e-ISSN: 2716-6546

ISSN: 2716-6546

International Journal of Instruction, Technology & Social Sciences
www.ijitsc.net

Internet of Things: Applications and Challenges at Higher Learning Institutions

[1]Arumugam Raman,
[2]Raamani Thannimalai

arumugam@uum.edu.my[1], drraamani@gmail.com[2]

[1]School of Education and Modern Languages, Universiti Utara Malaysia 06010 UUM Sintok, Kedah, Malaysia
[2]Ministry of Education, Malaysia

To cite this article:

Raman, A. & Thannimalai, R. (2020). Internet of Things: Applications and challenges at higher learning institutions. *International Journal of Instruction, Technology, and Social Sciences (IJITSS), 1*(2), Page 1-Page 15.

Internet of Things: Applications and Challenges at Higher Learning Institutions

Arumugam Raman, Raamani Thannimalai

Article Info

Article History

Received:
01 June 2020

Accepted:
19 July 2020

Keywords

Internet of things
Higher learning instituitions
Applications
Challenges

Abstract

The Internet of Things (IoT) is an inovative system where internet is connected to the physical world via ubiquitous sensors and is rapidly making its way into higher learning institutions. By modifying how higher institutions gather data, interface with students and automate processes, the IoT has the potential of revolutionizing education. Universities may offer opportunities to magnify content delivery, augment learner and faculty interaction when IoT devices are utilized. Massive open online courses, online software application and education applications make students co-creators and active individuals in acquiring their knowledge and experience. However, many challenges such as Malware, Distributed Denial of Service, data storage, data security, privacy, decentralized network management and connectivity come along with the use of internet:. This conceptual paper offers suggestions to overcome these challenges to address future threats to IoT and provides directions for future research.

Introduction

The Internet of Things (IoT) is a new system designed to increase connectivity between computer systems and is rapidly making its way into classrooms and higher institutions in ways never before imagined. In 1999, Kevin Ashton introduced the term IoT, which refers to a system where internet is connected to the physical world via ubiquitous sensors (Gokhale, Bhat & Bhat, 2018). IoT are uniquely identifiable connected objects with radio-frequency identification (RFID) technology. IoT applications are widely used in healthcare, automotive industries, transportations and is currently gaining acceptance in the higher education sector. Different from earlier innovations, IoT technologies are ubiquitous and inspire solutions to be intelligent and autonomous (Kahlert, 2016; Aldowah, Rehman, Ghazal & Umar, 2017).

Computers were brains without senses in the twentieth century; as it only relied on the input of information. This caused a lot of limitations because there is too much information to be keyed in through a keyboard or scanned with a barcode. In the twenty-first century, because of the wonders of IoT, computers can sense things for themselves. Networked sensors such as the GPS-based location sensing is already being widely used all over the world and is being taken for granted. Although the Global Positioning System (GPS) in cell phones were not tested until 2004, people of all walks of life today, are so dependent on the GPS to find their way around on a daily basis (Gabai, 2015).

Physical learning environments and structured learning has improved drastically over recent years and rapid improvement has taken place at education systems across the globe. IoT has also in evidently increased educational quality, and access thus paving the way for transformations in educational settings, managements and even leaderships in educational institutions all over the world. The Internet of Things is a revolution in advancing technology to change the lifestyles of humans (Li, Xu & Zhao, 2015) and it is synonym for a fully interconnected world (Gubbi, Buyya, Marusic & Palaniswami, 2013). According to IOT Analytics (August 8, 2018), the number of IoT devices that are active is expected to grow to 10 billion by 2020 and 22 billion by 2025.

