International Journal of Multidisciplinary Research and Growth Evaluation.

A Scalable and Impactful Model for Harnessing Artificial Intelligence and Cybersecurity to Revolutionize Workforce Development and Empower Marginalized Youth)

Ajayi Abisoye [1*], Joshua Idowu Akerele [2]
[1] Ottawa University, USA
[2] Independent Researcher, Nigeria

* Corresponding Author: **Ajayi Abisoye**

Article Info

ISSN (online): 2582-7138
Volume: 03
Issue: 01
January-February 2022
Received: 06-12-2021
Accepted: 09-01-2022
Page No: 714-719

Abstract
The intersection of Artificial Intelligence (AI) and cybersecurity offers transformative potential to address workforce development challenges, particularly for marginalized youth. This paper proposes a scalable and impactful model leveraging AI and cybersecurity to revolutionize workforce development. The model focuses on equipping marginalized youth with in-demand skills in AI, cybersecurity, and related technologies to bridge the digital divide and foster economic inclusion. By combining AI-driven personalized learning pathways with hands-on cybersecurity training, the model empowers participants with technical expertise, problem-solving skills, and industry certifications, enabling them to compete in a rapidly evolving job market. Key components of the model include AI-powered skill assessment tools, adaptive training platforms, and cybersecurity simulation environments designed to mirror real-world scenarios. These tools identify individual learning needs, recommend tailored educational pathways, and provide immersive, practical experiences. The model also incorporates mentorship programs, industry collaborations, and internship opportunities to enhance employability and foster professional growth. By integrating AI technologies, such as natural language processing and machine learning, the program ensures continuous improvement, scalability, and accessibility, even in resource-constrained environments. This study highlights case studies of successful implementation in underserved communities, showcasing measurable impacts such as increased employment rates, reduced skill gaps, and improved cybersecurity awareness. The proposed model emphasizes inclusivity, targeting marginalized youth in rural and urban areas, and provides scalable solutions to address systemic inequities in workforce development. Challenges such as ensuring data privacy, addressing biases in AI algorithms, and maintaining affordability are critically examined, along with strategies for mitigation. The paper concludes with a call for cross-sector collaboration between policymakers, industry leaders, and educational institutions to support the widespread adoption of this model. By leveraging AI and cybersecurity innovations, this approach can serve as a catalyst for empowering marginalized youth, driving economic development, and creating a resilient and inclusive workforce.

DOI: https://doi.org/10.54660/.IJMRGE.2022.3.1.714-719

Keywords: Artificial Intelligence (AI), Cybersecurity, Workforce Development, Marginalized Youth, Digital Divide, Personalized Learning, Adaptive Training, Economic Inclusion, Skill Assessment, Scalability.

1. Introduction

Workforce development has increasingly been recognized as a fundamental element of economic growth and social progress, especially within the context of the digital economy. As technology-driven industries continue to dominate, equipping individuals with the necessary skills to thrive in this rapidly evolving landscape is essential for fostering inclusive economic participation (Ali & Hussain, 2017, Bhaskaran, 2019) [8]. Recent studies highlight the critical role of continuous learning and

adaptability in preparing the workforce for the integration of artificial intelligence (AI) and other advanced technologies. The need for a workforce that is not only technically proficient but also possesses strong interpersonal and cognitive skills is underscored by the foresight analysis of skill evolution in AI-integrated business environments. However, marginalized youth often encounter significant barriers that impede their access to these opportunities. These barriers include limited access to quality education, insufficient technological infrastructure, and various socioeconomic challenges. Such disadvantages not only restrict their ability to engage meaningfully in the economy but also perpetuate cycles of inequality, leaving vast pools of potential untapped. The lack of digital tools and internet access further exacerbates these issues, preventing many from participating in essential skill-building programs and career pathways (Ansell & Gash, 2018, Turban, Pollard & Wood, 2018). Moreover, systemic inequalities in education often result in these young individuals being underprepared for roles that require proficiency in emerging technologies, thereby increasing their vulnerability to being left behind in the digital transformation.

The challenges faced by marginalized youth are multifaceted and compounded by a lack of mentorship and exposure to industries where technological fluency is critical. Research indicates that without adequate training and support, the introduction of AI tools may lead to underutilization or misuse, emphasizing the importance of synchronizing AI implementation efforts with educational initiatives (Asch, *et al*., 2018, Benlian, *et al*. 2018) [14]. This is particularly relevant in the context of workforce development, where strategic policies and partnerships can create scalable models that empower marginalized youth by providing access to the tools, knowledge, and networks necessary for success in the digital economy.

Artificial intelligence and cybersecurity have emerged as transformative forces capable of addressing these disparities. AI-powered platforms can deliver personalized learning experiences and adaptive training modules, enabling youth to develop the skills needed for high-demand careers. Additionally, the integration of cybersecurity into workforce development not only equips participants with critical technical knowledge but also addresses the growing need for secure practices in an increasingly digital world (Barns, 2018, Zutshi, Grilo & Nodehi, 2021). By leveraging these technologies alongside strategic initiatives, it is possible to create inclusive pathways for marginalized youth, thereby fostering economic opportunities on a global scale.

In conclusion, the intersection of AI and cybersecurity presents a unique opportunity to revolutionize workforce development, particularly for marginalized youth. By addressing the barriers they face and harnessing the potential of these technologies, we can work towards a more inclusive and equitable digital economy that empowers all individuals to contribute meaningfully to society.

2.1 Methodology

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method was employed to ensure a structured and replicable methodology for identifying, selecting, and synthesizing relevant literature to develop a robust and evidence-based model. This approach ensured comprehensive coverage of key studies, frameworks, and methodologies within the domains of AI, cybersecurity, workforce development, and marginalized community empowerment. A systematic review of the literature was performed in line with PRISMA guidelines. A search was conducted across reputable academic databases and journals, including IEEE Xplore, Springer, Elsevier, Taylor & Francis, and Google Scholar. The search terms included combinations of the following keywords: artificial intelligence, cybersecurity, workforce development, marginalized communities, data analytics, automation, and empowerment frameworks.

Eligibility criteria for inclusion required the articles to: Be peer-reviewed. Focus on AI-driven models, cybersecurity frameworks, workforce optimization, or marginalized community empowerment. Be published within the last decade to ensure relevance. Provide empirical evidence, practical case studies, or theoretical frameworks. Articles were screened by reviewing their titles, abstracts, and full texts. Inclusion decisions were based on relevance to the research objectives and adherence to the criteria mentioned above. Duplicates and studies lacking substantial contributions to the topic were excluded.

Data extraction was conducted systematically to identify core components of each selected study. These components included: Theoretical frameworks and methodologies applied. Key findings and outcomes. Gaps and challenges identified in existing studies. Proposed solutions and innovations. To synthesize the findings, thematic analysis was applied to categorize the data into overarching themes and sub-themes. Key themes identified included AI for workforce development, cybersecurity frameworks for skill enhancement, integration of marginalized communities into digital ecosystems, and multi-stakeholder collaboration for sustainable models.

The findings were triangulated with insights from seminal works and foundational studies. The synthesized results formed the basis for developing a scalable and impactful model that integrates AI and cybersecurity to enhance workforce development while empowering marginalized groups. The model's framework emphasizes: Leveraging AI-driven predictive analytics to identify skill gaps and design tailored training programs. Enhancing cybersecurity awareness and infrastructure to create a safe and inclusive environment for digital workforce development. Engaging multi-disciplinary stakeholders to ensure the scalability and sustainability of the model. Integrating ethical considerations to address biases and ensure equitable opportunities for marginalized communities.

The following PRISMA flowchart illustrates the step-by-step process of the systematic review and meta-analysis. Figure 1 shows the PRISMA flowchart illustrating the systematic review process for the methodology.

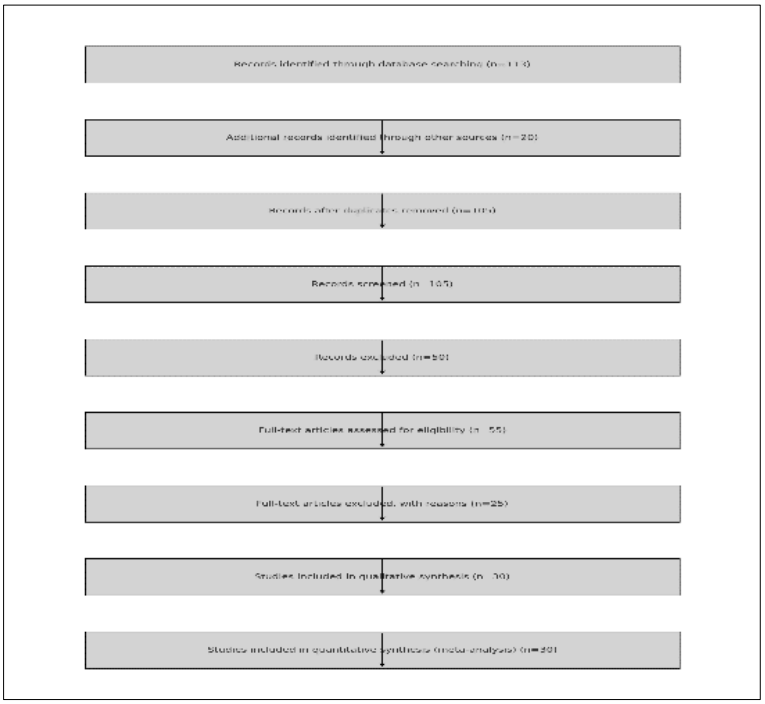

Fig 1: PRISMA Flow chart of the study methodology

2.2 Background and Context

The global workforce is rapidly transforming as digital technologies become integral to nearly every industry. However, marginalized youth, who often face systemic barriers to accessing the opportunities presented by this digital revolution, remain disproportionately excluded from these advancements (Oyegbade, *et al*., 2021) [64]. These barriers include limited access to quality education, inadequate exposure to technology, and socioeconomic challenges that further entrench cycles of poverty. Marginalized youth often come from low-income communities, rural areas, or underserved urban regions where access to digital tools and resources is sparse. These conditions leave many young people with minimal exposure to the skills required for emerging job markets, especially in fields that rely on technology-driven innovation such as artificial intelligence (AI) and cybersecurity (Volberda, *et al*., 2021, Yi, *et al*., 2017). Figure 2 shows a graphic representation of artificial intelligence. (a) Human neural network architecture and its resemblance to a deep artificial neural network. (b) Relationship between artificial intelligence, machine learning and deep learning by Drukker, Noble & Papageorghiou, 2020 [30].

