental building blocks used in encrypting and securing information. *Ciphers* branch out into various specialized forms, such as block ciphers, which operate on data in blocks and are integral to cryptographic systems. The branches of public key and secret key represent different approaches to encryption, emphasizing the use of different keys for secure communication. Ciphertext is the result of the encryption process, ensuring that data remains secure until it is decrypted with the correct key. *Digital signatures* add a layer of security, providing authenticity and integrity checks. The cryptology field encompasses all these aspects, including the study of *encryption algorithms* and *cryptosystems* that ensure the confidentiality, integrity, and authenticity of the data. Overall, there is good coverage of research papers on the concept of cryptography, which helps in understanding the concept's links. Fig 6. Shows the concept link tree generated by SAS.
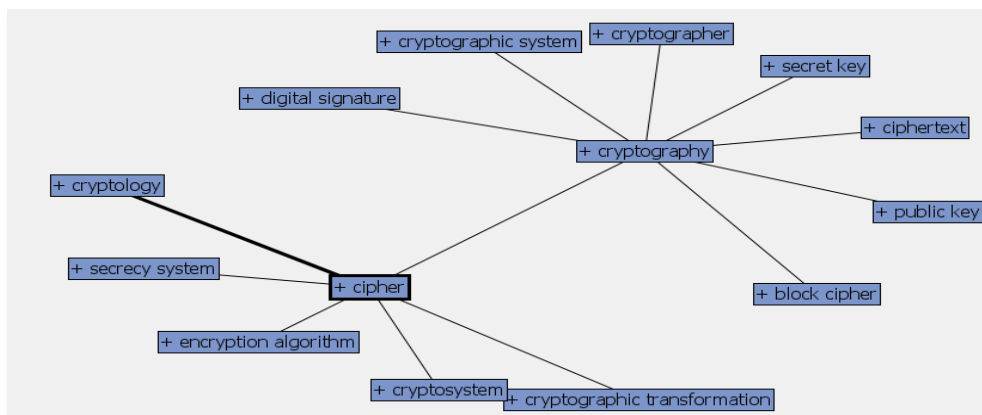
Figure 6. Concept Linkage for "Cryptography"

In Figure 7, referring to the term *"Cryptography,"* the term highlighted in the Title column. The respective text is fetched in the textfilter_snippet column (middle column), as shown in Figure 7. As the text is extensive, it is challenging to pinpoint the meaning, unlike finding concept links in sentiment analysis, which is relatively straightforward. Below is the list of papers on cryptography that contain all the concept links, as shown in Figure 7.

Figure 7. Documents showing Concept Linkage for " Cryptography"

Similarly, we would like to show the concept linkage of *"DDoS Attacks."* It includes all the attack-related information and the expanding WannaCry ransomware, a type of malware branch that we have observed. The terms indicate the potential reasons the ransomware attack could occur. Figure 8 represents the concept linkage for DDoS attacks.
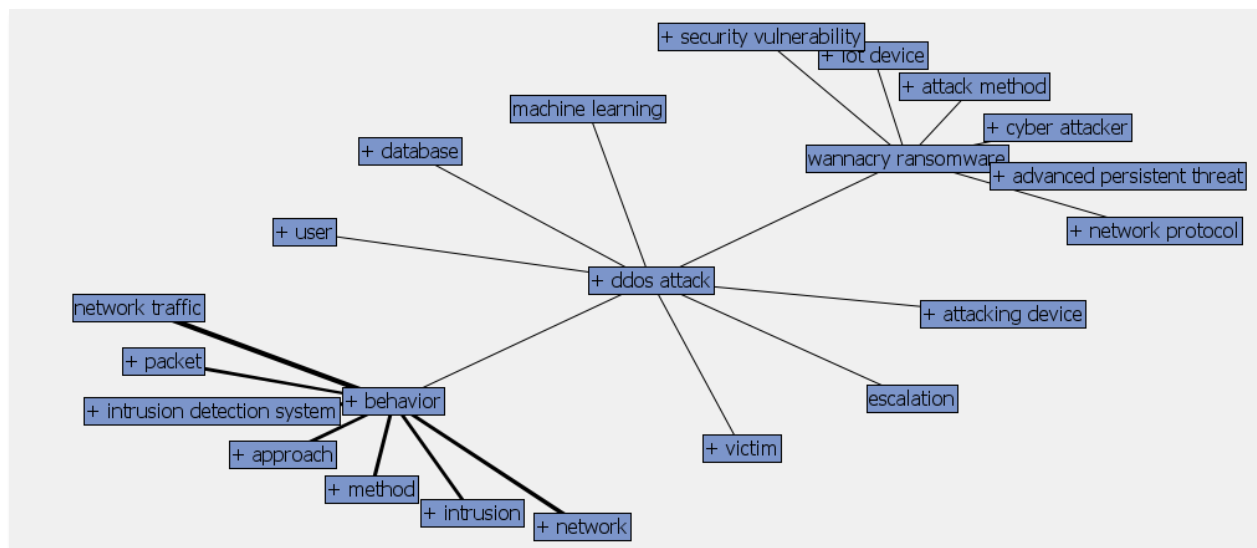
Figure 8. Concept Linkage for " DDoS Attacks"

