UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

University of Westminster

Trends in Computer Science

4COSC008C.1

Coursework II - Portfolio

Student Name: Vihangi Patterson
UOW Number: 19530646
Student ID: 20220011

Table of Contents

Table of figures

1. Employability and Career Planning

Introduction

Simply employability is the adaptable abilities required of someone to be employable. Those skills can be developed as we engage more in our desired career path. Career planning has five stages as Initiative, investigation, decision-making, planning, and execution. It’s important to plan your career path accordingly during your higher studies to become employable.

1.1. Employability and Career Planning

I'm interested in a wide variety of areas of the software industry. For instance, machine learning, AI, blockchain, and many more. However, I'm more interested in full-stack development, java and Python programming, machine learning, and artificial intelligence. I want to work as a software engineer after earning my bachelor's degree in software engineering. Software engineers are the employees of software firms who build code to address the needs of clients. I'm concentrating on full stack development in the realm of software engineering. Front-end and back-end development are the two components of full-stack development. The back end, sometimes referred to as server-side scripting, is where the source code is not accessible to the client side. Front-end development is also referred to as client-side scripting, which users can see on the browser. Artificial intelligence and machine learning are two further technological fields that intrigue me. Machine learning and artificial intelligence (AI) will be employed in this situation since technology plays a significant part in the growth of the world and will eventually replace most of the manual tasks we perform now. ... Many individuals mistakenly believe that both locations are the same. Any technique that imitates human behavior is considered artificial intelligence. For instance, when we utilize AI in a self-driving car, we are specifying every possible scenario that might occur when the car is being driven on the road. When it comes to automated machines, machine learning refers to the creation of systems that can use their own failures to teach themselves the rules.

Students are required to select an optional module for level 5 of the course to study the field in which they hope to find employment in the future. Considering my professional goals and personal interests, I intend to select server-side web development. As I've already explained, back-end development also refers to server-side web development. We learned front-end development utilizing languages like HTML, CSS, and JavaScript in level 4 of the course. The fundamentals of Python and Java were also taught to us. To perfect my front-end

technologies, I'm also taking some private courses, which means I have made progress toward becoming a full-stack web developer.

I want to find a position where I can program both front-end and back-end so that it can be useful in my areas of interest in the third year, which is our internship period. Since learning never stops, I intend to enroll in level 6's optional curriculum, Advanced Server-side Web Programming. Because I believe it will help me greatly in developing my profession as a full-stack developer. I also intend to self-learn a few back-end technologies before my level 5 begins because they will help me achieve my goals.

I have made every effort to attend every event that my university has sponsored, even though it has only been a year since I started this degree. Hackathons, Google Hash Code, IEEEXtreme, seminars, and many more are a few examples. I was able to assess my performance level and my degree of knowledge in several areas thanks to these activities. Even though I was unable to participate in any activities this semester, I am confident that I will have the opportunity to do so the following one. However, after learning more about these events, I am aware of where I need to focus my efforts.

I intend to pursue a master's degree in machine learning and artificial intelligence after I complete my bachelor's degree in 2026 so that I can focus on developing new inventions that fascinate me. Like self-driving cars, there will be many more products that rely on AI and machine learning; thus, I think that choosing to pursue these two subjects would be a tremendous contribution to a brighter future and technological advancement. Finally, I'd want to say that I'd like to continue working as a software engineer and eventually advance to becoming a software engineer and a machine learning engineer.

Conclusion

In the end, everything points to the fact that to secure a career route and become employable, we must have a clear understanding of our future, increase our knowledge, and seize any chance to fortify our path.

References

1. Anna P, Theodore H.K, (2019), *Full Stack Web Development Teaching: Current Status and a New Proposal.* 218-225 Available from: https://www.scitepress.org/Papers/2019/80662/80662.pdf [Accessed 15 December 2022].
2. Antero T. et al, *Full Stack is not what it used to be.* Available from : https://design.inf.usi.ch/sites/default/files/biblio/icwe2021-fullstack.pdf [Accessed 15 December 2022]
3. Firoz K. et al , *(2021), The future of software engineering: Visions of 2025 and beyond*. Vol 11, 3443-3450 Available from: https://www.researchgate.net/publication/353623646_The_future_of_software_engineering_Visions_of_2025_and_beyond [Accessed 15 December 2022].

2. Quantum Computing

Introduction

World changes day by day so does technology. As a result of research conducted in IBM scientist have been successful to make Quantum computers to outsmart conventional computers. Quantum computer's performance is billion times faster than a conventional computer.

Comparison between quantum computers and conventional computers can lead to more interesting topics like QC's impact on security.

