

UNIVERSITY OF
WESTMINSTER



INFORMATICS
INSTITUTE OF
TECHNOLOGY

Trends in Computer Science

Module: 4COS008C

PORTFOLIO

Abhinav Ratnathurai

w1904573

20211507

TABLE OF CONTENTS BOOKMARK

Contents.....	2
1. Employability and Career planning.....	3
2.	3
3. Artificial Intelligence (AI).....	5
Introduction.....	5
Impact on society.....	5
Applications of Artificial Intelligence.....	5
AI in Education.....	5
AI in Healthcare.....	6
AI in Finance.....	6
AI in Military.....	6
Conclusion.....	7
Reference.....	7
4. Internet of things (IoT) and cyber security implications.....	8
Introduction.....	8
Difference between IoT and traditional internet.....	8
Challenges created for cyber security.....	9
Solutions to overcome the challenges.....	9
Conclusion.....	10

1. Employability and Career Planning

The term "employability" has been around for a hundred years and is becoming more common. It finds a natural application in the context of job revival: it is recommended to increase a person's professional adaptability to many new occupations, or employability, rather than retaining them in their current position. I am willing to increase my skills by covering almost all the new technological aspects related to my main career, and these skills should be updated from time to time to establish myself in my future career. (Florent Noel, Geraldine Schmidt, 2022).

I'd like to pursue a potential specialization in the foundations of software engineering. To be a software engineer, I would learn all the hard skills, like learning Java, JavaScript, SQL, C++, C#, Python, and many more. Software engineers develop code, create charts and diagrams to graphically represent the product, and supervise a team of programmers in addition to doing these things. The demand for talented computer software engineers is rising. Engineers that specialize in computer software may work in practically any sector. I love accepting challenges and thinking of new, innovative ideas, and bringing them forward practically to the world. Creating new programs, making software, and engaging in group work with other software developers would encourage me and give me an energy boost to do my tasks productively and to be contemporary in this field.

- I'm planning to take the mobile app development optional module. This is because I prefer to create mobile software, and most mobile applications utilize a network connection to communicate with other computers. Today, every type of organization that comes to my mind is dependent on this sector, which is constantly expanding. I am very keen on some of the main categories of Mobile app development, which I believe would be much interesting as it involves the uses of HTML, CSS3, JavaScript, and so on, and would help throughout my future career.

Mobile app development may be divided into three categories:

1. Development of Native Apps:

When developing a native app, a developer makes an app specifically for an operating system, such as iOS or Android. It supports all of the functions that the OS offers and enables us to make the most of a mobile device's capabilities.

2. HTML5 and the Development of Web Applications:

Web applications are merely websites that offer the appearance and functionality of a real responsive website. They typically run in a browser and are written in HTML5, CSS, and JavaScript. Installing such an app only entails adding a bookmark to this website and designing

the resulting link as an app. They will adapt to the screen size of whichever device is called for since they are responsive.

3. Hybrid app development:

Half native apps and half online apps make up hybrid apps. They can take advantage of some native functionalities and be released via an app store. They rely on HTML shown in a browser because they are web applications as well. Despite having the appearance and use of native software, hybrid apps are just straightforward web applications that run in a browser. Without having to worry about creating two distinct applications, it lets the developers reach a bigger target audience and track how many people download their apps, among other things.

- I attended a presentation conducted by **Mr. Havindra Gunawardena**, who discussed the importance of employability and career planning. My understanding of his demonstration is that teamwork and communication are obvious examples of these employability skills, which are generic as opposed to job-specific, as opposed to professional or technical abilities. They are relevant to all job functions and working environments in all categories of industries. His key argument was that everyone should stay current in whichever field they choose, as this will help them advance along their chosen career path and accomplish more and more.

Additional actions I'd like to take while I'm a university student to support my job in the future include:

1. I am taking advantage of opportunities within my studies to develop employability skills, such as group project work, presentations, student exchange programs, internship subjects, industry and community project units, and mentoring programs.
2. I will participate in extracurricular activities like clubs and societies, sports, public speaking, special interest groups, or community activities because these opportunities will also help me demonstrate my skills in job applications.
3. Whenever possible, I would like to gain work experience through internships, vacation work, and volunteer work for not-for-profit organizations.
4. I will keep a log of my employment history, volunteer positions, and extracurricular pursuits. Make a note of the abilities acquired and the attributes displayed. A mass of testimonials from colleagues and lecturers that support your accomplishments and results, and add them to my portfolio.

REFERENCE

Florent Noel, Geraldine Schmidt. (2022). **Employability and Industrial Mutations Volume 4**. John Wiley & Sons, Inc. 111 River Street Hoboken, NJ 07030 USA. [Wiley-ISTE](https://learning.oreilly.com/library/view/employability-and-industrial/9781786307439/). Available from <https://learning.oreilly.com/library/view/employability-and-industrial/9781786307439/>. [Accessed 25.07.2022].