Cluster Results

The results in Figures 9,11 are obtained with the following panel settings of Text Cluster Node: SVD resolution set to low, Maximum SVD dimensions set to 25, and for the cluster option, Exact, with a cluster number of 5. We employed a trial-and-error approach with various combinations (Table 2), but this particular combination yielded the most effective clustering results. Refer to Figures 9, 10, and 11 for more precise terms and graphical representations.
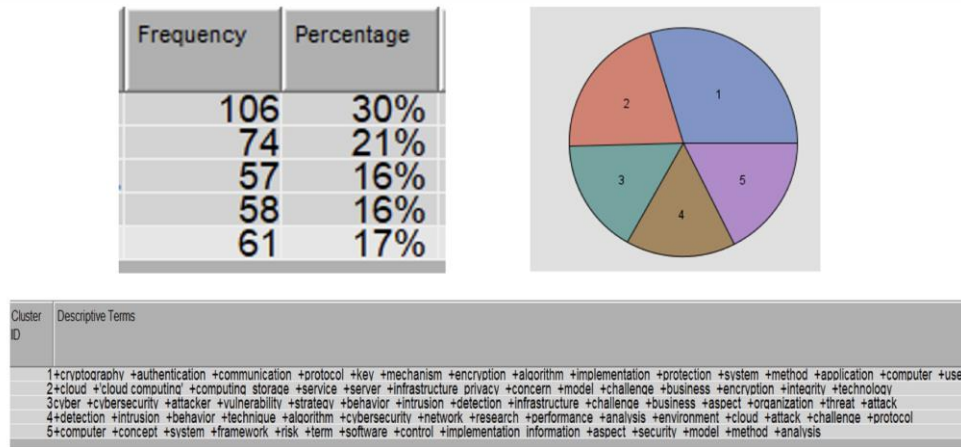