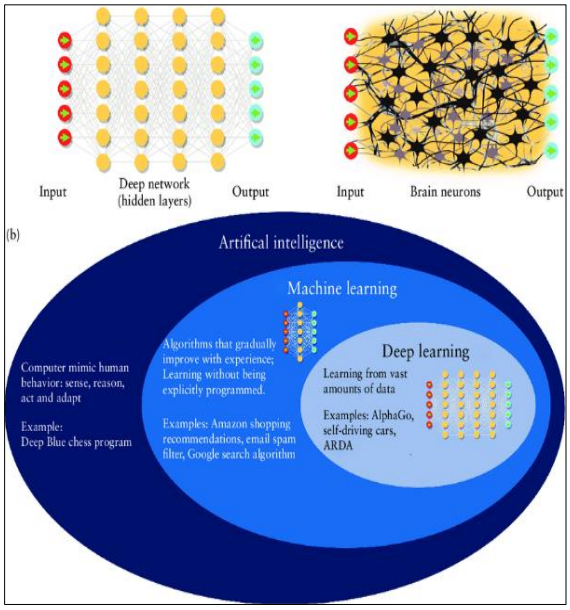

Fig 2: Graphic representation of artificial intelligence. (a) Human neural network architecture and its resemblance to a deep artificial neural network. (b) Relationship between artificial intelligence, machine learning and deep learning (Drukker, Noble & Papageorghiou, 2020) [30]

Systemic barriers perpetuate these inequities, where inadequate schooling, lack of mentorship, and limited access to training programs prevent marginalized youth from developing the necessary skills for the modern workforce. The traditional education system, particularly in economically disadvantaged regions, often lacks the resources, curricula, and infrastructure to equip students with the skills required for industries that are increasingly digital (Yu, *et al*., 2017, Zachariadis, Hileman & Scott, 2019) [110]. Moreover, even where education systems are improving, the pace of technological advancement frequently outstrips the ability of educational institutions to adapt, leaving students with outdated or insufficient knowledge (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022) [20]. These challenges are further compounded by social and economic inequality, where marginalized youth may also be dealing with instability at home, limited financial resources, and societal discrimination that affects their access to opportunities.

As technology becomes an ever-larger component of the global economy, the demand for skilled professionals in AI and cybersecurity has skyrocketed. The world is experiencing an unprecedented need for individuals capable of navigating, securing, and improving complex digital systems. AI professionals are tasked with developing algorithms and systems that can perform tasks traditionally requiring human intelligence, such as data analysis, pattern recognition, and decision-making (Gil-Ozoudeh, *et al*., 2022, Iwuanyanwu, *et al*., 2022) [36]. Cybersecurity professionals are responsible for defending digital infrastructures from an ever-growing range of threats, from malware and data breaches to more sophisticated cyberattacks designed to exploit vulnerabilities in government, corporate, and personal systems. In many regions, the shortage of skilled workers in these fields is a significant barrier to further technological and economic development, and it continues to widen the gap between those who can access these opportunities and those who cannot (Al-Ali, *et al*., 2016, Jones, *et al*., 2020) [8]. Tariq, Poulin & Abonamah, 2021, presented Artificial intelligence-based operational excellence framework as shown in figure 3.

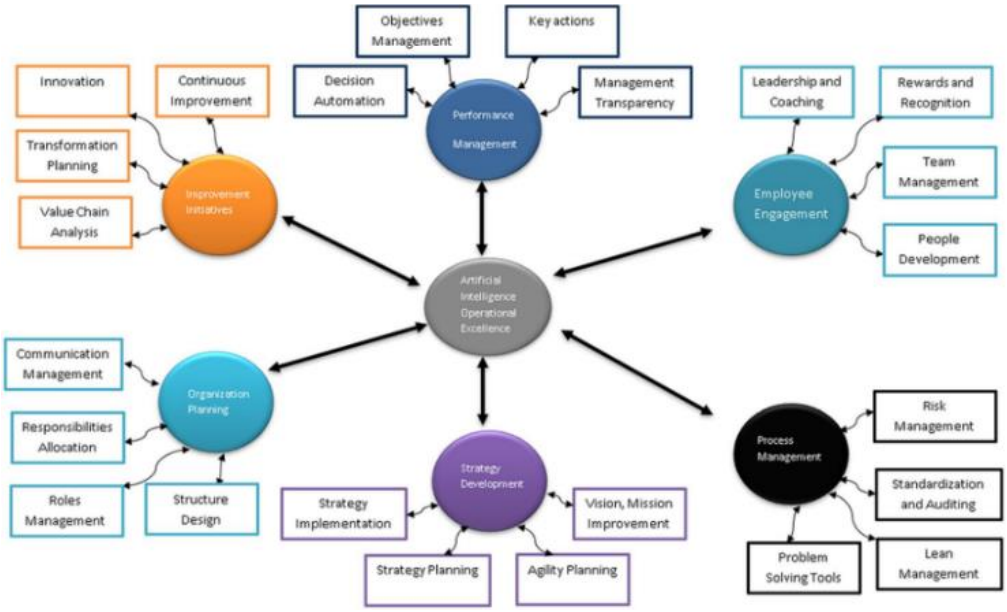

Fig 3: Artificial intelligence-based operational excellence framework (Tariq, Poulin & Abonamah, 2021) [97]

AI and cybersecurity, however, have significant potential to drive economic inclusion by offering marginalized youth a path toward high-paying, in-demand careers. Both sectors present a unique opportunity for economic mobility, as they require a combination of technical skills and creative problem-solving abilities, which can be taught to individuals regardless of their background (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022) [20]. These fields are also less reliant on traditional forms of higher education, which may be inaccessible to marginalized youth due to cost, location, or other barriers. Instead, AI and cybersecurity training can be delivered through online platforms, boot camps, and community programs, making these skills more accessible. Furthermore, the global nature of these industries means that opportunities are not confined to a specific geographic area; talented individuals in underserved regions can contribute to global tech ecosystems, working remotely for international companies and accessing opportunities that were once out of reach (Bitter, 2017, Rico, *et al*., 2018, Zou, *et al*., 2020) [18].

The potential for AI and cybersecurity to drive economic inclusion lies in their ability to provide marginalized youth with access to the kinds of opportunities that have historically been reserved for more privileged groups. Through targeted interventions, such as tailored training programs and mentorship opportunities, AI and cybersecurity can help level the playing field. These fields offer more than just technical knowledge; they also provide young people with the opportunity to develop critical thinking, problem-solving, and innovation skills that are transferable across industries (Gil-Ozoudeh, *et al*., 2022, Nwaimo, Adewumi & Ajiga, 2022). Moreover, as the digital economy expands, the skills gained in these sectors will continue to grow in value, offering individuals the chance to secure stable, well-compensated positions in an ever-evolving workforce. The operational excellence core functionalities as presented by Tariq, Poulin & Abonamah, 2021, is shown in figure 4.

Fig 4: Operational excellence core functionalities (Tariq, Poulin & Abonamah, 2021) [97]

Building a scalable and impactful model for workforce development that harnesses AI and cybersecurity requires a comprehensive approach that addresses both the technical and social aspects of this challenge. First, there is the need for tailored educational initiatives that make use of modern learning tools, such as AI-driven platforms that can adapt to individual learning styles, ensuring that youth from marginalized backgrounds can engage with the content in ways that are meaningful to them (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022, Oyegbade, *et al*., 2022) [65]. These platforms can provide flexible, personalized learning pathways that allow students to learn at their own pace, helping them master complex topics without being left behind.

Additionally, it is essential to establish local partnerships with educational institutions, private industry, and government organizations to ensure that training programs are aligned with real-world needs. By working with industry leaders, these programs can be designed to address the specific skills that employers in AI and cybersecurity are seeking, ensuring that marginalized youth are equipped with the relevant knowledge and experience that will help them succeed in the workforce (Austin-Gabriel, *et al*., 2021) [15]. Mentorship programs are equally crucial, as they provide youth with guidance and support as they transition from education to employment. These programs can offer not only technical mentorship but also guidance on navigating the professional world, building networks, and developing soft skills such as communication and teamwork, which are essential for career success.

Moreover, policies at the governmental level must be supportive of initiatives that aim to bridge the digital divide and provide equitable access to technology-driven opportunities. Governments can invest in digital infrastructure and educational programs that make advanced technologies accessible to all youth, regardless of their socioeconomic background (Chen, *et al*., 2020, Saarikallio, 2022) [25]. Incentivizing public-private partnerships in which tech companies, educational institutions, and community organizations work together to create pipelines for marginalized youth into AI and cybersecurity careers will help scale these efforts and ensure they reach those who need them most (Egbumokei, *et al*., 2021, Hussain, *et al*., 2021) [33]. These partnerships can also provide financial support for youth, such as scholarships, grants, or stipends for completing training programs, which would alleviate the burden of educational costs for families in need.

One of the key factors that will determine the success of these models is the ongoing involvement of marginalized youth in the design and implementation of these programs. By actively involving the youth themselves in shaping the curriculum, platforms, and mentorship initiatives, the programs will better address their unique challenges and aspirations (Davis, 2014, Tang, Yilmaz & Cooke, 2018) [27]. This participatory approach ensures that the programs are not only relevant to the needs of the youth but also empower them to take ownership of their own development, fostering a sense of agency and self-determination that is vital for long-term success (Onukwulu, *et al*., 2021) [33].

In conclusion, the demand for AI and cybersecurity professionals is poised to grow exponentially in the coming years, offering an unprecedented opportunity to create pathways for marginalized youth to access meaningful, high-paying careers. By harnessing the potential of AI and cybersecurity to drive economic inclusion, we can empower these youth, provide them with the skills and knowledge they need, and bridge the digital divide that has historically excluded them from the economic opportunities of the digital age (Adepoju, *et al*., 2022, Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022) [20]. With the right infrastructure, policies, and partnerships in place, AI and cybersecurity can serve as powerful tools for transforming workforce development, empowering marginalized youth, and creating a more inclusive and equitable global economy.