2.1. Quantum Computing

a quickly evolving technology referred to as quantum computing utilizes quantum physics principles to resolve difficult problems for conventional computers. One of the main sources of the quantum computer's processing power is the ability of bits to live in many states at once. Among the present centers of quantum computing research are the Los Alamos National Laboratory, MIT, IBM, Oxford University, and Oxford University.

Thanks to IBM Quantum, a technology that researchers had only just begun to imagine three decades ago is now accessible to hundreds of thousands of developers. With major software and quantum-classical orchestration improvements, our engineers regularly develop superconducting quantum processors with increasing power. This effort is advancing quantum computing, which has the potential to revolutionize speed and capacity.

2.2. How do quantum computers work?

Quantum computing utilizes subatomic particles like photons and electrons. Modern classic impulses' binary signals encode data as bits. Instead, operations in quantum computing create a qubit by using the quantum state of an object. These undefinable characteristics of an object, such as an electron's spin or a photon's polarization, are referred to as these states before the entity is acknowledged.

2.3. Conventional Computing

It alludes to the typical use of computing equipment. Typically, traditional computers handle two jobs. processing data in memory and producing outputs depending on the specifications by means of formulas, calculations, and algorithms.

Scientists and engineers use supercomputers to assist them with difficult tasks. Massive conventional computers known as supercomputers can have thousands of CPU and GPU cores. Strong classical computers typically struggle when presented with difficult problems to solve. Traditional computers commonly crash due to challenges that have multiple variables interacting in intricate ways.

2.4. Quantum computing vs Conventional computing

Simple quantum computers address problems that are too complex for regular computers by applying the principles of quantum physics.

Conventional computing	Quantum computing
Based on electrical circuits	Based on quantum mechanics
Low voltage or charge equals 0 and high charge equals 1, which determines the "bit" utilized for information storage and manipulation.	Information is stored and processed using quantum bits, commonly referred to as "qubits," which are based on the spin of an electron or the polarization of a single photon.
Takes billions of times to solve a complicated issue	These are the best for optimization of complicated issues
Traditional computers can function in a room temperature and have low error rates.	Due to their high mistake rates, quantum computers must be kept extremely cold.

Table 1 conventional vs quantum computing

2.5. Benefits and opportunities of Quantum computing

When used appropriately, quantum computers can be very speedy and helpful. They can perform calculations that would take modern supercomputers decades or perhaps millennia to complete. Scientists refer to this phenomenon as quantum supremacy.

For analysis and simulations of exceedingly complex systems involving enormous amounts of data, quantum calculations hold significant potential. Particularly the departments of natural sciences and digital marketing see great promise in this.

The greatest hope is that quantum computing would dramatically boost artificial intelligence (AI). These may then safely and successfully take over tasks like data analysis or forecasting in the future.

2.6. Impact of Quantum computing on computer security

Quantum computing has the potential to both benefit and harm information security. coding would have the biggest impact from quantum computing. Unlike traditional computers that employ algorithm number generators for coding. Quantum computers are good for cryptography since they are real random number generators. Unfortunately, a quantum computer's strength can also make it a deadly weapon in the hands of malicious people.

Conclusion

It can be concluded that quantum computing is the future of conventional computing, but it won't replace conventional computing as both quantum and conventional computing has its own specific performances.

References

1. Faroukh,Y.M.(2018). Quantum Computers Vs Conventional Computers: A Study on the Larger Scale, Sharjah Center for Astronomy and Space Sciences, University of Sharjah. Available from https://www.researchgate.net/publication/323993559_Quantum_Computers_Vs_Conventional_Computers_A_Study_on_the_Larger_Scale [Accessed 11 December 2022].

2. Barde, N., Thakur, D., Bardapurkar, P. and Dalvi, S. (2011). Consequences and Limitations of Conventional Computers and their Solutions through Quantum Computers. Leonardo Electronic Journal of Practices and Technologies, [online] 10(19), pp.161–171. Available from https://www.researchgate.net/publication/289608331_Consequences_and_Limitations_of_Co nventional_Computers_and_their_Solutions_through_Quantum_Computers [Accessed 12 December 2022].

3. Njorbuenwu,M.Swar,B and Zavarsky,P.(2019). A Survey on the Impacts of Quantum Computers on Information Security.*2019 2nd International Conference on Data Intelligence and Security (ICDIS).* South Padre Island, TX, USA. 28-30 June 2019.IEEE, 212-218. Available from https://www.researchgate.net/publication/336256881_A_Survey_on_the_Impacts_of_Quantum_Computers_on_Information_Security [Accessed 13 December 2022]

3. Internet of things and its cyber security implication

Introduction

Two of the most popular subjects are cyber security and the Internet of Things (IoT). The internet of things (IoT) is a system of linked devices that enables data transmission and reception. To protect data from hackers when IoT devices communicate over the internet, cybersecurity is essential. Perhaps the best example of IoT is your smart home, which connects your air conditioner, doorbell, smoke detectors, and security alarms to share data with the user via a smartphone application. Cybersecurity simply means protecting data from unauthorized access, which can have a range of detrimental impacts, including financial losses and a tarnished reputation.