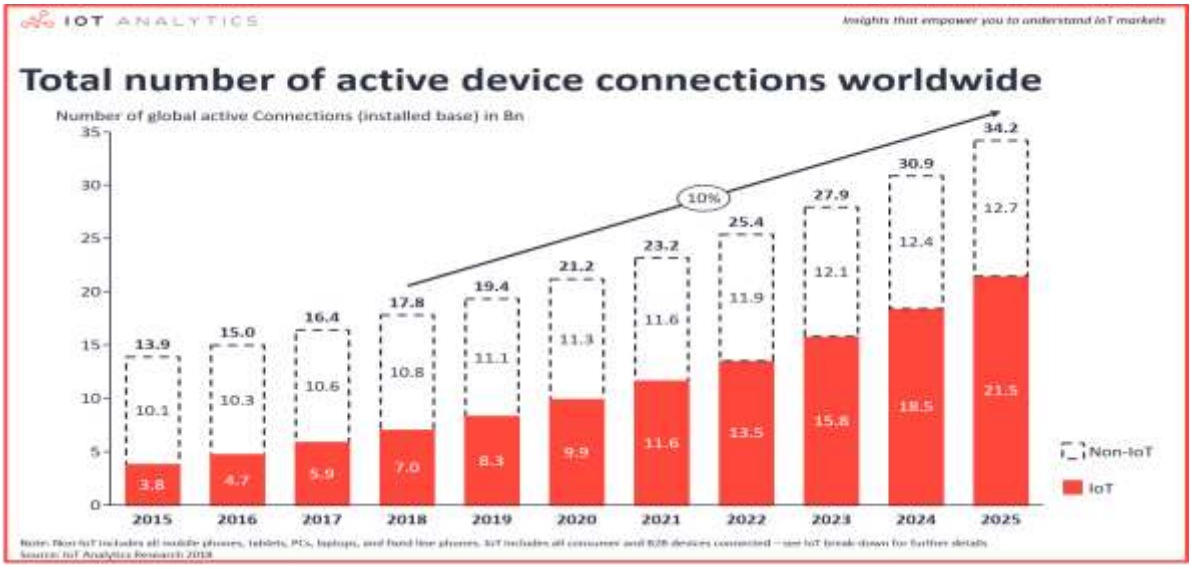

Figure 1. Total number of active device connections worldwide (Source: IoT Analytics Research, 2018)

By modifying how higher institutions gather data, interface with students and automate processes, the IoT has the potential of revolutionizing education. IoT heightens the standard of education when it is incorporated with innovations such as data analytics and individual flexibility. Besides other advantages, IoT enables education institutions to (i) improvise how lessons are disseminated as well as the ways students' performance are evaluated, using audio-visual equipment, electronic video clip recorders for lecture capture and internet screening (ii) support personalized methods to explore such as 'immersive electronic books' and 'game-based learning' (iii) proactively monitor institutions infrastructure (iv) utilize cost-efficient lighting, cooling and heating procedures (v) provide a secure environment for students as well as educators using digital security cams, intelligent door locks and linked institution transportation.

The IoT is rapidly emerging in educational settings at higher educational institutions. The seven categories of modern technologies, devices as well as strategies which revolutionize education settings are: consumer technologies, digital strategies, internet technologies, learning innovations, social networks, modern technologies and visualization innovations (Johnson, Becker, Estrada, & Freeman, 2015).The Iot being a component of Net modern technology has enabled every device to be linked to the internet thus opening up the entire world of innovations in education and all spheres of life. Looking from a wider angle, the Iot inclusion in the academic setting narrows the gap between conventional education settings and modern-day education demands by transforming traditional classrooms which are separated by place as well as time, right into linked classrooms which are combined by internet based communication devices. For this reason, Iot developments have influenced instructional techniques as well as boosted the delivery of course content by adding more resources and tools to or online, making learning more dynamic and interactive (Advanced MP Technology, n.d; Vujovic & Maksimovie, 2015).

