ISSN: 2093-5374 / E-ISSN: 2093-5382

Machine Learning for Cybersecurity: A Bibliometric Analysis from 2019 to 2023

Yulian Purnama[1], A. Asdlori[2], Eka Maya Sari Siswi Ciptaningsih[3], Kraugusteeliana Kraugusteeliana[4*], Agung Triayudi[5], and Robbi Rahim[6*]

[1]Universitas Islam Negeri Saizu Purwokerto, Purwokerto, Indonesia. yulianpurnama@uinsaizu.ac.id, https://orcid.org/0000-0001-6676-9590

[2]Universitas Islam Negeri Saizu Purwokerto, Purwokerto, Indonesia. asdlori@uinsaizu.ac.id, https://orcid.org/0009-0008-3670-0611

[3]Binus University, Indonesia. eka.ciptaningsih@binus.ac.id, https://orcid.org/0000-0002-0908-0508

[4*]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia. kraugusteeliana@upnvj.ac.id, https://orcid.org/0000-0001-9868-425X

[5]Universitas Nasional, Jakarta, Indonesia. agungtriayudi@civitas.unas.ac.id, https://orcid.org/0000-0002-1269-5888

[6*]Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia. usurobbi85@zoho.com, https://orcid.org/0000-0001-6119-867X

Received: July 28, 2024; Revised: September 08, 2024; Accepted: October 07, 2024; Published: December 30, 2024

Abstract

With the increasing breadth and sophistication of cyber threats, machine learning must be integrated into cybersecurity. This study uses a bibliometric analysis on 427 documents from 2019 to 2023 to pinpoint current trends in machine learning applications for cybersecurity. An exponential 96.55 percent yearly growth in publications is shown by our analysis of data from the SCOPUS database, indicating a spike in research activity. We identify eminent journals like IEEE Access that are leading the way in dissemination, and active contributors like Sarker IH. Key research themes, including malware detection, Internet of Things ecosystems, network security, and model accuracy optimization, are revealed through the examination of keywords and semantic topics. The adoption of deep learning is a sign of technological progress. According to our findings, machine learning integration is widely used in cybersecurity for tasks like threat intelligence and infrastructure monitoring, to name just two. Availability improvements are still given priority by reliable automation. Due to the increase in cyber threats, machine learning is becoming a necessary skill rather than an add-on. This research sheds light on the groundbreaking findings and exponential trajectory that are transforming machine learning's application in cybersecurity. Machine learning is ushered into a new era of intelligent and flexible cyber defense systems, which implies that sustained innovation through international cooperation will be crucial. Our timely bibliometric analysis establishes a framework for future cybersecurity and machine learning research, as well as for technological advancement.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 4 (December), pp. 243-258. DOI: *10.58346/JOWUA.2024.I4.016*

Corresponding author: [4]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia; [6*]Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia.

Keywords: Bibliometric Analysis, Cybersecurity, Machine Learning,

1 Introduction

Cybersecurity is now a top priority for governments, businesses, and people all over the world due to the increase in cyber threats in recent years (Rizki, 2019; Bronk, 2013; Fraley & Cannady, 2017). Bad actors have launched sophisticated attacks that have caused significant damage, so advanced defenses are required to protect infrastructure and sensitive data. The critical significance of the situation has necessitated extensive research into innovative security methods employing advanced technologies like machine learning (ML) and artificial intelligence. Machine learning provides significant functionalities for cybersecurity, embracing predictive threat modeling, real-time anomaly detection, and adaptive defense mechanisms. As a result, the integration of machine learning has emerged as an important focus in cybersecurity research and industry in the last five years (Liu et al., 2018; Handa et al., 2019; Fraley & Cannady, 2017; Ningsih et al., 2018; Poornimadarshini et al., 2024).

Recent literature relates the convergence of several significant elements with the increasing interest in machine learning-based cybersecurity (Sarker et al., 2020; Ahsan et al., 2022). The increasing amount of big data from sources including system logs, network traffic, and threat feeds has resulted in a greater amount of data for training machine learning algorithms. Innovations in computer power due to cloud computing and graphics processing units have made possible the training of more advanced machine learning models (Oh & Kim, 2020; Asvadishirehjini et al., 2022; Sunarti et al., 2023). Advances in deep neural networks have significantly enhanced machine learning's ability to recognize patterns, making it perfect for assessing cybersecurity risks (Demontis et al., 2017; Caviglione et al., 2021; Handa et al., 2019). The adoption of machine learning (ML) in cybersecurity has accelerated due to its success in related domains such as malware and fraud detection (Zhou et al., 2019; Pinto et al., 2022; Mustapa et al., 2023).

This ideal environment has led to a Cambrian explosion of research on machine learning applications in cybersecurity, ranging from insider threats to phishing. For specific cyber tasks such as malware classification, botnet identification, intrusion and anomaly detection, and attack prediction, researchers have customized machine learning (ML) algorithms such as support vector machines, random forests, and deep neural networks (Mary & Nalini, 2019; Surekha et al., 2024; Holbrook & Alamaniotis, 2021). Comparison tests show that neural networks perform better than other classifiers a lot of the time. Newer methods, such as deep reinforcement learning, have promise beyond supervised learning because they allow security systems to dynamically optimize defenses (Leon et al., 2022; Nguye & Reddi, 2021; Oh et al., 2023).

To analyze the growth and direction of this emerging research domain, bibliometric analyses offer valuable information. Bibliometrics involves statistical analysis of academic literature to uncover trends, patterns, and key contributions (Watrianthos et al., 2023; Windarto et al., 2023; Watrianthos & Yuhefizar, 2023; Ahmad et al., 2023). Previous bibliometric studies have examined trends in cybersecurity research in general (Duffy & Duffy, 2020; Sherlin & Nikila, 2022; Makawana & Jhaveri, 2018). However, there are still literature gaps in bibliometric assessments focused specifically on ML integration in cybersecurity. This article presents a bibliometric analysis of the literature on cyber security ML in the past five years (2019-2023). Bibliometric methods are utilized on the SCOPUS database to identify significant trends and patterns in this swiftly advancing field. The study timeline offers current insights into recent advancements in machine learning that are revolutionizing cybersecurity.

