Research Proposal (Draft)

Say again? The curious case of IoT interoperability.

An MSc Research Project

1. Context of the research

Internet of Things (IoT) is a new paradigm of connecting disparate devices together using the internet (IPv6). These devices generate data about their owners or the environment and transmit the data to a processor interested in the outcome of the sensor data. Despite the connectivity over internet, laptops, PCs or mobile phones are generally not considered to be IoT devices—they are often, however leveraged as gateways for IoT devices.

Around 2017, Baker et al. (2017) considered IoT to be a "relatively new field of research, and its potential use for healthcare is an area still in its infancy". Since then, IoT is considered a "hot topic" for every industry and research on IoT-based solutions shows that they are able to supply artificial intelligence (AI) algorithms with realtime data for prediction or diagnosis of diseases in a healthcare context. The IoT market is predicted to reach USD 534Bn by the year 2025 with an compounded annual growth rate of 19.95 (Buihan et al., 2021). For the healthcare sector, one benefit of IoT is how they support the transfer of hospital-based services into patient homes or the wider community, and so support innovative healthcare services (Calvillo-Arbizu et al., 2021) such as telemedicine or assisted living for the elderly.

2. Literature Review

Paper	Key points
Calvillo-Arbizu et al. (2021)	1) Security vulnerabitlies and requirements often neglected 2) CIA is hardly addressed in literature 3) Latency of networks 4) Lack of information standards like HL7 FHIR (only 2 papers) 5) Cloud cost not discussed 6) Cloud computing is a bottleneck
Baker et al. (2017)	7) "Standardisation is a key issue limiting progress in this area" 8) BLE is the best communications protocol for healthcare. 9) Does not list data standards relevant to healthcare
Bhuiyan et al. (2021)	10) Mentions "Encoding of HL7/SML" in the business layer. 11) Differences in vendors' hardware creates integration issues due to lack of standard protocols or regulations 12) Data privacy, security, protection, cost, Quality of Service (QoS) concerns 13) Authentication and authorisation is problematic for devices with low memory capacity. 14) 24/7 internet connections impact energy consumption.
Dhanvijay and Patil (2019)	15) Does not support multiple active sensor nodes at any given time. 16) Build an IoT architecture based on WBAN 17) Scalability is hampered because of several devices in a healthcare environment. 18) Identified lack of uniformity among connected medical devices that impacts scalability 19) Data privacy and security, low power,
Islam et al. (2015)	20) Proposed a security model therefore focused on security concerns like ○ Multi-protocol networks is challenging ○ Dynamic network topology ○ Energy, memory and computation limitations ○ C.I.A,
Mineraud et al. (2016)	21) Cloud-based platforms suffer traditional web and network security attacks

Paper	Key points
	22) Problem with protocol standardisation causes device integration issues. (they recommend CoAP, MQTT) Due to the lack of standards, they call for a model such as IPSO Smart Objects guidelines
Saleem et al. (2018)	23) Lack of standardisation and interoperability 24) Weak security and authentication
Noura et al. (2019)	25) Platforms are still not interoperable 26) No single standard among devices and platforms

3. Aims and Objectives of the Research Project

Aim. To propose a novel approach using machine learning (ML) in edge computing to drive better IoT device interoperability.

Objective 1: Establish the spectrum of IoT devices and (importantly) their *type of data*.

Objective 2: Define an ML model to support a single *type of data* and its variations.

Objective 3: Document the ML model accuracy on two or more IoT inputs for a given *type of data*.

Objective 4: Present findings of the feasibility of ML to learn new IoT data packets.

Assumptions.

- The IoT devices send simple packets of data, like “heartbeat” or “pulse” or “GPS”.

4. Significance

Reading the literature on IoT, it is unclear the reason why these devices do not implement a common data standard or communicate using a common network protocol. This lack of literature leaves the customer (and researcher) to seek further knowledge. Integrating several IoT devices into an organisation must ensure the devices are secure, and free from attack but also that they're easy to implement which is a challenge for software developers who are forced to write plug-ins for each new device.