Consequently, brand-new levels of connection as well as advanced discovery of strategies in academic practices are brought about by IOT. Besides these, certain difficulties like personal privacy as well as safety and security issues related to students can be brought about by IoT and has be dealt with promptly. In educational institutions, the important aspect of the IoT is its potential not only to raise education quality, but also to improve the education sector economically and socially (Maksimović, 2017).UNESCO has recognized some principles and values that underlie education for sustainable development as follows: (i) takes into consideration the wellness of the environment, society and economic systems (ii) is interdisciplinary, engages formal, non-formal and informal education and encourages lifelong learning (iii) is culturally suitable and also addresses material, context, global concerns and also regional top priorities and as a result have worldwide impacts and repercussions; iv) develops civil capability for community-based decision-making, social tolerance, environmental management, flexible workforce and quality of life; and satisfies the needs of the advancing nature of the sustainability principle. Nonetheless, instruction and learning for lasting advancement and also integrating facets of sustainability cannot be understood without techniques that require active participatory learning and also higher order thinking skills (Blewitt, 2010). Thus, students, educators and other staff members need to accept new means of instruction and learning, in order to obtain new skills and knowledge (Wals & Jickling, 2002).

Concept of IoT

The exact concept of Iot is still developing and is subjective. Generally, the IoT is defined as a "dynamic global network infrastructure with self-configuring capabilities based on standards and communication protocols" (Gokhale, Bhat & Bhat, 2018). Vermesan, Friess and Guillemin (2011), defined the IoT as an interaction in between the digital and physical worlds. The digital world communicates with the real world utilizing a huge selection of actuators and sensing units. Peña-López (2005) explained that the IoT as a paradigm in which computing and networking abilities are embedded in any sort of possible things. If possible, we utilize these abilities to query the state of the item and to alter its state. In typical parlance, the IoT describes a brand-new sort of world where practically all the gadgets and devices that we utilize are linked to a network. We can utilize them collaboratively to attain complicated jobs that need a high degree of intelligence. The evolution of the internet can be classified into five eras as shown in Figure 2 (Li, Xu & Zhao, 2015).

- The Internet of Documents-e-libraries, document based webpages
- The Internet of Commerce- e-commerce, e-banking and stock trading websites
- The Internet of Applications- Web 2.0
- The Internet of People-Social Networks
- The Internet of Things-Connected devices and machines

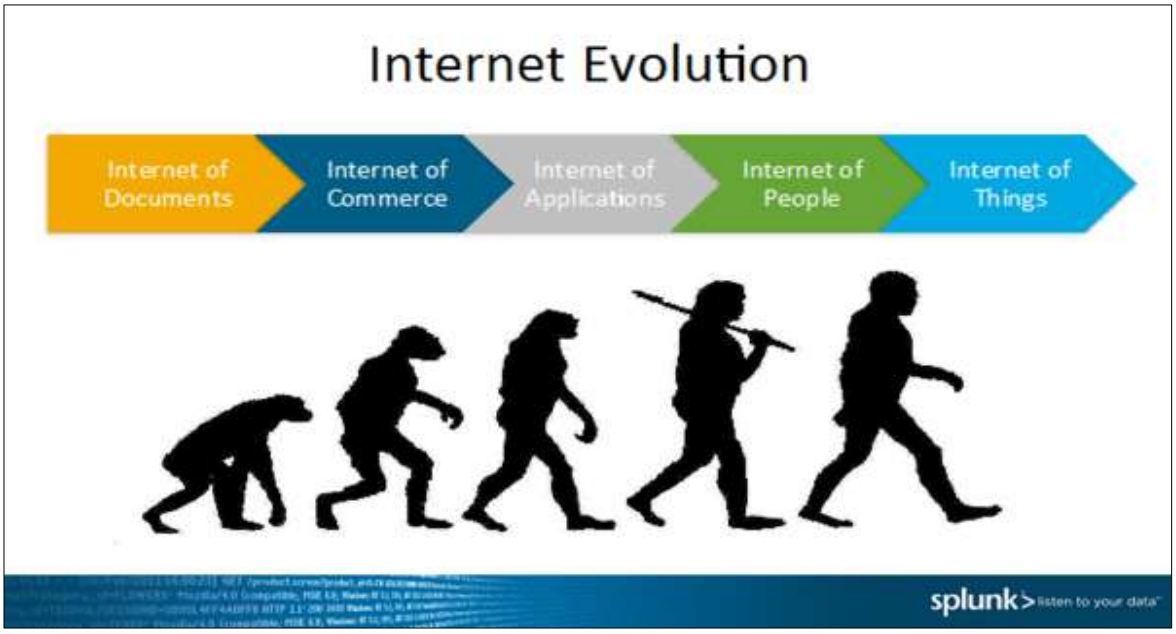

Figure 2. Evolution of the Internet (Source: The Next step in Internet Evolution, 2014)

As illustrated in Figure 3, devices, objects and things are connected by IoT to the internet infrastructure in a global physical network. This enables communication and interaction with internal and external environments. Furthermore, information exchange through information sensing devices can also take place according to standardized protocols (Aldowah et al., 2017).