2 Literature Review

Artificial Intelligence

Through utilizing algorithms, data, and processing capability to solve issues, detect trends, and offer insights, artificial intelligence (AI) is a futuristic technology that replics human intelligence from banking to healthcare, it is transforming industries and streamlining procedures to improve client experiences. Because they can handle vast amounts of data faster than humans, artificial intelligence systems can find trends or insights otherwise missed. From virtual assistants scheduling our calendars to sophisticated medical imaging tools enabling disease diagnosis, artificial intelligence is gradually ingrained in our daily lives (Negnevitsky, 2005; Gao & Liu, 2023; Haenlein & Kaplan, 2019).

Still, even with its great promise, artificial intelligence presents serious ethical and social problems. Data privacy, employment displacement, and the fairness of artificial intelligence decision-making systems continue to be issues of concern particularly when data errors produce biassed results (Russell & Norvig, 2016; Shneiderman, 2020). Moreover, even if artificial intelligence can automate some chores, it lacks the emotional intelligence and creativity humans bring to challenging problem-solving and interpersonal connections. Balancing the benefits AI presents with the need to solve its drawbacks will be vital as it develops to support a future of peaceful coexistence between people and robots.

Machine Learning

A subset of artificial intelligence, machine learning (ML) lets computers learn from experience without direct programming, hence enhancing their performance. Unlike conventional programming, in which a developer lays out guidelines and requirements for every scenario, machine learning systems use data to identify trends and generate conclusions or predictions. This technique frequently entails training models on extensive datasets, allowing them to "learn" to execute tasks such as image recognition, language translation, or engaging in intricate games like chess. Machine learning is integral to numerous technologies we engage with daily, including recommendation systems on streaming platforms and autonomous vehicles (Forghani et al., 2021; Liu et al., 2022; Gupta et al., 2021).

The essence of machine learning lies in its ability to generalize from examples. It’s like teaching a child to identify animals in pictures—not by telling them every detail of what makes a cat a cat, but by showing them enough examples that they start recognizing common traits. The more data the system has, the better it can distinguish between categories, detect anomalies, or forecast trends. However, just like human learning, ML models are not perfect. They may commit errors or cultivate biases derived from their training data, underscoring the necessity of employing broad and balanced datasets.

Machine Learning (ML) can be categorized into three primary types: Supervised Learning, Unsupervised Learning, and Reinforcement Learning. Each type varies in the methodology by which the algorithm acquires knowledge from data and the specific tasks it is intended to execute.

a. Supervised Learning
   In supervised learning, the model is trained with labeled data, indicating that the input data is associated with the accurate output. The algorithm acquires the ability to associate inputs with the appropriate outputs through these exemplars. This learning method is commonly employed for classification and regression applications. Predicting housing values (regression) and categorizing emails as spam or not (classification) are quintessential examples of supervised learning (Bolaj & Govilkar, 2016).

b. Unsupervised Learning
Unsupervised learning uses unlabeled data to indicate that the system learns free from direction about expected outcomes. The goal is to identify structures, trends, or correlations in the data—including cluster-based classification of like objects. Common applications for it include association rule learning, dimensionality reduction, and clustering (Sibyan et al., 2021).

c. Reinforcement Learning
Reinforcement learning operates on a reward-based framework, wherein the model acquires knowledge through interaction with its environment and receives feedback as rewards or penalties. It is frequently employed in situations requiring sequential decision-making, where the results of those decisions affect subsequent choices. This form of learning is prevalent in robotics, gaming AI, and autonomous systems (Kasim, 2016). Example Algorithms: Q-Learning, Deep Q-Networks (DQN), and Proximal Policy Optimization (PPO).

Cybersecurity

Cybersecurity is the defense against digital attacks of systems, networks, and data. Cybersecurity has become crucial for people, companies, and governments in a world growingly linked where personal and sensitive data is kept and sold online. Cyberattacks take many different forms: viruses, phishing scams, advanced hacking attempts aiming at data theft or alteration. These strikes can have disastrous effects on finances, identity theft, or major interruptions of vital services as energy systems or healthcare (Bastos et al., 2018).

A major issue in cybersecurity is keeping up with the rapid advancement of technology. Emerging technologies often exhibit vulnerabilities that can be exploited by adversaries. As the quantity of devices linked to the Internet of Things (IoT) increases, the potential access points for cybercriminals proliferate. Furthermore, with the proliferation of cloud computing, the protection of data privacy and security in these remote environments is becoming an increasing concern. Cybersecurity specialists are consistently involved in the pursuit of identifying and mitigating these vulnerabilities before they may be exploited.

Cybersecurity addresses human aspects as well as technological ones. Human mistake—including contact with dangerous links or the use of weak passwords—allows a significant fraction of cyberattacks to be effective. This emphasizes the need of knowledge and awareness in general education. By helping people to identify possible hazards and implement best practices—that is, by using two-factor authentication and routinely updating programs—the danger of breaches can be much lowered. Cybersecurity is the application of appropriate technologies and procedures together with the development of a culture of vigilance and responsibility all across an organization or community.

As cyber threats become more sophisticated, the need for robust cybersecurity strategies grows. Governments and corporations alike are investing heavily in this field, but individuals also play a key role in protecting their own data. In the end, cybersecurity is a shared responsibility, and staying safe in the digital world requires constant attention to evolving threats and proactive defense measures (Boyle et al., 2017; Kaufman et al., 1995).

Cyberattacks are deliberate attempts by malicious individuals or groups to compromise computer systems, networks, or data for various purposes, such as stealing sensitive information, disrupting services, or causing harm to individuals or organizations (Ganeshan et al., 2023). These attacks can take many forms, ranging from simple tactics to highly sophisticated strategies, often targeting vulnerabilities in software, hardware, or even human behavior. The motivations behind cyberattacks can vary widely—some attackers seek financial gain, while others may aim for political or social disruption, espionage, or just personal satisfaction.