Figure 9. Cluster terms for 5 clusters, frequency and percentages and pie chart of the clusters formed.
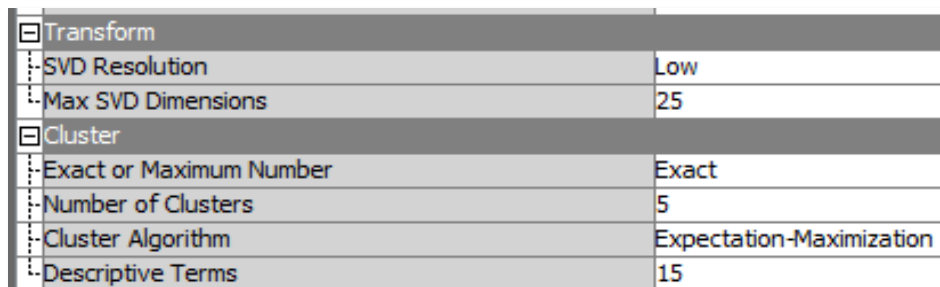
Figure 10. Text Cluster Node Panel Settings.
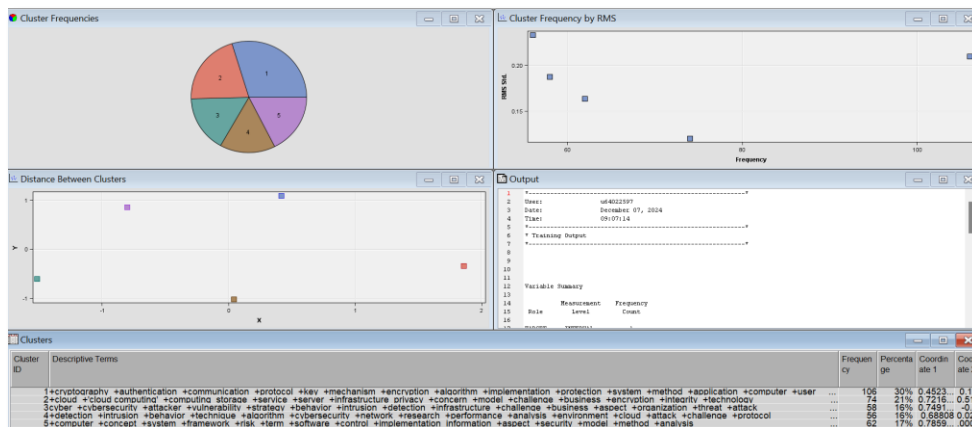
Figure 11. Results of Cluster Node.

Cluster descriptions for the finalized cluster results are listed in Table 1:

Table 1. Clusters and their descriptions.

Cluster	Description
Cluster 1	Cryptography and Security Protocols
Cluster 2	Cloud Computing and Privacy
Cluster 3	Cyber Security and Threats
Cluster 4	Intrusion Detection and Analysis
Cluster 5	General Security concepts and Frameworks

Here are some combinations we tried for cluster formations, but they did not yield significant results (Table 2). Combination 1 did not perform well; although the given cluster number was 5, the number of clusters formed was also 5, and it showed anomalies for 1 cluster. This might be due to high SVD resolution. Combination 2 was similar to Combination 1, but there were no anomalies. We observed that three of the clusters overlapped with each other. Combination 3 was the best outcome, with minimal overlapping and distinct clusters. Combinations used for the best clustering results are shown in Table 2:

Table 2. Combinations used for 5 clusters.

	Combination 1	Combination 2	Combination 3 (Best)
Frequency Weight/Term Weight	Log/Mutual Information	Log/Mutual Information	Log/Mutual Information
SVD Resolution	High	Low	Low
Max SVD Dimensions	200	100	25
Clustering Algorithm	Expectation-Maximization	Expectation-Maximization	Expectation - Maximization
Exact or Maximum	Exact	Exact	Exact
Number of Clusters	5	5	5

Topic Viewer Results

The topics provide a comprehensive overview of key areas in cybersecurity, including threat detection, cryptography, cloud computing, and risk management. The connections suggest opportunities for further exploration of how encryption protocols align with cloud security, the role of datasets in enhancing intrusion detection, and the use of algorithms in cyber solutions. Below is Table 3, which shows how each cluster, in Table 1, aligns with each topic from the topic viewer results. Figure 12, output by topic viewer in SAS.

Figure 12. Topics generated by the topic viewer.

Table 3. Topics aligning with respective Clusters.

Cluster Number	Cluster Description	Topics from Topic Viewer	Topic Description	Topic Number
1	Cryptography and Security Protocols	Cryptography, key, cryptosystems, encryption, protocol	Cryptography and security protocols	3
2	Cloud Computing and Privacy	Cloud, cloud computing, computing, storage, cloud environment	Cloud Computing and privacy	2
3	Cyber Security and Threats	Cyber, cybersecurity, cyber security, cyber threat, risk	Cyber security Threats and Attackers	1
4	Intrusion Detection and Analysis	Intrusion, packet, detection, host, intrusion detection system	Intrusion Detection and analysis	4
5	General Security concepts and Frameworks	Dataset, cybersecurity, detection, algorithm, IoT device	General security concepts and Frameworks	5

Additional Findings

Another critical finding we noted is that the number of authors was comparatively lower before 2010. Since 2010, there has been an increase in the number of authors, collaboration, and group research. Due to time constraints, we were unable to delve deeper into this topic; however, limited research is currently underway on this subject. Furthermore, the number of authors has been shown to affect the number of citations each paper receives (Quantifying Health, n.d.) , highlighting several significant key findings about the influence of the number of authors on the quality of a research paper.(Quantifying Health, n.d.)