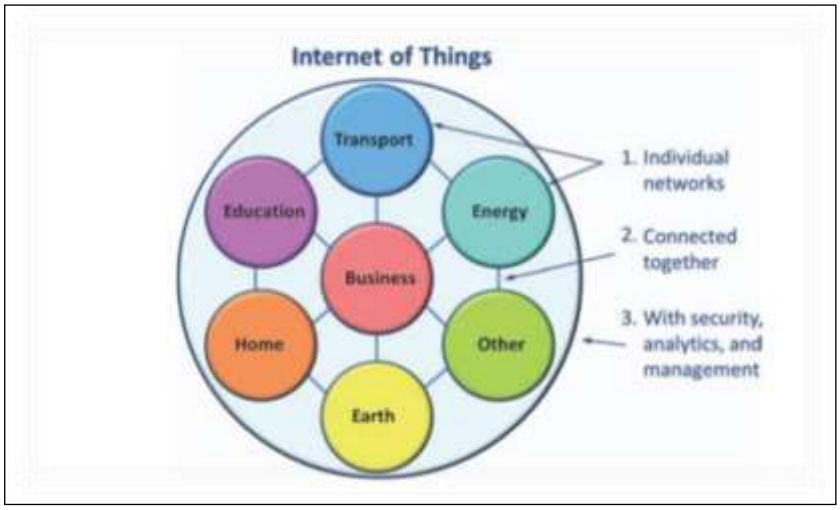

Figure 3. Iot viewed as a global network (Source: Cisco IBSG, April, 2011)

In the near future, connectivity for everything and everyone can be networked around the world with just the click of a mouse by using any service or network (Vermesan & Friess, 2013) in view of intelligent managing, tracking and identifying all kinds of things (Stankovic, 2014). As explained in Figure 4, IoT which is also known as the Internet of Everything is an extensive Internet-based network which multiplies tremendously the communication between Human to Human (H2H), Human to Things (H2T) and Things to Things (T2T).

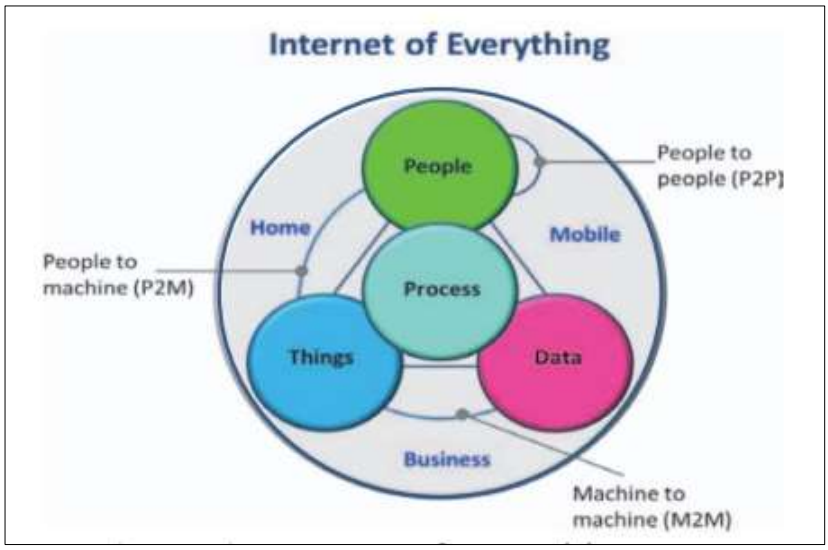

Figure 4. Internet of everything (Source: Cisco White Paper, April, 2011)