Here are some common forms of cyberattacks:

a. **Malware:** Malware (short for malicious software) refers to a variety of harmful software types designed to damage, disrupt, or gain unauthorized access to a computer system. This includes viruses, worms, trojans, and ransomware. Ransomware, for example, encrypts a victim's data and demands payment (often in cryptocurrency) in exchange for restoring access to the data.
b. **Phishing:** Phishing attacks involve tricking individuals into providing sensitive information, such as passwords, credit card details, or social security numbers, by pretending to be a trustworthy entity. Phishing often occurs via email, where attackers impersonate legitimate businesses or institutions to lure victims into clicking on malicious links or downloading infected files.
c. **Denial-of-Service (DoS) Attack:** The goal of a denial-of-service attack is to prevent authorized users from accessing a service by flooding a system, server, or network with traffic. A Distributed Denial-of-Service (DDoS) attack is a more sophisticated variant that employs a network of compromised computers or devices to overwhelm the target with traffic all at once.
d. **Man-in-the-Middle Attack (MITM):** A man-in-the-middle (MITM) attack occurs when an attacker discreetly listens in on two parties' conversations and tampers with them without their knowledge. The perpetrator can then listen in on discussions and potentially steal important data like passwords or bank account information.
e. **SQL Injection:** By taking advantage of security holes in website code, SQL injection attacks aim to compromise databases. An attacker can obtain unauthorized access to, alter, or remove data recorded in a database by injecting malicious code into a query field. This could result in catastrophic harm to individuals or enterprises.
f. **Zero-Day Exploit:** When hackers take advantage of a software flaw that the developer is unaware of, it's called a zero-day assault. Attackers can do a lot of damage before a fix is produced and applied because the vulnerability hasn't been found or patched yet.

If a cyberattack succeeds, it might have devastating effects. Businesses risk operational disruption, reputational harm, and significant financial losses; individuals risk identity theft, financial loss, or privacy violations. On a larger scale, cyberattacks on critical infrastructure, such as energy grids, healthcare systems, or transportation networks, can have far-reaching consequences, affecting millions of people and causing national security concerns.

Bibliometric

Bibliometrics is the science of measuring and analyzing scholarly literature, providing insights into the productivity and influence of academic research. It's a way to evaluate the impact of scientific work by examining patterns in citations, publications, and authorship (Watrianthos et al., 2022; Ellegaard, 2018). By using bibliometric tools, researchers and institutions can better understand which studies are having the most influence in a given field and how knowledge is spreading across different disciplines. Bibliometrics, for instance, can highlight how influential or basic that study is inside the scientific community by counting the times an item is cited by others.

Tracking academic output and effect at many levels—from individual researchers to whole institutions—is one of the primary applications of bibliometrics. Metrics such as the h-index evaluate not just the quantity but also the quality, or effect, of a scholar's works as shown by citations. Universities, funding organizations, and legislators can use this kind of study to guide decisions on research spending, promotions, and resource distribution. Finding new trends in science and pointing

out significant scholars or breakthrough studies influencing the direction of their respective disciplines also depend much on bibliometrics.

Nonetheless, bibliometrics has certain restrictions. Although publishing figures and citation counts have great value, they do not necessarily tell the whole picture. Some studies might be ahead of their time or concentrate on specific areas, therefore they might be revolutionary but slow to be mentioned. Moreover, not all references are equal; some can originate from low-impact sources or show critical replies instead of endorsements. Furthermore, the drive to raise citation numbers might result in behaviors like too high self-citation or citation networks, therefore distorting the actual impact of the work.

Notwithstanding these difficulties, bibliometrics is still a valuable instrument in the academic scene. It provides a means to measure the enormous amount of information generated and to draw attention to the efforts advancing science and education. Bibliometric tools are getting more complex as the field develops and provide a more complete picture of research influence including more recent measures like altmetrics, which consider social media mentions and online activity, so offering a wider view of how research is influencing events outside of scholarly journals.

3 Method

In this work, we investigate the main trends and patterns in cybersecurity machine learning applications spanning 2019 to 2023 by means of bibliometric analysis. Bibliometrics offers a whole picture of current research activity and its influence across time. It is a quantitative method of analyzing the academic literature. This methodology is especially suitable for our research since it enables the collection and evaluation of extensive datasets, facilitating the identification of critical trends, prominent authors, and important themes in the area (Ninkov et al., 2022; Lawani, 1981; Greener, 2022). This bibliometric approach correlates with the increasing recognition of the subject's significance in academic research, as shown by its widespread usage across different fields of science.

We used SCOPUS as our main source of data because it has a lot of indexes for peer-reviewed articles and other scientific books. Because its database contains a huge number of papers and citations (Burnham 2006; Singh et al., 2021). SCOPUS is the best choice for this kind of large-scale and general bibliometric study. The study mostly looked at papers that had "machine learning" in the title and "cybersecurity" in the title, summary, or keywords. We were able to be sure that our data set accurately showed how these two important groups came together by focusing on keywords. The analysis only looked at stories from 2019 to 2023. The data was first collected in January 2024. This time frame was picked to give a modern look at the subject, taking into account the most recent developments and debates.

In our bibliometric study, we followed common procedures in the field, such as normalizing term variants and taking case sensitivity into account. This method lets one get a better sense of the study area, which leads to a more accurate and uniform picture of the data. The way we did our study and the way we analyzed it are similar to how bibliometric analyses are done now, using tools like Biblioshiny (Aria & Cuccurullo, 2017; Radha & Arumugam, 2021) to help us. This makes sure that our methods are sound and that our results are correct.

4 Result and Discussion

In the year 2019–2023 the research is mostly publish how machine learning techniques change cybersecurity view. The research result shows how result crosses over into different fields by looking at data from 1s95 sources, such as scholarly papers and literature.

An analysis of 427 documents from this time period demonstrates a large corpus of research and growing interest in using machine learning to boost cybersecurity defense. The survey found a 96.55% yearly growth rate, indicating increased interest in machine learning and cybersecurity. This growth shows the changing cybersecurity landscape and the potential of machine learning technologies to create creative solutions. The materials, which average 1.94 years old, stress the timely and relevant research, guaranteeing that the conclusions are instantly applicable.

