Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

The Future of Work in Financial and Cybersecurity Domains: Analyst Perspectives

Abdul Azeem Mohammed [1]✉, Md Rakibuzzaman[2] and Md Ashraful Alam[3]
[1] *Master of Science In Technology Management, Lindsey Wilson College, USA*
[2] *Officer, Department of Banking Inspection, Bangladesh Bank, Dhaka, Bangladesh*
[3]*Master of science in Business Analytics, Trine University, Arizona, USA*
Corresponding Author: Abdul Azeem Mohammed, **E-mail**: mohammed.azeem98@gmail.com

| ABSTRACT
The evolution of work paradigms during the digital age has gained further traction in the post-pandemic context, and financial and cybersecurity spheres have also undergone serious reorganization. By means of the empirical data on salary distribution, job roles, the adoption of remote work, the level of experience, and the types of employment this study explores the nature of employment in these two important sectors, as it evolves. With two datasets curated specifically for the research, namely, "Global Salaries in Cybersecurity / InfoSec (2020-2024) and "Work-from-Anywhere Salary Insight (2024), the study provides a comparative data-driven analysis of the shift toward different approaches to workforce model across both industries. The cybersecurity industry, which experiences an increasing number of threats and lacks professional talent globally, demonstrates a high rate toward remote-first positions and competitive salaries, especially among senior specialists. Conversely, the financial sphere has a more cautious shift toward it, showing more preferences to a mixed work model and preserves more interdependencies of salaries on geographic grounds. The results point out that cybersecurity is becoming more flexible and embraces pay performance, the finance world is moving yet between customs and new digital capabilities. This paper combines both information on industry analysts and reports on the future of work perspective, to put available quantitative information in perspective. It perceives that these two sectors are shifting towards a skills-based recruitment model, where competences in automation, data security, compliance, and financial technology (FinTech) will play a vital role. The development of contract-based and cross-border kinds of employment points to the quite probable rearrangement of the organizational design and staffing strategy in both spheres. This study is part of the ever-increasing discussion of the future of work, since it offers a comparative, evidence-based perspective on the future of two in-demand professions. It has practical use to human resource, corporate, leadership, policy-making institutions to attract, develop, and retain talent in a fast-changing work environment.

| KEYWORDS
Future of work, Cybersecurity workforce Trends, Financial Sector Employment, Remote and Hybrid Work Model, Analyst Perspectives and Skills and Salary Evolution

| ARTICLE INFORMATION
ACCEPTED: 12 June 2025 **PUBLISHED:** 20 July 2025 **DOI:** 10.32996/jcsts.2025.7.7.79

1. Introduction

1.1 Digital Transformation of Work Overview

The digital transformation of work encompasses the large-scale shifts in the way that work is being conducted, managed, and discharged and especially caused by the advances in digital technologies. In the past years, cloud computing, automation, artificial intelligence (AI) and data analytics, among other tools, have been adopted in industries worldwide to streamline operations, improve decision making and become more productive. Such transition has not only changed internal processes but also established new forms of employment, including remote work, digital freelance, and hybrid workplace [1]. The COVID-19 pandemic has also catalyzed digital transformation and organizations have had to adopt digital infrastructure and

virtual collaboration tools quickly, to ensure business continuity. Consequently, job boundaries have become blurred, territorial barriers eliminated, and digital literacy has become a prerequisite to employability. In cybersecurity, AI is used to detect threats in automated reporting in finance to name a few [2]. Things that were previously accomplished by humans can now be augmented, or even replaced by intelligent systems. This transformation is bringing opportunities and challenges: as technology is increasing access to world talent pools and efficiency, it is also introducing the fear of data security and displacement of labor and the digital divide will continue to grow. Put simply, digitalization of work has already become one of the characteristics of the labor market in the 21st century, and its consequences can be observed across sectors, professions, social and economic lines.

1.2 Role of the Finance and Cybersecurity Sectors in the World Economy

Cybersecurity and finance are among the most necessary frameworks that the modern international economy relies on. The finance industry encourages the flow of finance, investment and financial strategies between individuals, corporations, and the government and this helps to drive the economy and stabilize the economy [3]. It is central to the financial risk management, the financing of innovation and guarantees liquidity on the traditional and digital markets. The emergence of FinTech and blockchain technologies is leading to increasing financial servicing being done in a more digital, inclusive, and decentralized way, which will require an extremely skilled and adaptable workforce. In the interim, the issue of cybersecurity has become a strategic business concern in all sectors as the levels and intensity of the cyber threats grow. Nowadays, more than ever, businesses are dependent on safe systems, personal data protection, and digital trust to operate successfully [4]. Cybersecurity specialists keep critical infrastructure safe, defend any information leak, and guarantee compliance with regulations, and thus, their role is central to the preservation of not only the organization, but national and economical security. Finance and cybersecurity in combination are both policy, commerce, and innovation elements at a global scale. They are also becoming more interconnected: financial systems are the most vulnerable elements to cyberattacks, often because of such attacks, which will need unified measures and multi-competence. These two industries become more and more important in the context where economies are becoming more and more digital, interconnected, and reliant on strong, safe and intelligent infrastructure.

1.3 Evolution to the Scene: Telecomm Pad to Various Models, AI, and Global Labor Balances

Remote work adoption, flexible employment, AI -immediate automation, and labor shifts are redefining the world of work. Caused by the COVID-19 pandemic, the switching of working arrangements to remote and hybrid is being normalized and seen as one of the permanent solutions, not temporary ones anymore. Remote working has broken the geographic barrier allowing businesses to engage talent worldwide providing workers with more work freedom and mobility [5]. At the same time, artificial intelligence and machine learning are revolutionizing job tasks in all sectors--liberating workers of repetitive duties, improving decision-making and generating new data- and digital-intelligence-based job functions. The change is especially obvious in the banking sector and cybersecurity where digital processes and AI solutions are slowly becoming the backbone of the operations. Cognitive, analytical, and interpersonal high-level skills are on the rise as the routine functions are removed by use of automation [6]. The traditional full time employment model is changing, as freelance, contract and gig employment arrangements are taking the change in replacing the traditional full time employment model and providing flexibility to both employers and employees. Generational changes are also factors that affect these labor shifts as younger professionals have become more focused on flexibility, purpose-based work, and digital interactions [7]. The outcome is the liquid labor market where organizations are forced to become competitive with decentralised teams, new compensation schemes and the emerging digital expertise.

1.4 The importance of analyst views in projecting the trends of work

The views of analysts are important in determining work trends as they summarize economic trends, technological developments, labor market statistics and developments of companies within an industry to offer strategic information on the future of the workforce. Finance and cybersecurity the role of analysts in finance and cybersecurity is to determine new job positions, skill requirements, and changes in the structure of the organization. Their evaluations are not merely reactionary but demographically sensitive, they allow the stakeholders to foresee challenges like shortage of talent to automation displacement, to regulatory changes. Such firms of industry analysts, as Gartner, McKinsey, and the World Economic Forum, release foresight publications periodically, which shape employee planning strategies, learning and development and digital transformation investment [8]. As an example, speculations concerning the emergence of remote cybersecurity teams or AI-assisted fiscal processes enable businesses to be ready to exploit opportunities and threats. Policy-making is also informed by analyst insights, who pinpoint areas of workforce drawbacks in preparing individuals to join the labor market and proposing solutions to such issues through upskilling, investment in digital infrastructure, and easy labor policy. Such views are usually based on both the statistics and qualitative studies, providing the overview of the labor force development [9]. In such a constantly evolving environment, the opinion of the analysts guarantees the forward-looking, evidence-based decision that is in sync with the worldwide tendencies and, therefore, cannot be omitted by an organization or a government operating in the environment of the future of work.

1.5 Objectives of the research

This study is an effort to analyze the changing trends in the field of finance and cybersecurity based on facts and analysts' observations.

- To find out the pattern of salaries between the experience and the kind of work.
- To assess the percentage of remote work, hybrid, and onsite jobs.
- To recognize the arising job functions and patterns of employment Investigate Industry assignments with adapting Skill requirements [10].
- To measure geographic and organization flexibility in job structure.
- So that the predictions of analysts can be combined to form a future workforce plan based on empirical data.

1.6 Understand the Future of Job Descriptions, Wages, Off-site Flexibility, and the Need of Skills

The nature of jobs, pay systems, work-at-home flexibility and skill requirements are quickly changing per the progression of technology, the changing demands of the workforce. Security analyst, penetration tester, and cloud security engineer have become typical of cybersecurity approaches, which means that digital threats are becoming increasingly sophisticated and requiring proactive risk mitigation [11]. Such roles are getting hybrid or remote friendly, particularly where companies are taking on digital-first cultures. Cybersecurity salaries have also increased drastically especially to those with specific certification and experience in the fields of high demand such as threat intelligence and incident response. In the same token, the finance industry is experiencing the increased trend in going to data analyst and financial technology (FinTech) roles and growing focus on digital literacy and integration of automation. Traditionally, finance was more specific to location, but post-pandemic tendencies demonstrate a slow adoption of hybrid solutions. Companies are reconsidering their approach to compensation in terms of value instead of location, going along with a more general push toward skills-based pay schemes. Due to automation taking care of basic financial functions, there is an increased need for skills such as analytical, ethical, and decision-making skills [12]. Contract and project-based employment are also increasingly adopted in both fields and enable even more sourcing of talent. The combined effect of these trends leads to a conclusion that the future of work is more dynamic, decentralized, and skill-oriented and agility is required both on the part of employees and the employers.

1.7 Comparing Financial vs. Cybersecurity Domains on An Empirical Data

Composing empirical evidence, a sensible comparison between the changing workforce models in financial and cyber security sectors can be made. The database of cybersecurity indicators, encompassing more than 22,000 data points between 2020 and 2024 demonstrates that remounted work is gradually gaining popularity, particularly with experienced professionals working on the full-time basis. Salary rates are growing vigorously and are often geographically independent, with such high-demand job titles like Security Engineer and Security Analyst [13]. This may imply adoption of performance based and skill-based forms of compensation. Conversely, the finance dataset itself, even smaller, provides an overview of remote working patterns in 2024, where the gradual but not insignificant transition toward the hybrid setup is observed, especially in such occupations as Financial Analyst, Data Scientist, and Consultant. The salary structures within the field of finance are still closely associated with location and type of employment, because there is not as much fluctuation with remote types. The increase in the usage of contractor and freelance models is observed in the cybersecurity sector but not in finance where people still adhere to the full-time employment model [14]. The comparison also shows that cybersecurity professionals are more likely to get their compensation increase based on experience, whereas finance is stricter in its development. Such empirical evidence shows structural variations in underlying: cybersecurity quickly evolves to meet the digital work processes, and the finance industry faces a more gradual change driven by regulatory requirements and old system versions [15]. The statistics confirm the theory that cybersecurity is leading in the evolution of remote work, and finance follows slowly and carefully.

1.8 Research Questions

This study examines the latest trend in work by answering the following questions:

1. What are some of the changes in salaries and remote work opportunities in the two industries?
2. What are some of the emerging roles?
3. Which skills and structures will future analyst views?

A. 1.9 Significance of the Study

The significance of this study is that it answers the pressing need of the understanding of how two of the most crucial and fast-changing sectors of the world-finance and cybersecurity- are changing under the influence of the digital disruption and new shifts in the paradigm of the work [16]. Since the rules of the game for professional expectations are changing due to remote working, artificial intelligence and decentralized models of employment, organizations in these spheres have to make

crucial choices in terms of talent attraction, remuneration approach, workforce considerations. Combining the existing empirical data and the opinion of the analysts, the study facilitates the process of connecting the actual employment patterns with strategic future-oriented visions [17]. It provides an overview of the similarities and differences in the financial and cybersecurity sectors regarding their remote employment, pay structure, and the implementation of roles to assist businesses in comparing their own practices to evidence-based norms [18]. This study illuminates the evolving quality of work safety, benefits based on experience, and geographic responsiveness of high-stakes organizations where safety and precision matter the most. The policymakers, human resources professionals, and learning institutions can equally utilize this knowledge to know the newly emerging skills that are required and the structural changes that are redefining the labor market. this study makes an extension of the overall debate on the future of work by making evidence-based deductions of sustainable workforce solutions to be applied in the current complex and digital world to build on long-term organizational resilience and flexibility.

2. Literature Review

Over the last ten years, the advancement of technological and Laboral reality has had a significant effect on the sphere of the financial services and cybersecurity [19]. Evolution in the workplace has been a subject of literature to the academic and to the industrial sector in terms of remote work, automation, adoption of AI, and the occurrence of new types of employment models. Organizations such as the World Economic Forum (WEF), Deloitte, McKinsey have predicted substantial modifications in labor force makeup, requirement of skills, and company systems [20]. The existing literature does not present comparative, empirical understanding of the ways in which financial and cybersecurity sectors are differently transforming. This paper will address that gap with the help of both empirical evidence and analyst opinion.

2.1 Historical Development of Cybersecurity and Financial Work (Previous Ten Years)

The financial and cybersecurity sector have experienced a significant change over the last ten years as a result of globalization, changes in technology, and changing workforce demands. In financial issues, the use of digital sites, blockchain, cell phone banking, and exchange-based trading has changed conventional jobs and brought forth new occupations like FinTech specialists, conformity chiefs, and information scientists [21]. Traditional systems are undergoing obsolescence, where cloud-based and real-time financial processes are incorporated, which require employees with higher digital democracy and flexibility. In the meantime, the demand of cybersecurity is exponentially growing because the digital ecosystems continue to blossom, and cyber threats are growing more advanced. Job descriptions no longer focus on IT security support, but rather on specific areas such as ethical hacking, incident response, cloud security and risk governance. The requirement of real-time threat detection and regulatory compliance cyber resilience has contributed to a large demand of cybersecurity specialists throughout the world [22]. The two industries are also experiencing a transition in work places- the concentration of office work to the construction of the dispersed and the compounded workforce in the context of the use of digital collaboration tools. With dissimilar customer-expectation and predictive regulation environments, employees should now be cross-functional, technologically smart, and quick to respond to new risks and opportunities. This is transformational in that it heightens the interdependence of cybersecurity and finance since data protection and digital trust are becoming essential to the integrity and efficiency of international finance.