The IoT is engaging innovation specialists to create smaller and progressively moderate remote frameworks that devour less power and can be coordinated into practically any kind of device (Jin, 2012). There are three parts of IoT which empower consistent associations which are: *Hardware:* comprised of sensors, actuators and inserted correspondence equipment, *Middleware*: on interest stockpiling and processing apparatuses for information investigation, and *Presentation*: perception and translation apparatuses which can be generally used at various stages and which can be intended for various applications (Gubbi, 2013). There are various potential methodologies for presenting low-control interchanges to an IoT hub, extending from reason planned conventions, for example, ZigBee to low power variations of Bluetooth, Wi-Fi and NFC. In spite of the fact that Wi-Fi is the most well-known type of coordinated remote innovation and the best power-per-bit transmission effectiveness, IoT improves different arrangements counting Radio Frequency Identification (RFID) innovation which is utilized all through business, industry and individual innovation frameworks and empowers structure of microchips for remote information correspondence (Gubbi et al., 2013). A portion of this innovation can include Wireless Sensor Network (WSN) to any sort of device, as Fitbit wearable wellness trackers, and books.

IoT Scenarios in Education

The benefits of the IoT are being discovered by traditional colleges and universities. In fact, Carnegie Mellon University introduced the first Internet-connected appliance (Coke vending machine) in 1982 (Symantec Corporation, 2015). Traditional colleges and universities may offer opportunities to magnify content delivery, augment learner and faculty interaction when IoT devices are utilized. Radio Frequency Identification (RFID) codes can be used to identify and trace people, processes, data, and things (Selinger, Sepulveda& Buchan, 2013). For instance, Northern Arizona University presently uses RFID tags embedded in student Identity Documents (ID) for attendance tracking; and the University of Illinois uses QR codes for students to access videos, maps, and other campus resources (0'Connor, 2010). Higher learning institutions can use IoT devices to initiate a campus lockdown system including electronic perimeter security and instant student, faculty, and police notifications (Lutz, 2014). The potential advantages of IoT technology on higher learning institutions are limitless.

Almost all aspects of our lives is transforming with the influence of IoT as a tool. With technology advancements and IoT, the education sector has become more innovative and efficient than ever before. Therefore, it has become a popular subject among present researchers who study innovative methods for learning, teaching and managing the entire education system. IoT solutions promise to make higher education institutions smarter as well as more efficacious at everything they do. Besides, helping enhancing learning experiences, improving educational outcomes and decreasing costs, the IoT has the ability to redefine how students, educators and administrators interact with technology and connect with devices in classroom environments. IoT solutions for higher education include the following:

• Improving instruction and optimizing learning outcomes with Smart white boards and alternative interactive digital media that can accumulate and analyse data for educators and learners to be utilized during interactive learning in classrooms.
• Reducing energy consumption by innovations such as smart temperature sensors; smart heating; ventilation and air condition equipment; and atomizing operations management
• Locations of students are monitored using smart student ID cards and attendance-tracking devices.
• Security for educators, students and staff are provided by wireless door locks, connected surveillance cameras and face recognition systems.
• Cutting-edge and automated systems in key areas of study, such as medicine, agriculture and engineering to enhance research fields.

Concept of Digital Campus

Digital Campus System is a significant platform for undergraduates to get a wide range of data (Ma, Zhou, Liu, Qiao, Han & Wang, 2014). New innovations are fervently influencing administration of higher education organizations. There is an expanding request for advanced education organizations, particularly, colleges to digitize their academic delivery methods and all campus activities. There is also a demand to academics and researchers to accept a digital based working environment (Ma et al., 2014). A well planned physical campus, totally incorporating technology, is a basic necessity for the structure of a digital campus. A functioning digitalized campus can be achieved by improving student's involvement by giving proper digital facilities for learning, teaching and research. Moreover, to be able to manage security threats, higher learning campuses must always keep innovating new strategies and have skilled technology leaders with futuristic visions.