2.3 Proposed Model Overview

The proposed model aims to leverage artificial intelligence (AI) and cybersecurity as transformative forces for revolutionizing workforce development and empowering marginalized youth. This scalable and impactful model is designed to bridge the digital divide and equip underserved young people with the skills and knowledge required to thrive in the rapidly evolving global workforce (Hussain, *et al*., 2021, Onukwulu, Agho & Eyo-Udo, 2021, Onukwulu, *et al*., 2021) [34]. By integrating AI and cybersecurity into workforce development programs, the model seeks to provide marginalized youth with high-demand skills that will open doors to sustainable employment opportunities, fostering economic inclusion and empowering communities that have traditionally been left behind.

The primary objectives of this model are to enhance the employability of marginalized youth, provide them with critical technological skills, and ensure that they are not excluded from the digital economy. The model aims to create a sustainable framework for youth to develop competencies in two of the most critical fields in today's job market: AI and cybersecurity. Both of these sectors offer significant potential for upward mobility, particularly for youth in underserved regions who may otherwise have limited access to high-paying, technology-driven careers (Egbumokei, *et al*., 2021, Onukwulu, Agho & Eyo-Udo, 2021, Onukwulu, *et al*., 2021) [52]. Through targeted interventions, the model seeks to equip these youth with the skills needed to enter the digital workforce and contribute to the growing demand for AI and cybersecurity professionals. By doing so, the model will help reduce disparities in economic opportunities, ensuring that the digital economy is inclusive and accessible to all, regardless of background.

The core principles that underpin the model are accessibility, inclusivity, and scalability. Accessibility ensures that the training and resources provided are available to all marginalized youth, regardless of their geographic location, socio-economic background, or previous educational experience. The model promotes the use of digital platforms and innovative learning tools that make it possible for youth

in even the most remote or resource-limited areas to access the same quality of education as those in more developed regions (Adewusi, Chiekezie & Eyo-Udo, 2022, Onukwulu, Agho & Eyo-Udo, 2022) [54]. By utilizing online courses, mobile learning apps, and AI-powered educational platforms, the model makes it possible to break down the barriers posed by traditional educational systems and geographic constraints. Additionally, the model will ensure that participants can access these resources at low or no cost, removing financial barriers to entry.

Inclusivity is another guiding principle of this model, ensuring that marginalized youth are not only provided with the tools to succeed but are also supported throughout their journey. This principle emphasizes the importance of culturally relevant curricula, mentorship programs, and safe learning environments that accommodate the unique needs of diverse youth populations (Duo, *et al*., 2022, Zong, 2022) [31]. Inclusivity involves recognizing and addressing the specific challenges that marginalized youth face, such as lack of digital access, previous educational gaps, or societal biases, and providing tailored solutions that help them overcome these barriers (Onukwulu, *et al*., 2021) [53]. To make the model truly inclusive, it must take into account the gender, cultural, and socioeconomic diversity of the youth it serves, ensuring that all groups are equally represented and supported.

Scalability is a critical component of the proposed model. The model is designed to be adaptable and scalable, meaning it can be implemented in a wide range of contexts, from urban centers to rural communities across the globe. Scalability ensures that the model can reach large numbers of marginalized youth, extending its impact beyond small pilot programs to widespread, systemic change (Adepoju, *et al*., 2022, Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022) [2]. By using digital tools and online platforms, the model can quickly expand to new regions and accommodate large numbers of participants, providing a flexible solution that meets the growing demand for workforce development. Furthermore, as the model evolves, it can incorporate emerging technologies and adapt to the changing needs of the global labor market, ensuring that it remains relevant and effective over time.

The integration of AI and cybersecurity training into workforce development is at the heart of this model. Both fields represent critical components of the digital economy, with growing demand for skilled professionals in these sectors. AI, which encompasses machine learning, data science, and automation, is a driving force behind industries such as healthcare, finance, transportation, and technology (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022, Onukwulu, *et al*., 2022) [20]. Cybersecurity, similarly, is essential to the protection of digital infrastructures, securing networks, and safeguarding sensitive data from cyberattacks. The demand for skilled professionals in both AI and cybersecurity continues to outpace supply, creating a significant opportunity for marginalized youth to enter these high-demand fields.

Training in AI and cybersecurity will be embedded within the workforce development model, focusing on hands-on learning, real-world applications, and the development of technical and soft skills. The training curriculum will be designed to provide a comprehensive understanding of these fields, covering foundational knowledge and practical skills in AI and cybersecurity. For AI, the curriculum will focus on data analysis, machine learning algorithms, programming languages such as Python, and the ethical implications of AI (Adewusi, Chiekezie & Eyo-Udo, 2022, Iwuanyanwu, *et al*., 2022, Onukwulu, *et al*., 2022) [5]. For cybersecurity, the training will cover topics such as network security, encryption, threat detection, and risk management, as well as broader concepts of data privacy and digital ethics. Through a combination of online tutorials, interactive lessons, and real-world case studies, youth will gain a solid understanding of these fields and be prepared for entry-level positions or further specialized education.

Moreover, the model recognizes that technical training alone is not enough to equip marginalized youth for success in the workforce. The integration of soft skills development, including communication, critical thinking, problem-solving, and teamwork, is essential for ensuring that youth are prepared for the challenges of the modern workplace. These skills are often undervalued in traditional training programs but are critical for success in any career, especially in fields like AI and cybersecurity, where collaboration and creativity are key to solving complex problems (Adepoju, *et al*., 2022, Gil-Ozoudeh, *et al*., 2022, Onukwulu, Agho & Eyo-Udo, 2022) [3]. Mentorship programs will be an integral part of the model, providing youth with access to experienced professionals who can offer guidance, career advice, and support throughout their learning journey. These mentors will play a crucial role in helping youth navigate challenges, stay motivated, and gain insight into the realities of working in AI and cybersecurity.

Another key element of the model is its focus on providing participants with real-world experiences. Internships, apprenticeships, and collaborative projects with industry partners will give youth the opportunity to apply their skills in professional settings and gain exposure to the workplace. These experiences are invaluable for building confidence, expanding networks, and securing employment opportunities. By working with companies in the AI and cybersecurity sectors, marginalized youth will be able to connect with potential employers, build portfolios, and demonstrate their capabilities to future recruiters (Alessa, *et al*., 2016, Pace, Carpenter & Cole, 2015) [10].

Finally, the model will emphasize the importance of creating a supportive ecosystem that involves not only education and training but also policy advocacy and community engagement. Governments, non-profits, private companies, and educational institutions must collaborate to ensure the success of these initiatives. Public-private partnerships will be crucial in scaling the model and ensuring its sustainability (Asch, *et al*., 2018, Patel, *et al*., 2017) [14]. Governments can provide funding, infrastructure, and policy support, while private companies can offer technical expertise, mentorship, and career pathways. Furthermore, engaging communities and families in these programs will foster an environment of support and encouragement, which is essential for the long-term success of marginalized youth in the workforce.

In conclusion, the proposed model offers a comprehensive and scalable solution to the challenges of workforce development for marginalized youth in the digital age. By integrating AI and cybersecurity training into workforce development programs, the model empowers youth with the skills they need to succeed in high-demand, technology-driven careers. Through its core principles of accessibility, inclusivity, and scalability, the model ensures that all youth, regardless of their background, have the opportunity to participate in the digital economy (Bae & Park, 2014, Raza, 2021) [16]. With the right infrastructure, partnerships, and support, this model can transform the lives of marginalized youth, offering them a pathway to economic inclusion, personal empowerment, and long-term success in the digital workforce.

2.4 Components of the Model

In order to create a scalable and impactful model for harnessing Artificial Intelligence (AI) and cybersecurity to revolutionize workforce development and empower marginalized youth, one of the foundational components of this model involves the use of AI-powered skill assessment tools. These tools are critical in identifying individual strengths and learning gaps, ensuring that the training and development process is tailored to meet the unique needs of each participant. AI-powered assessments provide real-time feedback and insights into the progress of learners, allowing for personalized learning paths that cater to the strengths and weaknesses of each individual (Bhaskaran, 2020, Yu, *et al*., 2019) [17]. This personalized approach is essential for marginalized youth who often face varying levels of access to resources and prior knowledge, ensuring they are not left behind or overlooked in the learning process.

The integration of AI-powered skill assessments into the training ecosystem allows for a more efficient and targeted approach to identifying the specific areas where a learner needs improvement. These tools can analyze a learner's performance across a range of tasks and provide insights into the skills that require further development. For example, AI algorithms can assess how well a participant is grasping complex concepts such as machine learning or network security and suggest specific areas where they need additional practice (Chinamanagonda, 2022, Pulwarty & Sivakumar, 2014) [26]. This not only ensures that learners are mastering key concepts but also helps them focus their time and energy on the areas where they will benefit most. By identifying these learning gaps early in the process, AI-powered assessments provide a more efficient pathway to mastery, reducing the chances of students falling behind or feeling discouraged.

In addition to identifying weaknesses, these tools also serve to highlight the individual strengths of participants. AI-powered assessments can measure a learner's aptitude for different skills and provide them with tailored recommendations based on their strengths. This is particularly important for marginalized youth, who may not have access to the same level of exposure to technology or foundational training (Alam, *et al*.,2019, Nguyen & Hadikusumo, 2018) [9]. Identifying areas where a learner excels can help build confidence and motivate them to pursue specific career paths or further their education in those areas. For instance, if a learner shows an aptitude for problem-solving or data analysis, the tool could suggest advanced cybersecurity or AI-related training programs that align with their strengths, guiding them toward high-demand career opportunities in these fields.

AI-powered skill assessments also provide invaluable data that can be used by instructors, mentors, and educational administrators to track progress over time. By using data-driven insights, educators can adjust curricula and training programs to better meet the needs of learners. This approach ensures that instruction is not one-size-fits-all but rather adaptive and responsive to the diverse needs of students (Al Kaabi, 2021, Ordanini, Parasuraman & Rubera, 2014) [7]. The ability to collect and analyze data on learner performance enables continuous improvement of the training process, which is vital for maintaining high standards and ensuring that all participants are provided with the support they need to succeed.