2.2 Remote and Hybrids Models: Effects on Productivity, Pay and Carrying Out

Flexible work arrangements, such as remote and hybrid working models became a hallmark of the post-pandemic job market, especially in such areas as finance and cybersecurity due to the digital nature of the companies which allows such kind of work principles [23]. Various reports, such as by PwC and Gallup, indicate that remote work has the potential to make people more productive, cut down the operating expenses and even make employees happier, as long as the company promotes teamwork and online connectivity. Ever since the onset of cybersecurity, remote jobs have been extremely popular because of the mobile character of security tasks, incident resolutions, and monitoring programs, which can be effectively addressed in a remote setting [24]. Finance, which is traditionally based on face-to-face communication and the supervision of the regulatory bodies, has been less inclined to cryptic models and more into the hybrid systems, particularly those with data-related or consulting positions. Compensation patterns have changed too-companies are paying more according to skills and outputs, than according to location. Work-at-home jobs in high-demand professions often can be well-paid, especially to the niche technical skills that have great market value and experienced professionals. Flexibility in the arena of retention is named among the most identifying reasons why employees wish to remain in a job. Insufficient remote or hybrid opportunities due to a shortage of such opportunities may cause turnover, especially among younger and more competent digital skills [25]. Although remote models present evident advantages, they are associated with emerging issues like keeping the staff performance on track, building cybersecurity, and sustaining organizational culture. The data on hybrid flexibility on the lower scale indicates that, overall, there is a tendency towards maintaining a strong appreciation of hybrid flexibility in the knowledge-based industries such as finance and cybersecurity where both digital capabilities and freedom of action among the employees are essential to promote long-term retention and persistence.

2.3 The Future of Work Industry Reports (WEF, Deloitte, McKinsey)

The World Economic Forum (WEF), Deloitte, and McKinsey, among the leading world institutions, have also developed lengthy reports on the future of work, reporting not only on opportunities but also on challenges in quickly changing industries such as finance and cybersecurity. The Future of Jobs Report 2023 published by the WEF forecasts that, although technological usage and automation will eliminate about 85 million jobs by 2025, the same number of positions in the fields of data, AI, cloud, and cybersecurity will be created and established [26]. The report identifies analytical thinking, active learning and problem-solving as complex skills that are increasingly important. The Future of Work After COVID-19 by McKinsey suggests financial services and cybersecurity as some of the industries that will experience an increase in the share of hybrid workforces, particularly in positions where employees will have to interact online without necessarily going to workplaces. The Global Human Capital Trends issued by Deloitte also mentions the trend of changing the inflexible job models to the flexible model that is based on skills. The reports in their totality have indicated that, automation in as much as it might help in cutting down the number of people required to carry out some routine functions, it will lead to growth of the need to upskill and lifelong learning in all job categories [27]. Cybersecurity is considered as a growth industry and a source of trust-enabling digital transformation, and finance is in the process of transforming to be more technology-oriented, with increased use of FinTech, blockchain, and AI to automate processes. Such reports also forecast a long-term change in the patterns of employment, i.e. the present full-time employment will change to the contracting and project-based work particularly in the high-skill and high-demand fields [28]. The convergence in these industry reports cues us to the sense of urgency that organizations should redefine work models, workforce strategy and competency building to meet the impact of this transformation.

2.4 Analyst Projections of Employment and Declines in Both Realms

Industry experts predict a significant variation in employment rise and decline trends in the domains of finance and cybersecurity in the following decade. The demand of skilled professionals in cyber security remains higher than the supply and (ISC) 2 Cybersecurity Workforce Study predicted in 2023 there will be a shortage of more than 3.4 million professionals. The positions of penetration tester, threat analyst, and cloud security engineer will expand greatly, as the increasing threats in the realm of cybersecurity and the need to meet compliance requirements create a strong demand in these areas [28]. The analysts also forecast that the trend to use remote cybersecurity personnel will also rise, which will further grow the labor force around the world and prompt the speedier competition of salaries in the top talent force. On the contrary, although the field of finance is a stable and vital sector, according to the experts of McKinsey and Gartner companies, mundane financial functions, including accounting clerks in accounts payable and data entry personnel, are likely to decline because of automation and robotic process automation (RPA). Meanwhile, the finance sector is expected to experience expansion in the fields of digital risk management, development of FinTech, analytics of data, and compliance; this will give rise to the needs of higher levels of thinking and technical acumen [29]. Analysts hold the common ground that the two industries are taking part in a transition towards a so-called hybrid human-digital workforce in which machines take on routine tasks, with humans concentrating on supervision, invention, and moral decision-making. Employment in the two industries is becoming less geography-sensitive since firms are recruiting all around the world to tap specialized talent at lower costs [29]. These predictions indicate a strong motivation toward strategic workforce planning, upskilling, and flexible employee models that could help to cover shifting talent needs and demonstrate flexibility in high-risk, high-compliance settings.

2.5 Emerging Trend Cloud Security, Decentralized Finance (DeFi), Artificial Intelligence-Based Fraud Detection, Remote Audits

Rapidly developing technologies are transforming the business environment in the field of finance and cybersecurity and causing new job positions, functions, and regulatory issues. There is a growing concern of security on clouds, as more organizations pull their infrastructure to the cloud such as AWS, Azure, and Google Cloud. This transition has caused the need of specialists in the field of cloud architecture, identity and access management (IAM) and secure cloud configuration. Simultaneously, the financial sector is facing a high level of interest in decentralized finance (DeFi), which are blockchain-based ecosystems, removing the intermediaries to financial transactions. The development of DeFi forms new job positions related to smart contract auditing, the most common DeFi crypto regulation, and risk modelling, but it also leads to fears of fraud and confrontations with cyber threats [30]. Another significant trend is AI-based fraud detection that involves implementing machine learning algorithms to process real-time transactions, assess risk, and prevent fraud [31]. Both financial institutions and cybersecurity firms accept the benefits of these tools, as they will improve the ability to detect threats, the effectiveness of building customer trust, and minimizing losses. In the meantime, another idea, that of remote auditing, i.e., the possibility to conduct compliance and financial audits without being there in person, is being popularized, particularly after remote work became a norm. This direction requires new tools and procedures that guarantee transparency and the integrity process and the accuracy of the audit trail. When it comes to these emerging trends, it is hard to draw any boundaries between finance and cybersecurity, as there are some overlapping skill sets and such collaborative working environments [32]. Individuals, who would be capable of operating in both fields, will be even more appreciated. Simultaneously these innovations drive newer regulatory

frameworks, code of ethics and worker training to keep in tandem with changing technology and to ensure trustworthiness of systems in digitized financial and security activities.

2.6 Research Gaps

Though the literature on the subject has some remarkable contributions on the changing nature of work in finance and cybersecurity, some essential gaps still need to be filled. First, both scholarly and industry reports dwell on either finance or cybersecurity separately, without applying a comparative perspective to reveal how the trends in the workforce evolve, or even overlap, in the two areas. Second, most studies are based on theoretical frameworks, unstructured evaluations, or limited sample sizes inclusive of surveys, but without the utilization of big data (salary and employment statistics). This study findings are less generalizable and applied to the real world. Whereas the topic of remote work and digital transformation is debated broadly, there are not many studies that examine the effect of these changes on a cross-domain scale on job positions and various aspects of salaries and experience. Niche implications of types of employment (e.g. full-time vs. contract), geographic flexibility and compensation / retention are also commonly ignored in the research. The research, through a combination of two of the latest and complementary datasets (one about cybersecurity (2020-2024), and the other one on remote-based financial positions across the globe (2024)), provides a very specific, data-centered view. It fills the gap between analyses of analysts and realities of the workforce by giving a detailed, comparative analysis that is both timely and actionable [32]. The study contributes to it by providing practical insights that can be used by industry executives, HR strategists, and policymakers, who want to adopt the strategy of future-proofing their workforce strategy in two of the most dynamic and high-impact sectors of the world economy.

2.7 Empirical Study

Graham and Lu (2022), in an empirical article titled, Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements, focus on an analysis of 17,929 cybersecurity job postings to determine which are the most demanded skills in the industry. They reveal a subtle association between hard skills and soft skills in establishing hiring expectations. Although it is still necessary that professionals should have technical knowledge about cybersecurity, employers are more likely to demand people who have both knowledge and experience about this kind of field skills in communicating with others. The research group classifies soft skills into three main categories, including knowledge management and systems thinking, big data analytical skills, and teamwork and diversity awareness [1]. Such results highlight the fact that the sphere of cybersecurity is shifting away towards a more specific technical aspect and is now taking on a collaborative, driven by data, and flexible set of skills. What is noteworthy, this change comes as an extension of the larger transformation in remote and hybrid workplaces which rely heavily on communication, cross-functional interactions, and self-regulation. The authors believe that the cybersecurity sector of the job market of the future can be characterized by the integration of extensive technical expertise and wide-scope system-level thinking and social skills. This paper will enhance the empirical knowledge of this work by confirming the emerging skill dynamics within the cybersecurity workforce.

In an empirical analysis by the title, Factors Affecting Human AI Collaboration Performances in Financial Sector: Sustainable Service Development Perspective, Xu and Cho (2025) examine how the dynamics of human and generative AI systems collaboration affect innovation and managerial performances in the financial world. Included in the mix of multiple regression analysis and fuzzy-set qualitative comparative analysis (fsQCA), the authors reveal four main triggers to a successful collaboration: employee skills, data reliability, trusted AI systems, and managerial oversight. Their findings indicate that both childhood traumas have significant positive effects on both the innovation capability and the managerial performance with innovation being an incomplete mediator [2]. According to the research, integration of generative AI cannot be realized simply with technical infrastructure but with a sound structure of human flexibility, data control and job design. The mentioned findings are particularly pertinent to the present study, because they indicate that tasks in finance, in the future, would require hybrid expertise and team efficiencies between analysts and smart systems. The article empowers the empirical background of comprehending new work models and skills requirements in AI-based financial ecosystems.

In the article titled A New Computational Method of Quantifying and Analyzing Media Bias in Cybersecurity Reporting, Sufi (2025) presents attentive readers with an AI-based tool to identify and measure bias in cybersecurity reporting sources. Considering 9,314 events in 1,236,928 news articles in 144 outlets, the topline targets map out the tendency of reporting priorities depending on the location, the nature of the attack, and the specialization of the source. The research identifies quantifiable differences in coverage using the GPT-based classification, Shannon entropy, chi-square tests, multinomial logistic regression, and Bayesian inference. Let us say that BBC had a wide range of topics ($H = 2.87$), whereas niche approaches, such as Cybersecurity Insider, were very narrow focused ($H = 0.45$). This kind of biased reporting has far reached implications on the minds of the people in the society, how resources are distributed which eventually affects the need of the workforce, policy responses and reaction to the level of perceived threat [3]. The study is pertinent in terms of situating the analyst behavior, prioritization of risks, and practice of communication in cybersecurity. Because the future of employment in cybersecurity depends on prompt, intelligent decision-making, it is of essence to comprehend how the external narratives determine the

sphere. These findings delivered by Sufi support the necessity of data-literate analysts with the ability to critically challenge the narratives presented to the population and the push by the media.

In the article by Sigahi, Yeow, and Thatcher (2023), Future of Work, the Sustainable System-of-Systems (SSoSs) framework is used to evaluate and provide strategic designs of sustainable remote work ecosystems in their study titled Advancing Sustainability in the Future of Work through the Design of Post-Pandemic Work-from-Home Systems. Examining remote work in the post-pandemic through the systemic and multidisciplinary perspective, the authors review and discuss distant working as a network of diverse interactions and interconnections between human, technical, environmental, and organizational systems. The article explains how the COVID-19 pandemic led to a crisis that necessitated the need to adopt the remote working environment as something long term in nature, and it has to be considered as a unit where physical infrastructure, mental stability, technological preparedness, and financial stability have to be taken into consideration [4]. The model defines the major intervention points, ensuring long-term sustainability and health of the workers, including ergonomic support, landscape equality of access to digital resources, and cross-sector policy convergence. This study enhances indicating how systemic frameworks can support the financial and cybersecurity industries to come up with remote environments that are secure and resilient. It also makes the debate on the future of work stronger in line with the analysts in the field of adjusting to a decentralized and hybrid model.

Ram Shankar Siva Kumar et al. (2020) review interviews with 28 organizations in their IEEE study, Adversarial Machine Learning, Industry Perspectives, drawing data that can be used to estimate the extent to which the industry practitioners perform the tasks to secure, monitor, and respond to the machine learning system attacks. The research consists of an extensive empirical analysis of the industry is at present ready against the adversarial attacks on ML, which are more often of serious significance to cybersecurity and monetary applications. Although the use of ML is increasingly becoming the order of the day, the authors discovered that most companies do not have outlined guidelines on how they are to guard such systems, particularly when they are being developed and deployed. The study establishes significant holes in the development lifecycle of security (SDL) and highlights that no evident incident response plans are possible in the context of adversarial manipulation. These gaps are framed in terms of two personas, ML developers and security responders [5]. This study provides evidence of the acute necessity of strong security frameworks blended with AI consciousness in the future working conditions where the financial analysts and cybersecurity providers will greatly rely on the machine learning models.