Analyzed research papers from 2016 to 2021 and found that the median number of authors increased from 3 to 6 in the past 2 decades. This is also reflected in our dataset. They also mentioned that single-authored papers are becoming less popular. Single-authored research papers receive 34.7% fewer yearly citations compared to multiple-authored papers.

When the number of authors is extensive, descriptive studies, particularly those involving the contributions of multiple individuals, become questionable. No one knows who contributed what to the research. Analytical Studies are vast subjects and require a group of authors at any point in time. Below are some snapshots of our data, which reveal a pattern of the number of authors varying over the years.

In Figures 13 and 14, the number of authors is increasing over the years. We can observe that Figures 13 and 14 show a lower number of authors compared to Figure 15. After 2010, large groups began collaborating on research papers.

Title	Link	Authors	Year	Number of Authors	Journal Name	Conference Name
ON DATA BANKS AND PRIVACY HOMOMORPHISMS	https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=	Ronald L. Rivest, Len Adleman, Michael L. Dertouzos	1978	3		
Problem areas in computer security assessment	https://dl.acm.org/doi/abs/10.1145/1499402.	S. Glaseman, R. Turn, R. S. Gaines	1977	3		AFIPS '77: Proceedings of the
Some cryptographic techniques for machine-to-machine data	https://ieeexplore.ieee.org/abstract/document/1451934	H. Feistel,W.A. Notz,J.L. Smith	1975	3	Proceedings of the IEEE	
A modular approach to computer security risk management	https://ieeexplore.ieee.org/abstract/document/8817285	ROBERT P. CAMPBELL, GERALD A. SANDS	1979	2		International Workshop on Managing
Access control mechanisms for a network operating system	https://ieeexplore.ieee.org/abstract/document/8817205	HELEN M. WOOD, STEPHEN R. KIMBLETON	1979	2		International Workshop on Managing
Human resources systematically applied to ensure computer security	https://link.springer.com/chapter/10.1007/3-540-08934-9_105	V. P. Lane ,F. G. Wright	1978	2		European Conference on Information Systems
Privacy and Security Issues in Information Systems	https://ieeexplore.ieee.org/abstract/document/1674604	Turn, Ware	1976	2	IEEE Transactions on Computers	
The protection of information in computer systems	https://ieeexplore.ieee.org/abstract/document/1451869	J.H. Saltzer, M.D. Schroeder	1975	2	Proceedings of the IEEE	
Encapsulation: an approach to operating system security	https://dl.acm.org/doi/abs/10.1145/1408800.	Richard L. Bisbey, Gerald J. Popek	1974	2		ACM '74: Proceedings of the
Secure System Architecture	https://dl.acm.org/doi/abs/10.1145/641668.6	David Stryker, David Weiss	1974	2	ACM SIGARCH Computer Architecture News	
Privacy and security in databank systems: measures of effectiveness,	https://dl.acm.org/doi/abs/10.1145/1479992.	Rein Turn, Norman Z. Shapiro	1972	2		AFIPS '72 (Fall, Part I)
Factors Affecting Distributed System Security	Factors affecting Distributed systems	D.M. Nessett	1987	1	IEEE Transactions on Software Engineering	
The Upper Layers of Open Systems Interconnection	Open system interconnection	Rainer W. G. Herbers (Head)	1987	1		2nd International Symposium on
Challenges and Directions in Fault-Tolerant Computing	Challenges	J. Goldberg	1986	1		
Security, Privacy, Safety and	Security in	Rein Turn				

Figure 13. Research papers from years 1971 - 1980 with number of authors.

