Unit 3 Seminar – Title: Peer Review Activity

In this seminar, we will be focusing on LO 3: “Evaluate critically existing literature, research design and methodology for the chosen topic.” One way this is done is by conducting a peer review of existing literature on a particular subject.

In preparation for this week’s seminar, you will need to source at least 2 papers in a Computing subject of your choice (AI, Cybersecurity, Data Science, or a general interest topic in Computer Science), provided they utilise two different types of research methods to achieve their goal/research aims. Now answer the following questions (please provide justifications for your answers) and be prepared to discuss them in the session:

- Familiarise yourself with the purpose, problem, objective or research question of each paper. Are they in line with your experience or thoughts on the topic, contributing to the collective body of knowledge in this area?
- Is the research methodology utilised in each paper appropriate for the stated purpose or question?
- In terms of data collection and analysis, is this also appropriate for the stated purpose or question? (We will discuss this further in upcoming units.)
- Does each paper support its claims and conclusions with explicit arguments or evidence?
- How would you enhance the work/paper?

Let's start with the first paper, a quantitative survey on Online Security Practices by Zhou et al. (2016). This paper focuses on the challenges service consumers face when choosing a web service, particularly regarding security. It also evaluates the current methods for comparing web services and explores potential future directions in this field.

The second paper, by Hassanzadeh et al. (2021), is a study that illuminates the fundamental understanding of data breaches among 35 participants. This paper adopts a qualitative approach to highlight gaps in understanding system vulnerabilities, causes, consequences, prevention methods, and subsequent steps, emphasising the necessity for enhanced communication.

1. **Familiarise yourself with the purpose, problem, objective or research question of each paper. Are they in line with your experience or thoughts on the topic, contributing to the collective body of knowledge in this area?**

The paper by Zhou et al. (2016) aimed to analyse online security practices, specifically focusing on consumers' decision-making processes when choosing secure web services. The study highlights the challenge of security in web services despite the introduction of Service Level Agreements (SLA) and Web Service Languages (WSDL). Consumers face dilemmas in expressing confidentiality and privacy requirements, comparing security attributes, and choosing from a large pool of services. WS-SecurityPolicy is insufficient for higher security requirements. The study contributes to understanding how web service security can be quantified and compared, offering valuable insights into consumers' challenges in this decision-making process. This study is highly relevant for individuals with an interest or experience in cybersecurity and web services as it addresses practical challenges encountered in the industry.

On the other hand, the study by Hassanzadeh et al. (2021) sought to assess participants' fundamental knowledge of data breaches and identify gaps in

understanding system vulnerabilities, causes, consequences, prevention methods, and follow-up procedures. The research question aimed to pinpoint these knowledge gaps and underscore the necessity for improved communication concerning data breaches. This study also underscored crucial gaps in comprehending data breaches, emphasising the significance of enhancing communication and educational efforts in cybersecurity. The insights provided are relevant for individuals involved in cybersecurity awareness or education, shedding light on the imperative need to address common knowledge gaps in this domain.

2. **Is the research methodology utilised in each paper appropriate for the stated purpose or question?**

The research methodology used by Zhou et al. (2016) is a quantitative survey method. It systematically reviews existing methods for quantifying and comparing web service security. It provides measurable and comparable data, making it suitable for the stated purpose or question, as per Ramos et al. (2017).

Hassanzadeh et al. (2021) used a qualitative study with 35 participants to investigate their understanding of data breaches. The research methodology was appropriate as it provided in-depth insights into participants' knowledge and perceptions, which are crucial for identifying gaps and improving communication strategies, according to Nyumba et al. (2018).