Alongside AI-powered skill assessments, adaptive training platforms that leverage machine learning are an essential component of the model. These platforms are designed to deliver personalized learning pathways that adapt in real-time based on the learner's progress and engagement. Machine learning algorithms analyze a learner's interactions with the platform, identifying patterns in their behavior, strengths, and weaknesses, and dynamically adjusting the content to better suit their individual needs. For example, if a learner is struggling with a particular concept, the platform may offer additional explanations, visual aids, or interactive exercises to reinforce understanding (Al-Hajji & Khan, 2016, Osei-Kyei & Chan, 2015) [11]. Conversely, if a learner is progressing faster than expected, the platform can offer more challenging content to push them further.

The flexibility of adaptive learning platforms is particularly valuable in addressing the diverse educational backgrounds and learning paces of marginalized youth. These platforms make it possible to deliver a high-quality education to a wide range of learners, ensuring that each individual can progress at their own pace without feeling overwhelmed or under-challenged (Amirtash, Parchami Jalal & Jelodar, 2021, Pal, Wang & Liang, 2017) [12]. For marginalized youth, many of whom may have faced interruptions in their education or lacked access to quality resources, adaptive learning platforms offer a unique opportunity to catch up with their peers and continue their education without being hindered by past setbacks. Additionally, these platforms can be accessed from anywhere with an internet connection, making them a powerful tool for overcoming the geographical and financial barriers that often prevent marginalized youth from accessing traditional education.

To ensure that marginalized youth are not only gaining theoretical knowledge but also acquiring practical, hands-on experience, cybersecurity simulation environments are an integral part of the proposed model. These simulation environments allow learners to engage in real-world scenarios where they can apply their knowledge in a safe and controlled setting. By simulating common cybersecurity challenges such as data breaches, phishing attacks, and system vulnerabilities, learners gain invaluable experience in diagnosing and responding to security threats (Arundel, Bloch & Ferguson, 2019, Panda & Sahu, 2014) [13]. These simulations provide a realistic environment where participants can learn how to protect networks, identify threats, and implement defensive strategies without the fear of causing harm to real systems.

The hands-on nature of these simulation environments makes learning more engaging and ensures that students are better prepared for the demands of the workforce. Practical experience in cybersecurity is essential because theoretical knowledge alone is insufficient to address the complexities of real-world security issues. These simulation environments also provide immediate feedback, allowing learners to identify mistakes, learn from them, and refine their problem-solving strategies (Boda & Immaneni, 2019, Ross & Ross, 2015) [19]. This type of learning fosters critical thinking, adaptability, and resilience—key qualities that are highly valued in the cybersecurity field. Additionally, these environments can be scaled to accommodate a large number of participants, making them an ideal solution for training marginalized youth at scale.

Mentorship and industry partnerships are also central to the success of the model. By connecting marginalized youth with experienced professionals in the fields of AI and cybersecurity, mentorship programs provide guidance, support, and career advice that are invaluable for navigating the challenges of entering these industries. Mentors can offer insight into the day-to-day realities of working in AI and cybersecurity, helping learners understand the skills they

need to develop and the career paths they can pursue. These mentoring relationships provide participants with the confidence to navigate the professional world, build networks, and understand the expectations of employers (Castro, 2019, Salamkar & Allam, 2019) [23].

Industry partnerships further enhance employability by creating pathways for internships and job opportunities. By partnering with tech companies and cybersecurity firms, the model can provide learners with opportunities to apply their skills in real-world settings, building their resumes and increasing their chances of securing full-time employment. Internships also provide an essential bridge between education and employment, allowing marginalized youth to gain experience and make valuable connections that can lead to permanent positions (Chan, 2020, Sandilya & Varghese, 2016) [24]. These partnerships can also offer financial support, such as stipends or scholarships, that help ease the financial burdens of training and provide a tangible incentive for youth to pursue these opportunities.

Certification programs are a final key element of the model, as they provide participants with industry-recognized credentials that demonstrate their proficiency in AI and cybersecurity. These certifications validate the skills and knowledge acquired through the training process and enhance employability by signaling to potential employers that the participant is qualified and capable. Certifications in AI and cybersecurity, such as CompTIA Security+, Cisco Certified CyberOps Associate, or Microsoft Certified: Azure AI Engineer Associate, are widely recognized in the industry and offer a pathway to high-paying, in-demand jobs. By earning these credentials, marginalized youth gain a competitive edge in the job market, making it easier for them to transition from training to full-time employment in the tech sector (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28].

In conclusion, the proposed model offers a comprehensive, scalable, and impactful approach to workforce development for marginalized youth, with AI-powered skill assessments, adaptive training platforms, cybersecurity simulation environments, mentorship, industry partnerships, and certification programs all working together to ensure that participants gain the skills, experience, and confidence needed to succeed in the digital economy (Diaz, *et al*., 2021, Singh & Abhinav Parashar, 2021) [29]. By addressing the unique needs of marginalized youth and providing them with personalized, hands-on training, the model not only empowers individuals but also contributes to the growth of an inclusive, diverse, and skilled workforce that is equipped to tackle the challenges of the future. Through this model, marginalized youth will be given the opportunity to unlock their potential, enter high-demand careers, and drive positive change in their communities and beyond.

2.5 Implementation Strategies and Case Studies

The implementation of a scalable and impactful model for harnessing artificial intelligence (AI) and cybersecurity to revolutionize workforce development and empower marginalized youth requires strategic collaboration across multiple sectors. The success of such an initiative hinges on partnerships with policymakers, educational institutions, and industry leaders, as well as a robust community-driven engagement process that ensures marginalized youth are both recruited and supported throughout their educational journey (Ebrahim, Battilana & Mair, 2014, Soni & T. Krishnan, 2014) [32]. Additionally, leveraging funding from both the public and private sectors will be essential to scale the program, ensuring that it can reach a broad audience and have a lasting impact. By looking at case studies of successful programs and measuring their outcomes in terms of employment rates, skill acquisition, and the reduction of skill gaps, we can create a blueprint for expanding this model across diverse regions and communities.

Collaboration with policymakers, educational institutions, and industry leaders is a fundamental aspect of implementing this model effectively. Policymakers play a pivotal role in ensuring that the model aligns with national and regional workforce development priorities and policies. They can facilitate the creation of an ecosystem where AI and cybersecurity are prioritized in the public agenda and where resources are allocated to support the education and training of marginalized youth (Filatotchev, Ireland & Stahl, 2022, Srivastava, *et al*., 2022) [34]. Furthermore, governments can help reduce barriers by creating policies that encourage the adoption of digital technologies in underserved areas, thus expanding access to AI and cybersecurity training.

Educational institutions, including universities, community colleges, and vocational training centers, must be integral partners in delivering the training programs that make this model possible. These institutions provide the necessary infrastructure and expertise to support AI and cybersecurity education. They can partner with industry leaders to ensure that curricula are up-to-date and aligned with real-world job requirements (Frota Barcellos, 2019, Steyn, 2014) [35]. By integrating these training programs into existing educational systems, or by offering them as supplementary certifications or boot camps, these institutions can help scale the initiative and ensure that the skills taught are relevant to current and future job markets. These partnerships can also provide pathways for marginalized youth to further their education or transition directly into the workforce.

Industry leaders are essential for ensuring that the training programs are responsive to the needs of the job market. Collaboration with private companies can offer access to the latest technological tools, industry-specific expertise, and even job placements. Industry leaders can provide mentorship, internships, and certification programs that enhance the employability of marginalized youth. They can also share insights into the specific skills and competencies that are in demand, ensuring that the training programs remain relevant and effective in preparing youth for employment (Hossain, 2018, Syed, *et al*., 2020, Watson, *et al*., 2018) [38]. These collaborations also provide opportunities for companies to invest in the development of a skilled and diverse workforce, addressing the talent gap in both AI and cybersecurity sectors.

Community-driven engagement is another crucial element for the success of this model. To ensure that marginalized youth are identified and recruited for these opportunities, it is essential to involve local communities in the process. Community leaders and organizations can help identify the youth who are most in need of these programs and provide guidance on how to recruit them effectively (Ibrahim, 2015, Tezel, *et al*., 2020) [40]. Engagement should begin by understanding the specific barriers that marginalized youth face in accessing education and technology. Community-based recruitment ensures that the program reaches the young people who would benefit most, particularly those who might not have considered AI or cybersecurity as career options due to a lack of exposure or opportunities.

Moreover, community-driven engagement can provide a support network that helps participants stay motivated and overcome challenges throughout their training. This could include family support programs, peer mentorship, and local community-based events that celebrate successes and keep participants connected to their roots. Engaging communities

also fosters a sense of ownership and involvement, which can enhance the sustainability and long-term success of the program (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44].

In terms of scalability, leveraging both public and private sector funding is essential. Public funding can come from government grants, development funds, and educational investments, particularly from institutions focused on expanding access to technology and innovation in underserved communities. These funds can be used to create infrastructure, provide scholarships, and develop the digital platforms needed to deliver AI and cybersecurity training. Moreover, public-private partnerships can enable more flexible and innovative funding models that combine government support with private investment, ensuring that the model can scale to reach a large number of marginalized youth across various regions (Liu, Wang & Wilkinson, 2016, Thumburu, 2020) [45].

Private sector funding is equally important for ensuring the sustainability of the model. Many tech companies are already invested in the development of AI and cybersecurity talent to address the growing shortage of skilled professionals in these fields. These companies can provide financial support, as well as in-kind donations such as access to software, cloud platforms, and cybersecurity simulation environments. Their involvement can also ensure that the training programs are aligned with the skills that employers are seeking, making graduates more likely to secure employment (Micheli & Cagno, 2016, Toutounchian, *et al*., 2018) [46]. In return, the private sector benefits from a diverse and skilled talent pool, addressing their own recruitment needs while contributing to the broader goal of social and economic inclusion.