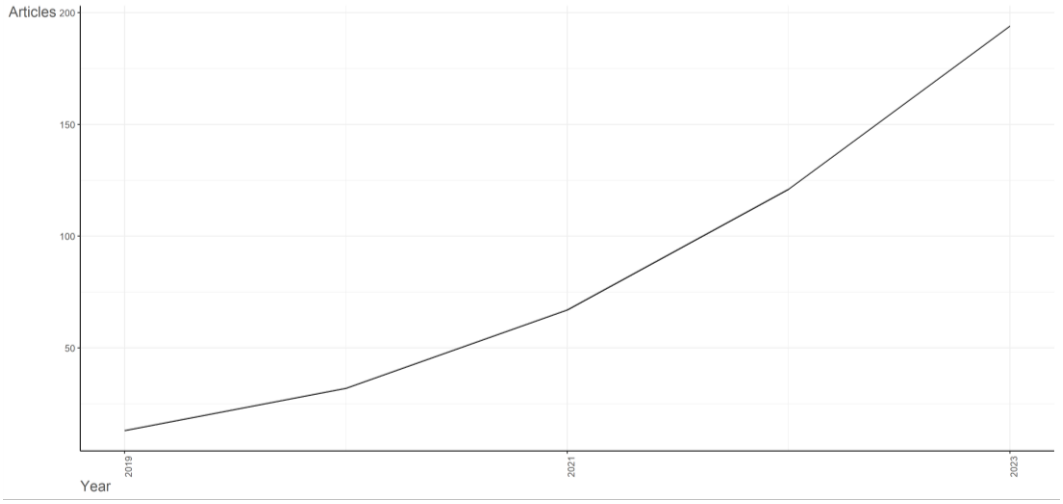

Figure 1: Annual Scientific Production

Figure 1 illustrates an exponential growth in research output on machine learning applications in cybersecurity from 2019 to 2023. The quantity of published publications on this subject increased from 13 in 2019 to 194 in 2023, representing a 1,392% growth over the five-year span. Upon further analysis, 2020 was a pivotal inflection moment, as the number of articles more than doubled from the prior year, totaling 32. The accelerated growth trend continued into 2021 and 2022, with annual article increases of 109% and 81%, respectively. In conclusion, 2023 experienced the most significant annual increase, with production nearly doubling compared to the total of 2022. Multiple factors are expected to influence these publication trends.

Cyber dangers have increasingly proliferated, evolved in complexity, and intensified in destructiveness during the last decade. Machine learning serves as a sophisticated approach to augment cyber defenses via functionalities including automated threat identification, real-time analytics, and predictive modeling. The proliferation of Big Data has facilitated numerous machine learning applications by supplying extensive datasets for algorithm training. The increasing significance of domains such as deep learning and neural networks facilitates more intricate pattern identification, which is optimal for examining the dynamic characteristics of cyberattacks. Considering the capacity of machine learning to revolutionize traditional cybersecurity methods, these publishing trends indicate that ML-based cyber defense will continue to be an increasingly significant focus in academia and industry in the forthcoming years. If growth persists at such rates, annual output may surpass 700 articles by 2028 according to extrapolation. This academic attention mirrors pressing real-world needs to

develop intelligent and agile cyberprotection. Ultimately, machine learning is poised to revolutionize nearly all aspects of cybersecurity in the years ahead, from infrastructure monitoring to incident response. To support these emerging solutions, dedicated research efforts will remain integral.

The average rate of citation per document is 14.56, demonstrating the significant impact and recognition that this research body has gained in the academic sphere. Citation patterns reveal valuable insights that complement publication trends. Articles from 2019 garnered the highest total citations per article (90.54), which is reasonable given their 6 years of accumulation of references. We see a sequential decline in per-article citations moving from 2020 (45.94 in 5 years) to 2021 (24.96 in 4 years) and 2022 (12.21 in 3 years). The 2.17 citations for 2023 articles (over 2 years thus far) underscore that accrual requires time.

However, when adjusting for citable years, the 2019 articles generated the most citations per year (15.09), followed by annual declines between 2020 and 2023. Two factors probably explain this trend: The lessening cumulative citable years for newer articles restricts the citation ceiling, whereas exponential publication growth spreads references across expanding outputs. Ultimately, while recent articles have accrued fewer total citations as a result of less citable time, their annual rates remain comparable to earlier work. Looking forward, citations should multiply rapidly as more articles refer to the exponentially expanding literature. Furthermore, surging outputs typically precede impact of the citation, as seminal works require time to diffuse through the research ecosystem to maturity of the citation.

The study also identified a wide range of topics and terminologies, including 2131 keyword plus (ID) and 1149 author keywords (DE), which form the discussion on the integration of machine learning into cybersecurity measures. The collaboration of this study was highlighted by the identification of 1546 authors, 23 of whom contributed a single document. Furthermore, the data reveal 24 documents with a single author and an average of 3.98 coauthors per document, with a significant rate of 31.85% of international coauthors. When viewed through the lens of machine learning, this highlights the importance of worldwide cooperation in order to overcome the myriad of difficulties that are associated with cybersecurity.

Top Contributing Authors and Journals

The dataset showing the most frequently cited local authors in machine learning studies for cybersecurity from 2019 to 2023 provides important insights into research contributions and collaborations. a combination of five articles written by Sarker IH and a fractional authorship of 1.87, there is a lot of collaboration. By this trend, it looks like Sarker IH has worked with other scholars a lot, coauthoring papers with them. The group of writers Khan, MA, Li, Z, Sun, Y, and Wen, S, who are each credited with writing four publications, is also interesting. The fact that their fractional contributions range from 0.63 to 0.79 shows how collaborative research is in this area and how they fit into bigger authoring teams.

Alsubhi K should be praised for writing three papers that have a fractional contribution of 1.25, making them the author with the biggest relative individual contribution. According to this measure, Alsubhi K is the main or only author on most of their papers. This shows that they are personally very committed to advancing study in this area. The data set shows that 21 writers contributed a total of 3 pieces, with 0.43 to 1.25 percent of the total amount of work. The different amounts of fractional contributions show that study collaboration can take many forms, including small projects done by individuals and large group efforts.

Sarker IH is the most productive author in the dataset. From 2020 to 2023, he or she produced three works that have been cited 490 times. Their paper in 2020 on cybersecurity data science is important; it has been cited 243 times, which is about half of all the citations for Sarker IH. The big effect this work had shows how well and how important Sarker IH's contributions are to the field of cybersecurity. "Cybersecurity Data Science: An Overview from a Machine Learning Perspective," a 2020 study by Sarker IH et al., gives a thorough and critical look at how data science, specifically machine learning, has changed cybersecurity operations (Sarker et al., 2020). This book creates a basic framework for future study in cybersecurity data science. It shows how machine learning is an important part of making complex and flexible security systems that can adapt to how cyber threats change.

