**Research Proposal Presentation transcript**

**Slide 1:**

Research Project Proposal

Hello everyone, my name is Ivan Chua,

This is my research proposal on Utilising and adapting IoT technology in secondary education in the United States (US)

**Slide 2:**

Introduction

The internet of things (IoT) is a term for the ever-growing network of physical objects that are connected to the internet. While IoT technology refers to inclusion of hardware, software, tools, systems, sensors to support IoT device and application.

According to Ali et al (2020), as shown in Figure 1, currently, there are 40 billion IoT devices deployed worldwide and by 2025 the numbers are expected to reach 76 billion. Hearon et al (2021) also echoed the same findings IoT devices are making people’s lives easier and no wonder the number are increasing each year.

How about the use of IOT technology usage in the education sector the United States? Let’s look at the next slide.

**Slide 3:**

IoT technologies are being increasingly adopted in secondary education in the US according to the search done by Grand View Research as shown in Figure 2.

These technologies can provide the students with new opportunities for learning, making learning more efficient and effective.

It’s therefore not surprise to see the utilisation and adoption continues to grow not only now but also in the future,

However, there are also a number of risks and challenges associated with using such technologies in the education sector(Hearon et al, 2021).

Let us look at an two examples

**Slide 4:**

First example.

According to InfoSecurity firm, the education sector in 2022 experienced a 44% increase in cyber-attacks when compared to 2021.

According to the report, they have found a major concern where the students connected to Free Wifi network without thinking about the security risks.

It is the ignorance and the lack of understanding about the security risks that gave the hackers the perfect opportunity to carry out the attack.

**Slide 5:**

Second example

In another report published by CheckPoint (see Figure 4), there has been an increasing trend in the number of cyber-attacks.

In 2021 alone, the researchers have seen the highest volume of attacks in the education sector, with an average of 1,605 attacks per organisation every week.

According to Hess (2022), education and research has the highest attack because there is no standard practice or policy for cyber security.

It is up to the school to decide how to defend themselves, and not all schools take cyber security seriously.

**Slide 6:**

Significance of the research.

There are two of them.

First, while there are many benefits of using IoT technologies in secondary school, but do the students know the risks associated with using such technology?

Do the students have security awareness? Do they know how to identify a security threat?

The dangers of the IoTs, especially those students who are new to it, which means that the IoT devices are either unsecured or not secured properly. This could lead to a hacker hacking into them, taking control of the device or even using it to get access to school’s system to steal sensitive information. According to Hearon et al. (2021)there are many security challenges to overcome and one of them is student’s awareness of security risk.

In a survey conducted by Pew Research shown in Figure 5, high school students have lowest scores in cybersecurity knowledge compared to those in higher education and this is worrying.

**Slide 7:**

The second significance of this research is to deep dive into the challenges faced by the students in learning IoT technologies.

One of the biggest challenges that students face is lack of prior knowledge or have no previous exposure to the topic. In the research conducted by Schneider et at. (2020), it was noted that students without prior IoT knowledge have difficulty with the theoretical concept and more time has to be given to them to complete the assigned task.

Another group of students also reported having difficulty with handling of IoT technologies, primarily in relation to basic electronics as these were new concepts to them

According to Hearon et al (2021), the lack of knowledge in the students make them vulnerable to social engineering attacks.

Another challenge is the issue of coding. Many IoT applications require coding, and not all students are familiar with this language Schneider et at., (2020).

It was however noted that there are many resources available to help students learn coding like the use of visual programming language rather than the traditional coding method.

Mechelen al et (2022) also highlighted that these emerging technologies were difficult for the secondary school students to comprehend due to complex and distributed nature.

Additionally, the vast majority of IoT devices are still new and constantly evolving, which makes it more challenging for students to keep up with the latest changes and updates (Moskal, 2018**), l**eaving the students feeling bad and disengaged as if they were not making good progress.

Therefore, the teachers have an active role to play in guiding the student, ensuring IoT devices are used properly and securely as cited by Hearon et al (2021) and Mechelen al et (2022)

**Slide 9:**

The aim and objective of this research are:

1. Assess the level of security awareness of the student handling IoT in secondary education

In hope to raise security risk awareness among the students as they play a critical role in the overall security wellness of the school.

1. Identify the challenges faced by the secondary students in learning IoT technologies

In hope to raise student’s ability awareness to the school management so that help can be rendered to them

**Slide 10:**

The two research questions are:

1. Do the secondary students understand the risk associated with IoT technologies?

The students may be tech savvy but do they really have the risk knowledge and understanding? This is what the research question hopes to answer.

1. What are the challenges faced by secondary students in learning IoT technologies?

The students may have jumped into the IOT technology bandwagon due to its popular demand, but as secondary students, are they coping well?

**Slide 11:**

Research Methodology

The research methodology is based on the Emerging Synthesis (Makaroff et al, 2016) methodology as it includes quantitative, qualitative,and other types of data like policies, commentaries, etc.

In addition, online searches will be carried out using Research Gate, ACM Digital Library, Google Scholar, the University of Essex Online Library platform and IEEE Xplore.

Lastly, to stay current, articles published between 2015 and 2022 will be used in this research.

**Slide 12:**

Ethical considerations

1. The participants will be given all the relevant information about the study.

This information should include the purpose of the study, the nature of the data that will be collected, how the data will be used, and who will have access to it.

1. The Participants’ consent will be required, and they should understand the risks in taking part in the study and that they are free to withdraw consent at any time.
2. Maintain integrity in ensuring the accuracy during publishing of the research result (Yip, 2016).
3. During the survey, participants will be also consent if they would like to participate in a phishing test.