This project seeks to uncover how to enable developers to more easily develop systems that can cater for an ever-increasing landscape of new IoT devices, with minimal changes to their software, by leveraging the power of machine learning to uncover the meaning of IoT data and "interpret" the output into a standard format which developers can then build against; thus, solving the complexity of IoT interoperability (hopefully, I don't know if it's possible… which is why it's a project).

5. Research Questions

RQ1: Why have IoT devices not adopted a single industry-accepted standard for data output?

This addresses a gap in the literature that has not examined in-depth the cause for integration difficulties. The question seeks to uncover ***data communication*** *and* ***network communication*** *issues involved in IoT devices. Answering this question supports the stated research aim.*

RQ2: What are the different types of IoT data and is it possible for machine learning to make strong predictions about what it represents?

This uncovers the many data formats that smaller IoT device providers may use without regard to any larger data standard. It tries to meet Objective (1) and (2).

6. Methodology

Quantitative analysis and literature review of standards, protocols and software frameworks or open source endeavours. I do not know fully know the type of data that will be quantified at this moment.

Me: Perhaps the project aim and objectives are too broad and may be unachievable within the specified project module length of approximately 6 months.

7. Appendix: Challenges on the IoT Seas

The literature related to IoT is broad and the following themes are mentioned frequently (in order of frequency):

1) Privacy, Authentication, Trust, Security (the CIA triad)
2) Data issues like latency (due to cloud networks), quality, standards, big data processing in the cloud
3) Lack of standards between devices both network and data,
4) Edge/Fog computing,
5) Blockchain (often in relation to protecting medical electronic health records),
6) Several proposed architectures that typically follow the same 3-, 4- or 5- layer pattern
7) Scalability issues,
8) Mobility issues when IoT devices move between networks,
9) Energy consumption (and various network protocols to reduce it),
10) Lack of location awareness,
11) Discussion about the various styles of communication networks, like Wireless Body Area Networks (WBAN), Wireless Sensor Network (WSN), Personal Area Network (PAN).

Literature exists for almost every entry listed, which I found tremendously hard to identify some gap of meaningful kind. However based on reading the literature, the **top three** concerns for IoT are: 1) security and 2) interoperability and 3) big data.

For the capstone module (provided I pass the RMPP module, of course!), I consider the following assumptions:

1. It is impossible to scan the complete, full list of every conceivable journal in every academic databases to determine whether or not a specific topic has *already* been addressed—this in itself is a challenge for machine learning and AI solutions to resolve; Let. The. Machines. Work!
2. The research artefact shall contain tables, diagrams, comparisons and critiques in it.
3. The master's-level research project is not required to make a *new contribution* into the field, as opposed to a PhD, just a *unique* one (according to Dawson, 2005 in their book titled “Projects in computing and information systems”).
4. It is too late to change my life's choice.

References

Baker, S.B., Xiang, W. & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, 5:26521-26544.

Bhuiyan, M.N., Rahman, M.M., Billah, M.M. & Saha, D. (2021). Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal*, 8(13):10474-10498.

Calvillo-Arbizu, J., Román-Martínez, I. & Reina-Tosina, J. (2021). Internet of things in health: Requirements, issues, and gaps. Computer Methods and Programs in Biomedicine, 208, p.106231.

Dhanvijay, M.M. & Patil, S.C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks, 153, pp.113-131.

Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. & Kwak, K.S. (2015). The internet of things for health care: a comprehensive survey. *IEEE Access*, 3:678-708.

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B. & Ande, R., (2018). ‘IoT standardisation: Challenges, perspectives and solution’. *Proceedings of the 2nd international conference on future networks and distributed systems*. 1-9.

Mineraud, J., Mazhelis, O., Su, X. & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. Computer Communications, 89, pp.5-16.

Noura, M., Atiquzzaman, M. & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications*, 24(3):796-809.