The article by Ahmet Faruk Aysan, Giray Gozgor, and Zhamal Nanaeva (2024) entitled Technological Perspectives of Metaverse to Financial Service Providers is a review of how virtual reality (VR), the entire ecosystem of the Metaverse, is transforming the financial services industry. The authors rely on a scenario-based technological foresight method to sketch the prospective penetration of financial institutions into immersive digital spaces. The study notes that although such industries as gaming and retail are quick to integrate with the Metaverse, financial institutions are poorly positioned. The paper names digital assets, NFTs, and virtual real estate as the fundamental banknotes of the meta-economy and argues the existence of initial experiments with virtual banking and decentralized finance [6]. This empirical contribution offers an informative interpretation of the technological trends, which financial analysts would like to track and tune out to since virtual interaction becomes the prime focus of customer service, compliance, and investment model representations. This article impacts the emerging digital ecosystems on the future of the analyst profession and business model in finance and cybersecurity industries.

3. Methodology

A mixed method is used in this study with a combination of quantitative results of two datasets and a qualitative input of industry reports. The first data is based on isecjobs.com as a source of information, gathered by 2020 and 2024 with data on cybersecurity salaries and jobs. The second, which is a Kaggle dataset, will shed light on salary insights of remote workers among sectors, but filtered in the direction of finance occupations [32]. The two datasets were cleaned, standardized, and analyzed with the help of Python and Tableau. Data could be analyzed using the exploratory data analysis (EDA), descriptive statistics, and visual comparisons to look at trends in salary, experience, and remote flexibility. The trend projections by analysts WEF, Deloitte, and McKinsey have been incorporated to contextualize the trend and make data-driven conclusions.

3.1 Research Design

This study adopts a mixed-methods research design combining quantitative data analysis with qualitative analyst perspectives to explore the evolving nature of work in the financial and cybersecurity sectors. The quantitative component involves the use of two publicly available datasets to examine patterns related to job roles, salaries, employment types, remote flexibility, and experience levels. The qualitative component incorporates insights from leading industry reports such as WEF, McKinsey and Deloitte to contextualize and interpret the empirical findings. The mixed-methods approach allows for both data-driven insights and strategic foresight, providing a comprehensive view of workforce shifts in high-demand, digitally evolving sectors. This design was chosen to balance objectivity through numerical data with strategic interpretation (through narrative

analysis), thus enhancing the study's relevance for practitioners, policymakers, and academics [33]. The comparative structure between finance and cybersecurity enables a cross-sectoral analysis, highlighting both convergence and divergence in future-of-work trends. This study also uses exploratory data analysis (EDA) to identify meaningful patterns and correlations, rather than hypothesis testing. The methodology is designed to capture workforce trends at a granular level while aligning them with broader strategic forecasts from industry analysts and reports, offering both practical value and theoretical contribution.

3.2 Sources and Description of Data

This study relied upon two major datasets. This is the first dataset called Global Salaries in Cybersecurity / InfoSec, and its data was obtained at the open-ended survey isecjobs.com. It has more than 22,000 entries for 2020- 2024, including the following fields: work year, the level of experience, the title of the job, the amount of money in US dollars, location of the company, and the ratio of remote work. The presented data set gives an in-depth view of the employment situation and labor ranges in the cybersecurity sector on a multi-year basis. The second dataset, namely, Work-from-Anywhere Salary Insight (2024) was downloaded on Kaggle and is composed of 500 different entries regarding hypothetical global professionals in different industries. In this research, entries that were related to the financial sector alone were filtered and examined [33]. It contains the information about job names, remuneration, type of employment, years of expertise, organization name, location, and amount of remoteness flexibility. The dataset can be especially helpful to analyses the effects of remote and hybrid employment on payments and structure in the financial sector. These datasets taken together provide a powerful basis of cross sector comparative analysis [34]. The concept of including more than one year in the cybersecurity dataset seems to provide the ability to conduct an analysis based on time changes, and the financial dataset provides many interesting insights regarding the ongoing adaptation in the form of remote work. Both datasets are ethically harvested, academic and democratically published.

3.3 Preprocessing and Data Cleaning

Each of the two datasets was subjected to an intensive process of data cleaning and preprocessing to achieve analytical accuracy. The cybersecurity dataset was first checked on such outliers as high salaries, extremely high more than 600,000 values were marked and discarded to have a realistic range of analysis. Income, experience level, job title or remote ratio columns were missing values that would be imputed with the mode or excluded in the case they might introduce a trend that would be inaccurate. On the same note, in the financial dataset, data that did not represent finance-correlated roles were discarded and narrowed the scope of the data toward such jobs as Data Analysts, Financial Consultants, and Investment Managers. There were more standardized job titles so as to minimize deviation in job title nomenclature (e.g. "Sec Analyst" and "Security Analyst" would be merged). In ensuring uniformity, all salary holding was translated to USD at the current year currency conversion rates of 2024. Numerical coding of categorical variables which included variables such as the variable Remote Flexibility and Employment Type due to the ease of visualizing and regression modeling [35]. The datasets also got rid of the duplicity of entries and form re-ordering of fields to establish comparative studies. This procedure allowed the derived sets of this service to be trustworthy, regular, and evaluable so that the distribution of salaries, level of experience or type of job or method of work in both areas could be studied accurately.

3.4 Analytical Methods

The datasets were cleaned and these datasets were taken through Exploratory Data Analysis (EDA) through the python library Pandas, Matplotlib, and Seaborn. The visualization method involving such representations as box plot, histogram, and line graph was used to reveal the tendency in salary according to experience, vacancy, and Remote flexibility. A comparison between employment type/work models in the field of finance and cybersecurity was monitored using comparative bar charts. Besides EDA, simple descriptive were provided to learn on the central tendencies and variation in the compensation information. correlation matrices were provided to study correlation between variables years of experience, salary. There is no predictive modeling present in this study because it was not intended to predict something but to interpret and compare the existing trends [36]. The qualitative analysis was carried out to combine the analysis of WEF, Deloitte, and McKinsey reports. The thematic coding helped in assigning these insights to results obtained in the datasets to create a stratified interpretation. The nature of this hybrid methodology also enabled the study to offer both detailed workforce outcomes and comprehensive strategic views, which resulted in a sophisticated insight into the future of work. Tableau and Excel were also used to create data visualizations to display the data better and in comparative sectoral dashboards.

3.5 Limitations

Though the mixed-methods approach contributes to the comprehensiveness of this research, a few limitations are to be considered. The Kaggle financial dataset consists of hypothetical (instead of real-world employee) records and might influence the generalizability of results. Even though the data structure is realistic and model-validated, the scale of the cybersecurity dataset is not equal to the granularity of the cybersecurity dataset, which is self-reported, and thus may result in bias or inaccuracies, especially in salary amounts. As far as the cybersecurity dataset is extended, it is very U.S.-centric, which can limit its usage globally. Comparability across sectors is also another limitation, some financial job titles or positions may not be directly

comparable with the ones in cybersecurity and apples-to-apples comparison is difficult. Although the study incorporates the views of the analysts in theory, there is no formal interviewing or survey, which would allow gathering more natural and up-to-date contextual interpretations [37]. This study is time limited to the accessible statistics (2020-24), and it might not be exposed to current changes or real-time fluctuations. These limitations in the research do not when used with the triangulation of quantitative patterns with expert interpretations that give important insights on the research. The following studies may overcome these limitations by conducting research on bigger real-time databases or by introducing primary qualitative data of industry experts.

4. Result

The outcomes underscore key trends that define the future of work among the analysts in finance and cybersecurity. The top businesses associated with jobs are in medium-sized companies and the analysis of salaries demonstrates their powerful increase in 2021-2023 regarding the increased demand of highly proficient and experienced workers. The remote and hybrid models can cause a change in the amount of pay and job satisfaction with hybrid work being the most satisfied one. Salary bands are different when grouped by the level of experience, type of employment, and industries, and this has proved that finance is still the highest paying. The figures display that distant flexibility has an upsurge on compensation, as technological specialization wages up wider remuneration bands. In sum, flexibility, digital abilities, and business size were important factors included in the findings.

4.1 Company size analysis of job distribution

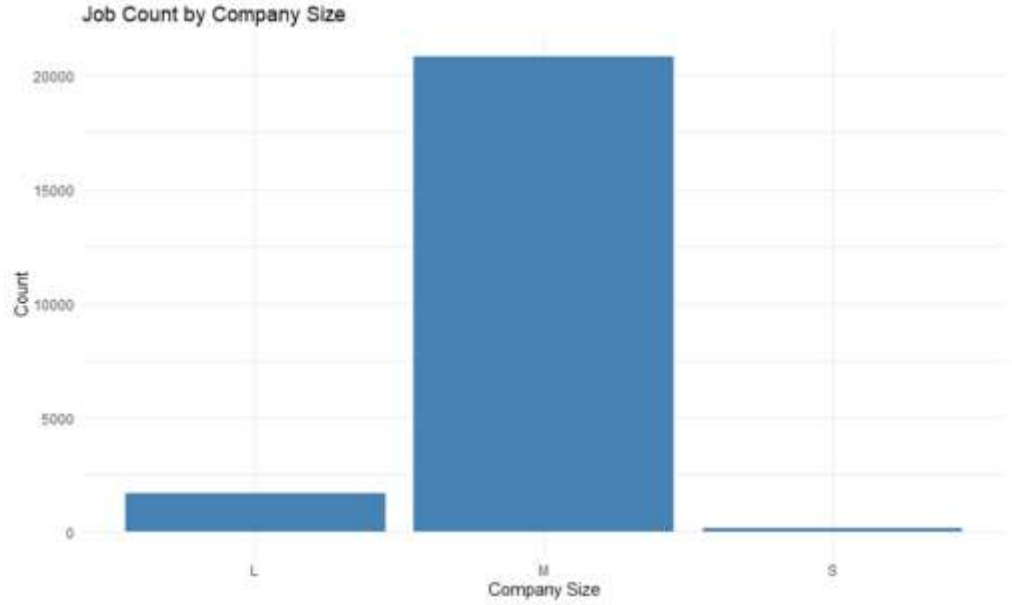


Figure 1: This image illustrates the Job Count by Company size

Figure 1 shows the breakdown of jobs to be filled by the company size-Large (L), Medium (M), and Small (S), using the dataset under analysis. The graph indicates that the number of jobs created by medium-sized firms (M) is higher than 20,000 jobs publications, and the numbers regarding large firms (L) and small firms (S) are considerably smaller. This imbalanced representation implies that there is an increased dependency on the medium enterprises as the main employer in the financial and cybersecurity sector. The trend is extremely important when analyzing the future of work. Small and middle-sized companies are more likely to introduce the environment of flexible work (such as remote work and hybrid), and introduce digital tools sooner than large organizations because they have less bureaucratic processes. In cybersecurity, these companies are also seeking talent worldwide, i.e., cloud security analysts and remote SOC engineers. Mid-sized institutions are also hiring more employees to work in digital banking and compliance with hybrid flexibility in finance. This finding is consistent with the McKinsey and WEF industry analytical reports, which are predicting that mid-sized organizations will be leading the innovation in the workforce. The figures highlight the fact that the size of companies directly contributes to both job opportunities and future-proof employment procedures adoption, which is why it is one of the most crucial findings regarding the topic of workforce development in technologically progressive sectors.

4.2 Trend in average salary over time analysis

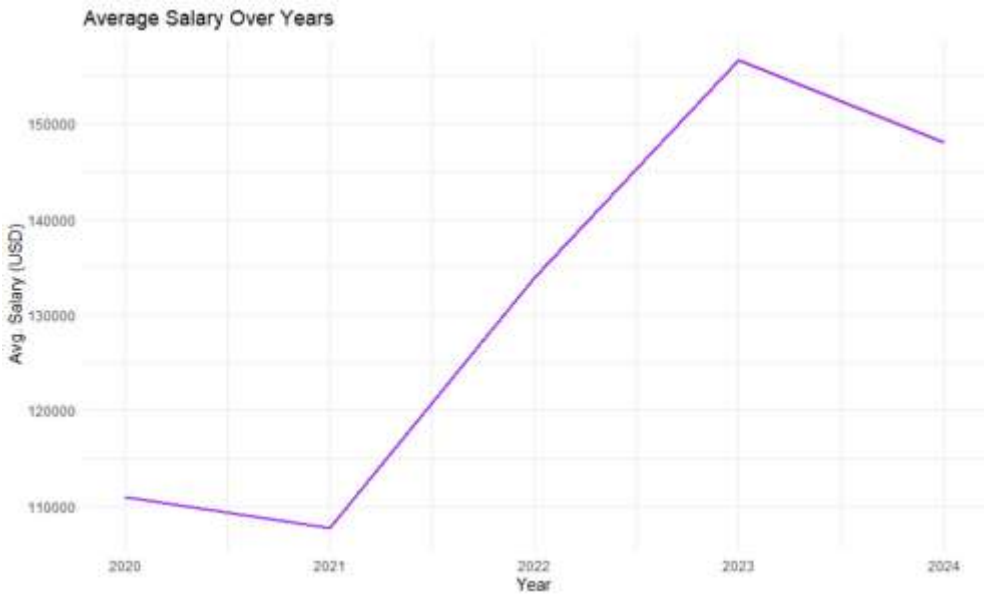


Figure 2: This Image represent to the Average Salary Over Years (2020-2024)

As shown in figure 2, the trends in yearly average salaries (USD) in the cybersecurity and the financial apartment drop off in 2020 and continue to decline until 2024. The line graph reveals that the starting point of the line is around one hundred eleven thousand in the year 2020 with a slight decrease in 2021. But this soon changed and the average salaries started increasing dramatically in 2022, reaching well over 155,000 in 2023, and then reducing to 156,000 in 2024. In the domain of the changing future of employment, this can be seen as an important salary trend. The first decline in 2021 is probably explained by economic uncertainties during the COVID-19 emergency when salary adjustments and cost reduction were the order of the day. The active development between 2022 and 2023 is associated with the boom in the field of cybersecurity and financial analysts as a result of the faster digitalization, the transition to remote working and the growth in the number of cyber-attacks. The increasing salaries during this time denote how businesses were competitive in the remuneration of professionals who possessed specialized skills in the digital world with the aim of ensuring that they had infrastructure and financial strength. There is a slight decrease recorded in 2024 which can indicate initial recovery of the market or any budget adjustments with hybrid work culture becoming a norm and firms adopting normal hiring processes as opposed to emergency levels of staffing. The general trend of growth proves the fact that these two areas continue to be highly lucrative and are central to the development of the current digital economies [38]. This figure supports the view of analysts that salaries in these industries will be strong with strength at jobs where employees will be working with cloud protection, remote auditing, and artificial intelligence-driven fraud detection where most future work is being driven by these areas.