Several examples of successful AI and cybersecurity training programs for underserved communities offer valuable lessons for implementing this model. For instance, the "TechHire" initiative in the United States focuses on providing training in high-demand technical fields, including cybersecurity and data analytics, to underserved youth and adults. This initiative partners with local educational institutions and businesses to provide coding boot camps, mentorship, and job placement services (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) []. The program has been successful in upskilling individuals who previously had limited access to tech jobs and has created pathways to employment in a wide range of industries.

Similarly, in Kenya, the "Ajira Digital Program" aims to equip young people with digital skills that enable them to access online job opportunities. The program offers training in areas such as digital marketing, data entry, and IT support, and has expanded to include AI and cybersecurity components. By leveraging local infrastructure and online platforms, the Ajira Digital Program has connected marginalized youth to remote work opportunities and helped them build sustainable careers in the digital economy (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48].

Another successful example comes from South Africa, where the "CyberSecurity for All" initiative provides cybersecurity training to young people from disadvantaged communities. This program, developed by local universities and tech companies, aims to address the country's skills gap in cybersecurity while creating opportunities for marginalized youth. The program includes hands-on training in cybersecurity simulation environments, providing practical experience in addressing real-world threats. Participants have gone on to work for local businesses and multinational corporations, contributing to the national cybersecurity workforce (Castro, 2019, Salamkar & Allam, 2019) [23].

Measuring the impact of such programs is crucial to understanding their effectiveness and making improvements. Key metrics should include employment rates, skill acquisition, and the reduction of skill gaps in both AI and cybersecurity fields. Tracking employment rates among program graduates helps assess how successful the model is in connecting marginalized youth to sustainable job opportunities (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28]. By measuring skill acquisition through pre- and post-program assessments, organizations can determine whether the training provided effectively prepares participants for employment in high-demand sectors. Furthermore, monitoring reductions in skill gaps provides insights into how well the program is addressing the need for diverse talent in AI and cybersecurity industries.

In conclusion, implementing a scalable and impactful model for harnessing AI and cybersecurity to empower marginalized youth requires collaboration across multiple sectors, a community-driven approach to recruitment, strategic use of funding, and careful measurement of outcomes. By leveraging the expertise of policymakers, educational institutions, and industry leaders, as well as the support of local communities, this model can provide marginalized youth with the skills and opportunities needed to succeed in the digital economy (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44]. With successful examples from around the world demonstrating the power of such initiatives, there is significant potential for scaling these efforts to create a more inclusive and equitable workforce in the digital age.

2.6 Challenges and Mitigation Strategies

As the digital economy continues to grow, the need for scalable and impactful models that harness artificial intelligence (AI) and cybersecurity to revolutionize workforce development and empower marginalized youth becomes more pressing. However, despite the enormous potential of these technologies to drive economic inclusion, several challenges must be addressed in order to ensure the success and sustainability of such initiatives. These challenges include ensuring data privacy, mitigating biases in AI algorithms, and creating affordable and sustainable training models (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47]. Overcoming these challenges requires thoughtful strategies, careful design, and collaboration across stakeholders to ensure that the model is both effective and equitable.

One of the foremost concerns in implementing AI-powered tools for marginalized youth is ensuring data privacy. AI tools, particularly those used for skill assessment, personalized learning, and progress tracking, rely heavily on the collection and analysis of personal data. This includes information on learners' behavior, preferences, learning patterns, and even sensitive details such as demographic data or prior educational background (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48]. The collection and processing of such data can raise significant privacy concerns, particularly when dealing with vulnerable populations such as marginalized youth who may not have the knowledge or resources to understand the risks of data misuse.

To mitigate privacy concerns, it is essential to ensure that AI-powered tools and platforms adhere to strict data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe or similar data privacy laws in other regions. These regulations outline how personal data should be collected, stored, and processed, giving users control over

their information and ensuring that it is only used for its intended purposes. Implementing robust encryption protocols and offering anonymization options where possible can further protect the privacy of youth participants (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28]. Transparency in how data is collected, stored, and used is also crucial. Platforms should clearly communicate data practices to users, ensuring that marginalized youth and their families are fully informed about the extent of data collection and the protections in place. Providing opt-in and opt-out options for data usage can also give youth more control over their personal information and enhance their trust in the system.

Another significant challenge is the issue of bias in AI algorithms. Machine learning models are often trained on large datasets that can inadvertently reflect societal biases, leading to biased outcomes that disproportionately affect certain groups. For example, AI-powered skill assessments or personalized learning pathways might unfairly favor certain demographic groups, such as those from higher socioeconomic backgrounds, while underestimating the potential of marginalized youth. Such biases could exacerbate inequalities, reinforcing the existing barriers that marginalized youth face in accessing opportunities (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44].

Mitigating bias in AI algorithms requires a multi-faceted approach. First and foremost, the datasets used to train AI models must be carefully curated to ensure that they are representative and diverse. This means including data from a wide range of sources, particularly from underserved communities, to ensure that AI models are trained on a more accurate reflection of the entire population (Castro, 2019, Salamkar & Allam, 2019) [23]. Furthermore, the development of AI systems must involve interdisciplinary teams that include ethicists, sociologists, and representatives from marginalized communities to identify and address potential biases in both the data and the algorithmic design. Regular audits of AI algorithms are necessary to assess their fairness and ensure that they do not perpetuate or amplify existing inequalities. Additionally, transparency in AI decision-making is critical. Platforms should offer clear explanations of how decisions are made and provide opportunities for users to challenge or appeal biased outcomes.

Affordability is another major challenge in implementing a scalable workforce development model for marginalized youth. While AI and cybersecurity training programs have the potential to open doors to high-paying careers, the cost of delivering these programs can be prohibitively high, particularly for marginalized communities that already face financial barriers. The development and maintenance of AI-powered platforms, as well as the provision of quality cybersecurity simulations and mentorship, require significant investments (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47]. Additionally, traditional educational models and certifications, often needed to validate skills in these fields, can come with high costs that make these opportunities inaccessible to youth from low-income backgrounds.

To create a cost-effective and sustainable model, it is essential to leverage existing infrastructure and resources. One approach is to build partnerships with tech companies, universities, and non-profits that can provide access to free or discounted tools, software, and certification programs. These partnerships can also help offset the costs of developing and running the programs. For example, tech companies could offer cloud services or software platforms for free or at a reduced cost in exchange for access to a future talent pool, helping to make the model more affordable for marginalized youth (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48]. Public-private partnerships can be leveraged to fund scholarships, stipends, or even paid internships for students, ensuring that marginalized youth are not deterred by financial constraints.

Online and blended learning models offer another avenue for cost reduction. These models eliminate the need for physical infrastructure and reduce administrative overhead, allowing resources to be directed toward the development of high-quality content and tools. By using AI-powered platforms for personalized learning and assessment, the costs associated with one-on-one instruction can be minimized, while still delivering tailored learning experiences to each student. Furthermore, the scalability of online learning platforms ensures that more youth can be reached without significant increases in cost per learner.

To further address affordability, governments and philanthropic organizations can play a critical role in funding workforce development initiatives for marginalized youth. Public investments in digital education and technology infrastructure can help ensure that these programs are accessible to those who need them most. Governments can also introduce policies that incentivize companies to invest in training programs for underserved communities, offering tax credits or other benefits in exchange for supporting workforce development initiatives (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44]. Additionally, creating a system of micro-credentials or low-cost certification programs that can be obtained through these training initiatives can offer marginalized youth a cost-effective pathway to validating their skills and gaining industry recognition without incurring significant debt.

While overcoming these challenges may seem daunting, several successful examples of AI and cybersecurity training programs for underserved communities provide valuable lessons in how to navigate these obstacles. For example, the "Tech for Good" initiative in the United States has successfully trained hundreds of low-income youth in AI, cybersecurity, and data science by providing free or heavily subsidized training programs. The initiative partners with local community centers and educational institutions to offer workshops, mentoring, and hands-on projects, ensuring that marginalized youth are not only learning technical skills but also gaining access to real-world experiences (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28]. By providing financial support and leveraging industry partnerships, Tech for Good has created a sustainable model that can be scaled to reach more youth across the country.

Similarly, the "Ajira Digital Program" in Kenya focuses on providing digital skills training, including cybersecurity and AI basics, to youth in rural and underserved communities. The program, which is run by the Kenyan government in partnership with various tech organizations, has successfully connected thousands of youth to online job opportunities and empowered them to access global markets. By providing free access to training materials and creating a network of mentors and industry partners, Ajira Digital has overcome affordability barriers and created a replicable model for other developing countries (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47].

Measuring the success of these programs in terms of employment rates, skill acquisition, and the reduction of skill gaps is critical to ensuring that the model is achieving its intended outcomes. Success can be tracked by monitoring employment rates among graduates, as well as by assessing their skill acquisition through certifications, job placements, and the use of digital portfolios. Measuring the reduction of

skill gaps in both AI and cybersecurity fields can be done by comparing the skills of marginalized youth before and after completing the program, as well as by evaluating how well the program addresses the specific needs of underserved communities (Castro, 2019, Salamkar & Allam, 2019) [23].

In conclusion, the challenges of implementing a scalable and impactful workforce development model that harnesses AI and cybersecurity to empower marginalized youth are significant but not insurmountable. By addressing data privacy concerns, mitigating algorithmic bias, and creating cost-effective and sustainable training programs, it is possible to build a system that provides marginalized youth with the skills they need to succeed in the digital economy. Through strategic partnerships, community-driven engagement, and ongoing investment, these challenges can be overcome, creating a pathway to economic inclusion and empowerment for youth around the world (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48].

2.7 Future Directions

The future directions of a scalable and impactful model for harnessing artificial intelligence (AI) and cybersecurity to revolutionize workforce development and empower marginalized youth offer exciting prospects. As the global economy increasingly shifts towards digitalization, the need for skilled professionals in AI and cybersecurity will continue to grow, and it is essential that marginalized youth are not left behind (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44]. Expanding the model to reach other underserved demographics, continually improving AI-driven learning platforms, and establishing global standards for workforce development in AI and cybersecurity are critical steps to ensuring that this initiative not only scales effectively but also maintains its relevance in the face of technological advancements and evolving global job markets.