Title	Link	Authors	Year	Number of Authors	Journal Name	Conference Name
SATURNE: a distributed computing	SATURE	Y. Deswarte, J. Fabre, J.	1988	6		Fault-Tolerant
Denial of service flaws in SDI software-an initial assessment	SDI software an initial assesment	K.A. Nyberg, Grebyn Corp., Vienna,	1988	4		4th Aerospace Computer Security Applications
On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses	Block Ciphers	Yuliang Zheng, Tsutomu Matsumoto, Hideki Imai	1989	3		Advances in Cryptology — CRYPTO' 89 Proceedings
Is the Data Encryption Standard a group? (Results of cycling experiments on DES)	Data Encryption Standard group	Burton S. Kaliski Jr., Ronald L. Rivest, Alan T. Sherman	1988	3	Journal of Cryptology	
Foundations of dialog engineering: the development of human-computer interaction. Part II	Foundations of dialogue engineering	Gaines, Brian R., Mildred L. Shaw	1986	3	International Journal of Man-Machine Studies	
Verifiable-text attacks in cryptographic protocols	Cryptographic protocols	L. Gong, Comput. Lab	1990	2		IEEE INFOCOM 1990
Artificial neural-net based dynamic security assessment for electric power systems	Artificial Neural net Based security	D.J. Sobajic,Y.-H. Pao	1989	2	IEEE Transactions on Power Systems	
Cryptanalysis: a survey of recent results	Cryptanalysis	E.F. Brickell, A.M. Odlyzko	1988	2	Proceedings of the IEEE	
Views and security in distributed database management systems	Sec in Distributed database management systems	E. Bertino , L. M. Haas	1988	2		Advances in Database Technology—EDBT
A survey of password mechanisms: Weaknesses and potential improvements. Part 1	Survey of Password mech.	David L. Jobusch, Arthur E. Oldehoeft	1987	2	Computers & Security	
Identity-based conference key distribution systems	Identity based conference key	Kenji Koyama, Kazuo Ohta	1987	2		Advances in Cryptology –
Public Protection of Software	softw.	Amir Herzberg, Shlomit S. Pinter	1985	2		Advances in Cryptology —
Elements of Cryptology	Elements of Cryptology	M. Davio, J.-M. Goethals	1983	2		

Figure 14. Research papers from the years 1981 - 1990 with a number of authors.

Figure 15. Research papers from 2010 - 2024 with number of authors.

Adding a new dimension to our research, focusing on journals and conferences published by different publishers, we have noticed that some Journals have more research published. Journals like these help upcoming submissions select the best journal for publishing their work. In the data collected, there are many conferences and Conference Series, which made it difficult to determine which one had the most impact. Therefore, we focused on Journals for now. Figure 16 provides details on the number of journals, conferences, and other research sources in our collected data. There are 200 journal-published research papers in our data and 72 Conferences. Different categories, such as books, theses, and notes, are 41.

Springer, Elsevier, IEEE, ACM, and MDPI made significant contributions to specific security-related journals, respectively. In 200 Journal Publications, 182 publications belong to Springer, Elsevier, IEEE, ACM, and MDPI. These publishers are well-established and recognized for their focus on highly academic and technical research. Their dominance indicates significant contributions to the dissemination of knowledge in the field of cybersecurity and related disciplines. MDPI is recognized for its open-access journals, making research more accessible to a broader audience. Figure 17., shows the numbers.

Years	Journals	Conferences	Others (Books, Theses, etc.)
1971-1980	12	11	2
1981-1990	15	12	13
1991-2000	26	8	8
2001-2010	22	8	1
2011-2020	49	21	10
2021-2024	76	12	7
Grand Total	**200**	**72**	**41**

Figure 16. Journals, conferences, and Other Research through the years.

Years	ACM	Elsevier	IEEE	MDPI	Springer	Grand Total
1971-1980	5	2	5			12
1981-1990		4	7		4	15
1991-2000		20	5			25
2001-2010		17	1		3	21
2011-2020		27	10	1	7	45
2021-2024	2	22	11	14	15	64
Grand Total	**7**	**92**	**39**	**15**	**29**	**182**

Figure 17. Number of Journals published through the years, for ACM, Elsevier, IEEE, Springer, and MDPI.