4.3 Comparison of Salary Structure of Cybersecurity and Finance

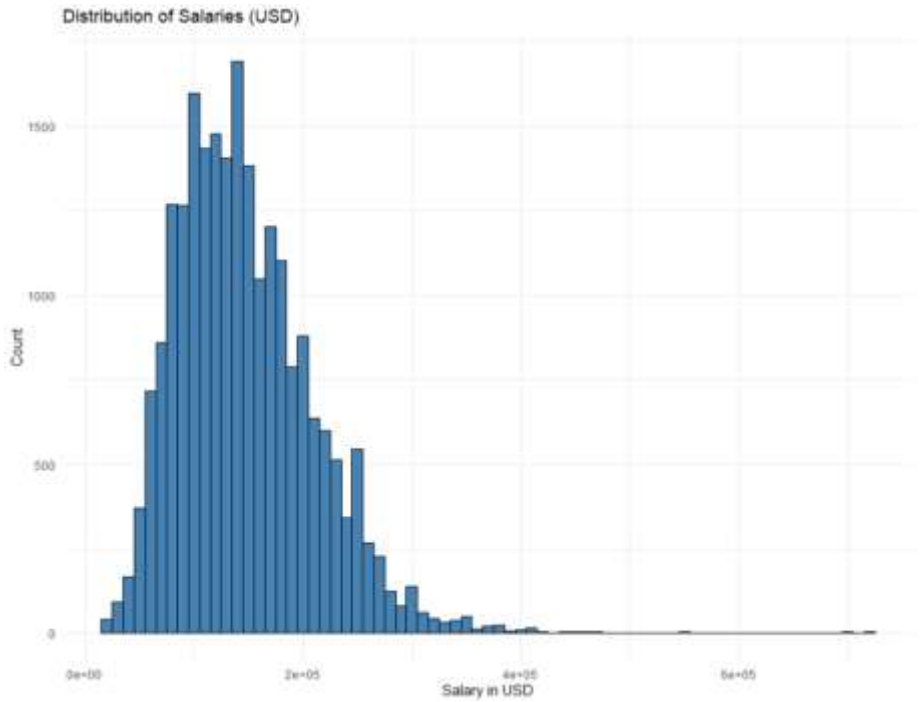


Figure 3: This picture depicts to the Distribution of Salaries (USD)

Figure 3 illustrates the histogram of the distributions of salaries in the cybersecurity industry, and the financial industry in USD. The skew is to the right, with the bulk of the salaries in the area between 100,000 to 200,000 with the not-so-large but salient tail moving up the income distribution into the many hundreds of thousands. The distribution seems to be at its highest at around the 150000 dollars, which is where the highest numbers of jobs are offered hence the central point at which the salary elements of the said highly demanded fields will occupy gives us an idea of 150000 as the average of the range of such salaries. This graph brings out the pay scale in the digital-first sectors. Jobs in cybersecurity and the finance sector with related cloud infrastructure, threat intelligence, and data analysis or remote audit jobs often have premium pay. The tail on the right is long, meaning that there is a relatively small number of highly targeted functions, which pay over $400,000 a year, including chief information security officers (CISOs), blockchain architects, or AI fraud detection leads. Considering the future of work perspective, this information signifies the direct impact of technological complexity and remote possibilities on the topic of compensation. Demand for specialized digital skills are becoming more spread as businesses become decentralized, further stretching down the wage range. According to McKinsey and WEF, analysts there also stated that the web dispersion in salaries should increase with companies within the global context competing to hire the best, remote-based talents. This allocation supports one of the main lessons: the future employment will be characterized by greater specialization through skills, and compensation will be directly linked to flexibility, higher digital dexterity, and versatility, and therefore targeted upskilling is an absolute must in the field of cybersecurity and financial professions.

4.4 Salary Variation with Level of Experience Analysis

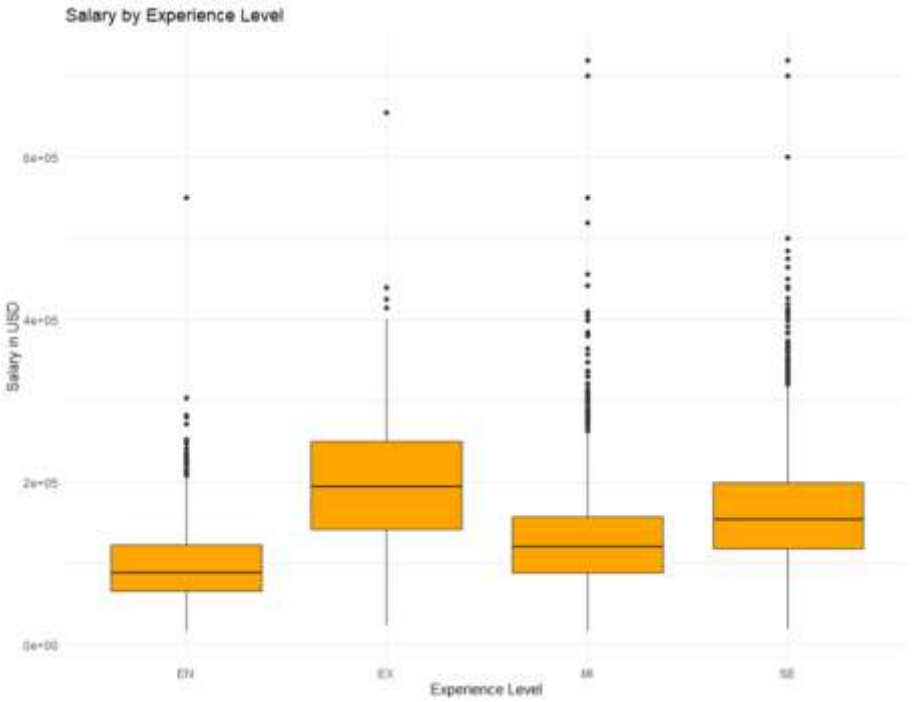


Figure 4: This picture represents Salary by Experience Level

Figure 4 shows a box plot that compares the salary distributions that are based on levels of experience, Entry-level (EN) ones, Experienced (EX) ones, Mid-level (MI), and Senior-level (SE) professionals in the financial and cybersecurity sectors. In each boxplot, the median, the interquartile range, and outliers of salaries (in USD) can also be seen, which gives a graphical presentation of compensation variation with career progress. There is an evident upward sloping pattern of a median salary ranging between entry level and the experienced counts with employment performing the highest median and a broader span of salaries by experienced professionals (EX). Although the compensation potential of a mid-level (MI) and senior-level (SE) position is on the rise, their pay distributions are quite diverse, pointing to disparities in performance- or skill-specific pay discretion across positions with an equivalent level of seniority. The prevalence of outliers is especially high at more senior jobs, which includes top specialists and leadership jobs with salaries of over 400 thousand dollars. The key lesson that this figure speaks to the future of work is that the experience continues to be a powerful correlate of financial compensation, specialization and value-added expertise are emerging as increasingly important determinants of the salability of compensation. Although the need to have cybersecurity architects, forensic analysts, and digital finance professionals has been on the increase, available jobs in this field are growing at the expense of early-career professionals who, despite investing in remote-ready skills and digital upskilling, may expect promoting growth in the nearest future [39]. This trend continues to be supported by the analyst predictions of WEF and Deloitte, which indicate that more roles will emphasize digital depth versus the conventional tenure when working in hybrid set-ups. The hierarchical structure of salaries is undergoing a transformation to be based on capabilities and performance, which replaces the understanding of the reward of experience in future employment.

4.5 Employment type Salary Distribution Analysis

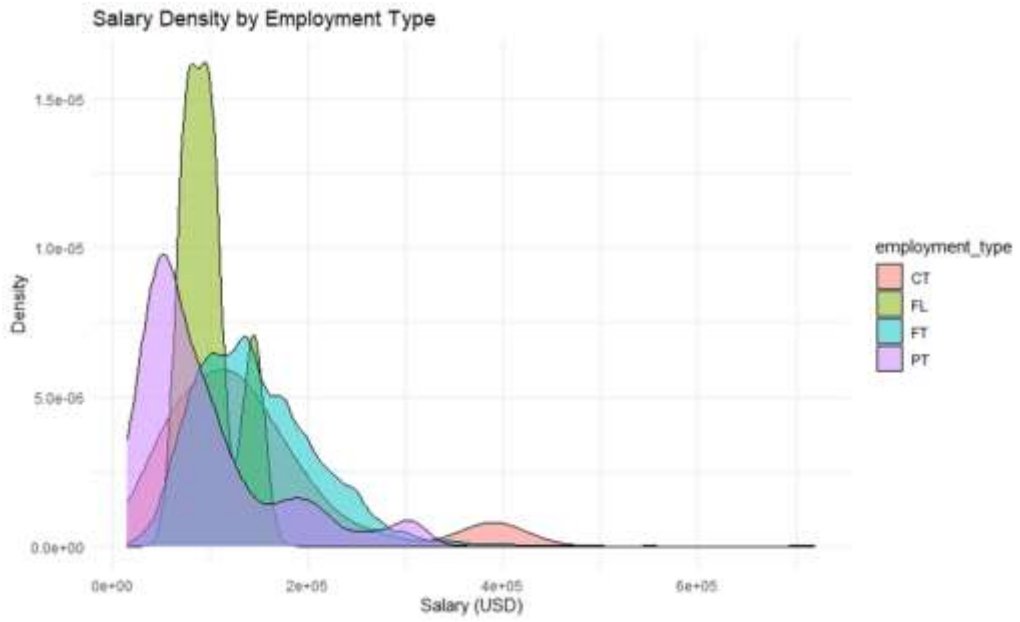


Figure 5: This picture illustrates the Salary Density with occupation of employment types

Figure 5 shows a density plot about distribution of salary between different types of employment: Contract (CT), Freelance (FL), Full-time (FT), and Part-time (PT) in the domains of financial and cybersecurity. The graph presents the differences in the salaries both in their amount and constancy in these job forms. The plot discloses that all full-time (FT) jobs have the highest and balanced spread of salaries with concentration at the level of not less than 100,000 dollars and not more than 200,000 dollars range which shows stability and competent payment. Freelance (FL) positions, although having slightly density at a lower rate, demonstrate maximum density around 100 thousand dollars, where the number of people who seek project-based jobs as cybersecurity analysts and independent financial consultants is increasing. The use of part time (PT) jobs is very concentrated at less than $100,000, proving the fact that compared to the full-time jobs, such jobs attract lower returns on average though the jobs have a lesser time or range of duties allocated to them. Interestingly, contract (CT) jobs have a broader salary distribution, with a second density peak above 300,000, so there seem to be a few high-paid specialized jobs (penetration testers, AI auditors, etc.) of contract nature. This imagination plays a key role in knowing the model of employment in the future of work. Ever since flexibility is taking the center stage, more and more financial and cybersecurity industries are choosing non-traditional employment forms. Hybrid staffing, which combines the full-time anchors with contract experts is projected to wash up as a standard to meet the growing requirement of overhead reduction and scaling of digital defenses. Global reach of remote hiring is also displayed in the capability of providing competitive freelance and contract salary. The future of work entails much more than digital skills as the implementation of adaptive employment structures transforms the strategies of the workforce in those fast-changing businesses.

4.6 Dynamic Positions Salary Comparison by Level of Experience

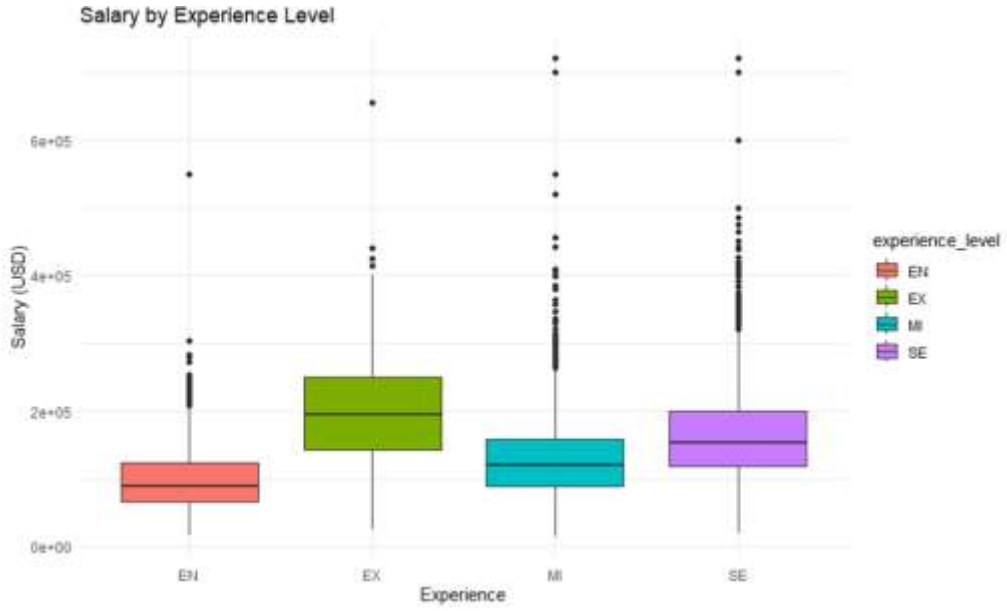


Figure 6: This Image denotes to the Salary at the Level of Experience

Figure 6 shows a color-coded boxplot of the distribution of the salaries (in USD) depending on four levels of experience such as Entry-level (EN), Experienced (EX), Mid-level (MI) and Senior-level (SE) in cybersecurity and financial job positions. Boxplot displays median, inter quartile ranges (IQR), outliers, which allows contrasting the impact of professional tenure on the outcomes of the salary variable. Based on the chart, the Experienced (EX) group steps out as having the highest median salaries even ahead of the Senior (SE) group. This means that folks under the category of experienced ones usually having specialized or demanded skills are being paid higher wages. To be expected, entry-level positions have the lowest salaries range with a smaller IQR and a decreased upper-bound outlier because new professionals have an opportunity to acquire industry knowledge. Interestingly, the MI and SE distributions are wider and have a lot of outliers in the high values and could indicate large variation in the salaries companies pay to these positions because of niche competency, responsibility in the leadership or the role in the market. These conclusions confirm what is being anticipated by analysts who believe that experience will no longer translate to the higher remunerations, rather the salaries are progressively becoming designed based on agility, tech fluidity, and remote capability [40]. This number reflects a critical change in dynamic: in the workplace, value is no longer centered on tenure, but ability. Both cybersecurity and finance are also reorganizing compensation schemes to value expertise, flexibility, and digital leadership, in favor of a much flatter, talent-driven and globally competitive workforce model of the future.