Technology can lessen operational expenses; heighten security on campus grounds; supply tools for scientists, scholars, undergraduates and staff. These advantages give genuine incentive to university operations, increase the experience of undergraduates, and researches. The digital campus consists of two primary parts. To start with, it recycles the IT Service Delivery Platform-facilities to supply network connection, movement and security for all applications and services throughout the campus. Secondly, it consists of many Internet of Things (IoT) applications running over the platform system to support the scholars of the university, allow learning and teaching activities, and improve student's experience. According to Cisco -"Digitizing Higher Education" - IoT applications vary from standard network applications as they support sensors and sensor data, instead of users and user information. IoT applications for the digital school consist of 5 primary classifications: Energy Monitoring and Control: Location and Attendance Systems: Video and Information Systems: Security and Access Control: Building Control and Management, as displayed in Figure 5

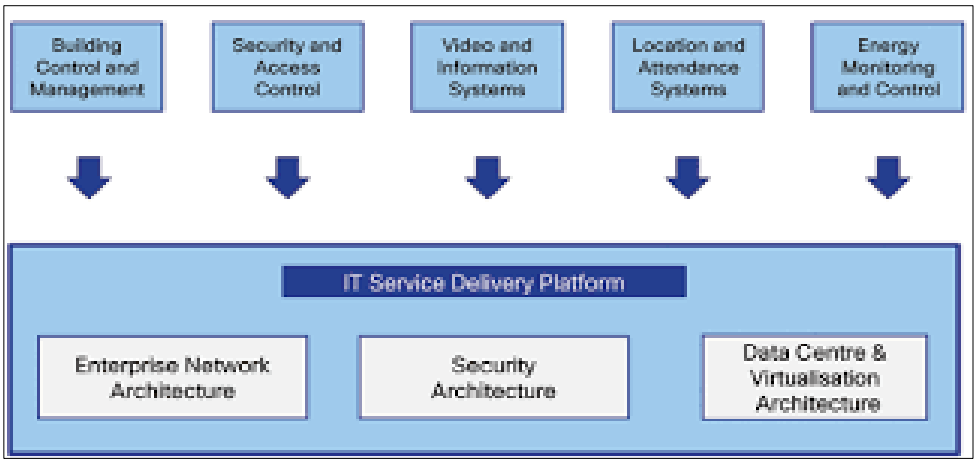

Figure 5. IoT Applications for the Digital Campus. (Source : Cisco: Digitizing Higher Education, https://www.cisco.com/c/dam/assets/docs/digitizing-higher-education.pdf)

IoT Architectural Model

Cloud computing has unrestricted abilities in regards to storage and processing power, and is typically incorporated with IoT innovation (Botta, De Donato, Persico, Pescapé, 2016). To highlight IoT systems, the Device-Cloud Mobile (DCM) design shown in Figure 6, is extensively utilized today in business IoT items. The IoT devices require link to the Back-end Cloud system, and assistance services by a user application (app) working on mobile phones. Sometimes, the app links straight with the IoT device utilizing the devices Wi-Fi hotspot abilities, which either processes the demands straight or bridges it to the Cloud Back-end system.

