Literature Review Outline - Utilising and adapting IoT technology in secondary education (KS3-KS5)

I: Introduction

Description of the Topic:

As internet and IoTs are become popular in secondary schools, how to utilise and adapting the IoTs effectively and compliant with rules and laws will become a concern nowadays.

The aim of this paper is to research how the IoTs are deployed in the institutions of the secondary education sector, the impact to the students and staff, how to increase thee and compliance to the latest rules and regulations. E.g., GPDR, to give the greatest convenience for staff and students, at the same time to minimise the impact simultaneously.

Big picture:

The utilisation of IoTs in the secondary education sector (KS3-KS5) can improve the quality of teaching, better tracking of students' behaviour, systematic class management and building security. But IoTs also create different side effects and impacts to students and staff or violations to the Government's regulations and rules. This paper will research and suggest the most efficient way to utilise the IoTs and comply with regulations and laws, to minimise the impacts on students and staff.

Why is it important to explore the topic:

As IoTs and the internet are very popular for school education and more functions, for example, manage the classes in school, store, access and transmit students' personal information. The IoT may cause different impacts on students, on both the privacy and information security. It is significant because we need to balance between the efficient use of IoT and compliance with laws and regulations to protect the rights of students and staff:

".....related to IoT devices including development, deployment, security, privacy, and ethics. For every new device, a set of procedures and algorithms need to be developed to enable them to connect, interact, monitor, analyze, and augment the device's physical attributes. Given that the data generated and processed by the IoT devices contain a large amount of private information; processing, archiving, and preserving information security of the data collected from IoT devices is an important issue that cannot be neglected" (Canbaz. Et al, 2022).

II: Main body

Utilisation of IoTs in secondary education sector (KS3-5):

A: Overview:
A general review of different kinds of IoTs and their utilisation in secondary institutions.

B: The use IoTs in the secondary institutions:

I. IoTs in secondary institutions:
   "-IoT-based Smart classroom; this involved the use of IoT devices and technology for lecturing and learning processes in academic organizations all over the world which provides new innovative approaches to education and classroom management. Examples of IoT devices found in a classroom to further education include; Interactive Whiteboards, Tablets and Mobile devices, Student ID Cards, 3-D Printers, Wireless door locks, Temperature Sensors, Security Cameras, Electric Lighting, Smart HVAC systems, Attendance Tracking Systems, Room Temperature Sensors, etc." (Alexei. Et al, 2021).

II. Computing technologies are used in IoTs:
"The use case offers ample opportunities to teach basics of IoT, that is TCP/IP protocol, IP addressing, HTTP protocol, WWW servers, basics of HTML, Lua programming language, event driven programming and basics of PHP programming." (Jaklie, 2020).

III. Although the studies above share the same commonalities, they are from different views: the first one is about the hardware, while the latter is about the t the technology's involvement.

Benefits of utilising IoTs in the secondary education sector (KS3-5):

A: Overview:
IoT helps the secondary schools to improve the quality of learning, increase the intention of learning of students, and increase the efficiency of schools' managements.

B. Benefits of deploying IoTs in secondary schools:

I. What IoTs can work for secondary schools:
"The Internet of Things can be understood as a large network with different connected types of objects, able to communicate with each other and exchange information, regardless of whether they belong to the same group. The network creation consisting of mutually communicating devices provides the user with the possibility of more effective management of all connected devices." (Francisti. Et al, 2020).

II. How the IoTs can help to increase the efficiency of learning:
"...Introduction of electronic gadgets in the educational sector helps in the increase of students' interest. Introduction of new features in their learning process helps them become more inquisitive and enables them to think and apply concepts in a much effective manner. IoT also helps to increase the level of enthusiasm in students. Interactive e-learning session help students understand easier and encourage them to come up with more questions..." (Mishra. Et al, 2020).

III. How the IoTs and improve the efficiency of schools' managements:
"....suggests that smart objects can be used in classrooms for improving teaching and learning. He also mentions to the role of the IoT in enabling remote presence for students, optimizing classroom and campus environments, students' health and safety and saving energy and resources. Chalapathy Neti, vice president, education innovation at IBM, says that IoT allows administrators to understand students' needs and manage buildings more efficiently....." (Bagheri. Et al, 2017).

The above studies have demonstrated different benefits from different aspects, when the IoTs are utilised and adapted in the secondary institutions.

Challenges and problems when utilising and adapting the IoTs in secondary institutions:

A: Overview:

Although there is a great benefit and convenience for secondary schools, with the utilisation of the IoTs, but there are lots of concerns and impacts to students and staffs, especially the privacy and data security. Also, the compliance of regulations and laws is the other major concern.

B: Privacy concerns of utilising the IoTs:

I. "*A large portion of these connected devices is in the category of the IoT devices designed to ease people's daily lives. With the overwhelming presence of IoT in our lives, from smart appliances to industrial IoTs, there is drastic concern surrounding IoT device security breaches"* (Canbaz. Et al, 2022).