2. Artificial Intelligence

With the development of artificial intelligence, the quest to build intelligent computers that mimic human activity has intensified. Recent developments in computer science have led to an explosion of definitions and explanations of what constitutes AI systems. As an example, "the capacity of a digital computer or computer-controlled robot to do activities generally associated with intelligent individuals" is how AI has been defined. AI systems are gaining ground across a range of sectors, including healthcare, education, communications, transportation, agriculture, and more. Today's modern world requires frequent interaction with artificial intelligence (AI)-powered software. (Selin Akgun, Christine Greenhow, 2021).

IMPACT ON SOCIETY

The productivity of our workplaces may be significantly increased by artificial intelligence, which can also help humans accomplish more work. By customizing them for a specific individual or situation, AI may assist in enhancing the effectiveness and quality of public services and products. AI has the potential to significantly advance our knowledge of illness and medicinal interventions. AI systems can currently execute a variety of particular healthcare-related activities better than human experts.

To enable more time for planning and legislation, AI can help with early warning systems for hazards like disease epidemics.

Resource management may be improved by AI-based modeling of complex systems, which may be especially crucial for reducing the consequences of climate change.

AI can assist in determining the present challenges that have the most effective solutions, as well as enhance our understanding of the problems and the science required to tackle them. (Jess Whittlestone, Sam Clarke, 2022).

Applications of Artificial Intelligence

Artificial Intelligence in Education:

The majority of artificial intelligence (AI) in education has been centered on online systems or information technology, including intelligent tutoring systems, intelligent virtual laboratories, and intelligent assessment systems. It could improve students' mechanical and spatial comprehension of actual building processes in classes. IoT technology can imitate brain processes in a physical environment to perceive and comprehend people's cognitive behaviors, which appears to improve human cognition and performance. It was evident that AI has advanced significantly in recent years, mostly as a result of more affordable processing and data availability. Nevertheless, student data may be disclosed, shared, or utilized improperly. How we acquire, assess,

and disseminate large amounts of data and the findings of data analysis will always be a problem for educators and AI programmers.

AI in healthcare:

Clinical trials with AI support manage a lot of data and deliver very precise results. It has cost a lot of effort and money to do this. But the success rate is really low. Therefore, clinical trial automation has demonstrated value for AI and the healthcare industry. Artificial intelligence has an impact on patient outcomes in healthcare. Medical AI companies develop systems that support patients on all levels. A proposed method for detecting high-risk mothers and lowering maternal mortality and postpartum complications is as follows:

- a) Using artificial intelligence and electronic health data, determine whether expectant mothers are significantly at risk of complications during delivery (AI).
- b) Using digital technologies to increase patient access to routine and care routines (i.e., more complex and frequent treatment) during pregnancy.

The Application of AI in Entertainment:

The reason why music and video streaming services succeed is that they provide material for people of all demographics with a variety of likes and preferences. These businesses utilize machine learning and AI algorithms to assess user performance and demographics to encourage consumers' preferences for watching or listening closely while maintaining their regular involvement. Screenwriting, location scouting, creating shot lists, storyboarding, budgeting, recording, scheduling, and editing are just a few of the numerous techniques needed for movie production. AI can provide a platform that can accomplish all these tasks. (Xuesong Zhai et al., 2021).

Application of AI in Finance:

With the development of general artificial intelligence (GAI), economics and finance have grown more dynamic and integrated in recent decades. Financial judgments, quantitative trading, and financial risk management are just a few of the operations that AI helps the financial sector expedite and improve.

Implementing AI in banking has enormous advantages for work automation, fraud detection, and providing individualized suggestions. The following AI use cases in the front and middle office can revolutionize the financial sector:

- Ensuring flawless, week-long customer interactions.
- Minimizing the need for tiresome effort.
- This reduces cognitive mistakes and misleading results. (Longbing Cao, 2020).

CONCLUSION

A greater understanding of the distinctions between artificial intelligence (AI) and human cognition is necessary to better prepare for the society of the future, in which AI will have a far more pervasive impact on our lives. The most pronounced differences between human intelligence and animal intelligence are seen in social and metacognitive abilities. Even while technological advancements are expected to make AI work better, it will still be a product of human action.

REFERENCES

Jess Whittlestone, Sam Clarke. (2022). **AI Challenges for Society and Ethics. Computers and Society. 2-4. Available from** <https://doi.org/10.48550/arXiv.2206.11068>. [Accessed 26.07.2022]

Longbing Cao. (2020). **AI in Finance: A Review. 3-5. Available** from <https://ssrn.com/abstract=3647625>. [Accessed 27.07.2022]

Selin Akgun, Christine Greenhow. (2021). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics. 1-5. Available from* <https://doi.org/10.1007/s43681-021-00096-7>. [Accessed 26.07.2022]

Xuesong Zhai, Xiaoyan Chu, Ching Sing Chai, Morris Siu Yung Jong, Andreja Istenic, Michael Spector, Jia-Bao Liu, Jing Yuan, and Yan Li. (2021). A Review of Artificial Intelligence (AI) in Education from 2010 to 2020. 12-13. Available from <https://doi.org/10.1155/2021/8812542>. [Accessed 26.07.2022]

