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

Introduction

The use of IoT has become popular in secondary education institutions. IoTs play significant roles in school, from building security classroom management to students' assessment and behaviour management. McRae., et al. (2018) suggested that the use of technologies and education has been long and complex, from pure computer science education to full IoT utilisation in schools. IoTs not only improve the management but also create new pathways for the learners, helping them to process and mobilise their creativity and ideas, integrating the learning and teaching environment.

However, there are impacts of the quick rising of the use of IoT devices. Every student has one tablet or laptop in his or her hand, smartboard instead of a traditional blackboard, which able to connect to the internet, access any data and files, accessing office software, such as PowerPoint, etc; both students and staffs may need to access multimedia files, such as YouTube, or doing projects which need communication or demonstration of their work on social media, for example, Instagram, Facebook, LinkedIn, etc.

Besides academics, IoTs also participate the school management. From sensors, CCTV around the buildings and blocks, the use of RFID and smartcards, with every student's personal information, to record their attendance; instead of paper register, teachers are now using software like SIMS (2021) to find, analyse and manipulate the students and class information, attendance, attainment management, safeguarding and budgeting, to access data, do the reports, connect with different departments parents, and making decisions.

While the secondary education sectors are enjoying the benefits of IoTs adaption and utilisation, challenges are also coming forward. Cyberattacks on IoT devices become popular, with the growing of IoT related security regulations, for example, the GPDR and DSS, the security of IoTs become the biggest concern. In fact, the impact of IoT-related security risk to the institutions are increasing and more widespread, and the senior management will need to proactively invest and plan the IoT cybersecurity (Lee, 2020).

Canbaz., Et al. (2022) suggested the utilisation of IoT devices, not only about the development and deployment, but also about the security, privacy and ethics. IoT devices store, process and transmit loads of data and information, much of them involve privacy and personal data. Therefore, we cannot neglect how do the IoT devices process, archive, and preserve the collected information, in secured procedures and algorithms.

The use IoT devices in secondary education institutions

IoT devices are widely used inside the classroom and beyond (Canbaz Et al., 2022). In most secondary education institutions, IoT can be classified into two categories: Standard storage and teaching.

Canbaz., Et al. (2022) also suggested smart campuses become popular in schools, standard storage, including the most sensitive personal data, are widely utilised to IoT devices. For example, intelligent doors and sensors, with RFID card reader, the smart card will contain the personal information; intelligent registers, such as SIMS (2021), teachers can do the attendance registration in class and access every student's personal information. For example, their photos, SEN and health information, academic and behaviour track record, and even their home address and parents' contact information. Other innovative campus IoT components, such as intelligent libraries, laboratories, course management systems, may also store and archive different personal records of students and staff. Other intelligent IoT devices in the classroom, such as smart boards, tablets and computers, also can access any data once there is a network connection.

Because of the Wuhan virus pandemic, remote lessons become popular, especially in the last 3 years. Besides the IoT hardware devices, such as computers, smartphones, tablets, which are widely utilised and adopted, the use of related networking technologies, which are the TCP/IP protocol, HTTP/HTTPS protocol, SSL/TLS, etc. Also, application servers also participate in these activities, such as www servers, collaborative servers (Google Workspace and Microsoft 365) and email servers; events are driven by different languages, such as PHP and Java, etc. These IoT related technologies store, access and process lots of data, including personal privacy and personal ones (Jaklié, 2020).

Benefits of utilising IoT devices and technologies in the secondary education sector (KS3-5):

With the use of IoT devices and technologies, besides can improve the quality of learning, students and teachers can find the learning and teaching materials more efficient; lessons become interactive and innovative; IoT devices are also able to improve the school management, from building security, programme management and students' management; smart register helps staff to track every student on every aspect, from attendance, academic and behaviour track record, their SEN need and health conditions, etc.

IoTs can make classroom teaching easier, interactive and practical. Mishra., Et al. (2020) suggested that IoT devices, including laptops and tablets, provide a learning platform for students and become part of everyone’s life. Through the multi-media and online learning activities, students can do the learning interactively, connect with other classmates and make the lesson's content more exciting and interactive. Teachers also can reduce the time of pure teaching, by deploying different learning activities with students during a lesson; they also can research for teaching materials online, which is more effective and reduce the workload of staff. IoT in the classroom, such as a smartboard, able to connect to the internet, the teacher can present different learning materials with different formats, from Microsoft Office files to YouTube videos. These help to increase the students’ interest of learning.

Besides the interest in learning, IoT also helps a teacher assess every student's progress through the learning activities on IoT. Assessment can be done seamlessly by utilising different interactive activities on the IoT; it also helps a teacher have a more accurate, comprehensive and progressive evaluation of students, compared with the only one-time examination.

IoT also makes learning becomes borderless. As e-learning and distance learning becomes popular and necessary, due to the pandemic, IoT can increase the accuracy and reduce errors in the delivery of a lesson; students can save their time and afford when doing e-learning with IoT: easy access to data and e-book searching; research, compare different materials in projects, communicating with the team members remotely, etc. With the easy access of facilities, such as e-libraries and e-laboratories, Learning with IoT can also help protect the environment, reduce paper use, and support learning progress to become more efficient.