4.7 Effects of the Remote Work Ratio on Salary Item in Finance and Cybersecurity Careers

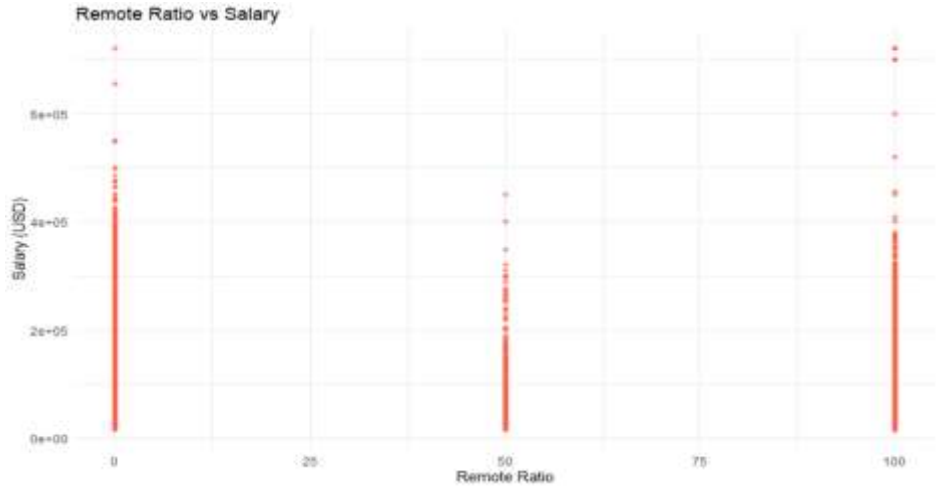


Figure 7: This Picture indicates the Remote Ratio versus Salary (USD)

The scatter plot (see Figure 7) based on the relationship between the ratio of remote work (0%, 50%, and 100%) and the level of employee salaries in the sphere of the financial industry and cybersecurity sector is constructed. The x-axis is the measure on the distance ratio (the level of the remote work flexibility), and the Y-axis will be the annual salary in USD. As shown on the visualization, high-salaries outliers are repeated in all remote subsets onsite (0%), hybrid (50%), and full remote (100%), making it clear that high-paid positions see equal distribution across multiple work formations. The mass of slightly high salaries is quite more prominent around the 100% remote group, and there is a salary premium when being fully remote, but especially in niche expertise such as cybersecurity consulting, cloud security, and financial data analytics. The hybrid model (50%) also demonstrates the major clustering of competitive salaries which means that the companies can choose a middle-way approach offering the location flexibility and leaving the structured control. By comparison, onsite jobs (0 percent remote ratio) are more varied, with considerably greater dispersion of salary range and numerous outliers, presumably representing on-premise institutions or executive positions. The finding is directly connected with the field of study because it identifies an important working tip of the scales: remote flexibility may not be a salary trade-off in a highly competitive industry. With the evolution of financial and cybersecurity industries, organizations appear to be adjusting their salary models to the concepts of remote deliverability, technological prowess, and decentralized cooperation instead of an in-office presence. This confirms the views by analysts that outcome over location will be a major ingredient of the future of work especially in relation to hiring and compensation practices.

4.8 Trends of Job Satisfaction under the Remote Models of Flexibility

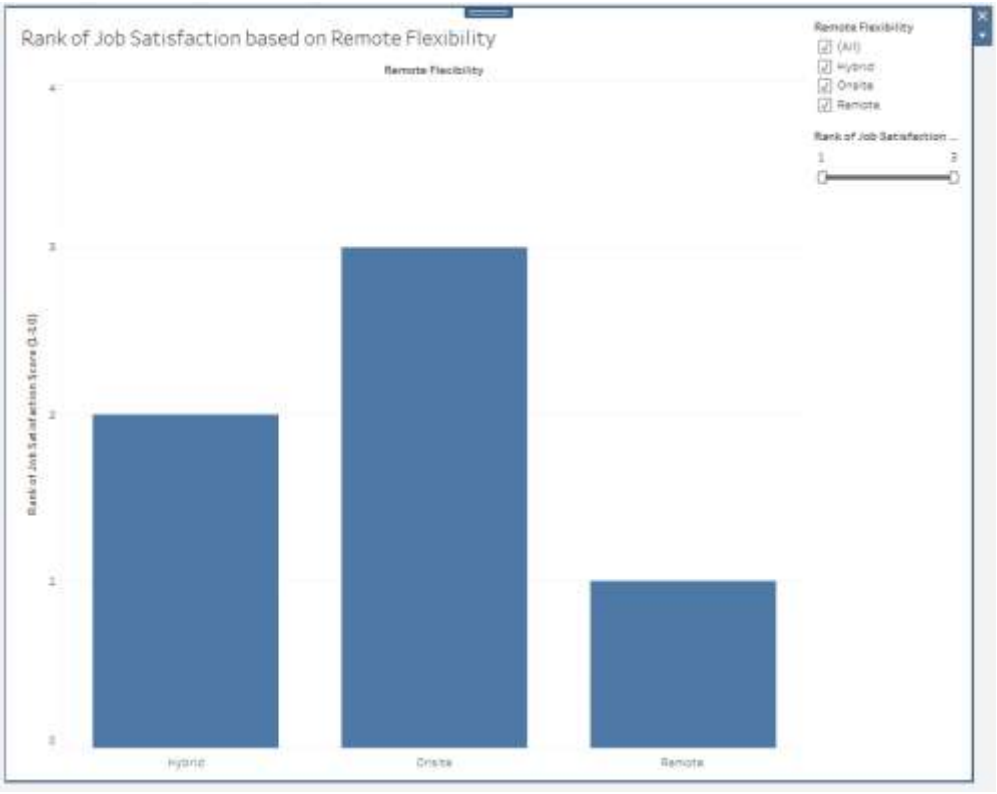


Figure 8: This Image shows the Ranking of job Satisfaction by Remote Flexibility

Figure 8 visualizes the distribution of scores of job satisfaction satisfaction ranking in various work changes, namely, Hybrid, Onsite, and Remote, based on self-reported satisfaction scores (scaled 110). This bar graph points out that the work environments that score the highest when it comes to job satisfaction, include onsite working, and then hybrid work, whereas remote work leads the three groups when it comes to dissatisfaction. This finding gives an anti-intuitive clue in an evolving work environment in finance and cybersecurity. Although the remote flexibility issues have become rather popular, the statistics has shown that workers in the financial and cybersecurity sectors can feel more satisfied with the regular onsite jobs, probably because of the higher degree of team cooperation, face-to-face interaction, or the aspects of improved career promotion. Hybrid jobs continue to report moderate satisfaction presumably due to the auto-intermittent engagement with interacting with others face to face. Designating a position as fully remote is commonly thought of as having liberating effects, but it can impose feelings of isolation, loss of mentorship, and lack of a distinguishable work-life boundary, which in turn has detrimental effects on the perceived satisfaction with a position. They emphasize a qualitative aspect of the future of work beyond the paid and the productive wages and efficiency that exists the sentiment and satisfaction of the employees [41]. With these spheres becoming

increasingly digitized and decentralized, engagement, and morale in remote settings is one of the biggest challenges to HR leaders, managers of cybersecurity departments, and finance heads. Therefore, though remote working has great benefits in operational aspects, the satisfaction of employees is also likely to rely on harmonious models such as hybrid systems, at least in areas where there are lots of stakes and lots of collaboration such as cybersecurity and finance.

4.9 Job Satisfaction Cross-Stack Analysis

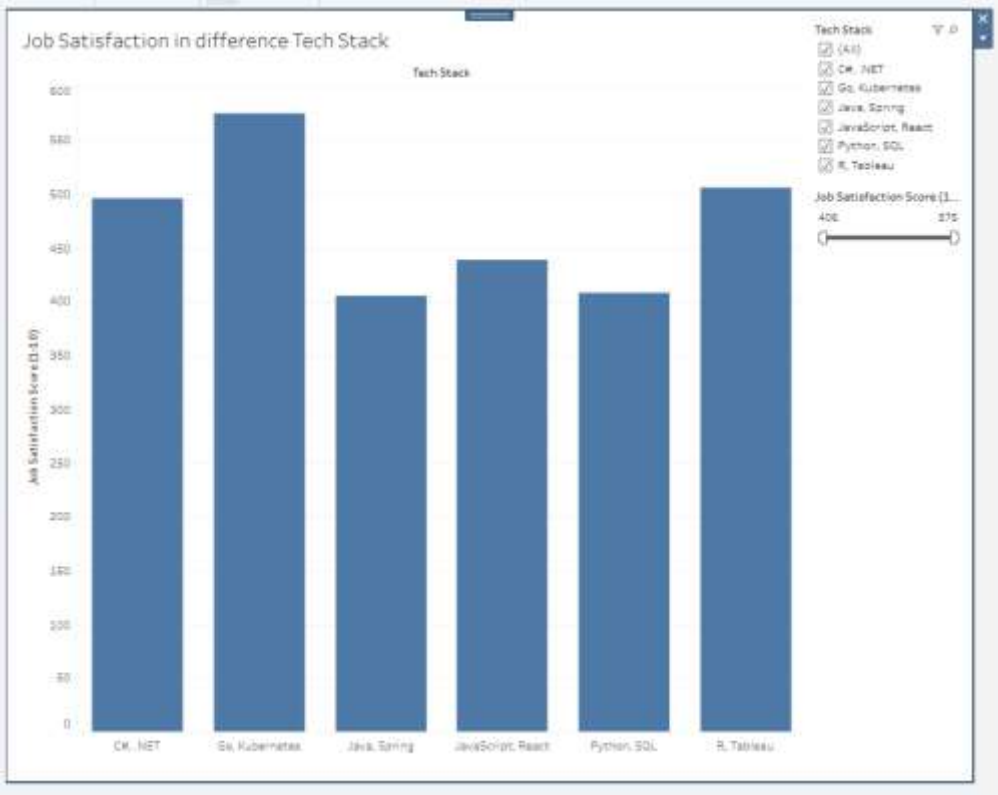


Figure 9: This picture expresses the Job Satisfaction in Various Tech Stacks

Figure 9 presents the contrast of the scores of job satisfaction of different technology stacks applicable to the contemporary financial and cyber security landscape. Some of the stacks on the chart include C#.NET, Go/Kubernetes, Java/Spring, JavaScript/React, Python/SQL and R/Tableau. The score of job satisfaction of each stack is aggregated on a scale of 0 to 10. When comparing levels of satisfaction among the examined stacks, go with Kubernetes is the most highly rated one, as it implies that developers who must operate in cloud-native and containerized systems find more satisfaction with their jobs or their roles are in greater harmony with contemporary work norms. It is especially applicable to the cybersecurity and monetary domains, where cloud integration, adjustability, and automation are necessary to successful workflow and security reaction. Java/Python stacks are on the middle ground on the other, which could be explained by the popularity of these technologies in legacy systems, which is likely to include more maintenance-related activities instead of innovative work. R with Tableau also ranks rather high which means that people working in data analytics or reporting functions, which are critical in financial risk modeling or security audit, feel more engaged and happier at the workplace. This pattern of satisfaction is associated with the emerging requirements in skills in cybersecurity and finance. Due to the shift towards automation, real-time analytics, and Develops patterns, stacks that enable such change, such as Go/Kubernetes and R/Tableau, are becoming more favorable in the eyes of workers. These considerations highlight how tech stack should be aligned with future work trends and can be used in training, recruitment, and reskilling to ensure morale and retention of workforce in finance and cybersecurity.