3. Internet of Things (IoT) and cybersecurity implications.

INTRODUCTION

The network of physical objects commonly referred to as things, such as appliances, cellphones, cars, streetlights, infrastructure components, industrial machinery, and so forth, is known as the Internet of Things (IoT) (the T in IoT). The Internet of Things (IoT) today consists of physical objects that have some level of intelligence and computing power built into them, as well as the means that allow them to connect to the Internet ecosystem and the entire Internet's computing infrastructure, including computers and user devices. Because they are situated at the center of two heterogeneous items—physical objects and digital systems—these platforms are frequently referred to as middleware software. To complete the work, middleware typically combines high and low-level logic, as well as high and low-level languages. The advancement of the industry is due to the convergence of various technologies, including machine learning, ubiquitous computing, widely accessible sensors, and sophisticated embedded systems. The Internet of Things (IoT) network consists of browser internet of things devices' technology, including processing, sensing, and communication methods, to acquire, exchange, and rely on the data they learn from their surroundings. IoT devices link to IoT gateways or other edge devices, which either send data to the cloud for analysis or analyze it locally, to convey the sensor data they receive. These gadgets periodically converse with other gadgets that are similar to them and act on the information they share. Even though individuals may engage with the devices to set them up, give directions, or retrieve data, the devices do the majority of the work without the users' help. (Anand Tamboli, 2022).

What is the distinction between IoT and traditional Internet?

The foundation for the principles is what distinguishes the Internet of Things from the Internet of Everything. Physical items are the main focus of the Internet of Things. The four components that make up the Internet of Everything are individuals, objects, information, and operations. Our daily lives now include the Internet of Things. It consists of "smart" linked gadgets like:

- Network automobiles
- Home helpers with voice recognition
- Workout monitors
- Ambient air gauges.

The Internet of Everything, which offers applications for every industry, expands these common uses. Here are several examples: Manufacturing can use sensors for equipment monitoring and predictive maintenance to reduce downtime and the expenses associated with inefficiencies. To track consumption and seek methods to cut expenses, municipalities can employ smart meters in residential and commercial buildings to monitor water and power usage. Delivery schedules and routes may be optimized by logistics businesses using the sensors and gadgets aboard delivery vehicles to lower costs and increase customer satisfaction.

Challenges created for Cybersecurity

IoT device security entails defending the system and its users from illicit internet connectivity from both inside and outside the network. Vulnerabilities impact the services, the gadget, the user's data, and their persona.

IoT sensor data, IoT devices, the prevalence of IoT sensors, network interfaces with IoT, and several other sources are among the sources of cybersecurity concerns.

IoT security issues and dangers originate from connectivity. Wireless connection, processing capacity, and low-power capabilities all suffer from a lack of human interaction.

Data confidentiality is a significant source of security challenges for IoT devices and services. Users of IoT devices and sensitive data should be shielded against unauthorized access.

Among the causes of security threats and concerns are improper updating, a lack of security procedures, and user ignorance. (Chukwuere, Joshua, 2022).

Solutions to overcome the challenges

Monitoring and control:

This procedure entails keeping an eye on hardware and software to detect potential risks and weaknesses. Threats may be avoided and detected with the help of this technique.

Software upkeep: IoT device owners should regularly update their software timely. By doing so, security features will be improved and vulnerabilities will be reduced.

Data security:

Every device linked to an IoT network is vulnerable. Therefore, it is necessary to identify and regulate security against unauthorized access and modification. To provide authentication and identifiable access to private data and information to protect user privacy and access. Every IoT-connected device must use encryption for data transmission over the internet.

Stop data management:

Look for any unauthorized personal information and restrict connections to networks and IoT devices.

Incident detection:

This entails identifying cybersecurity problems early using appropriate and ongoing network analysis.

Privacy Breach Detection:

IoT cybersecurity and cyberspace should be monitored to find any privacy breaches. Indication of security breaches caused by outside hackers that want to compromise customers' privacy.

Conclusion

The idea behind the Internet of Things is to connect the physical world of things with the digital world of information technology. The IoT has the potential to significantly expand access to information and is expected to change businesses and organizations across almost every industry.

REFERENCE

Anand Tamboli. (2022). Build Your Own IoT Platform: Develop a Flexible and Scalable Internet of Things Platform 2 ed. Apress. Available from <https://learning.oreilly.com/library/view/build-your-own/9781484280737/>. [Accessed 26.07.2022]

Chukwuere, Joshua. (2022). Internet of Things (IoT) Cybersecurity Challenges and Mitigation Mechanisms. 4. 235-240. Available from https://www.researchgate.net/publication/360016691_Internet_of_Things_IoT_Cybersecurity_Challenges_and_Mitigation_Mechanisms. [Accessed 26.07.2022]