Unit 6: The Great Debate: The Future of the Internet

1. Describe how a number of alternative next-generation internet solutions will operate.

The term "Future Internet" describes the new Internet frameworks created to make way for the Internet's next generation. The internet is complicated to control because of the increase in internet traffic. Conflicts between the internet's stakeholders will significantly impact its future architecture (Mohammed & Ralescu, 2023).

According to Overton (2017), due to antiquated protocols like TCP/IP, the existing internet has constraints that affect mobility, IP address management, and quality of service. The next-generation internet should address the limitations.

The internet has revolutionised the global way we connect and access services. New network architectures are required to combat network distortions as internet users rise. Edge computing and 5G networks are examples of technologies improving machine-to-machine communication. Platforms must compromise between allowing people to express themselves freely and blocking offensive or dangerous content while managing user-generated content online. Firewalls, encryption, and robust security measures are necessary to address the critical concerns of privacy and security. Increasing mobile device energy efficiency is essential. Virtual testbeds promise a more efficient, private, and secure internet in the future by enabling the testing and validation of innovative internet architectures before deployment (Mohammed & Ralescu, 2023).

Many Next Generation Internet (NGI) solutions are under development to address these problems and offer a user-centric, scalable, and secure experience. Emerging and future technologies include a wide range of state-of-the-art products in data and algorithms, computer and communication resources, and applications (Research and

Innovation, 2020). For instance, here are some notable examples of the future and emerging technologies:

- One example is the creation and application of nano- and bio-nano-things and networks; they can completely transform computation and communication methods.
- A growing interest is paid to quantum computing and communications, particularly hardware security and quantum information networks, to create post-quantum secure systems.
- Researchers are also looking into the possibility of using terahertz waves for high-speed, high-capacity communication in an area that is gaining interest: extreme THz communications. For future technologies to operate safely and securely, fundamental anonymity and security support must be provided for all network elements and functions.
- Finally, neuromorphic hardware is being developed for edge-based low-power and low-latency event-based artificial intelligence (AI), which might significantly enhance AI systems' functionality and energy efficiency.

2. Explain how these solutions address key challenges.

As technology advances, IP networks encounter obstacles such as attacks and IP address depletion. Innovative Internet architecture is being developed to meet the increasing demands for security, mobility, and distributed networking. These projects include data networking, Content-Aware Searching Retrieval and streaming, MobilityFirst, and expressive Internet Architecture. The objective is to shift from host-centric networks to content-centric, mobility-centric, or service-centric networks. Nevertheless, these designs present challenges regarding network security and scalability, control, and isolation (Ding et al. 2016).

The current state of the internet is facing several obstacles affecting its functionality, security, accessibility, and equity. To ensure a secure, fair, and accessible online experience, we must address these challenges promptly (Ray, 2023).

Dadhich (2023) notes that the internet has significantly changed communication and business conduct. However, the current centralised approach has raised concerns about privacy, security, and content regulation. Decentralisation aims to distribute power, data, and computational resources across a vast network of nodes, creating a more secure and democratic online ecosystem. Therefore, the Internet has become an essential aspect of our daily lives. Still, it encounters various challenges that need to be addressed to continue being a valuable tool for people globally. One of the most significant issues is centralisation, where a few dominant companies control most infrastructure and data, making the Internet vulnerable to outages, censorship, and data breaches (Stansberry et al., 2019).

Regarding security challenges, Yaacoub et al. (2023) highlight that the open protocols on which the internet depends make it a target for cybercriminals. Software and hardware vulnerabilities can be exploited to steal data, commit identity theft, and cause financial losses.

Concerning privacy, which is also a significant concern, the current internet is based on a system of surveillance and data collection, raising concerns about user privacy and the potential for misuse of personal information (Quach et al., 2022).

In addition, the internet's architecture does not promote innovation, making it difficult for new players to enter and develop new applications. This lack of innovation hampers progress and limits the internet's potential (Amour, N.D.).

Fortunately, emerging alternative next-generation internet solutions can address these challenges. Decentralisation can improve resilience and privacy, while blockchain can enhance security and data transparency. Programmability can lead to more personalised and efficient internet usage, while cognitive intelligence can make the internet more user-friendly and intuitive. By addressing these challenges, we can create a more secure, decentralised, and innovative Internet that serves the needs of people worldwide.

For example, Rawat & Reddy (N.D.) proposed the Software-defined networking (SDN) paradigm, which offers high flexibility and ease through centralised control, allowing for network programming that adapts network parameters in real-time to optimise resource utilisation and performance. Additionally, SDN provides enhanced security, energy efficiency, and network virtualisation.

References:

- Mohammed, S.A. & Ralescu, A.L. (2023). Future Internet Architectures on an Emerging Scale—A Systematic Review. *Future Internet*, [online] 15(5), p.166. doi:https://doi.org/10.3390/fi15050166.
- Overton, D. (2017). *Next Generation Internet Initiative – Consultation.* Available at: https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf [Accessed 20 Dec. 2023].
- Mohammed, S.A. & Ralescu, A.L. (2023). Future Internet Architectures on an Emerging Scale—A Systematic Review. *Future Internet*, [online] 15(5), p.166. doi:https://doi.org/10.3390/fi15050166.
- Research and Innovation (2020). *Draft proposal for a European Partnership under Horizon Europe Smart Networks and Services*. [online] Available at: https://research-and-innovation.ec.europa.eu/system/files/2020-07/ec_rtd_he-partnership_smart-networks-services.pdf.
- DING, W. YAN, Z. & DENG, R. H. (N.D.). *Shibboleth Authentication Request*. [online] Available at: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=7526334 [Accessed 20 Dec. 2023].
- Ray, P.P. (2023). Web3: A comprehensive review of background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*. doi:https://doi.org/10.1016/j.iotcps.2023.05.003.
- Dadhich, D. (2023). *Embracing the Decentralized Internet: A Paradigm Shift towards an Equitable and Resilient Digital Ecosystem*. [online] Available at: https://www.linkedin.com/pulse/embracing-decentralized-internet-paradigm-shift-towards-dadhich/ [Accessed 20 Dec. 2023].
- Rawat, D. B. & Reddy, S. R. (N.D.). *Shibboleth Authentication Request*. [online] Available at: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/7593247 [Accessed 20 Dec. 2023].
- STANSBERRY, K., ANDERSON, J. & RAINIE, L. (2019). *5. Leading concerns about the future of digital life*. [online] Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/2019/10/28/5-leading-concerns-about-the-future-of-digital-life/.
- Yaacoub, J.-P.A., Noura, H.N., Salman, O. and Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, [online] 3. doi:https://doi.org/10.1016/j.iotcps.2023.04.002.
- Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, [online] 50(1). doi:https://doi.org/10.1007/s11747-022-00845-y.
- Amour, L. (n.d.). *The Internet: An Unprecedented and Unparalleled Platform for Innovation and Change*. [online] Available at: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2012-chapter10.pdf.