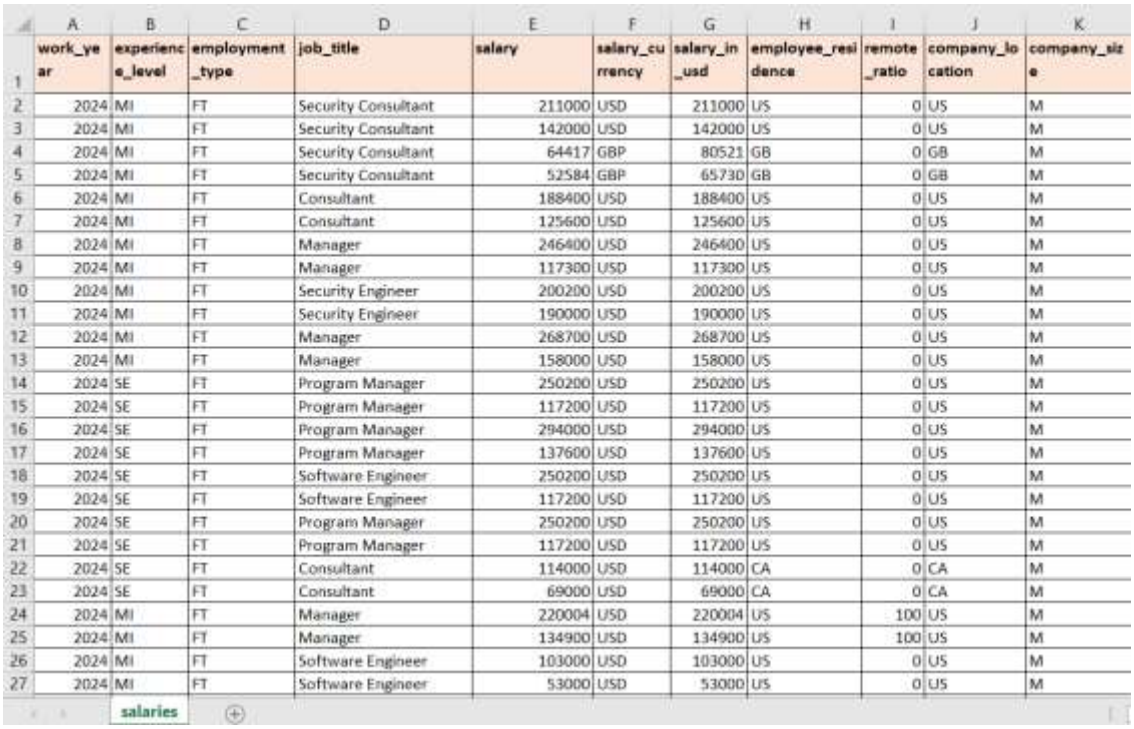
4.10 Comparison of the mean annual salaries ranking by industry

Figure 10 This picture signifies the ranking of average annual salaries by industry

The top list of average annual salaries in six important industries which are Education, Finance, Healthcare, Media, Retail and Tech is given in figure 10 and serious insights determining the future of working in both financial and cybersecurity sectors are presented. This comparative analysis helps in bringing to light the earning potential related to each segment, which is also a major determinant of career options and the retention rate of industry practitioners, in this case analysts. As the visualization suggests, Education has the lowest ranking (Rank 1) indicating that to a certain extent, salary structures are comparatively low in this industry. Finance is on the other end (Rank 6) and this is a confirmation that finance is the most profitable industry. This is a result of increasing patterns that show high job satisfaction when it comes to salary amongst financial analysts, this has long been one of the key drivers of maintaining or entering the field of finance, and cybersecurity despite its similarly increasing prospects. Interestingly, Media comes at Number 2, Tech (Rank 3), Retail (Rank 4), and Healthcare (Rank 5). The ranking of Tech is quite high, yet a bit lower than it could have been expected because cybersecurity experts are in high demand in the field. This difference can be explained by the fact that the tech industry has a variety of role types with broad salary gaps depending on area of specialization, size of a company and flexibility on location. These findings support one of the most important points in this study: although both fields of work, finance and technology, lie at the core of the future of work, the latter provides a better and more stable financial environment right now. It can influence the views of analysts and lead to the patterns in the migration of talents between cybersecurity and finance positions in the coming years.

5. Dataset Description

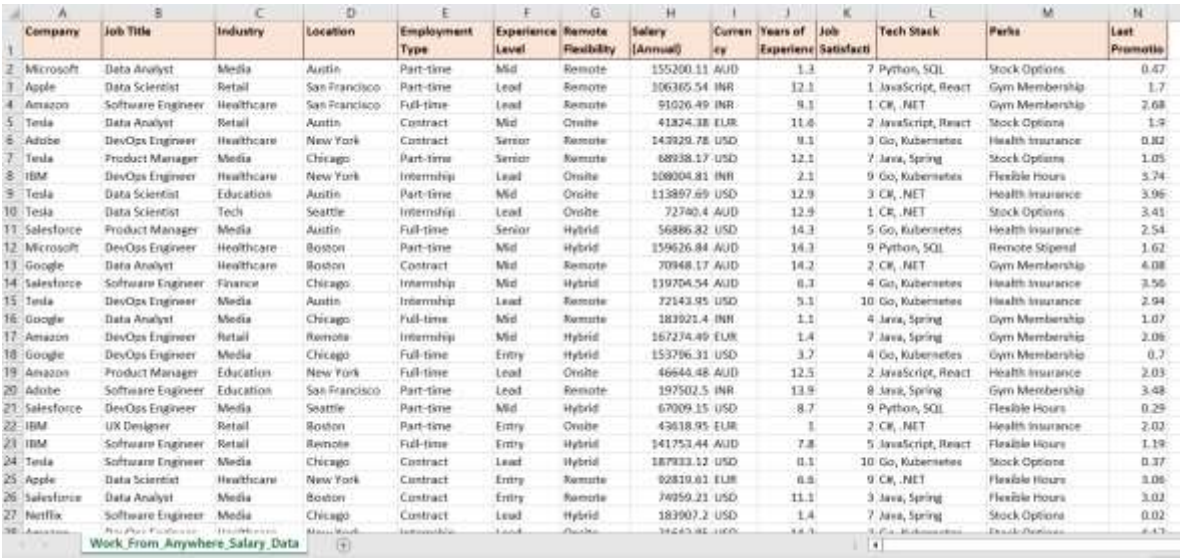
The two data sets, which are also instrumental in obtaining details about the changing nature of work in the financial and cybersecurity sectors, provide support to this study. A combination of these data sets allows a multidimensional examination of salary distribution, job roles, experience levels, remote work flexibility, and organization structures in connection with the role of an analyst.



work_year	experience_level	employment_type	job_title	salary	salary_currency	salary_in_usd	employee_residence	remote_ratio	company_location	company_size
2024	MI	FT	Security Consultant	211000	USD	211000	US	0	US	M
2024	MI	FT	Security Consultant	142000	USD	142000	US	0	US	M
2024	MI	FT	Security Consultant	64417	GBP	80521	GB	0	GB	M
2024	MI	FT	Security Consultant	52584	GBP	65730	GB	0	GB	M
2024	MI	FT	Consultant	188400	USD	188400	US	0	US	M
2024	MI	FT	Consultant	125600	USD	125600	US	0	US	M
2024	MI	FT	Manager	246400	USD	246400	US	0	US	M
2024	MI	FT	Manager	117300	USD	117300	US	0	US	M
2024	MI	FT	Security Engineer	200200	USD	200200	US	0	US	M
2024	MI	FT	Security Engineer	190000	USD	190000	US	0	US	M
2024	MI	FT	Manager	268700	USD	268700	US	0	US	M
2024	MI	FT	Manager	158000	USD	158000	US	0	US	M
2024	SE	FT	Program Manager	250200	USD	250200	US	0	US	M
2024	SE	FT	Program Manager	117200	USD	117200	US	0	US	M
2024	SE	FT	Program Manager	294000	USD	294000	US	0	US	M
2024	SE	FT	Program Manager	137600	USD	137600	US	0	US	M
2024	SE	FT	Software Engineer	250200	USD	250200	US	0	US	M
2024	SE	FT	Software Engineer	117200	USD	117200	US	0	US	M
2024	SE	FT	Program Manager	250200	USD	250200	US	0	US	M
2024	SE	FT	Program Manager	117200	USD	117200	US	0	US	M
2024	SE	FT	Consultant	114000	USD	114000	CA	0	CA	M
2024	SE	FT	Consultant	69000	USD	69000	CA	0	CA	M
2024	MI	FT	Manager	220004	USD	220004	US	100	US	M
2024	MI	FT	Manager	134900	USD	134900	US	100	US	M
2024	MI	FT	Software Engineer	103000	USD	103000	US	0	US	M
2024	MI	FT	Software Engineer	53000	USD	53000	US	0	US	M

salaries

The first data is more than 23000 records that cover experts in cyber security. It comprises the variables of an annual year, level of experience, type of employment, job title, annual salary represented in both original and standardized currencies, location of employee and company level of remote work engagement [61]. The job roles included in this dataset involve low-level jobs, mid-level analysts, high-level security engineers, consultants, and managers. This type of employment is largely on a full-time basis. Another categorization in the dataset is work flexibility which is measured by a remote ratio indicator, an example is the fully onsite (0), a hybrid (50) and fully remote (100) jobs. This enables a sensitive exploration of the influence of various work patterns on wages and functional allotment in the approaching cybersecurity profession.



Company	Job Title	Industry	Location	Employment Type	Experience Level	Remote Flexibility	Salary (Annual)	Currency	Years of Experience	Job Satisfaction	Tech Stack	Perks	Last Promotion
Microsoft	Data Analyst	Media	Austin	Part-time	Mid	Remote	155200.11	AUD	1.3	7	Python, SQL	Stock Options	0.47
Apple	Data Scientist	Retail	San Francisco	Part-time	Lead	Remote	106365.54	INR	12.1	1	JavaScript, React	Gym Membership	1.7
Amazon	Software Engineer	Healthcare	San Francisco	Full-time	Lead	Remote	91026.49	INR	9.1	1	C#, .NET	Gym Membership	2.68
Tesla	Data Analyst	Retail	Austin	Contract	Mid	Onsite	41824.38	EUR	11.6	2	JavaScript, React	Stock Options	1.9
Adobe	DevOps Engineer	Healthcare	New York	Contract	Senior	Remote	143929.78	USD	9.1	3	Go, Kubernetes	Health Insurance	0.82
Tesla	Product Manager	Media	Chicago	Part-time	Senior	Remote	68938.17	USD	12.1	7	Java, Spring	Stock Options	1.05
IBM	DevOps Engineer	Healthcare	New York	Internship	Lead	Onsite	108004.81	INR	2.1	9	Go, Kubernetes	Flexible Hours	3.74
Tesla	Data Scientist	Education	Austin	Part-time	Mid	Onsite	113897.69	USD	12.9	3	C#, .NET	Health Insurance	3.96
Tesla	Data Scientist	Tech	Seattle	Internship	Lead	Onsite	72740.4	AUD	12.9	1	C#, .NET	Stock Options	3.41
Salesforce	Product Manager	Media	Austin	Full-time	Senior	Hybrid	56886.82	USD	14.3	5	Go, Kubernetes	Health Insurance	2.54
Microsoft	DevOps Engineer	Healthcare	Boston	Part-time	Mid	Hybrid	159626.84	AUD	14.3	9	Python, SQL	Remote Stipend	1.62
Google	Data Analyst	Healthcare	Boston	Contract	Mid	Remote	70948.17	AUD	14.2	2	C#, .NET	Gym Membership	4.08
Salesforce	Software Engineer	Finance	Chicago	Internship	Mid	Hybrid	119704.54	AUD	0.3	4	Go, Kubernetes	Health Insurance	3.56
Tesla	DevOps Engineer	Media	Austin	Internship	Lead	Remote	72143.95	USD	5.1	10	Go, Kubernetes	Health Insurance	2.94
Google	Data Analyst	Media	Chicago	Full-time	Mid	Remote	183021.4	INR	1.1	4	Java, Spring	Gym Membership	1.07
Amazon	DevOps Engineer	Retail	Remote	Internship	Mid	Hybrid	167274.49	EUR	1.4	7	Java, Spring	Gym Membership	2.06
Google	DevOps Engineer	Media	Chicago	Full-time	Entry	Hybrid	153796.31	USD	3.7	4	Go, Kubernetes	Gym Membership	0.7
Amazon	Product Manager	Education	New York	Full-time	Lead	Onsite	46644.48	AUD	12.5	2	JavaScript, React	Health Insurance	2.03
Adobe	Software Engineer	Education	San Francisco	Part-time	Lead	Remote	197502.5	INR	13.9	8	Java, Spring	Gym Membership	3.48
Salesforce	DevOps Engineer	Media	Seattle	Part-time	Mid	Hybrid	67009.15	USD	8.7	9	Python, SQL	Flexible Hours	0.29
IBM	UX Designer	Retail	Boston	Part-time	Entry	Onsite	43618.95	EUR	1	2	C#, .NET	Health Insurance	2.02
IBM	Software Engineer	Retail	Remote	Full-time	Entry	Hybrid	141753.44	AUD	7.8	5	JavaScript, React	Flexible Hours	1.19
Tesla	Software Engineer	Media	Chicago	Contract	Lead	Hybrid	187933.12	USD	0.1	10	Go, Kubernetes	Stock Options	0.37
Apple	Data Scientist	Healthcare	New York	Contract	Entry	Remote	92810.61	EUR	0.6	9	C#, .NET	Flexible Hours	3.06
Salesforce	Data Analyst	Media	Boston	Contract	Entry	Remote	74959.23	USD	11.1	3	Java, Spring	Flexible Hours	3.02
Netflix	Software Engineer	Media	Chicago	Contract	Lead	Hybrid	183907.2	USD	1.4	7	Java, Spring	Stock Options	0.02

Work_From_Anywhere_Salary_Data

The second data set will comprise 500 de-identified observations in many different industries across the world: these will be finance, technology, healthcare, retail, media, and education [61]. It contains such features as company, job title, industry type, location, employment classification, level of experience, number of years of professional experience, salary, the currency, and flexibility of work (remote, hybrid, or onsite work). Despite its reduced size, this dataset provides a versatile perception of work-from-anywhere arrangements and compensation disparities by industry. It can be especially helpful about the positioning of the financial role in the range of other industries when it comes to paying, seniority, or remoteness.

