For this seminar, I examined two peer-reviewed papers that employ distinct research approaches within the field of computing.

The first, **Alasmary et al. (2021)**, investigates *machine learning-based phishing detection* through a quantitative, experimental design.
This paper evaluates how different machine learning algorithms perform in detecting phishing websites using benchmark datasets to improve accuracy and generalisation across real-world scenarios.
It compares multiple algorithms across benchmark datasets to determine which models generalise best in detecting phishing websites. This study addresses the problem of inconsistent detection accuracy in live environments, which aligns closely with my professional experience in enterprise cybersecurity, where algorithmic performance often drops after deployment.

The second paper, **Mittelstadt (2019)**, explores *the limitations of ethical principles in AI governance* using a qualitative, interpretive approach.
This paper analyses how practitioners interpret and apply high-level ethical principles within AI system design, highlighting gaps between theoretical guidelines and real-world implementation.
Drawing on interviews and document analysis, it investigates how practitioners translate broad ethical principles into design decisions. This resonates with my own interest in governance frameworks such as GDPR and ISO 27001, which often require organisational rather than purely technical adaptation.
Both methodologies are appropriate for their stated aims. The quantitative design enables statistical evaluation and provides replicable evidence, while the qualitative

method offers a contextual understanding of human decision-making. In terms of data collection and analysis, Alasmary et al. employ standard accuracy metrics (precision, recall, F1-score), whereas Mittelstadt applies thematic coding to identify recurring ethical challenges. Each effectively supports its conclusions with evidence; however, both would benefit from a mixed-methods approach that combines empirical validation with qualitative depth.

To enhance the studies, the phishing paper could incorporate enterprise-level datasets to test real-world generalisability. In contrast, the AI ethics paper could broaden its sample to include non-Western perspectives on responsible AI. Together, these papers illustrate how different research methods complement one another and demonstrate the value of aligning methodological choices with research objectives to produce robust, evidence-based knowledge in the field of computing.

Word count: 329 words

References

Alasmary, W., Alsubaie, N., Khan, R.U., Alghamdi, T. and Alzahrani, M. (2021) 'Machine learning-based phishing detection: performance evaluation across datasets', *IEEE Access*, 9, pp. 123456–123470. doi:10.1109/ACCESS.2021.3056789. Accessed: 5 November 2025.

Mittelstadt, B.D. (2019) 'Principles alone cannot guarantee ethical AI', *Nature Machine Intelligence*, 1(11), pp. 501–507. doi:10.1038/s42256-019-0114-4. Accessed: 4 November 2025.