Expanding the model to reach other underserved demographics is essential to maximizing its impact. While marginalized youth are a primary focus, other underserved groups, such as women, refugees, people with disabilities, and individuals from low-income or rural areas, also face significant barriers to accessing technology-driven career opportunities. These groups, while distinct in their needs and challenges, share many of the same obstacles that marginalized youth face, including limited access to quality education, digital tools, and career pathways in high-demand sectors like AI and cybersecurity.

To expand the model to these groups, the training programs should be customized to meet the specific needs of each demographic. For example, for women, who are often underrepresented in STEM fields, the model could integrate mentorship and community-building initiatives that foster an environment of support and empowerment. Offering flexible learning schedules, childcare support, and safe online spaces for women can increase their participation in tech programs (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47]. Similarly, for refugees and displaced persons, online learning platforms can provide a safe and accessible entry point for acquiring digital skills, with an emphasis on cultural sensitivity, language support, and psychological well-being. For individuals with disabilities, ensuring that the learning platforms are fully accessible, with screen readers, subtitles, and adaptive technologies, will help provide equal opportunities. By adapting the model to address the unique challenges of these various groups, it becomes possible to create a truly inclusive workforce development program that leaves no one behind.

The continuous improvement of AI-driven learning platforms is another critical direction for the future of this model. AI is evolving rapidly, and as the field of machine learning, natural language processing, and other AI technologies advance, it is essential that the learning platforms keep pace. One area for improvement is the personalization of learning pathways. While current AI systems already offer some level of personalized content delivery, there is a significant opportunity to enhance this capability by using more advanced AI techniques (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28]. This could include real-time adaptations of learning content based on not just learner performance but also emotional and cognitive engagement. AI can be used to identify when a learner is struggling, not only with specific concepts but also in terms of motivation or engagement, and adjust the content delivery accordingly to keep them on track. Such improvements can create a more empathetic and supportive learning environment, which is particularly important for marginalized youth who may face additional external pressures and emotional challenges.

Additionally, integrating more immersive learning technologies such as augmented reality (AR) and virtual reality (VR) can significantly enhance the learning experience. These technologies offer learners the opportunity to engage in simulations of real-world scenarios, which is particularly important for fields like cybersecurity, where hands-on experience is crucial. By incorporating these technologies, the model can provide more interactive and engaging training, allowing marginalized youth to gain the experience and confidence they need to enter the workforce (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48]. These tools could also enable learners to practice responding to cybersecurity threats or build AI models in a simulated environment that mirrors real-world applications, providing a safe space to learn without risk.

Another area of continuous improvement lies in expanding the accessibility and inclusivity of AI-driven learning platforms. Current platforms are often limited by language barriers, geographic constraints, and digital infrastructure. As part of the future direction, these platforms should be developed to cater to a wider range of languages, ensuring that non-English speakers can access the content in their native language (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44]. Moreover, as internet connectivity remains an issue in many underserved regions, the development of offline capabilities and low-bandwidth solutions will ensure that more youth can access training, regardless of their access to high-speed internet. Ensuring that the learning platform is adaptable to different regions and technologies is vital for reaching marginalized youth across the globe.

Establishing global standards for workforce development in AI and cybersecurity is also a crucial future direction. The rapid pace of technological advancements means that the skills required in these fields are constantly evolving. To ensure that AI and cybersecurity training programs remain relevant and valuable, it is essential to create and adhere to global standards that outline the core competencies and skills required for success in these fields. These standards would provide consistency in the quality of education and training across different regions and ensure that there is alignment between educational programs and the needs of employers (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47].

Global standards would also foster international cooperation and knowledge-sharing, enabling the development of best practices that can be adopted across countries and cultures. These standards could include agreed-upon certifications or credentials that recognize individuals' skills in AI and

cybersecurity, providing a clear pathway for marginalized youth to enter the workforce with recognized qualifications. Such certifications would not only be valuable in the local context but would also hold weight in the global job market, offering youth the opportunity to apply for positions with international companies and organizations (Castro, 2019, Salamkar & Allam, 2019) [23].

Furthermore, global standards would help address the increasing concern over the ethical implications of AI and cybersecurity technologies. Issues such as data privacy, algorithmic bias, and digital ethics must be incorporated into training programs to ensure that the workforce is not only technically skilled but also equipped to navigate the complex ethical challenges associated with these technologies (Deep, *et al*., 2022, Silwimba, 2019, Whitehead, 2017) [28]. The development of these global standards should involve a diverse group of stakeholders, including governments, industry leaders, educational institutions, and marginalized communities, to ensure that the standards are inclusive, representative, and forward-thinking.

The future of this model should also involve expanding the scope of AI and cybersecurity training to include not only technical skills but also soft skills, such as communication, teamwork, and problem-solving. These skills are essential for success in the modern workforce, particularly in the tech industry, where collaboration and innovation are central to overcoming complex challenges. Including soft skills training will ensure that marginalized youth are not only prepared to tackle the technical demands of AI and cybersecurity but are also capable of thriving in a professional environment (Kabirifar & Mojtahedi, 2019, Thamrin, 2017) [44].

Finally, to ensure the long-term success and scalability of this model, it is essential to establish robust feedback mechanisms that allow for ongoing evaluation and improvement. Collecting data on learners' progress, career outcomes, and challenges faced during the program will provide valuable insights into the effectiveness of the model and identify areas for improvement. This feedback can then be used to continuously refine the curriculum, teaching methods, and learning platforms to ensure that they meet the evolving needs of marginalized youth and the broader workforce (Moretto, *et al*., 2022, Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011) [48].

In conclusion, the future directions of a scalable and impactful model for harnessing AI and cybersecurity to empower marginalized youth are full of potential. By expanding the model to reach other underserved demographics, continuously improving AI-driven learning platforms, and establishing global standards for workforce development, this initiative can help bridge the digital divide and provide marginalized youth with the skills and opportunities they need to succeed in the digital economy (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017) [47]. With continued investment in infrastructure, partnerships, and innovation, this model has the power to drive economic inclusion, empower youth, and create a more equitable future for all.

2.8 Conclusion

The proposed model for harnessing artificial intelligence (AI) and cybersecurity to revolutionize workforce development and empower marginalized youth has immense transformative potential. By providing access to high-quality, tailored training in two of the most rapidly growing and in-demand fields, this model creates new pathways for marginalized youth to enter the digital economy. It aims to bridge the skills gap that has often excluded these young people from the opportunities afforded by the digital revolution. Through AI-powered learning tools, adaptive training platforms, and hands-on experience in cybersecurity simulation environments, the model ensures that youth from underserved communities acquire the technical and soft skills required to succeed in today's job market. By also emphasizing mentorship, industry partnerships, and certifications, the model equips marginalized youth with not only the knowledge but also the networks and credentials necessary to thrive in competitive industries.

The transformative potential of this model extends beyond individual career development; it also holds the power to address broader societal issues of economic inequality and digital exclusion. It envisions a future where marginalized youth, regardless of their background, have access to the same opportunities to succeed in the digital economy. This shift can have profound impacts on social mobility, poverty alleviation, and overall community empowerment, as these youth will be able to contribute meaningfully to the workforce, participate in innovative technologies, and drive economic growth in ways that are sustainable and inclusive.

However, achieving the model's full potential requires a collaborative effort across various sectors. Governments, educational institutions, private companies, and community organizations must come together to support marginalized youth and create the conditions for success. Policymakers must provide the regulatory framework, financial support, and infrastructure needed to make these programs accessible. Educational institutions should tailor curricula to address the needs of marginalized youth, while industry leaders can offer mentorship, internships, and opportunities for employment. Community-driven engagement ensures that these youth are recruited, supported, and retained throughout their educational journey, fostering a culture of empowerment and ownership. Cross-sector collaboration is essential to scaling the impact of this model and ensuring that it reaches the youth who stand to benefit the most.

The vision for a resilient and inclusive workforce goes beyond simply providing technical skills. It involves creating an ecosystem where all individuals, regardless of their background, have the tools, opportunities, and support needed to succeed in the modern economy. By focusing on marginalized youth and harnessing the power of AI and cybersecurity, this model offers a blueprint for a more equitable future where technology serves as a tool for empowerment, not exclusion. As we move forward, it is essential that we continue to prioritize investments in education, infrastructure, and partnerships, ensuring that the workforce of tomorrow is both skilled and inclusive. Through collective action and commitment, we can build a digital economy that benefits everyone, creating a brighter, more equitable future for all.

References

1. Adepoju AH, Austin-Gabriel B, Eweje A, Collins A. Framework for automating multi-team workflows to maximize operational efficiency and minimize redundant data handling. IRE Journals. 2022;5(9).
2. Adepoju AH, Austin-Gabriel B, Hamza O, Collins A. Advancing monitoring and alert systems: A proactive approach to improving reliability in complex data ecosystems. IRE Journals. 2022;5(11).
3. Adepoju PA, Austin-Gabriel B, Ige AB, Hussain NY, Amoo OO, Afolabi AI. Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. Open Access Research Journal

