Research Proposal Presentation Outline:
Homomorphic Encryption in IoT

Slide 0: Title Slide including Project Title, Student Name, Programme, Module + Unit

Slide 1: Current Concerns in IoT

- **Privacy and Security Issues:**
    - Growing surface of attack caused by exponential growth of IoT devices connected to the Internet
    - Upholding the CIA: Confidentiality, Integrity, and Availability
    - Data privacy and device trust needs to be ensured
    - Full end-to-end security deployment to protect sensitive data or remotely controlled devices
    - Concerns especially for medical or financial applications, PPI and sensitive data need to be considered

- **Hardware Constraints:**
    - Restrictions and constraints regarding:
        - Components and devices
        - Computational and power resources
    - Evaluating sensitive data is difficult due to device resource and bandwidth concerns

➔ Data is often stored in the cloud to provide ubiquitous access to data, and to leverage computational power
    - **Problem**: facilitates data sharing with third-party services and other users, but bears serious privacy risks

Sources: Mahmoud et al (2015); Peralta et al (2019); Shafagh et al (2017)

Slide 2: Homomorphic Data Encryption

- Introduce Homomorphic Encryption (HE) as a potential remedy to the highlighted issues
- Encryption scheme is said to be homomorphic if the encrypted data can be directly computed from without any intermediate decryption
- With HE, data can be securely stored in the cloud whilst still allowing resource-intensive computations on the data in an encrypted state
- Different degrees of HE includes fully, somewhat and levelled homomorphic encryption
- Data and results can be relayed back to a secure endpoint and decrypted there

➔ **Research Question:** Can Homomorphic Encryption be utilised in IoT to overcome current concerns?

Sources: Brakerski (2019); Fountaine & Galand (2007); Matsumoto & Oguchi (2021)

Slide 3: Aims and Objectives

- Establish a way to implement Homomorphic Encryption schemes in Python (common language for IoT applications)
- Implement a PoC IoT application for the medical industry using differing degrees of HE, as well as a version using industry-standard encryption (asymmetric)
- Utilise the PoC to benchmark the performance of HE vs conventional encryption methods in terms of speed, resource consumption and bandwidth
- Evaluate whether HE encryption poses a practical solution to overcome current issues within IoT

Slide 4: Key Literature

- Highlight key literature and review of current scholarly sources on HE and IoT

Slide 5: Research Methodology and Risks

- **Design:**
  - Conclusive research design to evaluate suitability of HE within IoT
  - Quantitative evaluation of benchmark results and metrics
- **Ethical Considerations:**
  - Results need to be analysed and conveyed honestly and objectively regardless of outcome
  - Discrepancy of data needs to be disclosed where applicable
- **Risks:**
  - IoT Devices have limitations in computing power
  - If HE is too resource-intensive comparatively ➔ not suitable for application within IoT
  - Computation with HE may be too limited to be useful within the external stack

Slide 6: Artefacts

- Highlight artefacts that will be created
- Implementation of comprehensive Python Library for Homomorphic Encryption schemes:
  - Generation of initial key pair (private, public)
  - Encryption algorithm to encrypt messages from plain text using public key
  - Evaluation and operation functionality to compute the data in its encrypted state
  - Decryption algorithm to decrypt messages using private key

- Implementation of a PoC IoT application using various industry-standard encryption schemes and the HE python library
    - Simple IoT Device + Controller setup
    - Cloud / External hub for computational assignments
- Benchmarking of performance, resource overhead and speed of the different schemes using custom python scripts for measurement

Slide 7: MSc Capstone Project Plan incl. Timeline

List of References

Brakerski, Z. (2019) ‘Fundamentals of Fully Homomorphic Encryption – A Survey’, in: Goldreich, O. (eds) *Providing Sound Foundations for Cryptography.* New York: Association for Computing Machinery. 543-563. DOI: https://doi.org/10.1145/3335741.3335762

Fontaine, C. & Galand, F. (2007) A Survey of Homomorphic Encryption for Nonspecialists. *EURASIP Journal on Information Security* 2007(013801): 1-10.

Mahmoud, R., Yousuf, T., Aloul, F. & Zualkernan, I. (2015) ‘Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures’, *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. London, UK, 14-16 December. Piscataway: IEEE. 336-341. DOI: https://doi.org/10.1109/ICITST.2015.7412116

Matsumoto, M. & Oguchi, M. (2021) ‘Speeding up encryption on IoT devices using homomorphic encryption’, *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*. Irvine, CA, USA, 23-27 August. Piscataway: IEEE. 270-275. DOI: https://doi.org/10.1109/SMARTCOMP52413.2021.00059+

Peralta, G., Cid-Fuentes, R.G., Bilbao, J. & Crespo, P.M. (2019) Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges. *Electronics* 8(827): 1-14. DOI: https://doi.org/10.3390/electronics8080827

Shafagh, H., Hithnawi, A., Burkhalter, L., Fischli, P. & Duquennoy, S. (2017) ‘Secure Sharing of Partially Homomorphic Encrypted IoT Data’, *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems.* Delft, Netherlands, 6-8 November. New York: Association for Computing Machinery. 1-14. DOI: https://doi.org/10.1145/3131672.3131697