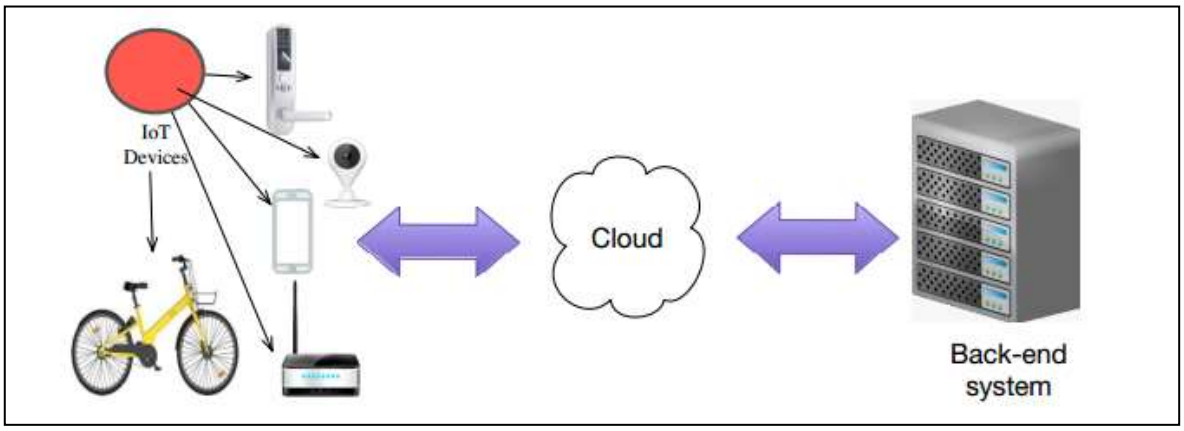

Figure 6. Device-Cloud-Mobile IoT Architectural Model

The Device-Cloud-Mobile IoT Architectural Model was used by Tan, Wu, Lee & Zu (2018) to design a Teaching Management System with applications of RFID and IoT Technology. The system architecture is as illustrated in Figure 7. In the proposed system, to form an integrated IoT system for teaching management, mobile terminal, RFID reader, RFID card, Node MCU and QR code are utilised.

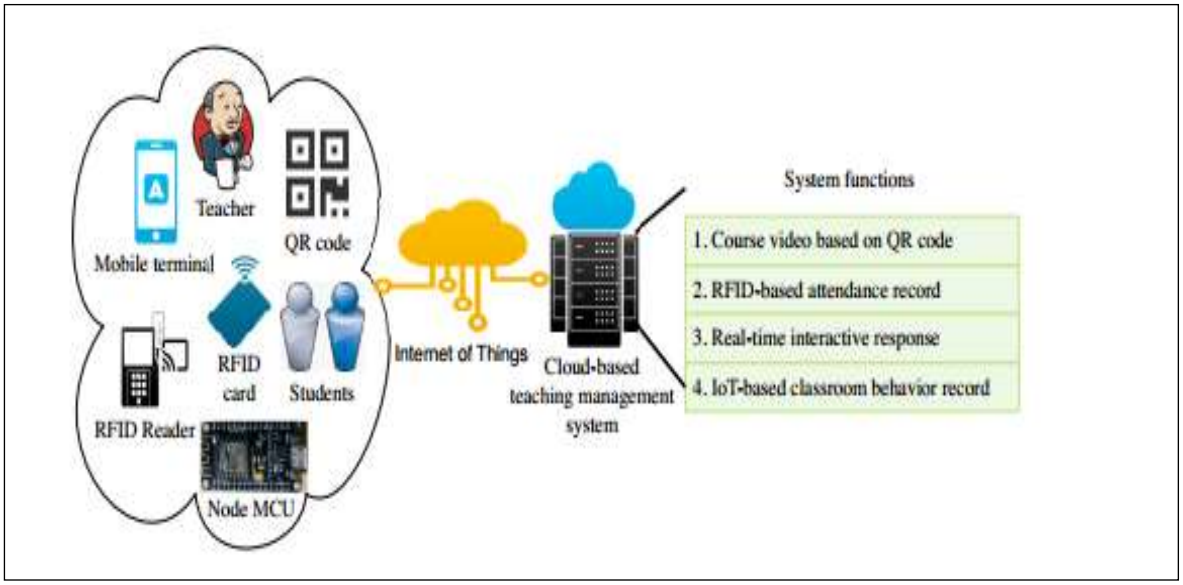

Figure 7. IoT-based Teaching Management System architecture. (Source: Tan, Wu, Lee & Zu, 2018)

The functions of this system are as the following:

- *Course video based on QR code*

The course, which is taped as video materials, is kept on the Cloud-based Teaching Management System, and students can view them with their own smart devices through scanning the QR codes which can link directly to their curriculum. This is extremely practical for students' who are self-learning and they are totally free to pace out their learning according to their own capabilities.

