University of Westminster

School of Computer Science and Engineering

Module Code & Name: 4COSC08C: Trends in Computer Science.

Assignment Type: Coursework 2

Topic: Employability and career planning- Reflective writing.

Name : pasindu sandeepa

Uow ID : w1838841

IIT ID : 20200879

Contents

introduction

An arrangement between an employer and a worker in which the employee agrees to do particular responsibilities is known as employment. In exchange, the employee is paid a salary or an hourly wage. Although employees can negotiate some components of an employment agreement, the majority of the terms and conditions are under the discretion of the employer. The contract can be terminated by either party.

A verbal agreement, a written correspondence, or a job offer letter can all be used to describe an individual employee's employment agreement. A job offer can be implied during an interview or formalized in a written employment contract.

The process of selecting on career options, creating career objectives, and deciding on educational and developmental programs to increase the skills needed to attain career goals is referred to as career planning. It's a crucial aspect of a person's self-evaluation.

Different job alternatives should be thoroughly investigated in order to establish a match between one's strengths and the opportunities offered by each. To create and progress as a worker, career planning entails constant learning and improvement.

Employability and career planning

Computer science is a sought-after and lucrative career option for tech-savvy persons interested in the latest computer discoveries. According to the US Bureau of Labor Statistics, computer and information technology (IT) occupations are predicted to grow at a faster-than-average rate of 11% from 2019 to 2029.Current computer science trends include cloud computing, information security, and big data collection and storage.

The evolution of computer science is unavoidable, and it has a significant impact on the nature of work and the jobs that are currently in demand. For example, ten years ago, manual accountants and mechanics were in high demand, but they are now deemed antiquated. Employees were once divided into numerous categories, such as white-collar and blue-collar workers.

All workers, including blue-collar workers, technical staff, and executives, are impacted. However, because these professions are ever-changing, it's difficult to foresee what a person might wish to do in the future. Career planning is seen as a key action and responsibility that young adults, recent graduates, and individuals must conduct in order to ensure that their skills and certifications will last at least 20 years and allow them to advance. In the specialist profession, career goals and objectives change regularly due to the volatile and dynamic corporate environment. I've always wanted to work in the software engineering sector as a social entrepreneur.

I met a career advisor who was quite inspiring, and his thought processes and thinking were very similar to mine. he is my uncle. He is a software engineer at 99x. I started to follow him. because he is a very successful person in this field. I believe I have a lot to learn from him. His thinking sample was a criticism of my questions and reasoning process. He became intrigued when I expressed my aim and who I wanted to become, and he gave me a number of basic ideas on how I should begin my career and minor adjustments I should make throughout the early development stage before completing the full procedure. He disclosed a few new concepts that were highly thorough and more of an eye opener for the engineering and federal fields to foster with the necessary actions and activities.

Future career

In my first few years as a new graduate in the corporate sector, one of my career goals is to climb the corporate ladder., then developing exotic talents and abilities for personal development before deciding to start my own business. As a social entrepreneur, I want to help create a world that is fair, just, and prejudice-free, one that promotes growth and well-being, as well as a profitable existence for all people.

Conclusion

my target is to be a full stack software engineer.In order to do that, I have to choose my path in level and level modules acknowledging my goals. My opinion is choosing "software engineering" is the best path. In level 5 under the Data Science theme, there is an optional module called “Network Software Engineering”. Network Software Engineering focuses on designing, building and installing software for existing or new networks and infrastructures. Often, organizations require bespoke software solutions. By writing and creating these platforms, networking software engineers allow organizations to operate more efficiently, maximize their productivity and function securely. Not only that,Analytical skills to determine how existing software can be enhanced,Ability to work under pressure,In-depth knowledge of network engineer software tools and coding languages has software engineers. During my career planning, I decided to pursue a profession in software engineering. When we pursue the vocation that I picked, it is not simple. When it comes to achieving my job goals, I will have to overcome a variety of obstacles. It will not be easy, and it will become more difficult as you progress toward graduation, but it will all be worthwhile. One of the first stages, according to them, is to balance my time between studying and practicing.

References

- S. Chatterjee, "Software Engineering Practice in Computer Science Courses," 19th Australian Conference on Software Engineering (aswec 2008), 2008, pp. 611-616, doi: 10.1109/ASWEC.2008.4483252.

- F. Meziane and S. Vadera, "A comparison of computer science and software engineering programmes in English universities," 17th Conference on Software Engineering Education and Training, 2004. Proceedings., 2004, pp. 65-70, doi: 10.1109/CSEE.2004.1276512.

- https://www.thebalancecareers.com/steps-to-create-a-career-development-plan-1917798

- http://career.iresearchnet.com/career-development/employability/

University of Westminster

School of Computer Science and Engineering

Module Code & Name: 4COSC08C: Trends in Computer Science.