II. "These features make it difficult to apply many traditional security solutions to IoT, including the widely used public key scheme and IP-based security solution. Due to insufficient IoT security design, it is often easier to compromise IoT devices than conventional computers." (Sha. Et al, 2018).

C: The risk of data loss:

I. "The IoT environment is advantageous because it configures the user's surrounding as a connected environment to provide convenience. However, because most IoT devices are connected to the Internet, their security can be challenged by a single vulnerability. A malicious attacker may steal confidential information stored on IoT devices, monitor the user's life, or, if necessary, the user's personal information may be unauthorisedly used." (Park. Et al, 2019).

II. "In education, how much students want to expose about themselves is related to privacy (it concerns to each person's option), but security concerns the fact that what, for example, students do not want to show, is safe." (Tomás. Et al, 2020).

D: The possibility of violation to regulations and laws:

I. *"The IoT will increase both sources and amounts of personal data collected. Data aggregation across such multiple data streams makes it more informative about a specific individual's preferences and behavior..... Therefore, regulators and policy-makers need to harmonize and define personal data so that it will be required to anonymize or de-identify this data at the point of collection."* (Garg, 2018).

II. *"Privacy laws generally protect personal information by giving individuals control over if how their personal information is handled by governments and businesses. Organisations using IoT devices that collect or use personal information must abide by laws and regulations that prescribe how personal information can be handled."* (OVIC, 2021).

The above studies have demonstrated different impacts and risks, when the IoTs are utilised and adapted in the secondary institutions.

Conclusion:

What are the contributions of this literature to the field?

To help the secondary institutions understand how to utilise the IoTs correctly and compliant with the laws and regulations, despite enjoying their convenience and benefits.

What are the overall strengths?

The paper can list what the most popular IoTs in secondary schools are and how to utilise and adapt them to fulfil the legal and privacy requirements.

What are the overall weaknesses?

As the title and setting, the study only covers the secondary education sector, but not the general use of IoTs in daily life.

What might be missing?

Other education sector, for example, higher education, is missing in the study.

What are some next steps for research? The next steps should explicitly address how to "correct" for strengths, weaknesses, and gaps

To have broader research of using the IoTs in the education sector, other education sectors should be included in the study, especially higher education.

The study will be more comprehensive if there is a guide or toolkit, to teach the management of schools and MATs, how to utilise the IoTs with compliance policies, for example, the GPDR, DSS, etc.

One example is Data protection: a toolkit for schools from the DfE (DfE, 2018).

References:

1. Canbaz, A., OHearon, K., McKee, M. and Hossain, M. (2022). IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond. 2021 ASEE Annual Conference, [online] (33905), p.2-4. Available at: https://strategy.asee.org/iot-privacy-and-security-in-teaching-institutions-inside-the-classroom-and-beyond.pdf [Accessed 10 Feb. 2022].

2. Alexei, Arina & Alexei, Anatolie. (2021). Analysis of IoT security issues used in Higher Education Institutions. International Journal of Mathematics and Computer Applications Research. 9. 2277-2286. 10.47191/ijmcr/v9i5.01.

3. A. Jaklié, "Educating the Educators for Introducing Internet of Things to Primary and Secondary Schools' Curriculums," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, pp. 632-635, doi: 10.23919/MIPRO48935.2020.9245223.

4. Francisti, J., Balogh, Z., Reichel, J., Magdin, M., Koprda, Š. and Molnár, G., 2020. Application Experiences Using IoT Devices in Education. Applied Sciences, [online] 10(20), p.7286. https://doi.org/10.3390/app10207286.

5. Mishra, Aryan & Karthikeyan, J. & Barman, Binoy & Veettil, Roy. (2020). Journal of Critical Reviews REVIEW ON IOT IN ENHANCING EFFICIENCY AMONG HIGHER EDUCATION

INSTITUTIONS. 10.31838/jcr.07.01.109.

6. BAGHERI, Maryam and HAGHIGHI MOVAHED, Siavosh (2017). The Effect of the Internet of Things (IoT) on Education Business Model. In: 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE Computer Society, 435-441.

7. Sha, K., Wei, W., Andrew Yang, T., Wang, Z. and Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, pp.326–337.

8. Park, M., Oh, H., & Lee, K. (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors (Basel, Switzerland), 19(9), 2148. https://doi.org/10.3390/s19092148

9. Tomás, Cecília & Teixeira, Antonio. (2020). Ethical Challenges in the Use of Iot in Education: On the Path to Personalization. EDEN Conference Proceedings. 217-226. 10.38069/edenconf-2020-rw-0024.

10. Garg, R. (2018). Open data privacy and security policy issues and its influence on embracing the Internet of Things. First Monday, 22(5).

11. Office of the Victorian Information Commissioner. (2021.). Internet of Things and Privacy - Issues and Challenges. [online] Available at: https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/

12. Data protection: a toolkit for schools Open Beta: Version 1.0. (2018). [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf.