Informatics Institute of Technology

Trends in Computer Science

4COSC008C

Coursework II: Portfolio

Mohamed Akram Gazali

UOW Number - w1956088

IIT Number - 20221038

Employability and career planning- Reflective writing

Contents

Employability and career planning- Reflective writing

1. Introduction

As a future student interested in a career in web development, I understand the importance of career planning to succeed in this field. It involves setting goals and identifying my interests in web development, acquiring the necessary skills and experience, and finding job opportunities that align with my career aspirations. I will also have to stay up-to-date on industry trends and continuously learn and adapt to new technologies to stay competitive in the job market. With careful planning and dedication, I am confident that a career in web development can be rewarding and fulfilling.

The TCS module has been extremely helpful in my career planning. For instance, I have been able to learn about new programming languages and frameworks that are in high demand in the job market, which I believe would help me to take informed decisions about my education and career path. Additionally, by keeping track of trends in different applications and industries, such as machine learning or cybersecurity, I have been able to focus my studies and career goals in areas that are likely to be in demand in the future.

2. Selection of Optional Modules

The future for web developers looks bright, as the demand for web development skills is expected to continue growing in the coming years. According to the US Bureau of Labor Statistics, employment of web developers is projected to grow 8% from 2020 to 2030, faster than the average for all occupations. In addition to traditional web development, there is also growing demand for developers with skills in emerging technologies such as cloud computing, artificial intelligence, and the internet of things. Therefore, I'm planning to select server-side web development and mobile application development as my level 5 optional modules. Server-side web development involves building and maintaining the back end of a website or web application, including the server infrastructure, database management, and server-side scripting. Mobile application development, on the other hand, involves creating applications for mobile devices, such as smartphones and tablets. [1]

Furthermore, I have always been an admirer of apple products due to their user experience and design. I would love to design and develop applications for apple using the swift programming language. Therefore, I believe that selecting advanced server-side web programming and mobile native application development will be the most suitable choice as my level 6 optional modules. Advanced server-side web programming involves developing complex, high-performance web applications using advanced techniques and technologies. Mobile native application development involves creating applications specifically for a particular mobile platform, such as iOS or Android. [2]

By gaining expertise in both of these areas, I can broaden my skillset and become more versatile as a developer, which can make me more attractive to potential employers and increase my job opportunities.

3. Employability events

In addition to my coursework, I have also attended several employability-related events to help me prepare for my future career. For example, I recently attended a careers fair where I had the opportunity to network with professionals from a variety of companies and learn more about potential job opportunities. I also participated in a workshop on resume building and interview skills, which helped me to improve my job search strategies and better understand what employers are looking for in potential hires.

I've also come to understand the significance of obtaining applicable certificates and credentials. These qualifications are highly valued by many IT organizations and may be an important tool for proving your knowledge and ability to prospective employers.[3]

4. Further steps for the future

Looking ahead, there are a few further steps that I need to take to prepare for my future career as part of my studies. First, I plan to continue building my technical skills through coursework and hands-on projects. I also plan to seek out internships or part-time jobs in the field to gain practical experience and develop a stronger understanding of the industry. Finally, I will continue to network with professionals and stay up-to-date with industry trends and developments through events, conferences, and online resources.

5. Conclusion

The research which was involved in the TCS module has given me insights into the two emerging and exciting fields which are machine learning and quantum computing were able to give me a positive impact on my career planning. It changed my perspective and gave me a new approach to reconsidering my specialization and pathway for my future. Since I’m a first-year student I know I have a lot more learning gaps to be filled and eventually once I discover and learn more, I will be able to choose an exciting pathway that I love and perhaps will keep me motivated to work every day.

In conclusion, trends in computer science had a significant impact on my career planning. By focusing on specific specialisms and taking relevant coursework, attending employability-related events, and staying up-to-date with industry trends, I am confident that I can build a successful and fulfilling career in the field of computer science.

Word count: 828 words

6. References

[1] “Software Developers, Quality Assurance Analysts, and Testers: Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics,” Software Developers, Quality Assurance Analysts, and Testers : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics, Sep. 09, 2022. https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm (accessed Dec. 16, 2022).

[2] “Introduction to the server side - Learn web development | MDN,” Introduction to the server side - Learn web development | MDN. https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Introduction (Accessed Dec. 19, 2022).

[3] V. Kruglyk and V. Osadchyi, “Preparation of future web developers to knowledge certification and employment in universities of Ukraine,” Information Technologies in Education, no. 23, pp. 7–21, Jul. 2015, doi: 10.14308/ite000531. (Accessed Dec. 17, 2022).

QUANTUM COMPUTING

Contents

1. Introduction

Quantum computing represents a significant advance in the field of computing, with the potential to revolutionize a wide range of industries and applications. The birth of quantum computing can be traced back to the early 1980s when the first theoretical proposals for quantum computers were developed. Since then, significant progress has been made in the development of quantum hardware and algorithms, paving the way for the emergence of practical quantum computing systems.

In this report, we will explore the basics of quantum computing, including how it differs from conventional computing, the new opportunities, benefits, and the impact it might have on computer security in the future.

2. What is Conventional computing?

Conventional or classical computing refers to the use of computer hardware and software to perform tasks such as storing, processing, and retrieving data. It involves the use of computer programs that are written in a specific programming language and executed by a central processing unit (CPU) in a computer. Classical computing systems are based on the use of bits, which are digital units of information that can have a value of either 0 or 1. (Van Meter, 2014)

3. What is Quantum computing?

Quantum computing is defined as "Quantum computing is a type of computing that uses quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. It is based on the principles of quantum mechanics, which is a branch of physics that deals with the behavior of matter and energy at the atomic and subatomic levels ". Quantum computers are used to solve problems that are too complex or too time-consuming for classical computers to handle. Anon (2021)

4. Key differences between quantum and conventional computing

In a quantum computer, data is stored in quantum bits, or qubits, which can represent both 0 and 1 simultaneously. Superposition refers to the ability of a quantum system, such as a qubit, to exist in multiple states simultaneously. This is in contrast to classical systems, which can only exist in a single state at any given time. "Superposition allows quantum computers to perform multiple calculations at the same time, potentially making them much faster than classical computers for certain tasks". (Gyongyosi and Imre, 2019)

Entanglement is a phenomenon in which the quantum states of two or more particles are correlated, even when the particles are separated by large distances. This allows the quantum states of the particles to be correlated and manipulated, potentially allowing for faster and more efficient computation than is possible with classical systems. (Gyongyosi and Imre, 2019)

5. Opportunities

5.1 Optimization and machine learning

Quantum computers can use quantum algorithms to find the global minimum of a function more efficiently than classical computers, making them potentially useful for tasks like optimization and machine learning.

5.2 Drug discovery and materials design

Quantum computers can help with tasks like identifying potential drugs and designing new materials by simulating the properties of molecules and materials at a quantum level.

5.3 Artificial intelligence

Quantum computers could potentially be used to improve the performance of artificial intelligence algorithms by allowing them to process and analyze more data efficiently.

6. Benefits

Quantum computers can perform certain calculations much faster than classical computers, which could allow them to solve problems that are currently impractical or impossible to solve with classical computers. For example, quantum computers can use quantum algorithms like Shor's algorithm to factorize large numbers much faster than classical computers, which could be used to break modern encryption methods (Bhatia and Ramkumar, 2020). Furthermore, due to the faster calculations quantum computers can immensely help with increased precision, real-time analytics, enhanced optimization, and improved machine learning.

7. Security

Quantum computing could have significant implications for cybersecurity. One of the main ways in which quantum computing could impact computer security is by enabling the breaking of modern encryption methods. Quantum computers can use quantum algorithms like Shor's algorithm to factorize large numbers much faster than classical computers. (Preskill, 2018).

On the other hand, quantum computing could also provide new opportunities for enhancing computer security. For example, quantum computers could be used to design new, more secure encryption methods that are resistant to quantum attacks. In addition, quantum computers could be used to perform complex risk analyses and simulations to help identify and mitigate potential security vulnerabilities (Sharma and Ketti Ramachandran, 2021).

8. Conclusion

In conclusion, quantum computing and classical computing are two distinct approaches to computation that have their strengths and weaknesses. Quantum computers have the potential to solve certain problems much faster than classical computers, but they are also more expensive and difficult to build and maintain. Classical computers, on the other hand, are more widely available and easier to use, but they are limited in their ability to solve certain types of problems. Overall, it is likely that both types of computers will continue to play a role in the field of computation, depending on the specific needs of a given problem.

Word count: 822 words

9. References

Anon (2021). Quantum Computing Fundamentals Addison-Wesley Professional. Available from

https://learning.oreilly.com/library/view/quantum-computing-fundamentals/9780136793830/

[Accessed 06 December 2022].

Van Meter, R. (2014). Quantum Computing’s Classical Problem, Classical Computing’s Quantum Problem. Foundations of Physics, 44 (8), 819–828. Available at https://doi.org/10.1007/s10701-014-9807-z.

Gyongyosi, L. and Imre, S. (2019). A Survey on quantum computing technology. Computer Science Review, 31, 51–71. Available at https://doi.org/10.1016/j.cosrev.2018.11.002. [Accessed 18 December 2022].

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. Available at https://doi.org/10.22331/q-2018-08-06-79. [Accessed 18 December 2022].

Sharma, N. and Ketti Ramachandran, R. (2021). The Emerging Trends of Quantum Computing Towards Data Security and Key Management. Archives of Computational Methods in Engineering, 28 (7), 5021–5034. Available at https://doi.org/10.1007/s11831-021-09578-7. [Accessed 18 December 2022].

Bhatia, V. and Ramkumar, K.R. (2020). An Efficient Quantum Computing technique for cracking RSA using Shor’s Algorithm. 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA). Available at https://doi.org/10.1109/iccca49541.2020.9250806. [Accessed 18 December 2022].