3. **In terms of data collection and analysis, is this also appropriate for the stated purpose or question? (We will discuss this further in upcoming units.)**

The study by Zhou et al. (2016) compiles and analyses existing methods for quantifying and comparing web services, focusing on security as a top priority. The analysis involves systematic comparison and evaluation of these methods. The data collection and analysis methods are appropriate, as they allow for a comprehensive review of

current practices, identification of challenges, and future directions. According to Fleetwood (2023), quantitative research uses statistical techniques to analyse numerical data, identify trends, and draw insights. This type of research is commonly used in natural and social sciences, often involving experiments and surveys. Qualitative methods, on the other hand, focus on non-numerical data and are frequently used in conjunction with quantitative research.

Hassanzadeh et al. (2021) collected and analysed data through interviews with 35 participants. Thematic analysis was used to identify common knowledge gaps and perceptions. This approach is suitable as it provides detailed qualitative data, revealing nuanced understandings and knowledge gaps. Further discussion will be provided in upcoming units. Kaplan & Maxwell (2005) state that quantitative research methods are increasingly utilised in evaluation studies, especially in computer systems and information technology. These methods involve inductive data collection and analysis to understand issues and situations. They help address validity threats and offer insight into real-life phenomena and their context.

4. **Does each paper support its claims and conclusions with explicit arguments or evidence?**

Zhou et al. (2016) comprehensively review existing literature and methods, backed by evidence and comparisons, to support their claims and conclusions. They also conduct detailed analyses of different security quantification methods.

Hassanzadeh et al. (2021) presented evidence from participant interviews, using direct quotes and thematic analysis to support their conclusions regarding knowledge gaps and improved communication. The theme analysed participants' views on data breaches, identifying key elements, trends, and themes. The paper systematically presents qualitative data from these interviews.

5. **How would you enhance the work/paper?**

As Dawson (2015) emphasises, the paper by Zhou et al. (2016) could be improved by including case studies of successful and unsuccessful web service selections based on security metrics and by incorporating user feedback from service consumers using these quantification methods.

Steinert et al. (2006) emphasise the importance of thorough research, qualitative methods, and participant feedback when evaluating faculty development programs. They also emphasise the need for innovative assessment techniques, standardised teaching scenarios, and addressing bias in response shifts. Therefore, improvements to the work of Hassanzadeh et al. (2021) should include a larger and more diverse sample size for broader insights and a long-term study to observe how participants' understanding develops with targeted educational interventions.

References:

Dawson, C. (2015) *Projects in Computing and Information Systems: A Students Guide*. 3rd ed. Harlow Pearson.

Hassanzadeh, Z., Biddle, R. & Marsen, S. (2021) User Perception of Data Breaches. *IEEE Transactions on Professional Communication*, 64(4), pp.1–16. Available from: https://doi.org/10.1109/tpc.2021.3110545.

Kaplan, B. & Maxwell, J.A. (2005) Qualitative Research Methods for Evaluating Computer Information Systems. *Health Informatics*, [online] pp.30–55. Available from: https://doi.org/10.1007/0-387-30329-4_2.

Nyumba, T., Wilson, K., Derrick, C.J. and Mukherjee, N. (2018) The Use of Focus Group Discussion methodology: Insights from Two Decades of Application in Conservation. *Methods in Ecology and Evolution*, [online] 9(1), pp.20–32. Available from: https://doi.org/10.1111/2041-210X.12860.

Ramos, A., Lazar, M., Filho, R.H. & Rodrigues, J.J.P.C. (2017) Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys & Tutorials*, 19(4), pp.2704–2734. Available from: https://doi.org/10.1109/comst.2017.2745505.

Steinert, Y., Mann, K., Centeno, A., Dolmans, D., Spencer, J., Gelula, M. & Prideaux, D. (2006). A systematic review of faculty development initiatives designed to improve teaching effectiveness in medical education: BEME Guide No. 8. *Medical Teacher*, 28(6), pp.47–526. Available from: https://doi.org/10.1080/01421590600902976.

Zhou, B., Shi, Q. & Yang, P. (2016) A Survey on Quantitative Evaluation of Web Service Security. *Liverpool John Moores University*. Available from: https://doi.org/10.1109/trustcom.2016.0130.