A basic study by Sarker IH that showed the start of Cybersecurity Data Science (CDS) is a big step forward in the field of cybersecurity. This paper presents CDS, a unique, cross-disciplinary approach utilizing machine learning to filter and investigate vast volumes of cybersecurity data. By use of more advanced, data-driven approaches, this initiative aims to make security systems smarter and more automated, so displacing older, less advanced solutions. These intricate systems are meant to precisely identify and block cyberattacks, therefore ushering in a new phase of cybersecurity strategies. This paper provides a lot of material on the several ways in which machine learning techniques could be applied in cybersecurity. This paper presents a lot of material on how to apply controlled and unsupervised learning, neural networks, deep learning, and other approaches like reinforcement learning and semi-supervised learning. The discussion of these techniques underlines their applicability in establishing robust security policies, spotting unusual trends, and cybercrime prediction. This reveals how adaptable and successful machine learning is in improving defense systems.

According to analysis, in machine learning and cybersecurity research, the impact of current sources and the fast growth of new ones is far more essential than publication number. The dynamic character of academic publishing in these disciplines is shown by the capacity of emerging publications to rapidly convey their influence. With 855 citations over 43 papers, IEEE Access boasts the most. With the volume of publications, this is expected. By publishing several important papers, the journal's h-index of 13 and g-index of 29 show its major influence on the subject.

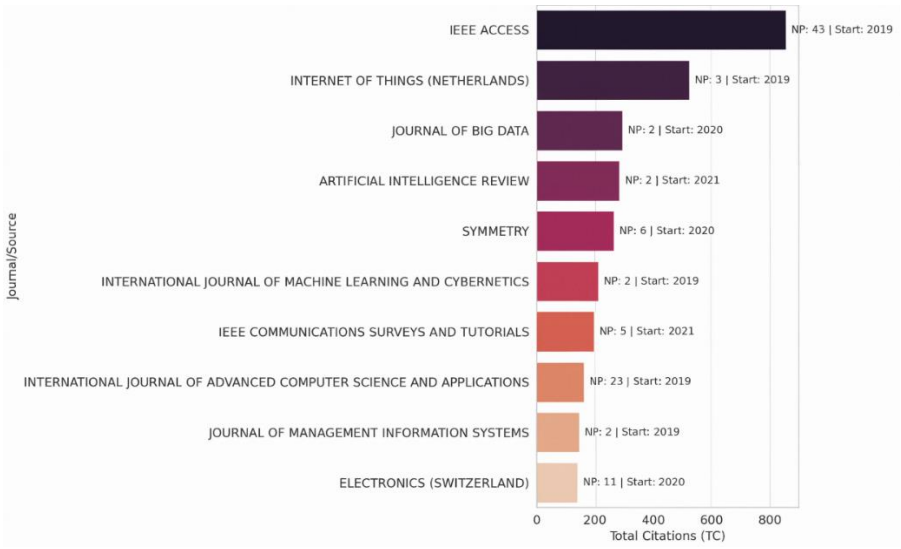

Figure 2: Top 10 Journals/Sources by Total Citation

Figure 2 shows each journal's total citations, demonstrating its academic and scientific value. IEEE Access leads the pack with a high citation count, demonstrating its vital role in spreading machine

learning for cybersecurity research. The visualization extends this tale by annotating each bar with the number of publications (NP) and the year each source began contributing to this topic. Each journal's productivity and historical impact are better understood with this dual-layered annotation. This complex graphic shows that a journal's impact must be measured based on its citation count, amount of contributions, and duration of influence. Early journals built a basis for future study and showed lasting value by continued citations. Recent journals have made substantial contributions to cybersecurity machine learning discourse, as shown by their high citation metrics.

Research Focus and Trends

Our analysis of frequently occurring author keywords reveals several salient trends in the evolution of research interests within the intersecting domains of machine learning and cybersecurity. The most striking observation is the continued primacy of terms machine learning and cybersecurity, which emerge as the predominant authors keywords in the dataset. Their ubiquitous appearance in 290 and 188 publications, respectively, underscores machine learning and cybersecurity as the twin pillars of inquiry that propel advancements in this field. Beyond these core themes, we discern a burgeoning scholarly emphasis on state-of-the-art techniques like deep learning and learning algorithms that promise to expand the frontiers of machine learning's applicability to pressing cybersecurity challenges. The discourse is also progressively encompassing new technologies like the 'Internet of Things', which present fresh and complex security vulnerabilities requiring innovative machine learning solutions.

The prevalence of keywords such as 'intrusion detection,' 'network security,' and 'computer crime' points towards intensifying research activity aimed at deploying machine learning within specific subdomains of cybersecurity. There appears to be a special research thrust towards advancing machine learning's role in network intrusion detection systems, as evidenced by the recurring emergence of associated keywords like 'anomaly detection' and 'classification.' An in-depth reading of keyword patterns reveals an optimistic outlook for machine learning-driven evolution across the cybersecurity landscape, with growing integration across application areas and emerging technologies. Our data set contains signals of a research community steadily expanding the boundaries of discovery through refinement of existing techniques and exploration of uncharted problem spaces.

Table 1: Five Different Topics based on Abstract

Topic	Keywords	Interpretation
Topic 1 - Malware and Phishing Detection	Detection, learning, machine, malware, dataset, phishing, accuracy, model	This topic seems to focus on the use of machine learning to detect malware and phishing activities, with an emphasis on accuracy and the use of specific datasets.
Topic 2 - Network Security and Data Analysis	Network, attacks, data, learning, model, machine, cybersecurity, systems	Research in this area appears to focus on the application of machine learning to network security, analyzing data to detect and prevent cyberattacks.
Topic 3 - ML in cybersecurity systems	Learning, ML, machine, security, cyber, attacks, systems, cybersecurity	This topic probably covers the broader application of machine learning (ML) in cybersecurity, including the development and enhancement of security systems.
Topic 4 - IoT Security and Attack Detection	Learning, Machine, IoT, Attacks, Detection, Network, Security, Data	A focus on the intersection of IoT (Internet of Things) and cybersecurity, with machine learning being used to detect and mitigate attacks on networked IoT devices.
Topic 5 - Malicious Activity Detection and Model Accuracy	Based, learning, machine, data, malicious, model, attacks, accuracy.	This subject examines the accuracy and reliability of machine learning models for malicious activity detection.

Table 1 illustrates the Latent Dirichlet Allocation (LDA) topic modeling, showing five popular studies in the field of machine learning applications for cybersecurity. Each topic contains a unique lexical footprint, indicating the primary study focuses and methodologies. The starting topic focuses on

the utilization of machine learning in the identification of malware and phishing. This topic likely covers studies utilizing machine learning algorithms on chosen datasets to develop predictive models for detecting malware and phishing threats, with keywords such as "detection," "malware," "phishing," and "dataset." The focus on performance indicators like "accuracy" highlights the need for dependable threat detection.