Should they agree, effort will be taken to sure no harm cause to the participants.

1. Lastly, to ensure Personal Identification Information or PII are not collected during the use of online survey platform and phishing test (e.g. IP addresses)

**Slide 13:**

Risk Assessment

Based on the ethical consideration, a risk assessment was carried out.

For each risk item, a severity level rating and a likelihood of occurrence rating will be assigned.

An overall rating is computed by multiplying these two values and a value of greater than 3 requires attention, close monitoring and checking, to ensure it does not go out of control.

For Severity Level, there are 3 levels: 1 - Low, 2 - Medium , 3 - High. It is an indication of how severe the risk should it happened.

For Likelihood of occurrence, there are also 3 levels similar to severity level. It is an indication of how likely the risk will occur.

From the risk assessment analysis as shown in Table 1.

Focus needs to be given to ensure accuracy in presentation of information from primary and secondary research sources, as it has a rating of 4.

**Slide 14:**

There were a number of literature materials available related to this research. The key ones are shown in Table 2:

1. Hearon et al (2022)

It discusses the issues and challenges related to IoT and security breaches caused by user and system vulnerability.

2. Moskal et al (2022)

It provides report on the opportunities and challenges of incorporating IoT in education

3. Schneider et al (2020)

It discusses the challenges faced by students in using IoT technologies

4. Makaroff et al (2016)

It provides guidance on the research methodology

**Slide 15:**

Artefacts that will be created in this research project

1. Answers and responses from questionnaires.

This is done via online survey platform and in person interviews should there be a requirement.

2. Test phishing results from the participants

The is the data collected from those who have consented to participate in the phishing test.

3. Findings and conclusions from the questionnaire analysis, phishing test will be filed together with the raw data.

4 Provide recommendations for research questions.

As part of this project, observation and recommendations will be made available to the school management, it will be part of the artefacts

**Slide 16:**

Timeline for the proposed activities.

As shown in Table 3, the minimum duration is 31 weeks and maximum is 36 weeks.

The buffer timeline is in anticipation of additional time required to obtain participant’s consent and carrying out the survey.

**Slides 17 to 19**

They are the references used in this research proposal.

Thank you and this is the end of the research proposal.

**References**

Alessandro Mascellino (2022), Education Sector Experienced 44% Increase in Cyber-Attacks Over Last Year.

<https://www.infosecurity-magazine.com/news/education-experienced-44-increase> [Accessed: 22-Nov-2022]

Ali, Omer & Ishak, Mohamad Khairi. (2020) Bringing intelligence to IoT Edge: Machine Learning based Smart City Image Classification using Microsoft Azure IoT and Custom Vision. Journal of Physics: Conference Series. 1529. 042076. DOI:10.1088/1742-6596/1529/4/042076

Check Point Research: Cyber Attacks Increased 50% Year over Year (2021),

<https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/> [Accessed: 24-Nov-2022]

G. Schneider, F. Bernardini and C. Boscarioli, "Teaching CT through Internet of Things in High School: Possibilities and Reflections," 2020 IEEE Frontiers in Education Conference (FIE), 2020, pp. 1-8, doi: 10.1109/FIE44824.2020.9274184

Rick Hess (2022), Why Are Schools a Target for Cyberattacks? <https://www.edweek.org/technology/opinion-why-are-schools-a-target-for-cyberattacks/2022/10> [Accessed: 22-Nov-2022]

KENNETH OLMSTEAD AND AARON SMITH (2017), What the Public Knows About Cybersecurity <https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/> [Accessed: 23-Nov-2022]

Maarten Van Mechelen, Rachel Charlotte Smith, Marie-Monique Schaper, Mariana Aki Tamashiro, Karl-Emil Kjær Bilstrup, Mille Skovhus Lunding, Marianne Graves Petersen, Ole Sejer Iversen (2022) Emerging Technologies in K–12 Education: A Future HCI Research Agenda. <https://doi.org/10.1145/3569897>

Moskal, M., Christian, A., Laurenson, T. and Rountree, N., (2018) Internet of Things” as a capstone project: reflections on an educational initiative. Retrieved from Cintrenz: <https://www.citrenz.ac.nz/conferences/2018/pdf/2018CITRENZ_1_Moskal_IoT.pdf>

O'hearon, Keejoh & Mckee, Michael & Hossain, Nour & Canbaz, M Abdullah. (2021). IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond.

<https://peer.asee.org/iot-privacy-and-security-in-teaching-institutions-inside-the-classroom-and-beyond.pdf> [Accessed: 22-Nov-2022]

Schick-Makaroff, Kara & MacDonald, Marjorie & Plummer, Marilyn & Burgess, Judy & Neander, Wendy. (2016) What Synthesis Methodology Should I Use? A Review and Analysis of Approaches to Research Synthesis. AIMS Public Health. 3. 172-215. 10.3934/publichealth.2016.1.172.

<http://dx.doi.org/10.3934/publichealth.2016.1.172>

Susan Morrow (2020), Critical security concerns for the education industry

<https://resources.infosecinstitute.com/topic/critical-security-concerns-for-the-education-industry/> [Accessed: 22-Nov-2022]

Yip C, Han NR, Sng BL (2016) Legal and ethical issues in research. Indian J Anaesth Sep;60(9):684-688. DOI: 10.4103/0019-5049.190627. PMID: 27729698; PMCID: PMC5037952.

Victor Rivero (2020), EdTech Market Size 2016-2027

<https://www.edtechdigest.com/2020/11/19/edtech-market-size-2016-2027/>

[Accessed: 22-Nov-2022]