The use of IoT and its technologies also can secure the campus and classroom access control. Bagheri., Et al. (2017) suggested that IoT can create a safe, secure learning environment. Two new technologies: RFID (Radio-frequency Identification) and NFC (Near Field Communication), can deploy and utilise the IoT devices, to simplify the access control and secure the campus effectively. NFC also can connect to the sensors, and provide real-time classroom information; RFID can integrate with the school register: students' attendance can be recorded when they use their student card, with an RFID tag, to access the classroom doors. Information such as when do they enter or leave the classroom, their Geolocation, how long have they stayed in the classroom, the frequency of entering and leaving the classroom, can be traced and recorded to the school's register database in real-time.

Besides the security and access control, RFID can monitor the health condition of particular students. For example, those who have medical needs and PE specialists, students. As IoT is prevalent in the medical industry, Smartwatch and fitness bands are the two most popular IoT devices to monitor a person's essential health condition, for example, blood pressure and heartbeats. With the combination of IoT and RFID technology, an e-health solution can be utilised: Combining with the student's health data, for example, medical history, prescriptions, Electrocardiography (ECG) results, the IoT and e-health solution can give warnings and records if there is any abnormal health condition occurs; for distance learning, the IoT device also can remind the students to stand up and do some exercises, if they have been sit in front of a computer too long; the relevant data can also deliver to the e-health system, for analysing and process, which helps the institution to improve the design and giving students any solution or advice.

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

As the IoT devices and platforms are widely used in the secondary schools, systems and networks security, encryption of personal data, privacies and the related compliant policies being a concern in the community.

Canbaz. et al. (2022) suggested that, although the utilisation of IoT devices has given great convenience to people's daily lives, there are many concerns about the privacies and security. For example, personal information will be transmitted when you log into an educational website; you may send some secrets to others by using the IoT handheld device, such as smartphones and tablets; or you need to input your credit card information to purchase any educational materials. IoT devices will store, process, and transmit any of the financial data and personal data, which is common in daily lives. It will be a serious concern if there are any security breaches.

KrishnaKanth. et al. (2016) said that IoT data are usually stored on the cloud, supposing there is no unauthorised access. Although the privacy and access policies can also be specified on the cloud, for example, the conditional access policies on Microsoft 365 (Microsoft, 2021); or the cloud can manage the IoT devices, such as Windows 10 laptops, Androids and iOS, with domain security and compliance policies, to prevent unauthorised access or cyber security attack, like ransomware and phishing (Microsoft, 2022).

But not every IoT can be managed securely. Some simple IoT devices, for example, CCTV, sensors, card readers, are under the threat of cyber security attack, once they have connected to the network and internet; backdoor of IoT devices is the biggest security concern: each of them may run different micro-OS, the firmware update from vendors may not immediately after a security vulnerability is found; and they are not easy to have centralised management, compare with computing IoT devices.

The security vulnerabilities of IoT devices, may also cause privacy leaking and human error. In secondary education sector, how much of a student what is expose, is their choice and privacy, but the security concern of IoT, may not able to give a user confidence, that what they don't want to disclose, is safe. There are many cases, for example, some privacy videos in their smartphones are being leaked and exposed to the public, due to the human error, or external intrusion and attack (Tomás et al., 2020).

Garg (2018), mentioned that the utilisation of IoT will increase the size of data collection, both the number of sources and amounts. Data aggregation from a number of data streams, for example, cookies on the browsers when students are browsing different websites on their IoT devices, may give detailed information of the preferences and behaviours of any specific person, and such a data collection may violate the laws and regulations. For example, the GPDR. Therefore, the regulators and policymakers of academy trusts need to specify the policies, to harmonise and define the personal data, to make them become anonymous and won't be used for data collection.

Privacy laws and regulations are also applicable to secondary education institutions. They are used to protect and regulate the use of personal information, which the organisation handles. As IoT devices are part of the assets from the institution, it is challenging to make IoT compliant with storing, processing and transmitting personal data. Not only sets up policymakers' policies but also involves technical strategies, such as encryption and access policies.

Conclusion

Utilisation and adaption of IoT, can ease the school management, increase the quality of teaching, and enhance the students' interest of learning. But we also need to pay attention about the security, privacy and violation of regulations during the deployment.

Cyber security issue of IoT, including the identifying and locating IoT object, authentication and authorization, user privacy, lightweight cryptosystems and security protocols, software vulnerability and their operation system platforms, and the utilisation of sensor wireless networks, should do a detail research, for example, the background of the IoT vendors and their track records, shadow the experience of other users' institutions, create a detailed utilisation plan and compliance policies, any cyber security plan, network and system security measure deployment, both hardware and software, and emergency response plan once there is any compliance violation, cyberattack and human error (KrishnaKanth et al., 2016).

2053 words

References:

1. McRae, L., Ellis, K. and Kent, M. (2018). Internet of Things (IoT): Education and Technology. [online] Available at: https://ncsehe.edu.au/wp-content/uploads/2018/02/IoTEducation_Formatted_Accessible.pdf [Accessed 16 Feb. 2022].

2. eloise (2021). SIMS for Secondary Schools. [online] ESS SIMS. Available at: https://www.ess-sims.co.uk/sims-for-secondary-schools.

3. Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), p.157.

4. 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].

5. 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.

6. 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.

7. 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.

8. K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016, pp. 315-318, doi: 10.1109/ICICCS.2016.7542301.

9. ErikjeMS (2021). Set conditional access policies for Windows 365. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/windows-365/enterprise/set-conditional-access-policies [Accessed 18 Feb. 2022].

10. BrendaCarter (2022). Manage devices with Intune. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/microsoft-365/solutions/manage-devices-with-intune-overview?view=o365-worldwide [Accessed 18 Feb. 2022].

11. 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.

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