The second topic focuses on research about the utilization of machine learning in network security and the analysis of cyber attack data. The prominent terms "network," "attacks," "data," and "systems" imply research focused on using machine learning methodologies to examine network traffic data and identify aberrant behaviors that signal cyber invasions. This aligns with the increasing network-centric nature of cyber threats. The third area pertains to extensive research on the incorporation of machine learning into cybersecurity systems for the purposes of attack prevention and response. Research in this field, encompassing keywords such as "learning," "security," "attacks," and "systems," is expected to investigate enhancements in cyber defense via machine learning-based methodologies, including automated threat detection and vulnerability detection.

Topic four highlights an increasing application domain, employing machine learning for security across IoT environments. The main keywords "IoT," "attacks," and "detection" suggest research focused on reducing IoT's cybersecurity threats through machine learning-based attack identification and prevention. The rapid application of IoT could increase its vulnerabilities through advanced security mechanisms. Finally, subject five underscores the advancement of machine learning models for identifying fraudulent behavior, especially focusing on accuracy metrics. Studies likely concentrate on increasing model performance to improve the reliability of detecting threats such as malware, phishing, or network intrusions, utilizing terminology like "malicious," "model," and "accuracy." Precision is essential for reliable security automation.

By integrating various subjects, we can discern prevalent tendencies. The primary focus of the research is the application of machine learning for threat detection across several domains, including malware and network intrusions. The model's accuracy is significantly underscored, highlighting the necessity for dependable security systems. This has resulted in the modification of methodologies for a varied cyber environment, encompassing the Internet of Things. Advanced techniques, such as deep learning, are increasingly prevalent, indicating a progression in the methodologies underpinning cybersecurity machine learning. Our analysis yields critical insights into the prevailing goals, applications, and trajectories within the swiftly advancing research domain at the convergence of machine learning and cybersecurity.

5 Conclusion

This comprehensive research, covering the period from 2019 to 2023, has carefully examined the incorporation of machine learning in cybersecurity, revealing notable insights and trends. The extraordinary yearly growth rate of 96.55% in this sector indicates a rapidly transforming environment, where machine learning serves not just as an additional instrument, but as an essential element in the advancement of innovative cybersecurity solutions. The average document age of 1.94 years underscores the relevance and timeliness of the research, assuring its direct applicability to current cyber threats. The exponential growth of research, especially after 2020, reflects the increasing complexity and sophistication of cyber threats, requiring advanced solutions such as machine learning. This trend is further validated by elevated citation rates, particularly for foundational publications in cybersecurity data science, highlighting the community's acknowledgment of their significant influence.

Authorship trends show a diverse and cooperative research community with prolific contributors like Sarker IH and emerging thought leaders, demonstrating a dynamic interaction of individual and collaborative research. The field involves cybersecurity, data science, intrusion detection, and future technologies including Internet of Things. The demand for smart and flexible cyber defences drives the research in machine learning-based cybersecurity expected to increase. Advanced machine learning techniques combined with cybersecurity will change cyber threat prediction, detection, and mitigating action. The debate on cybersecurity machine learning depends much on our work. It emphasizes the importance of ongoing innovation and cooperation in this fast changing field, thereby providing the foundation for next studies aiming at understanding and handling the challenging cybersecurity issues of the digital age.

References

[1] Ahmad, S. T., Watrianthos, R., Samala, A. D., Muskhir, M., & Dogara, G. (2023). Project-based learning in vocational education: A bibliometric approach. *International Journal of Modern Education and Computer Science*, *15*(4), 43-56. https://doi.org/10.5815/ijmecs.2023.04.04

[2] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555. https://doi.org/10.3390/jcp2030027

[3] Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics*, *11*(4), 959-975. https://doi.org/10.1016/j.joi.2017.08.007

[4] Asvadishirehjini, A., Kantarcioglu, M., & Malin, B. (2022, April). GINN: fast GPU-TEE based integrity for neural network training. In *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy* (pp. 4-15). https://doi.org/10.1145/3508398.3511503

[5] Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of things: A survey of technologies and security risks in smart home and city environments. Living in the Internet of Things: Cybersecurity of the IoT - 2018. https://doi.org/10.1049/cp.2018.0030

[6] Bolaj, P., & Govilkar, S. (2016). Text classification for Marathi documents using supervised learning methods. *International Journal of Computer Applications*, *155*(8), 6-10. https://doi.org/10.5120/ijca2016912374

[7] Boyle, R. J., Challa, C. D., & Clements, J. A. (2017). Valuing Information Security: A Look at the Influence of User Engagement on Information Security Strength. *Journal of Information Privacy and Security*, *13*(3), 137-156. https://doi.org/10.1080/15536548.2017.1357387

[8] Bronk C (2013) Risk-Intelligent Governance in the Age of Cyberthreats. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2270853

[9] Burnham, J. F. (2006). Scopus database: a review. *Biomedical digital libraries*, *3*. https://doi.org/10.1186/1742-5581-3-1

[10] Caviglione, L., Wendzel, S., Mileva, A., & Vrhovec, S. (2021). Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *12*(4), 1-3. https://doi.org/10.22667/JOWUA.2021.12.31.001

[11] Demontis, A., Melis, M., Biggio, B., Maiorca, D., Arp, D., Rieck, K., ... & Roli, F. (2017). Yes, machine learning can be more secure! a case study on android malware detection. *IEEE transactions on dependable and secure computing*, *16*(4), 711-724. https://doi.org/10.1109/TDSC.2017.2700270

[12] Duffy, B. M., & Duffy, V. G. (2020). Data mining methodology in support of a systematic review of human aspects of cybersecurity. In *Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management. Human Communication, Organization and Work: 11th International Conference, DHM 2020, Held as Part of the 22nd HCI International*

Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22 (pp. 242-253). Springer International Publishing.

[13] Ellegaard, O. (2018). The application of bibliometric analysis: disciplinary and user aspects. *Scientometrics*, *116*(1), 181-202. https://doi.org/10.1007/s11192-018-2765-z

[14] Forghani, A., Kazemi, S., & Bruce, D. (2021). A machine-learning approach to generalisation of GIS data. *International Journal of Geoinformatics*, *17*(2), 41-59.

[15] Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In *SoutheastCon 2017* (pp. 1-6). IEEE. https://doi.org/10.1109/SECON.2017.7925283

[16] Ganeshan, A., Jayagopalan, S., Perumal, B., & Sarveshwaran, V. (2023). Secure identity key and blockchain-based authentication approach for secure data communication in multi-WSN. *Concurrency and Computation: Practice and Experience*, *35*(28), e7861. https://doi.org/10.1002/cpe.7861

[17] Gao, Y., & Liu, H. (2023). Artificial intelligence-enabled personalization in interactive marketing: a customer journey perspective. *Journal of Research in Interactive Marketing*, *17*(5), 663-680. https://doi.org/10.1108/JRIM-01-2022-0023

[18] Greener, S. (2022). Evaluating literature with bibliometrics. *Interactive Learning Environments*, *30*(7), 1168-1169. https://doi.org/10.1080/10494820.2022.2118463

[19] Gupta, R. Y., Mudigonda, S. S., & Baruah, P. K. (2021). A comparative study of using various machine learning and deep learning-based fraud detection models for universal health coverage schemes. *International Journal of Engineering Trends and Technology*, *69*(3), 96-102. https://doi.org/10.14445/22315381/IJETT-V69I3P216

[20] Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, *61*(4), 5-14. https://doi.org/10.1177/0008125619864925

[21] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), e1306. https://doi.org/10.1002/widm.1306

[22] Holbrook, L., & Alamaniotis, M. (2021). Survey of machine learning algorithms to detect malware in consumer internet of things devices. *International Journal on Artificial Intelligence Tools*, *30*(04), 2150020. https://doi.org/10.1142/S0218213021500202

[23] Kasim, M. F. (2016, October). Playing the game of Congklak with reinforcement learning. In *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICITEED.2016.7863309

[24] Kaufman, C., Perlman, R., & Speciner, M. (1995). Network Security: Private Communication in a Public World. *Network Security*.

[25] Lawani, S. M. (1981). Bibliometrics: Its theoretical foundations, methods and applications. *Libri*, *31*(Jahresband), 294-315. https://doi.org/10.1515/libr.1981.31.1.294

[26] Leon, M., Markovic, T., & Punnekkat, S. (2022, July). Comparative evaluation of machine learning algorithms for network intrusion detection and attack classification. In *2022 international joint conference on neural networks (IJCNN)* (pp. 01-08). IEEE. https://doi.org/10.1109/IJCNN55064.2022.9892293

[27] Liu, C., Yang, S., Di, D., Yang, Y., Zhou, C., Hu, X., & Sohn, B. J. (2022). A machine learning-based cloud detection algorithm for the Himawari-8 spectral image. *Advances in Atmospheric Sciences*, *39*(12), 1994-2007. https://doi.org/10.1007/s00376-021-0366-x

[28] Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE access*, *6*, 12103-12117. https://doi.org/10.1109/ACCESS.2018.2805680

[29] Makawana, P. R., & Jhaveri, R. H. (2018). A bibliometric analysis of recent research on machine learning for cyber security. *Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development, IoT4TD 2017*, 213-226. https://doi.org/10.1007/978-981-10-5523-2_20

[30] Mary, S. J., & Nalini, C. (2019). Improving DDoS Attack Predection Performance using Ensambling Techniqes. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(3), 4760-4763. https://doi.org/10.35940/ijrte.C6860.098319

[31] Mustapa, M., Rahmah, U., Cakranegara, P. A., Firdaus, W., Pratama, D., & Rahim, R. (2023). Implementation of Feature Selection and Data Split using Brute Force to Improve Accuracy. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(1), 50-59. https://doi.org/10.58346/JOWUA.2023.I1.004

[32] Negnevitsky, M. (2005). *Artificial intelligence: a guide to intelligent systems*. Pearson Education.

[33] Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(8), 3779-3795. https://doi.org/10.1109/TNNLS.2021.3121870

[34] Ningsih, S. R., Manurung, R. T., Bahtiar, A., Firdaus, W., Kusniarti, T., Budiana, N., ... & Sari, V. I. (2018, November). Information System Design E-Assignment in High School to Increase the Effectiveness of Learning. In *Journal of Physics: Conference Series* (Vol. 1114, No. 1, p. 012103). IOP Publishing. https://doi.org/10.1088/1742-6596/1114/1/012103

[35] Ninkov, A., Frank, J. R., & Maggio, L. A. (2022). Bibliometrics: methods for studying academic publishing. *Perspectives on medical education*, *11*(3), 173-176.. https://doi.org/10.1007/s40037-021-00695-4

[36] Oh, J., & Kim, Y. (2020). Job placement using reinforcement learning in GPU virtualization environment. *Cluster Computing*, *23*(3), 2219-2234. https://doi.org/10.1007/s10586-019-03044-7

[37] Oh, S. H., Jeong, M. K., Kim, H. C., & Park, J. (2023). Applying Reinforcement Learning for Enhanced Cybersecurity against Adversarial Simulation. *Sensors*, *23*(6), 3000. https://doi.org/10.3390/s23063000

[38] Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing the Relevance of Cybersecurity Training and Policies to Prevent and Mitigate the Impact of Phishing Attacks. *Journal of Internet Services and Information Security*, *12*(4), 23-38. https://doi.org/10.58346/JISIS.2022.I4.002

[39] Poornimadarshini, S., Sindhu, S., Veerappan, S., Arvinth, N., & Muthusamy, S. (2024). Bibliometric Analysis of IJISS Journal based on Citation and Publication Relevant Metrics. *Indian Journal of Information Sources and Services, 14*(4), 153–158. https://doi.org/10.51983/ijiss-2024.14.4.24

[40] Radha, L., & Arumugam, J. (2021). The research output of bibliometrics using bibliometrix R package and VOS viewer. *Shanlax International Journal of Arts, Science and Humanities*, *9*(2), 44-49. https://doi.org/10.34293/sijash.v9i2.4197

[41] Rizki, A. (2019). Lion's Roar in SEA: Singaporean Way in Increasing the Awareness of Cybersecurity. *Jurnal Sentris*, *1*(1), 39-69.

[42] Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson.

[43] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*, 41. https://doi.org/10.1186/s40537-020-00318-5

[44] Sherlin, D., & Nikila, I. (2022). Detection and Diagnosis of Brain Tumor Using Wavelet Transform and Machine Learning Model. *International Academic Journal of Innovative Research*, *9*(1), 01–05. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0901

[45] Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human–Computer Interaction*, *36*(6), 495-504. https://doi.org/10.1080/10447318.2020.1741118

[46] Sibyan, H., Suharso, W., Suharto, E., Manuhutu, M. A., & Windarto, A. P. (2021, February). Optimization of Unsupervised Learning in Machine Learning. In *Journal of Physics:*

Conference Series (Vol. 1783, No. 1, p. 012034). IOP Publishing. https://doi.org/10.1088/1742-6596/1783/1/012034

[47] Singh, V. K., Singh, P., Karmakar, M., Leta, J., & Mayr, P. (2021). The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics*, *126*, 5113-5142. https://doi.org/10.1007/s11192-021-03948-5

[48] Sunarti, S., Rohim, R., Darmawati, B., Syahrul, N., Firdaus, W., Iswanto, A., ... & Kastanya, H. (2023). Measuring vitality of oral tradition: A study of Cigawiran. *International Journal of Society, Culture & Language*, *11*(3), 202-212. https://doi.org/10.22034/ijscl.2023.2007254.3100

[49] Surekha, S., Sindhu, S., Veerappan, S., & Arvinth, N. Bibliometric Study: Natural and Engineering Sciences. *Natural and Engineering Sciences*, *9*(2), 376-385. https://doi.org/10.28978/nesciences.1574466

[50] Watrianthos, R., & Yuhefizar, Y. (2023). Exploring research trends and impact: A bibliometric analysis of RESTI Journal from 2018 to 2022. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *7*(4), 970-981. https://doi.org/10.29207/resti.v7i4.5101

[51] Watrianthos, R., Ahmad, S. T., & Muskhir, M. (2023). Charting the growth and structure of early ChatGPT-education research: A bibliometric study. *Journal of Information Technology Education: Innovations in Practice*, *22*, 235-253. https://doi.org/10.28945/5221

[52] Watrianthos, R., Ambiyar, A., Rizal, F., Jalinus, N., & Waskito, W. (2022). Research on Vocational Education in Indonesia: A Bibliometric Analysis. *JTEV (Jurnal Teknik Elektro dan Vokasional)*, *8*(2), 187-192. https://doi.org/10.24036/jtev.v8i2.117045

[53] Windarto, A. P., Wanto, A., Solikhun, S., & Watrianthos, R. (2023). A Comprehensive Bibliometric Analysis of Deep Learning Techniques for Breast Cancer Segmentation: Trends and Topic Exploration (2019-2023). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *7*(5), 1155-1164. https://doi.org/10.29207/resti.v7i5.5274

[54] Zhou, Y., Kantarcioglu, M., & Xi, B. (2019). A survey of game theoretic approach for adversarial machine learning. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(3), e1259. https://doi.org/10.1002/widm.1259

Authors Profile

Yulian Purnama, completed Bachelor of English Education Department (S1), Faculty of Teacher Training and Education from Universitas Ahmad Dahlan (1999); Master of Linguistics (S2) Faculty of Cultural Sciences Universitas Gadjah Mada (2006). Faculty Member of Tarbiyah and Teacher Training Universitas Prof. K.H. Saifuddin Zuhri Purwokerto (since 2008). Major research on English Language Teaching, Linguistics, Cultural Studies, Sociolinguistics, English for Tourism, Educational Entrepreneurship.

A. Asdlori, Completed Bachelor of Islamic Education Study Program, Faculty of Tarbiyah, IAIN Sunan Kalijaga Yogyakarta (1989). Master of Islamic Studies, Postgraduate Program, Islamic University of Malang (2002). Doctoral Program of Islamic Studies, Postgraduate Program, UIN Sunan Kalijaga Yogyakarta (2019). Faculty Member of Tarbiyah and Teacher Training Universitas Prof. K.H. Saifuddin Zuhri Purwokerto (since 1991). Major research on Islamic Studies, Professor of Islamic Education Science.

Eka maya Sari Siswi Ciptaningsih, completed Bachelor of Economics (S1) from Inholland University, The Netherland (2004); Master of Small Medium Entreprises (S2) From IPB, Indonesia (2012) and the Doctor of Management Program (S3) State University of Jakarta (UNJ), Indonesia (2015) Faculty Member of Business Creation, Binus Business School (2019- Present) Major research on Small Medium Entreprises, E-Business and Human Resorces, Strategic and Sustainability Business.

K. Kraugusteeliana, completed Bachelor of Information System (S1) Faculty of computer science from Universitas Budi Luhur (1998); Master of Computer (S2) Faculty of Computer STTBI Benarief (2004), Master of Management (S2) Faculty of Business and Economics Universitas Budi Luhur (2007). Faculty Member of Information Sistem Universitas Pembangunan Nasional Veteran Jakarta (2014). Major research on IT tourism, healthy, it governance. We interested research in DSS, Big DATA, VR-Virtual Reality, IT Risk, and Audit System Information with several framework like COBIT, SUS, EUQ, ITIL, ISO 27001, Heuristic Evaluation, TAM, UTAUT, WEBQUAL, IPA, NIST-SP series, Octave allegro Achieved the following IT certified-Certified Artificial Intelligent Practicioner (2021), Certified Data Science Associate (2022), COBIT from ISACA (2024), BI-Business Intelligence Certified (2024).

Agung Triayudi, born in South Lampung, 19 June 1986. Completed his final education at the doctoral degree in information communication technology at Asia e University Malaysia. Currently working as a lecturer at the Faculty of Communication and Information Technology, National University. He is Associate Professor in Master Program of Information Technology, Faculty of ICT, Universitas Nasional. He was appointed as Dean of ICT Faculty Universitas Nasional since 2023. His research areas are Data Mining, Decision Support System, Machine Learning and AI.

Robbi Rahim, is an Indonesian academic with a Doctoral degree in Protocol Cryptography from Universiti Malaysia Perlis. He has expertise in the fields of data mining, big data, and Rapid Miner, all of which are related to the processing and analysis of large datasets. Rahim's doctoral thesis focused on the study of Protocol Cryptography, which involves securing communication protocols using cryptographic techniques. His contributions to research in various fields, including computer science and information technology, have been significant. Since 2017, Rahim has been working as a lecturer at Sekolah Tinggi Ilmu Manajemen Sukma. In his current role, he teaches and mentors students in the areas of data mining, big data, and Rapid Miner. His expertise in these fields has enabled him to bring a unique perspective to his teaching, helping students to develop the skills and knowledge needed to succeed in today's technology-driven world.