INTERNET OF THINGS

Contents

1. Introduction

IoT is a system of devices that can communicate and share data and with other systems over the internet. The IoT has the potential to bring significant benefits and efficiencies, such as improved communication and automation, reduced costs and energy consumption, and enhanced safety and security. However, the IoT also raises significant cyber security concerns due to the large number of devices that can be targeted and the sensitive data that can be accessed.

In this report, we will explore the Internet of things (Iot), the difference between IoT and the traditional internet, the cyber security issues of these devices, and how these issues can be resolved.

2. Iot and the traditional Internet

Traditional internet refers to the global network of interconnected computers that allows for the exchange of information and communication through various devices such as laptops, smartphones, and tablets, On the other hand, the Internet of Things (IoT) refers to the interconnected network of physical objects that are equipped with sensors, software, and other technologies that allow them to collect, share, and exchange data. While the traditional internet relies on human intervention to access and transmit data, IoT relies on machine-to-machine communication to collect and share data automatically. This difference is significant because it allows IoT to provide a wide range of services, including automation, real-time monitoring, and predictive maintenance, which are not possible with traditional internet. Traditional internet is primarily used for communication and information exchange, IoT utilizes connected devices to gather and share data for various applications. [1]

3. Iot and its cyber security issues

One of the biggest and most well-known IoT attacks in history is the Mirai botnet attack, which occurred in 2016. The Mirai botnet was a network of infected IoT devices, such as routers, cameras, and DVRs, that were used to launch distributed denial of service (DDoS) attacks against websites and other online services.

One major concern is the potential for IoT devices to be compromised and used as entry points for cyber-attacks. These devices often have weak security measures, making them vulnerable to hacking and malware infections [2]. For example, a hacker could gain access to a smart home system and use it to gather personal information or to control devices within the home. Similarly, an attacker could compromise a connected car or medical device and use it to cause harm or disruption.

Another issue is the lack of standardization in IoT security. Many IoT devices are manufactured by smaller companies that may not have the resources or expertise to implement robust security measures [2]. This can lead to inconsistencies in the level of protection offered by different devices, making it difficult for users to assess the security of their IoT systems.

Furthermore, the complexity of IoT systems can make it difficult to detect and respond to security breaches. With many different devices and networks involved, it can be challenging to identify the source of a problem and to implement a fix [3]. This complexity is further exacerbated by the fact that many IoT devices cannot receive updates or patches, making it difficult to address vulnerabilities as they are discovered.

4. Solutions to these issues

To address these issues, several solutions can be implemented. First, there should be a focus on building secure IoT devices from the start, incorporating strong security protocols and regular updates [4]. This can be achieved through the implementation of industry standards and regulations, such as the ISO/IEC standards for information security management.

In addition, there should be a focus on educating users on the importance of securing their IoT devices and providing them with the necessary tools and resources to do so. This can include implementing using strong passwords and security tools such as firewalls and antivirus software.

Furthermore, a promising approach is the use of blockchain technology, which can provide a decentralized and secure platform for storing and exchanging data in the IoT. Blockchain can enable the creation of tamper-proof and transparent records of transactions and interactions, as well as provide a secure and efficient means of verifying and authenticating devices and data. [5]

By implementing these solutions, the security of IoT devices can be improved, protecting against potential attacks and breaches.

5. Conclusion

In conclusion, IoT has the potential to bring numerous benefits and it also poses significant cybersecurity risks. These risks include the potential for IoT devices to be compromised and used as entry points for cyber-attacks, the lack of standardization in IoT security, and the complexity of IoT systems making it difficult to detect and respond to security breaches. To address these issues, there should be a focus on building secure IoT devices and educating users on how to protect them, as well as implementing industry standards and regulations and utilizing security tools. Ensuring the security of these interconnected devices is crucial to protect against potential attacks and maintain the trust of users.

Word count: 813 words

6. References:

[1] K. J. Kim, “Interacting Socially with the Internet of Things (IoT): Effects of Source Attribution and Specialization in Human-IoT Interaction,” Journal of Computer-Mediated Communication, vol. 21, no. 6, pp. 420–435, Oct. 2016, doi: 10.1111/jcc4.12177.

[2] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of Things Security: Challenges and Key Issues,” Security and Communication Networks, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[3] S. A. Kumar, T. Vealey, and H. Srivastava, “Security in Internet of Things: Challenges, Solutions and Future Directions,” 2016 49th Hawaii International Conference on System Sciences (HICSS), Jan. 2016, Published, doi: 10.1109/hicss.2016.714.

[4] M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, “Internet of Things Security: A Survey,” 2018 International Conference on Advanced Science and Engineering (ICOASE), Oct. 2018, Published, doi: 10.1109/icoase.2018.8548785.

[5] Y. Abbassi and H. Benlahmer, “IoT and Blockchain combined: for decentralized security,” Procedia Computer Science, vol. 191, pp. 337–342, 2021, doi: 10.1016/j.procs.2021.07.045.