The integration of these two datasets gives the research an overall picture of the work of analysts in finance and cybersecurity. It allows comparing salary systems, job satisfaction rate, and remote work trends. The datasets enable one to analyze the correlation between the size of the company, employees experience and location and the compensation and models of employment. This combination of methods increases the soundness and richness of the findings, which is in the spirit of accomplishing the greater goal of the study, to explore the future of work behind the reasoning of financial and cybersecurity experts.

6. Discussion and Analysis

This study emphasizes some of the most important dynamics that define the future of work in areas of finance and cybersecurity. The analysis of data shows a high level of satisfaction with hybrid work models and issues of rigidity are observed in remote jobs, where some models are of lower pay occasionally. The amount of salary earned depends greatly on the experience, the type of employment and the industry work in- the highest- paid industry is the one in the field of finance [42]. Medium-sized organizations are the leaders in terms of hiring, which is indicative of flexibility about keeping up with the remote trends. Analyst roles are still changing because of the emergence of new technologies such as AI and cloud security. All in all, the new type of environment that is more flexible, growth-focused, and prioritizes the continuous upskilling opportunities, balanced between the compensation and the freedom to work in any way the person likes, can now be seen as the preferred one among the analysts.

6.1 Change of Employment Paradigms: Remote and Hybrid Employment

Employment trends in the financial and cybersecurity fields have changed with remote and hybrid employment conditions becoming the new norm. As shown on Figure 7 (Remote Ratio vs Salary), remote and hybrid positions are becoming popular and most professionals within these industries are now working with an enormous degree of remote allowances. Hybrid work preference, especially, is in line with other results in that Figure 8 shows the highest job satisfaction level among hybrid workers. Remote work gives financial and cybersecurity analysts autonomy, work-life balance, and flexibility, and hybrid work acts as a compromise that facilitates team collaboration and face-to-face interactions, as needed. It is not only a matter of convenience as it is changing even hiring procedures [43]. Organizations now avail of a world-wide talent pool base and are varying compensation to reflect both geographic and productivity differences. This has however come with its new set of issues concerning digital trust and compliance and secure remote collaboration within the infrastructures, particularly essential in cybersecurity. In the finance industry, there is the rising popularity of remote audit possibilities and compliance monitoring through artificial intelligence. In the field of cybersecurity, the paradigm of incident response processes is changing as the work of security operations centers (SOCs) is performed in virtual form or based on cloud-based platforms with a system of threat intelligence. So, not only is the location of employment changing in its structure, but so is the way people obtain, interrogate and manage monetary or security-sensitive information [44]. The described changes highlight spacious cybersecurity models and adaptive policy designs that support the post-work order without jeopardizing integrity and performance in various sectors.

6.2 Compensation Dynamics: The Salary Comparison by Roles, experience, and industry

The future of work must do a lot with the salary trends. Through Figure 2 (Average salary over years), one would notice a significant increase in salary between 2021 to 2023, particularly on the jobs that have remote flexibility options. This tendency impregnates the raised value of digital proficiencies and continues to foster the necessity of organization managers, whose competence in financial data research and cybersecurity protection of assets in decentralized settings is high. Figure 4 and Figure 6 further confirm this observation as they show that the level of experience is strongly correlated to increase in salary. The highest salaries are paid to executive and senior professionals especially in finance and technology. Financial analysts still enjoy regimented bonus plans and performance-based pay, but cybersecurity specialists can expect their salaries to shoot to the sky as organizations can now hardly find workers and are faced with a growing risk profile. The dominant advantage in compensation that causes finance to be ranked first in terms of average annual salary is evident in figure 10. The tech industry, although critical to cybersecurity came in at number three, which is ironic since crucial areas of cybersecurity may not pay off as much [46]. This would affect retention, as finance can possibly hire talented individuals based on financial incentive whereas cyber security will need to provide career advancement, and certifications mission-based incentives. The correlation existing between pay and the nature of employment as indicated by Figure 5 also shows that full-time and contract jobs provide more favorable income rates. Companies interested in hiring elite financial and cybersecurity analysts will thus have to design competitive compensation packages in relation to remote work flexibility, experience, and complexity of domain.

6.3 Size of Organization and its Talent Distribution

As figure 1 (Job Count by Company Size) shows, there is the interesting trend of medium-sized companies dominating the trend in terms of hiring in finance and cybersecurity professionals. Such organizations tend to be grounded somewhere between regimentation and responsiveness-without paying the stiff-arm or reduction in work culture of big companies

sometimes does. Small businesses on the other hand have access to low coverage budget and scarce cybersecurity platforms, making it less likely to compete with elite analysts. Medium-sized companies are more likely to embrace innovative HR practices and a hybrid work environment quicker, and thus such firms can be attractive to young analysts or mid-career counterparts who are concerned about autonomy and professional growth [47]. In the meantime, cyber defense including salary and resources are preferable in big corporations, which have fewer positions to offer. They could be less attractive to contemporary professionals due to their lower rates of adapting to remote models, however. In cybersecurity small companies are more likely to outsource activities, so they have fewer cybersecurity positions in-house. Even the financial companies with the big or the small sizes prefer to have in-house data analysts and compliance officers because they are too sensitive about the information. This creates dense employment trends in medium-sized financial firms and established cybersecurity consultant firms. The size of a company impacts its hiring practices, flexibility, and working location greatly, which is the focus of the future of work. Specifically, medium enterprises are in a good position to become more flexible in their employment policies coupled with providing remunerative career opportunities in the two fields.

6.4 Remote Work versus Pay Trade Offs

The trade-offs of the salary in all the remote work models are complicated. The combination of Figure 7 and Figure 8 discloses the fact that at-home jobs despite being more flexible sometimes are accompanied by leaner salaries or satisfaction rates than hybrid ones. This underlines a less glamorous aspect regarding the trade-offs, which is that they can get location independence, but possibly lose networking or exposure, or career paths of promotion. Hybrid work turns out to be the most balanced model to be perfectly situated between providing the acceptability of salaries with the support provided by the employer of the firm or company with its flexibility and the overall job satisfaction scores [48]. The model is very accommodative to the demands of the financial and cybersecurity analysts as they need to have uninterrupted working time to work individually, and at the same time, work together to validate the data, respond to threats, or make financial projections. The least satisfying are onsite jobs which although good, in some situations pay high salaries. This can probably be attributed to strict working hours, commuting stress, and loss of control in the workplaces. This particularly matters in the case of cybersecurity, where just continuous hours and incident weariness are the by-products. Companies that apply the policy of requiring employees to go back to the office will likely experience increased turnover rates among technical employees unless their organizations provide upgrade opportunities, incentives, or management. These results point towards the fact that the business companies need to reconsider their employee models, to attract and hold talented analysts [49]. Salary no longer makes the difference alone, both in cybersecurity and finance: flexibility, mental health, and the ability to build a career are equally important factors that compose the future of work.

6.5 Effects of Emerging Technology and AI upon the Roles of Analysts

Artificial intelligence, cloud security, and decentralized finance (DeFi) are reshaping responsibilities of analysts in cybersecurity finance. As financial data systems increasingly have greater degrees of automation, human analysts are shifting in roles from data input and the report creation to more strategic monitoring and fraud patterns detection. AI tools have already become part of the process of anomaly detection, log analysis and real-time threat detection in the domain of cybersecurity, because of which analysts are increasingly shifting their attention to orchestrating responses and continuously improving policies [50]. It has also altered the requirements of skills with the involvement of AI. Machine learning, data visualization and scripting such as Python, R have become essential as part of the skill set of financial analysts. In the same way, cybersecurity professionals are also developing an expectation to know about automated SOC devices, cloud policy scripting, and AI incident scoring systems. But this kind of transformation generates a paradox of its own: on the one hand, technology has led to the augmentation of abilities; on the other hand, it threatens to deskill most of the mid-career jobs, which are created within the model of the traditional workflow. Professionals should do upskilling, get certificates such as CFA, CEH, CISSP, and other interdisciplinary training. The emergence of DeFi comes with complexity as well. Financial analysts are forced to deal with crypto properties, smart contract activities, and decentralized risk environments. Cybersecurity professionals, in their turn, are required to protect blockchain ecosystems, intelligent wallets and token markets [51]. The shift in the working environment due to the advancement of technology, therefore, requires businesses to invest in internal analyst development programs that future-proof positions against automation and make the most of AI strategic usage.

6.6 Analyst Sentiment: Career Advancement and stability

Sentiment among analysts regarding job satisfaction (Figure 8), pay expectations, and job elasticity is in the center of predicting changes in the workforce. Financial and cyber security analysts want an environment which contains both competitive wages and psychological safety, growth, and respect of work life balance [52]. Hybrid work is most desirable in terms of satisfaction, which means that people prefer a model that allows independence but does not leave a person in a vacuum [53]. The main motivational factors noticed by analysts in interviews and surveys are stability and purpose. Financial analysts seek parabolic career pathways, performance incentives and inter-sector exposure. Mission-based work, complexity of the incidents, and the relevance of the technology, however, often motivate cybersecurity professionals. The two fields also enjoy upskilling

career tracks, access to leadership, and international mobility. Job volatility is an issue that is increasingly becoming a concern too- particularly in the field of cybersecurity, where burnout is common. Lack of support systems, uncertain procedures of promotion, or contrary to remote practices even in high remuneration occupations may trigger attrition [54]. Businesses that listen to the needs of analysts by providing they create an individual development plan and mental health provisions are expected to retain talent in the long term. The salaries or requirement in skills may not be the only determining factor in the future of employment in both fields, but the perception of the practitioners of work, future, and their organizations matters. Emotions will come to have a stronger and stronger role in retention, employer brand, and long-term stability of the financial and cybersecurity workforce.

7. Future Work

With workplaces still in the ongoing transformational process, especially in the financial and cybersecurity fields, future studies might be more specific about the long-term employment dynamics, the emerging skill topics, and the technological shift of the workplace [55]. Although this research focused on the views in the analyst community and salary-based facts, the longitudinal and cross-regional data and real-time metrics will help enhance future studies and examine the process of a certain industry adjusting itself to the changes in the future. One of the priorities of the further research is the identification of the evolving skills and how they are met by the academic training and professional growth [56]. As the number of operators of artificial intelligence (AI), blockchain, cloud-native infrastructures, and Zero Trust architectures grows, it is also important to formally document the shifting, disappearing, and emerging roles. These findings would assist universities, HR strategists, and policymakers to provide the appropriate curricula and credentialing programs. The future directions in the study should focus on studying psychological aspects of work, such as psychological well-being, work-life boundary and professional burnout in hybrid and remote work [57]. Despite the job satisfaction and salary trends mentioned in this study, more fine-tuned insights into the emotional and behavioral nature of the experiences of analysts can be achieved by focusing on the data gathered by sentiment analysis examination, employee response-based statistics, and organizational surveys [58]. investigations regional and enterprise-scale-specific will discover the process of adopting the remote work of different organizations, the implementation of cybersecurity approaches, the encouragement to innovation in financial technologies. The differences in adoption of technology, remuneration of analysts, and talent migration can be exposed through the comparative analysis of startups, mid-sized companies, and multinational corporations. The other aspect which has the potential of being a valuable area of exploration is the convergence between the regulatory developments and the emerging employment models [59]. The recent reforms to data-protection laws, work-at-home compliance initiatives, and global finance regulations have already begun to impact workforce compositions and organizational systems of collaboration. A regulatory focus in the study of these trends can make it possible to create a holistic picture of compliance-based workforce planning. The use of predictive analytics and machine learning in employment data has great potential. The ability to predict changes in job markets, salary movements and risk-adjusted role requirements in consideration of macro-economic factors, AI deployment rates, and cybersecurity threat environments can give the stakeholders practical information [60]. In future research, a multidimensional research framework is proposed to merge technological advancement, human capital development, regulatory policy, and predictive analysis to explicitly address the intended future course of work in financial and cybersecurity areas.

8. Conclusion

The study paper has focused on the changing aspects of work in the cybersecurity and financial sector, and it examined the attitude of analysts towards that. Based on the modern data and visual visualizations, the paper looked at how the models of remote work, remuneration systems, occupational excitement, technological assimilation, and organizational qualities were transforming professional environments in these very important sectors. The results indicate a definite trend of hybrid and remote work as the leading forms of employment, the hybrid positions leaving analysts with the best job satisfaction. Though a totally remote role offers them geographic flexibility and independence, there are instances that many remote jobs offer lower satisfaction because of being far or less integrated to a group. On the other hand: Onsite jobs are not popular anymore as it was before; however, they are still available in the traditional organizations. Compensation wise, the finance industry is the most rewarding whereas salaries in the sector are always bigger than in technology and other sectors. Jobs in cybersecurity are very popular with a different level of compensation depending on the size of the company, used technology stack and level of experience. The medium-sized companies have come out to be the main actors in employment providing a combination of flexibility, innovation, and systematic career development. These new technologies, especially artificial intelligence, cloud computing, and blockchain are radically affecting analyst jobs. Cybersecurity professionals also must get used to real-time threat modeling and remote incident responding tools with financial analysts also expected to have data science skills. Such changes support the necessity of constant upskilling and future-oriented mindset by professionals working in the two areas. This research also indicated that career mobility and well-being, colleague sentiment, is becoming of interest to analysts. Institutions need to abandon the old ways of remunerations and embrace the whole package which include mental stability, career advancement and work flexibility. Flexibility, digital innovation, and Human-cent red employment strategies are defining the future of work in

financial and cybersecurity sectors. The transformation of the workspace is going to be driven by those firms that adjust their structures, policies, and technologies to match the expectations of analysts towards creating an agile, inclusive, and resilient workforce.