3.1. Implications that are connected to IoT

Authenticity, authorization, confidentiality, and integrity are what they are. Programmers who ensure confidentiality make sure that the data can't be viewed or misused even if the gadgets fall into the wrong hands. The ongoing monitoring and updating of user data is referred to as data integrity. A server uses a process known as authentication and authorization to determine if a client is allowed access to the resources.

They are authenticity, authorization, confidentiality, and integrity. When a programmer ensures confidentiality, they make sure that even if the devices end up in the wrong hands, those persons can't read the data or use it improperly. Data integrity refers to the constant monitoring and updating of user data. A server assesses whether a client is permitted access to **the resources through a procedure known as authentication and authorization.**

3.2. IoT vs traditional internet

IoT technology has previously encountered issues. Several conventional network ideas gave rise to a new era of communications technology. The Internet of Things (IoT) can be viewed as an extension and expansion network based on the Internet, despite being separate from both traditional networks and the so-called Internet of people. The key difference between the Internet of Things and traditional networks is who is producing the material. In contrast to how content is consumed on the traditional internet, which is based on requests, the Internet of Things works by sending notifications or initiating actions when certain interest criteria are met. We may also say that traditional internet is based on the virtual world, whereas IoT is based on the real world.

As actual devices are not virtual, safeguarding them is one of the worst aspects of IoT security. Given that Internet of Things devices require human interaction, manufacturers must ensure that they as actual devices are not virtual, safeguarding them is one of the worst

aspects of IoT security. Manufacturers must ensure that IoT devices are built appropriately by default because they require human interaction to function. IoT devices and services that fall short of industry standards could be a significant risk vector. These could pose a challenge to the ability of IoT services to survive. For instance, devices that are ill-made, out-of-date, or counterfeit pose very real threats to IoT-enabled systems. Another significant cyberattack that targets IoT devices with inadequate security measures is ransomware. In ransomware, the user's data is not misused; rather, the user is contacted and asked to pay the ransom. Because not every user of a smart device can afford to pay ransom demands made by hackers, this puts them at danger and puts them in a difficult situation. Mobile phones, intelligent wearables, and many more devices are among those targeted by ransomware. Users can take precautions by using complicated passwords to make it more difficult for hackers to access our data.

Conclusion

I would like to draw the conclusion from the facts stated above that it would be highly appreciated by the customers who are purchasing the desired goods and having their wants met if a program or application was created employing various online security and other security measures. It is not how the application was programmed, but rather how well the user uses the application. As more and more new technology is developed and user-created defects are discovered, we may anticipate a progressive increase in security consequences soon. As a result, we should be aware of the issues we are facing.

References

1. Mirza A, et al. (2017)*Security Issues on the Internet of Things (IoT): A Comprehensive Study*. Vol 8, 383 -388. Available from : https://thesai.org/Downloads/Volume8No6/Paper_50-Security_Issues_in_the_Internet_of_Things.pdf [Accessed 10 December 2022].
2. Muhammad S, (2017) *CYBER SECURITY AND INTERNET OF THINGS.* Vol 7, 77-96 . Available from: https://www.researchgate.net/publication/324982960_CYBER_SECURITY_AND_INTERNET_OF_THINGS [Accessed December 11 2022].
3. Samuel T, Knud E, Reza T, (2017) *Cyber Security Threats to IoT Applications and Service Domains.* Available from: https://www.researchgate.net/profile/Samuel-Tweneboah-Koduah/publication/317283254_Cyber_Security_Threats_to_IoT_Applications_and_Service_Domains/links/5ab50b510f7e9b68ef4be69c/Cyber-Security-Threats-to-IoT-Applications-and-Service-Domains.pdf [Accessed December 7 2022].
4. Zainab H, Hesham A, Mahmoud M, (2015) *Internet of Things(IoT): Definitions, Challenges and Recent Research Directions.* Vol 128, 37-47. Available from : https://www.researchgate.net/publication/320532203_Internet_of_Things_IoT_Definitions_Challenges_and_Recent_Research_Directions [Accessed 7 December 2022].
5. Hassan,Q.(2018). *Internet of Things A to Z: Technologies and Applications.* Available from https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119456735.ch1[Accessed 10 December 2022]