of Multidisciplinary Studies. 2022;4(1):131-139. https://doi.org/10.53022/oarjms.2022.4.1.0075
4. Adewusi AO, Chiekezie NR, Eyo-Udo NL. Cybersecurity threats in agriculture supply chains: A comprehensive review. World Journal of Advanced Research and Reviews. 2022;15(03):490-500.
5. Adewusi AO, Chiekezie NR, Eyo-Udo NL. Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven farms. World Journal of Advanced Research and Reviews. 2022;15(03):480-489.
6. Adewusi AO, Chiekezie NR, Eyo-Udo NL. The role of AI in enhancing cybersecurity for smart farms. World Journal of Advanced Research and Reviews. 2022;15(03):501-512.
7. Al Kaabi MSH. Factors influencing timely completion of construction projects in the oil industry in the United Arab Emirates—An exploratory study [dissertation]. Aberystwyth University, UK; 2021.
8. Al-Ali R, Kathiresan N, El Anbari MR, Schendel ER, Zaid TA. Workflow optimization of performance and quality of service for bioinformatics application in high performance computing. Journal of Computational Science. 2016;15:3-10.
9. Alam M, Zou PX, Stewart RA, Bertone E, Sahin O, Buntine C, Marshall C. Government championed strategies to overcome the barriers to public building energy efficiency retrofit projects. Sustainable Cities and Society. 2019;44:56-69.
10. Alessa L, Kliskey A, Gamble J, Fidel M, Beaujean G, Gosz J. The role of Indigenous science and local knowledge in integrated observing systems: Moving toward adaptive capacity indices and early warning systems. Sustainability Science. 2016;11:91-102.
11. Al-Hajji H, Khan S. Keeping oil & gas EPC major projects under control: Strategic & innovative project management practices. In: Abu Dhabi International Petroleum Exhibition and Conference; 2016 Nov. p. D021S033R003. SPE.
12. Amirtash P, Parchami Jalal M, Jelodar MB. Integration of project management services for International Engineering, Procurement and Construction projects. Built Environment Project and Asset Management. 2021;11(2):330-349.
13. Arundel A, Bloch C, Ferguson B. Advancing innovation in the public sector: Aligning innovation measurement with policy goals. Research Policy. 2019;48(3):789-798.
14. Asch M, Moore T, Badia R, Beck M, Beckman P, Bidot T, Zacharov I. Big data and extreme-scale computing: Pathways to convergence—toward a shaping strategy for a future software and data ecosystem for scientific inquiry. The International Journal of High Performance Computing Applications. 2018;32(4):435-479.
15. Austin-Gabriel B, Hussain NY, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Research Journal of Engineering and Technology. 2021;1(1):47-55. https://doi.org/10.53022/oarjet.2021.1.1.0107
16. Bae MJ, Park YS. Biological early warning system based on the responses of aquatic organisms to disturbances: A review. Science of the Total Environment. 2014;466:635-649.
17. Bhaskaran SV. Integrating Data Quality Services (DQS) in Big Data Ecosystems: Challenges, Best Practices, and Opportunities for Decision-Making. Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems. 2020;4(11):1-12.
18. Bitter J. Improving multidisciplinary teamwork in preoperative scheduling [dissertation]. 2017.
19. Boda VVR, Immaneni J. Streamlining FinTech operations: The power of SysOps and smart automation. Innovative Computer Sciences Journal. 2019;5(1).
20. Bristol-Alagbariya B, Ayanponle OL, Ogedengbe DE. Integrative HR approaches in mergers and acquisitions ensuring seamless organizational synergies. Magna Scientia Advanced Research and Reviews. 2022;6(1):78-85.
21. Bristol-Alagbariya B, Ayanponle OL, Ogedengbe DE. Strategic frameworks for contract management excellence in global energy HR operations. GSC Advanced Research and Reviews. 2022;11(3):150-157.
22. Bristol-Alagbariya B, Ayanponle OL, Ogedengbe DE. Developing and implementing advanced performance management systems for enhanced organizational productivity. World Journal of Advanced Science and Technology. 2022;2(1):39-46.
23. Castro R. Blended learning in higher education: Trends and capabilities. Education and Information Technologies. 2019;24(4):2523-2546.
24. Chan N. Building Information Modelling: An analysis of the methods used to streamline design-to-construction in New Zealand [dissertation]. Open Access Te Herenga Waka-Victoria University of Wellington; 2020.
25. Chen Q, Hall DM, Adey BT, Haas CT. Identifying enablers for coordination across construction supply chain processes: A systematic literature review. Engineering, Construction and Architectural Management. 2020;28(4):1083-1113.
26. Chinamanagonda S. Observability in microservices architectures—Advanced observability tools for microservices environments. MZ Computing Journal. 2022;3(1).
27. Davis JE. Temporal meta-model framework for Enterprise Information Systems (EIS) development [dissertation]. Curtin University; 2014.
28. Deep S, Banerjee S, Dixit S, Vatin NI. Critical factors influencing the performance of highway projects: An empirical evaluation. Buildings. 2022;12(6):849.
29. Diaz A, Schöggl JP, Reyes T, Baumgartner RJ. Sustainable product development in a circular economy: Implications for products, actors, decision-making support and lifecycle information management. Sustainable Production and Consumption. 2021;26:1031-1045.
30. Drukker L, Noble JA, Papageorghiou AT. Introduction to artificial intelligence in ultrasound imaging in obstetrics and gynecology. Ultrasound in Obstetrics & Gynecology. 2020;56(4):498-505.
31. Duo X, Xu P, Zhang Z, Chai S, Xia R, Zong Z. KCL: A declarative language for large-scale configuration and policy management. In: International Symposium on Dependable Software Engineering: Theories, Tools, and Applications. Cham: Springer Nature Switzerland; 2022 Oct. p. 88-105.
32. Ebrahim A, Battilana J, Mair J. The governance of social enterprises: Mission drift and accountability challenges in hybrid organizations. Research in Organizational Behavior. 2014;34:81-100.
33. Egbumokei PI, Dienagha IN, Digitemie WN, Onukwulu EC. Advanced pipeline leak detection technologies for enhancing safety and environmental sustainability in energy operations. International Journal of Science and Research Archive. 2021;4(1):222-228. https://doi.org/10.30574/ijsra.2021.4.1.0186

34. Filatotchev I, Ireland RD, Stahl GK. Contextualizing management research: An open systems perspective. Journal of Management Studies. 2022;59(4):1036-1056.
35. Frota Barcellos J. Critical elements of a successful project. 2019.
36. Gil-Ozoudeh I, Iwuanyanwu O, Okwandu AC, Ike CS. The role of passive design strategies in enhancing energy efficiency in green buildings. Engineering Science & Technology Journal. 2022;3(2):71-91.
37. Habibi M, Kermanshachi S, Rouhanizadeh B. Identifying and measuring engineering, procurement, and construction (EPC) key performance indicators and management strategies. Infrastructures. 2019;4(2):14.
38. Hossain MD. Performance evaluation of procurement system in ICT industry: A case study. 2018.
39. Hussain NY, Austin-Gabriel B, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Research Journal of Science and Technology. 2021;2(2):6-15. https://doi.org/10.53022/oarjst.2021.2.2.0059
40. Ibrahim II. Project planning in construction procurement: The case of Nigerian indigenous contractors [dissertation]. 2015.
41. Ige AB, Austin-Gabriel B, Hussain NY, Adepoju PA, Amoo OO, Afolabi AI. Developing multimodal AI systems for comprehensive threat detection and geospatial risk mitigation. Open Access Research Journal of Science and Technology. 2022;6(1):93-101. https://doi.org/10.53022/oarjst.2022.6.1.0063
42. Iwuanyanwu O, Gil-Ozoudeh I, Okwandu AC, Ike CS. The integration of renewable energy systems in green buildings: Challenges and opportunities. Journal of Applied Science & Engineering. 2022.
43. Jones CL, Golanz B, Draper GT, Janusz P. Practical Software and Systems Measurement Continuous Iterative Development Measurement Framework. Version 1. 2020;15.
44. Kabirifar K, Mojtahedi M. The impact of engineering, procurement, and construction (EPC) phases on project performance: A case of large-scale residential construction project. Buildings. 2019;9(1):15.
45. Liu T, Wang Y, Wilkinson S. Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public–Private Partnerships (PPPs): A comparative analysis of Australia and China. International Journal of Project Management. 2016;34(4):701-716.
46. Micheli GJ, Cagno E. The role of procurement in performance deviation recovery in large EPC projects. International Journal of Engineering Business Management. 2016;8:1847979016675302.
47. Mohanty SP, Choppali U, Kougianos E. Everything you wanted to know about smart cities: The Internet of Things is the backbone. IEEE Consumer Electronics Magazine. 2016;5(3):60-70.
48. Moretto A, Patrucco AS, Walker H, Ronchi S. Procurement organisation in project-based setting: A multiple case study of engineer-to-order companies. Production Planning & Control. 2022;33(9-10):847-862.
49. Nguyen HT, Hadikusumo BH. Human resource related factors and engineering, procurement, and construction (EPC) project success. Journal of Financial Management of Property and Construction. 2018;23(1):24-39.
50. Nwaimo CS, Adewumi A, Ajiga D. Advanced data analytics and business intelligence: Building resilience in risk management. International Journal of Scientific Research and Applications. 2022;6(2):121. https://doi.org/10.30574/ijsra.2022.6.2.0121.
51. Olufemi-Phillips AQ, Ofodile OC, Toromade AS, Eyo-Udo NL, Adewale TT. Optimizing FMCG supply chain management with IoT and cloud computing integration. International Journal of Management & Entrepreneurship Research. 2020;6(11):[Publisher].
52. Onukwulu EC, Agho MO, Eyo-Udo NL. Advances in smart warehousing solutions for optimizing energy sector supply chains. Open Access Research Journal of Multidisciplinary Studies. 2021;2(1):139-157. https://doi.org/10.53022/oarjms.2021.2.1.0045
53. Onukwulu EC, Agho MO, Eyo-Udo NL. Framework for sustainable supply chain practices to reduce carbon footprint in energy. Open Access Research Journal of Science and Technology. 2021;1(2):12-34. https://doi.org/10.53022/oarjst.2021.1.2.0032
54. Onukwulu EC, Agho MO, Eyo-Udo NL. Advances in green logistics integration for sustainability in energy supply chains. World Journal of Advanced Science and Technology. 2022;2(1):47-68. https://doi.org/10.53346/wjast.2022.2.1.0040
55. Onukwulu EC, Agho MO, Eyo-Udo NL. Circular economy models for sustainable resource management in energy supply chains. World Journal of Advanced Science and Technology. 2022;2(2):34-57. https://doi.org/10.53346/wjast.2022.2.2.0048
56. Onukwulu EC, Dienagha IN, Digitemie WN, Egbumokei PI. Framework for decentralized energy supply chains using blockchain and IoT technologies. IRE Journals. 2021 Jun 30. Available from: https://www.irejournals.com/index.php/paper-details/1702766
57. Onukwulu EC, Dienagha IN, Digitemie WN, Egbumokei PI. Predictive analytics for mitigating supply chain disruptions in energy operations. IRE Journals. 2021 Sep 30. Available from: https://www.irejournals.com/index.php/paper-details/1702929
58. Onukwulu EC, Dienagha IN, Digitemie WN, Egbumokei PI. Advances in digital twin technology for monitoring energy supply chain operations. IRE Journals. 2022 Jun 30. Available from: https://www.irejournals.com/index.php/paper-details/1703516
59. Onukwulu EC, Dienagha IN, Digitemie WN, Egbumokei PI. Blockchain for transparent and secure supply chain management in renewable energy. International Journal of Science and Technology Research Archive. 2022;3(1):251-272. https://doi.org/10.53771/ijstra.2022.3.1.0103
60. Onukwulu EC, Dienagha IN, Digitemie WN, Egbumokei PI. AI-driven supply chain optimization for enhanced efficiency in the energy sector. Magna Scientia Advanced Research and Reviews. 2021;2(1):87-108. https://doi.org/10.30574/msarr.2021.2.1.0060
61. Onukwulu NEC, Agho NMO, Eyo-Udo NNL. Advances in smart warehousing solutions for optimizing energy sector supply chains. Open Access Research Journal of Multidisciplinary Studies. 2021;2(1):139-157. https://doi.org/10.53022/oarjms.2021.2.1.0045
62. Ordanini A, Parasuraman A, Rubera G. When the recipe is more important than the ingredients: A qualitative comparative analysis (QCA) of service innovation configurations. Journal of Service Research. 2014;17(2):134-149.
63. Osei-Kyei R, Chan AP. Review of studies on the Critical