Now, focusing on what those Journals are, contributed by the five publishers, Elsevier and IEEE had the top Journals. Computers & Security is a journal that has featured numerous security-related research studies since its inception in the 1980s, followed by IEEE Access. Based on research concepts, visibility, and ease of evaluation, one can choose between the top-published journals for their subsequent research publication. Figure 18 shows the details of the journals that have been most published from 1970 to 2024, from Elsevier, Springer, IEEE, ACM, and MDPI. We have considered all journals that have at least two publications.

Springer published a significant number of conference papers on cryptography in the 1980s. The conference was a series. Lecture Notes in Computer Science is a significant book series published by Springer, covering numerous conference papers related to security, networks, and other related topics. We have not analyzed the details of conferences and other research due to time and resource limitations.

Limitations

Our Text Mining project has many directions. Considering the results section, due to time constraints and a lack of sufficient resources, we have made our best efforts in this research and project. Data collection was the primary task, as every paper had to be manually checked and added to the spreadsheet without duplication over a period of many years. We were able to gather only 314 research papers on security-related research from major journals on Google Scholar. Many other publishers have published research on security-related issues, which we were unable to access. If a comprehensive database with sufficient literature is available on the research topics, publishers, journals, and conference details, it would be beneficial for projects like ours to identify more valuable and important Trends and Insights. Cluster formation has improved since we initiated the project, but many segments in security have not yet been added to the dataset.

Conclusion & Implications

The primary objective of this project is to identify trends in journals and publishers. We have found that IEEE, Springer, and Elsevier have made significant contributions to security research compared to other publishers based on the data we collected. Major popular publishers, such as ACM, MDPI, Taylor & Francis, Wiley, etc., may also have published some research work that we did not collect. Over the years, security-related issues have increased drastically. The 1980s marked the peak of cryptography, during which many researchers extensively discussed the topic. Machine Learning systems, also known as Expert Systems in the 1970s, faced many security-related issues that were then researched. The data collected contains different segments of concepts, including cloud computing, cybersecurity, intrusion detection, and

cryptography. All of these can be helpful for further research on each specific topic. The Computers & Security Journal, published by Elsevier, is the top journal based on our data. Elsevier mainly focuses on a Journal-Centric research approach and prefers stable and long-term achievements. IEEE and Springer focus on numerous conferences, making it easy for individuals to pitch their research ideas with a high scope of visibility. Elsevier, IEEE, and Springer dominate the journal market and MDPI's emergence as an open-access source after 2010 signals a shift in publishing preferences.
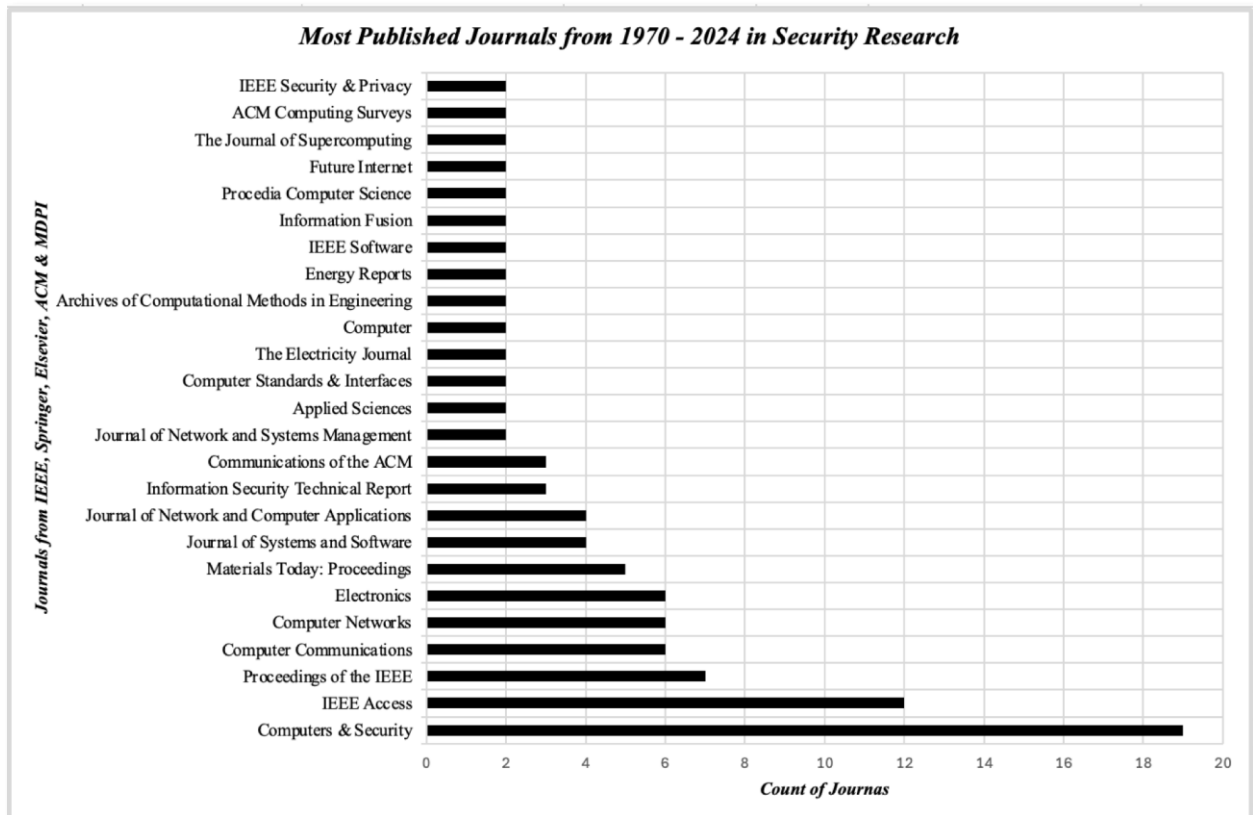
Figure 18. Most published journals from 1970 to 2024 in Security Research.