Assignment Type: Coursework 2

Topic: AI and Ethics

Name : pasindu sandeepa

Uow ID : w1838841

IIT ID : 20200879

Contents

Introduction

The ability of a digital computer or computer-controlled robot to execute tasks generally associated with intelligent beings is the short answer to What is Artificial Intelligence.

A layperson with only a rudimentary understanding of technology would associate it with robots. Artificial Intelligence, they believe, is a terminator-like figure that can act and think for itself.

If you ask an AI researcher about artificial intelligence, he or she will tell you that it is a set of algorithms that can produce outcomes without being explicitly directed to do so. Artificial intelligence is the intelligence displayed by computers. In today's world, Artificial Intelligence has become highly popular.

In this report we can find out the advances Artificial Intelligence has made, its impact on society and the ethical questions in AI.

AI and Ethics

Artificial Intelligence, or simply AI, refers to a machine's ability to mimic human intelligence. Learning, logic, reasoning, perception, and creativity, which were long thought to be unique to humans, are now being copied by technology and applied across all industries.

The advances Artificial Intelligence has made

Vision, voice recognition and generation, natural language processing, picture and video production, multi-agent systems, planning, decision-making, and the integration of vision and motor control for robots have all made significant development in the field of AI. In addition, groundbreaking applications in a range of sectors such as games, medical diagnosis, logistics systems, autonomous driving, language translation, and interactive personal support were developed. The sections that follow give instances of a variety of significant advancements.

Bots and virtual assistants are improving their ability to mimic natural speech. It's already tough to tell whether you're talking to a real person or a robot, especially when it comes to chatbots. Many businesses currently prefer to engage with clients through algorithms.

We are approaching a moment when human-machine interactions will be as prevalent as human-machine interactions. We all despise calling technical help since, towards the end of the day, the personnel may be inept, impolite, or exhausted. Bots, on the other hand, have practically limitless patience and benevolence.

Impact on society

A wonderful example of AI in action is monitoring massive quantities of Internet traffic in real time to uncover potential cybersecurity dangers that have never been seen before — allowing us to take countermeasures before a threat takes hold. Scanning through hundreds of thousands of internet logs to find the precise pattern that could indicate a cyberattack would be hard for humans.

That isn't to argue that machines will completely replace people. Utilizing these next-generation technologies will provide humans with enormous power. The impact of AI on our lives will not be seen or appreciated immediately, but one thing is certain: advancement is continual and unavoidable.

The ethical questions in AI

Today, AI ethics is more about asking the right questions than giving the correct answers. Artificial intelligence may or may not ever equal or surpass human intelligence. However, given how quickly and unpredictably it is evolving, it would be exceedingly irresponsible not to consider efforts to ease the transition and limit the potential of severe effects.

Humans rule the globe because they are the most intelligent species. What if AI one day outsmarts us? It will anticipate our behaviors, so merely turning off the computer will not suffice: the computer will defend itself in ways we have yet to imagine. What impact will the fact that we are no longer the world's most intelligent species have on us?

Humanity has so far successfully turned all brilliant technologies into advanced weaponry, and AI is no exception. We're don't just talk about action-movie war robots here.AI can be used maliciously to do injury in almost any industry, such as manipulating data, stealing passwords, and interfering with the work of other software and systems. Cybersecurity is a key concern nowadays as once AI gets internet access to learn, it becomes vulnerable to hacker attacks. Perhaps the only way to safeguard AI is to use AI to protect AI.

Conclusion

We conclude that if a machine can convincingly impersonate a human in the eyes of a competent observer, it is intelligent. AI systems are now routinely used in a variety of fields, including economics, medicine, engineering, and the military, as well as being integrated into many typical home computer software applications, conventional strategy games, and so on. AI is an interesting and fulfilling science. Artificial intelligence is a subfield of computer science that deals with the automation of intelligent behavior. AI is now defined as "the study of mechanisms underlying intelligent behavior through the creation and evaluation of objects that attempt to perform such mechanisms." As a result, it may be concluded that it functions as an artificial human brain with incredible artificial thinking capabilities.

References

- E. Bradley and P. Chung, "AI tools: development trends and selection," IEE Colloquium on Strategic Research Issues in AI in Engineering, 1990, pp. 8/1-8/3

- T. Yukitake, "Innovative solutions toward future society with AI, Robotics, and IoT," 2017 Symposium on VLSI Circuits, 2017, pp. C16-C19, doi: 10.23919/VLSIC.2017.8008499.

- M. Sadi and U. Guin, "Test and Yield Loss Reduction of AI and Deep Learning Accelerators," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, doi: 10.1109/TCAD.2021.3051841.

University of Westminster

School of Computer Science and Engineering

Module Code & Name: 4COSC08C: Trends in Computer Science.

Assignment Type: Coursework 2

Topic: Internet of things and its cyber security implications

Name : pasindu sandeepa

Uow ID : w1838841

IIT ID : 20200879

Contents

Introduction

The Internet of Things, often known as the Internet of Objects, will revolutionize the world.