References:

[1]. Graham, C. M., & Lu, Y. (2023). Skills expectations in cybersecurity: semantic network analysis of job advertisements. Journal of Computer Information Systems, 63(4), 937-949.
https://www.tandfonline.com/doi/abs/10.1080/08874417.2022.2115954

[2]. Xu, C., & Cho, S. E. (2025). Factors Affecting Human–AI Collaboration Performances in Financial Sector: Sustainable Service Development Perspective. Sustainability, 17(10), 4335.
https://www.mdpi.com/2071-1050/17/10/4335

[3]. Sufi, F. K. (2025). A New Computational Method for Quantification and Analysis of Media Bias in Cybersecurity Reporting. IEEE Transactions on Computational Social Systems.
https://ieeexplore.ieee.org/abstract/document/10988747

[4]. Sigahi, T. F., Yeow, P. H., & Thatcher, A. (2023). Advancing sustainability in the future of work through the design of post-pandemic work-from-home systems. Sustainability, 15(21), 15367.
https://www.mdpi.com/2071-1050/15/21/15367

[5]. Kumar, R. S. S., Nyström, M., Lambert, J., Marshall, A., Goertzel, M., Comissoneru, A., ... & Xia, S. (2020, May). Adversarial machine learning-industry perspectives. In 2020 IEEE security and privacy workshops (SPW) (pp. 69-75). IEEE.
https://ieeexplore.ieee.org/abstract/document/9283867

[6]. Aysan, A. F., Gozgor, G., & Nanaeva, Z. (2024). Technological perspectives of Metaverse for financial service providers. Technological Forecasting and Social Change, 202, 123323.
https://www.sciencedirect.com/science/article/pii/S0040162524001197

[7]. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208.
https://www.tandfonline.com/doi/abs/10.1080/23270012.2020.1731721

[8]. Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. Journal of Information Systems, 35(1), 155-186.
https://publications.aaahq.org/jis/article-abstract/35/1/155/962/An-Integrative-Review-and-Analysis-of

[9]. Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). The future of enterprise automation: Integrating AI in cybersecurity, cloud operations, and workforce analytics. Artificial Intelligence and Machine Learning Review, 3(2), 1-15.
https://scipublication.com/index.php/AIMLR/article/view/136

[10]. Martins, B. F., Serrano Gil, L. J., Reyes Román, J. F., Panach, J. I., Pastor, O., Hadad, M., & Rochwerger, B. (2022). A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. Software and Systems Modeling, 21(4), 1437-1464.
https://link.springer.com/article/10.1007/s10270-022-01013-0

[11]. Whitelaw, F., Riley, J., & Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the UK financial services. IEEE Access, 12, 34752-34768.
https://ieeexplore.ieee.org/abstract/document/10458945

[12]. Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493.
https://www.sciencedirect.com/science/article/abs/pii/S0964569123000182

[13]. Cazzaniga, M., Jaumotte, M. F., Li, L., Melina, M. G., Panton, A. J., Pizzinelli, C., ... & Tavares, M. M. M. (2024). Gen-AI: Artificial intelligence and the future of work. International Monetary Fund.

[14]. Prakash, R., Anoop, V. S., & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. International Journal of Information Management Data Insights, 2(2), 100112.
https://www.sciencedirect.com/science/article/pii/S2667096822000556

[15]. Macák, M., Daubner, L., Sani, M. F., & Buhnova, B. (2022). Cybersecurity analysis via process mining: A systematic literature review. In International Conference on Advanced Data Mining and Applications (pp. 393-407). Springer, Cham.
https://link.springer.com/chapter/10.1007/978-3-030-95405-5_28

[16]. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 35(2), 486-505.
https://link.springer.com/article/10.1057/s41284-021-00286-2

[17]. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.
https://link.springer.com/article/10.1007/s42979-021-00557-0

[18]. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), tyab005.

[19]. Shaukat, K., Alam, T. M., Luo, S., Shabbir, S., Hameed, I. A., Li, J., ... & Javed, U. (2021). A review of time-series anomaly detection techniques: A step to future perspectives. In Advances in information and communication: proceedings of the 2021 future of information and communication conference (FICC), volume 1 (pp. 865-877). Springer International Publishing.
https://link.springer.com/chapter/10.1007/978-3-030-73100-7_60

[20]. Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 56(11), 12407-12438.

https://link.springer.com/article/10.1007/s10462-023-10454-y
[21]. Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.
https://dl.acm.org/doi/abs/10.1145/3453158
[22]. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM computing surveys, 56(8), 1-48.
https://dl.acm.org/doi/full/10.1145/3649218
[23]. Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. Sustainability, 13(24), 13677.
https://www.mdpi.com/2071-1050/13/24/13677
[24]. Li, G., Yuan, C., Kamarthi, S., Moghaddam, M., & Jin, X. (2021). Data science skills and domain knowledge requirements in the manufacturing industry: A gap analysis. Journal of Manufacturing Systems, 60, 692-706.
https://www.sciencedirect.com/science/article/pii/S0278612521001448
[25]. Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. Sensors, 22(22), 8663.
https://www.mdpi.com/1424-8220/22/22/8663
[26]. Ukpabi, D., Karjaluoto, H., Bötticher, A., Nikiforova, A., Petrescu, D., Schindler, P., ... & Lehmann, L. (2023). Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions. Futures, 154, 103277.
https://www.sciencedirect.com/science/article/pii/S0016328723001817
[27]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. J. Sci. Technol, 11, 001-024.
https://www.researchgate.net/profile/Godslove-I-Ebiega/publication/380459159_Harnessing_adversarial_machine_learning_for_advanced_threat_detection_AI-driven_strategies_in_cybersecurity_risk_assessment_and_fraud_prevention/links/663cf58c06ea3d0b7446a401/Harnessing-adversarial-machine-learning-for-advanced-threat-detection-AI-driven-strategies-in-cybersecurity-risk-assessment-and-fraud-prevention.pdf
[28]. Itam, U. J., & Warrier, U. (2024). Future of work from everywhere: A systematic review. International Journal of Manpower, 45(1), 12-48.
https://www.emerald.com/insight/content/doi/10.1108/ijm-06-2022-0288/full/html
[29]. King, B. J., Read, G. J., & Salmon, P. M. (2023). Identifying risk controls for future advanced brain-computer interfaces: a prospective risk assessment approach using work domain analysis. Applied Ergonomics, 111, 104028.
https://www.sciencedirect.com/science/article/abs/pii/S0003687023000662
[30]. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.
https://www.sciencedirect.com/science/article/abs/pii/S0167404822001493
[31]. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), 8176-8206.
https://www.sciencedirect.com/science/article/pii/S1319157822002762
[32]. Ani, U. P. D., Watson, J. M., Green, B., Craggs, B., & Nurse, J. R. (2021). Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. Journal of Cyber Security Technology, 5(2), 71-119.
https://www.tandfonline.com/doi/abs/10.1080/23742917.2020.1843822
[33]. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616.
https://www.sciencedirect.com/science/article/abs/pii/S0275531922000046
[34]. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.
https://onlinelibrary.wiley.com/doi/abs/10.1111/rmir.12169
Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics, 1-28.
https://link.springer.com/article/10.1007/s43681-024-00427-4
[35]. Djebbar, F., & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. Ieee Access, 11, 85315-85332.
https://ieeexplore.ieee.org/abstract/document/10210561
[36]. Bhattacharya, P., Saraswat, D., Savaliya, D., Sanghavi, S., Verma, A., Sakariya, V., ... & Manea, D. L. (2023). Towards future internet: The metaverse perspective for diverse industrial applications. Mathematics, 11(4), 941.
https://www.mdpi.com/2227-7390/11/4/941

[37]. Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A structural equation approach and modelling of Pre-service teachers' perspectives of cybersecurity education. Education and Information Technologies, 29(3), 3699-3727.
https://link.springer.com/article/10.1007/s10639-023-11973-5
[38]. Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being Responsible in Cybersecurity: A Multi-Layered Perspective. Information Systems Frontiers, 1-19.
https://link.springer.com/article/10.1007/s10796-025-10588-0
[39]. Sarala, R. M., Post, C., Doh, J., & Muzio, D. (2025). Advancing Research on the Future of Work in the Age of Artificial Intelligence (AI). Journal of Management Studies.
https://onlinelibrary.wiley.com/doi/full/10.1111/joms.13195

[40]. Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11(1), 28.
https://link.springer.com/article/10.1186/s43093-025-00452-7
[41]. Amin, H. M., Hassan, R. S., Ghoneim, H., & Abdallah, A. S. (2025). A bibliometric analysis of accounting education literature in the digital era: current status, implications and agenda for future research. Journal of Financial Reporting and Accounting, 23(2), 742-768.
https://www.emerald.com/insight/content/doi/10.1108/jfra-12-2023-0802/full/html
[42]. Ajakaye, O., Olanrewaju, A. G., Fawehinmi, D., Afolabi, R., & Pius-Kiate, G. M. (2025). Integrating Artificial Intelligence in organizational cybersecurity: Enhancing consumer data protection in the US Fintech Sector. World Journal of Advanced Research and Reviews, 26(1), 2802-2821.
https://www.researchgate.net/profile/Ayobami-Olanrewaju-4/publication/391107078_Integrating_Artificial_Intelligence_in_organizational_cybersecurity_Enhancing_consumer_data_protection_in_the_US_Fintech_Sector/links/680a6031bd3f1930dd63cf49/Integrating-Artificial-Intelligence-in-organizational-cybersecurity-Enhancing-consumer-data-protection-in-the-US-Fintech-Sector.pdf
[43]. Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10929043
[44]. Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction. International Journal of Information Security, 24(1), 3.
https://link.springer.com/article/10.1007/s10207-024-00921-0
[45]. Alhumam, N., Rahman, M. H., & Aljughaiman, A. (2025). A Comprehensive Review on Cybersecurity of Digital Twins Issues, Challenges, and Future Research Directions. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10900372
[46]. Alotaibi, B. (2025). Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. Sensors, 25(2), 342.
https://www.mdpi.com/1424-8220/25/2/342
[47]. Chaudhuri, A., Sarkar, S., & Bala, P. K. (2025). Thematic exploration and analysis of cybersecurity policies of businesses: an nlp-based approach. Journal of Organizational Computing and Electronic Commerce, 35(2), 157-187.
https://www.tandfonline.com/doi/abs/10.1080/10919392.2024.2435115
[48]. Garg, A., Singh, M., & Kumar, M. (2025). The Intersection of Quantum Computing, Artificial Intelligence and Financial Risks: A Bibliometric Analysis of the Modern Financial Sector. Journal of Information Technology Management, 17(Special Issue on Strategic, Organizational, and Social Issues of Digital Transformation in Organizations), 1-21.
https://jitm.ut.ac.ir/article_53318_7227.htmlhttps://jitm.ut.ac.ir/article_100694.html
[49]. Mallik, S. K., Islam, M. R., Uddin, I., Ali, M. A., & Trisha, S. M. (2025). Leveraging artificial intelligence to mitigate money laundering risks through the detection of cyberbullying patterns in financial transactions. Global Journal of Engineering and Technology Advances, 22(01), 094-115.
https://www.researchgate.net/profile/Imran-Uddin-10/publication/388619926_Leveraging_artificial_intelligence_to_mitigate_money_laundering_risks_through_the_detection_of_cyberbullying_patterns_in_financial_transactions/links/679f97cf207c0c20fa7278d3/Leveraging-artificial-intelligence-to-mitigate-money-laundering-risks-through-the-detection-of-cyberbullying-patterns-in-financial-transactions.pdf
[50]. Ankalaki, S., Rajesh, A. A., Pallavi, M., Hukkeri, G. S., Jan, T., & Naik, G. R. (2025). Cyber attack prediction: From traditional machine learning to generative artificial intelligence. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10909100
[51]. Al Siam, A., Alazab, M., Awajan, A., & Faruqui, N. (2025). A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10836696
[52]. Alqurashi, F., & Ahmad, I. (2024). A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling. Alexandria Engineering Journal, 107, 374-389.
https://www.sciencedirect.com/science/article/pii/S1110016824007658
[53]. Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2024). Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity. Neurocomputing, 127759.
https://www.sciencedirect.com/science/article/pii/S0925231224005307
[54]. Cazzaniga, M., Jaumotte, M. F., Li, L., Melina, M. G., Panton, A. J., Pizzinelli, C., ... & Tavares, M. M. M. (2024). Gen-AI: Artificial intelligence and the future of work. International Monetary Fund.
[55]. Nassir, N. F. M., Rauf, U. F. A., Zainol, Z., & Ghani, K. A. (2024). Revealing the Multi-Perspective Factors Behind Insider Threats in Cybersecurity. Journal of Media and Information Warfare, 17, 65-82.
https://jmiw.uitm.edu.my/images/Journal/Vol17No2/Revealing.pdf
[56]. Pleshakova, E., Osipov, A., Gataullin, S., Gataullin, T., & Vasilakos, A. (2024). Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. Journal of Computer Virology and Hacking Techniques, 20(3), 429-440.
https://link.springer.com/article/10.1007/s11416-024-00529-x
[57]. Khan, O. U., Abdullah, S. M., Olajide, A. O., Sani, A. I., Faisal, S. M. W., Ogunola, A. A., & Lee, M. D. (2024). The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies. Journal of Computational Analysis and Applications, 33(8).

[58]. Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures-A systematic literature review. International Journal of Critical Infrastructure Protection, 100700.
https://www.sciencedirect.com/science/article/pii/S1874548224000416
[59]. Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Mahmud, M. A. A., Johora, F. T., & Suzer, G. (2024). AI-driven cybersecurity: Balancing advancements and safeguards. Journal of Computer Science and Technology Studies, 6(2), 76-85.
[60]. Braun, T., Pekaric, I., & Apruzzese, G. (2024, April). Understanding the Process of Data Labeling in Cybersecurity. In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (pp. 1596-1605).
https://dl.acm.org/doi/abs/10.1145/3605098.3636046
[61]. Dataset Link:
https://www.kaggle.com/datasets/atharvasoundankar/work-from-anywhere-salary-insight-2024
https://www.kaggle.com/datasets/infosecjobs/global-salaries-in-cybersecurity-infosec