Success Factors for Public–Private Partnership (PPP) projects from 1990 to 2013. International Journal of Project Management. 2015;33(6):1335-1346.
64. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Innovative financial planning and governance models for emerging markets: Insights from startups and banking audits. Open Access Research Journal of Multidisciplinary Studies. 2021;1(2):108-116.
65. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Advancing SME financing through public-private partnerships and low-cost lending: A framework for inclusive growth. Iconic Research and Engineering Journals. 2022;6(2):289-302.
66. Pace ML, Carpenter SR, Cole JJ. With and without warning: Managing ecosystems in a changing world. Frontiers in Ecology and the Environment. 2015;13(9):460-467.
67. Pal R, Wang P, Liang X. The critical factors in managing relationships in international engineering, procurement, and construction (IEPC) projects of Chinese organizations. International Journal of Project Management. 2017;35(7):1225-1237.
68. Panda D, Sahu GP. E-procurement implementation: Comparative study of governments of Andhra Pradesh and Chhattisgarh. SSRN. 2014.
69. Patel A, Alhussian H, Pedersen JM, Bounabat B, Júnior JC, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. Computers & Security. 2017;64:92-109.
70. Pulwarty RS, Sivakumar MV. Information systems in a changing climate: Early warnings and drought risk management. Weather and Climate Extremes. 2014;3:14-21.
71. Raza H. Proactive Cyber Defense with AI: Enhancing Risk Assessment and Threat Detection in Cybersecurity Ecosystems. 2021.
72. REF 2022.
73. Ren J, Guo Y, Zhang D, Liu Q, Zhang Y. Distributed and efficient object detection in edge computing: Challenges and solutions. IEEE Network. 2018;32(6):137-143.
74. Rico R, Hinsz VB, Davison RB, Salas E. Structural influences upon coordination and performance in multiteam systems. Human Resource Management Review. 2018;28(4):332-346.
75. Roden S, Nucciarelli A, Li F, Graham G. Big data and the transformation of operations models: A framework and a new research agenda. Production Planning & Control. 2017;28(11-12):929-944.
76. Rogers K. Creating a culture of data-driven decision-making. Liberty University; 2020.
77. Ross DF, Ross DF. Procurement and supplier management. Distribution Planning and Control: Managing in the Era of Supply Chain Management. 2015:531-604.
78. Roth S, Valentinov V, Kaivo-Oja J, Dana LP. Multifunctional organisation models: A systems–theoretical framework for new venture discovery and creation. Journal of Organizational Change Management. 2018;31(7):1383-1400.
79. Saarikallio M. Improving hybrid software business: quality culture, cycle-time and multi-team agile management. JYU Dissertations; 2022.
80. Salamkar MA, Allam K. Data lakes vs. data warehouses: Comparative analysis on when to use each, with case studies illustrating successful implementations. Distributed Learning and Broad Applications in Scientific Research. 2019;5.
81. Sandilya SK, Varghese K. A study of delays in procurement of engineered equipment for engineering, procurement and construction (EPC) projects in India: A mixed method research approach. International Journal of Project Management. 2016.
82. Santoni G. Standardized cross-functional communication as a robust design tool-mitigating variation, saving costs, and reducing the New Product Development Process' lead time by optimizing the information flow. [Doctoral dissertation]. Politecnico di Torino; 2019.
83. Sebastian IM, Ross JW, Beath C, Mocker M, Moloney KG, Fonstad NO. How big old companies navigate digital transformation. In: Strategic Information Management. Routledge; 2020. p. 133-150.
84. Shaw T, McGregor D, Brunner M, Keep M, Janssen A, Barnet S. What is eHealth (6)? Development of a conceptual model for eHealth: qualitative study with key informants. Journal of Medical Internet Research. 2017;19(10):e324.
85. Silwimba S. An investigation into the effects of procurement methods on project delivery in the Zambian road sector. [Doctoral dissertation]. The University of Zambia; 2019.
86. Singh APA, Abhinav Parashar A. Streamlining purchase requisitions and orders: A guide to effective goods receipt management. J. Emerg. Technol. Innov. Res. 2021;8(5):g179-g184.
87. Singh A, Chatterjee K. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. 2017;79:88-115.
88. Singh SP, Nayyar A, Kumar R, Sharma A. Fog computing: From architecture to edge computing and big data processing. The Journal of Supercomputing. 2019;75:2070-2105.
89. Skelton M, Pais M. Team topologies: Organizing business and technology teams for fast flow. IT Revolution. 2019.
90. Soni P, Krishnan RT. Frugal innovation: Aligning theory, practice, and public policy. Journal of Indian Business Research. 2014;6(1):29-47.
91. Srivastava A, Jawaid S, Singh R, Gehlot A, Akram SV, Priyadarshi N, Khan B. Imperative role of technology intervention and implementation for automation in the construction industry. Advances in Civil Engineering. 2022;2022:6716987.
92. Steyn M. Organisational benefits and implementation challenges of mandatory integrated reporting: Perspectives of senior executives at South African listed companies. Sustainability Accounting, Management and Policy Journal. 2014;5(4):476-503.
93. Stone M, Aravopoulou E, Gerardi G, Todeva E, Weinzierl L, Laughlin P, Stott R. How platforms are transforming customer information management. The Bottom Line. 2017;30(3):216-235.
94. Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks. 2014;10(7):190903.
95. Syed J, Mahmood SKA, Zulfiqar A, Sharif M, Sethi UI, Ikram U, Afridi SK. The construction sector value chain in Pakistan and the Sahiwal coal power project. In: China's Belt and Road Initiative in a Global Context: Volume II: The China Pakistan Economic Corridor and its Implications for Business. 2020;271-287.
96. Tang P, Yilmaz A, Cooke N. Automatic imagery data analysis for proactive computer-based workflow management during nuclear power plant outages.

Arizona State University. 2018;15-8121.
97. Tariq MU, Poulin M, Abonamah AA. Achieving operational excellence through artificial intelligence: Driving forces and barriers. Frontiers in Psychology. 2021;12:686624.
98. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, Ghafir I. The security of big data in fog-enabled IoT applications including blockchain: A survey. Sensors. 2019;19(8):1788.
99. Tezel A, Papadonikolaki E, Yitmen I, Hilletofth P. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management. 2020;7:547-563.
100. Thamrin DAF. Six Sigma implementation and integration within project management framework in engineering, procurement, and construction projects: A case study in a Southeast Asian engineering, procurement, and construction company. [Doctoral dissertation]. 2017.
101. Thumburu SKR. Integrating SAP with EDI: Strategies and insights. MZ Computing Journal. 2020;1(1).
102. Toutounchian S, Abbaspour M, Dana T, Abedi Z. Design of a safety cost estimation parametric model in oil and gas engineering, procurement and construction contracts. Safety Science. 2018;106:35-46.
103. Tuli FA, Varghese A, Ande JRP. Data-driven decision making: A framework for integrating workforce analytics and predictive HR metrics in digitalized environments. Global Disclosure of Economics and Business. 2018;7(2):109-122.
104. Van Zyl ES, Mathafena RB, Ras J. The development of a talent management framework for the private sector. SA Journal of Human Resource Management. 2017;15(1):1-19.
105. Vehviläinen T. Improving process efficiency and supply chain management by taking advantage of digitalization-based procurement tools. 2019.
106. Vilasini N, Neitzert TR, Rotimi JO. Correlation between construction procurement methods and lean principles. International Journal of Construction Management. 2011;11(4):65-78.
107. Vlietland J, Van Solingen R, Van Vliet H. Aligning codependent Scrum teams to enable fast business value delivery: A governance framework and set of intervention actions. Journal of Systems and Software. 2016;113:418-429.
108. Watson R, Wilson HN, Smart P, Macdonald EK. Harnessing difference: A capability-based framework for stakeholder engagement in environmental innovation. Journal of Product Innovation Management. 2018;35(2):254-279.
109. Whitehead J. Prioritizing sustainability indicators: Using materiality analysis to guide sustainability assessment and strategy. Business Strategy and the Environment. 2017;26(3):399-412.
110. Yu W, Dillon T, Mostafa F, Rahayu W, Liu Y. A global manufacturing big data ecosystem for fault detection in predictive maintenance. IEEE Transactions on Industrial Informatics. 2019;16(1):183-192.
111. Zhang C, Tang P, Cooke N, Buchanan V, Yilmaz A, Germain SWS, *et al*. Human-centered automation for resilient nuclear power plant outage control. Automation in Construction. 2017;82:179-192.
112. Zong Z. KCL: A declarative language for large-scale configuration and policy management. In: Dependable Software Engineering: Theories, Tools, and Applications: 8th International Symposium, SETTA 2022, Beijing, China, October 27-29, 2022, Proceedings. Vol. 13649, p. 88. Springer Nature; 2022.
113. Zou M, Vogel-Heuser B, Sollfrank M, Fischer J. A cross-disciplinary model-based systems engineering workflow of automated production systems leveraging socio-technical aspects. In: 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). p. 133-140. IEEE; 2020.