Everything, including we, is affected. This may appear to be a bold claim but consider the influence the Internet has already had on education, communication, commerce, science, and other fields. Government, as well as mankind Clearly, the Internet is one of the most significant and powerful technologies available today. In all human history, there have been some incredible creations. Consider that the Internet of Things is the next evolution of the Internet, representing a massive leap forward in its development. Ability to collect, analyze, and disseminate data that can be transformed into information, knowledge, and wisdom and, in the end, wisdom in this setting, the Internet of Things becomes extremely significant. Users can gain deeper automation, analysis, and integration inside a system with IoT solutions.

They increase the range and precision of these areas. Sensing, networking, and robotics are all part of the Internet of Things. The Internet of Things takes advantage of recent software advancements, lower hardware prices, and modern attitudes about technology. Its new and advanced aspects result in significant changes in how products, goods, and services are delivered, as well as the social, economic, and political implications of those changes.

Internet of Things and its Cyber Security implications

The concept of connecting things and gadgets of all kinds through the internet is known as the Internet of Things. In order to communicate with similarly connected devices or machines, an increasing number of objects and systems in our life are getting integrated with network connectivity and processing capability.

Risk minimization is essential for effective cyber security. Organizations should routinely update software and "patch" devices to remedy security weaknesses in order to prevent IoT attacks. This method locks each device independently, ensuring that the technology cannot be easily modified. Additionally, it is critical that enterprises avoid using generic passwords or the same password for many devices and systems, especially in the IoT. The implementation of multi-factor authentication can add an extra layer of protection to logins and passwords. Finally, risk mitigation planning can help prepare the sector with safe IoT practices, such as monitoring for network infiltration or suspicious behavior and preparing response plans for cyber security incidents. Individuals, the corporate sector, and the public sector can all profit from the Internet of Things in terms of cost and convenience. As a result of these varied tools and technologies, as well as the increasing flow of data between channels, there is a greater vulnerability to threats. Because these things are frequently used in day-to-day operations, the data that could be taken

from these networks provides hackers with sensitive, valuable information – particularly in the defense industry. Individuals and organizations should take the necessary precautions to reduce cyber security threats and guarantee that IoT devices are connected to a secure network.

Difference between IOT and traditional internet

As the global internet has grown, virtual linkages have emerged, affecting real-world products and activities. Everything is connected to everything else, resulting in a dispersed ecology that goes far beyond object interconnection. The Internet of Things has become a crucial part of many businesses' digital transformation efforts. The identity of the content creator is the primary distinction between the internet of things and the internet. Content is consumed on a request basis on the traditional Internet. When a condition of interest is detected in the IoT, the material is frequently consumed by sending a notice or executing an action. The internet of things is a network of physical objects embedded with technology that connect to the internet and other devices. These gadgets record and communicate data about how they're used and where they're located. The three types of IoT data are status data, automation data, and location data, which differ depending on the device that generates it and the use case. The Internet is a large network that links millions of computers and other electronic devices all around the world. The Internet allows anyone to acquire almost any information, communicate with anyone on the planet, and do a lot more. The internet is characterized by decentralization. Nobody owns the internet, and no one has authority over who can use it.

The internet is focused with both content creation and sharing, but the IoT is primarily concerned with content creation. The internet is based on both the physical-first and digital-first conceptions, whereas the IoT is based on the physical-first approach. The internet employs both point-to-point and multipoint connections, whereas the internet uses both.

The challenges it creates for cyber security

Many firms struggle to secure their IoT networks and devices, even though IoT security should be a basic component of an organizational cybersecurity strategy. The top five issues for protecting IoT in the enterprise are discussed below. When it comes to security standards, the Internet of Things is a bit of a wild west. Because there is no universal standard for firms and niches, each company must set its own rules and guidelines. The standardization makes it more difficult to protect IoT devices, as well as to allow machine-to-machine (M2M) communication without increasing security risks. If an app wasn't built with cloud connectivity in mind, it's likely to be exposed to today's cyber threats. For example, more contemporary encryption standards may not be compatible with certain older assets. Making outmoded programs Internet-ready without making big changes is risky, but it's not always possible with historical assets. They've been hacked together over years (perhaps decades), making even basic security changes a major undertaking.

References

- Anon., n.d. [Online]
  Available at: https://www.simplilearn.com/iot-cybersecurity-article

- callan, r., 2003. *Artificial intelligence.* basingstoke: Palgrave Macmillan.

- Dubber, M. D. F. D. S., 2020. *The Oxford handbook of ethics of AI.* new york: oxword university press.

- li shangbang, X. L. D., 2017. *securing the internet of things.* s.l.:cambridge,massachusetts,syngress.

- Ramgir, M., 2019. *internet of things.* 1st ed. india: pearson education india.