SAS provided objective clustering, separating research on cryptography, cloud privacy, intrusion detection, and other related topics, which is helpful for anyone entering the cybersecurity field to see where research is concentrated. While specific trends, such as an increase in authorship, can be identified manually, the goal of this research is to demonstrate the scalability and value of text-mining methods for analyzing large bodies of literature. As cybersecurity research continues to grow rapidly, automated techniques such as SAS text mining become increasingly essential for discovering latent themes, concept linkages, and topic distributions, especially for datasets that are significantly larger than our initial 314-paper sample.

Future Directions

Focusing on Conferences and other research may provide a significant lead, as we have noticed that books and book chapters have been very prominent in the past decade. By focusing more on book chapters and conferences, we can gain a whole new perspective. There are numerous unexplored areas in security-related research, including individual cyberattacks and cyber warfare. Collecting research papers specifically on

these topics and analyzing them can provide many valuable insights. Refining the research paper search to 5-year periods can cover many self-established publishers that were missed in our data. Focusing on a specific journal or a specific conference can also yield good results. With all these future directions fed into SAS Enterprise Miner, it can identify important keywords and help us understand the focus of journals or Conference papers.

References
(The research papers selected for this study are available upon request.)

Devo. (2023, October 20). *Demystifying the Role of a cybersecurity Researcher*. Retrieved from https://www.devo.com/blog/demystifying-the-role-of-a-cybersecurity-researcher/

Hennick, C. (2023, May 10). *The Importance of Cybersecurity in University Research Projects*. Retrieved from https://edtechmagazine.com/higher/article/2023/05/importance-cybersecurity-university-research-projects

Quantifying Health. (n.d.). *Does the number of Authors Matter? Data from 1,01,580 Research Papers*. Retrieved from https://quantifyinghealth.com/number-of-authors-of-research-papers/

Riskrecon by Master Card. (2023, June 20). *What we Learn from Cybersecurity Research*. Retrieved from https://blog.riskrecon.com/cybersecurity-research

The Royal Society. (n.d.). *Progress and Research in Cyber Security*. Retrieved from https://royalsociety.org/news-resources/projects/cybersecurity-research/

US National Science Foundation. (n.d.). *Cybersecurity*. Retrieved from https://new.nsf.gov/focus-areas/cybersecurity#image-caption-credit-block