- *RFID-based attendance record*

In China, many universities and colleges have started using the *Smart School Card System* which utilizes HF RFID cards as students' identification device. Students swipe the RFID card before entering classes. The suggested system can record student's duration in the class and can be used for student evaluation. This system can motivate students to be disciplined and punctual for lectures.

- *Real-time interactive response*

In a real-time teaching, learning and facilitation session, an instructor can utilize the Teaching Management System to distribute practice worksheets through a QR code provided to students, and after that via smart mobile devices (such as IPAD and Smart phones) students can scan the QR code which gives access the worksheets in the Cloud-based system. Students are then required to respond and interact with the instructor immediately. At the same time, the students' ID number and name will be recorded. The system can document student's answers and the time taken to complete tasks. The instructor can examine the total students' response to each worksheet. If it is discovered that many of the students are not able to respond correctly to the task/worksheet, the instructor can deduce that the lesson did not achieve its objective and another method of instruction must be used to make the students understand the lesson better. The real time interactive response can be used for course evaluation and for instructors to innovate their instruction methods to make learning more effective.

Potential IOT Applications in Higher Education

Technology as a main enabler of education in the 21st Century can be practiced in different methods in order to transform the education sector (National Research Council, 2000). IoT makes learning based upon real-world issues; supplies resources to improve learning; enhances feedback, modifies instructional methods; allowing instructors to enhance their abilities; and encourages collaboration among stakeholders to transform the education sector. The characteristics noted above for enhancing education sector are substantially strengthened by a phenomenon called the IoT. The IoT is based upon the connection of devices besides basic devices. These devices or "things" are Internet capable and managed, able to engage autonomously not just with users, however with other devices, and

produce important information daily. The information produced by IoT can be quickly gathered, measured, kept and processed, attaining in this method, important insight and understanding (Morphus, 2016). Together with the various IoT applications and advantages in all elements of our lives, the IoT holds the prospective to empower academic practices and environment, through virtual, shared, smart teaching and learning environment (Vujović and Maksimović, 2015). In other words, the IoT allows significant improvement in instructional technology and not only virtual class and online tutorials. Typical existence of Internet-capable innovation and smart devices (e.g. tablets, smart boards, and so on) in the classroom makes conversations and lessons livelier and more intriguing. Massive Open Online Courses (MOCC), online software application and education applications make students co-creators and active individuals in acquiring their knowledge and experience (Brandt, 2016). The IoT assists lecturers to make their work more practical and effective, through the automation of various jobs and faster access to student data. Because the IoT holds the possibility to change our society, economy and all elements of individual's lives, its essence depends on the power of connection and collaboration. The fast advancement and adoption of the IoT needs unparalleled collaboration. The development and enhancement of IoT-supported education likewise counts on a collaboration of all stakeholders.

The IoT addition in education allows students to access their courses or lab workouts at any time, from anywhere they can log on, and select whichever manual they wish to obtain knowledge from. Together with access to courses customized according to student's requirements and choices, the students are able to select the pace of work, to repeat the lessons that they haven't fully grasped. They are also able to keep track and assess their own progress. The availability of unique IoT technologies and devices at any given time inspires students to work independently or to collaborate online with other students or lecturers, establishing analytical abilities and own understandings (Stošić, 2015). With the aid of IoT, Wireless Sensor Networks (WSN), Radio-Frequency Recognition (RFID) chips and Cloud-based applications, students have the capability to research many real-world issues, obtain information in real-time and effectively enhances their learning experience (Ralhan, 2017). The smart devices executed in the classroom, such as digital highlighters and interactive boards (Figure 8), considerably streamline the learning experience and improve the collaboration amongst students, instructors, mentors and colleagues throughout the world (Maksimović, 2017).

Figure 8. The smart and interactive classroom (Maksimovic, 2017)

Smart applications can be applied in many sectors. These applications are not yet easily accessible; nevertheless, initial research study shows the capacity of IoT applications in enhancing the lifestyle in our society. Two widely used IoT applications are higher education are as the following:

Interactive learning

Learning in the 21st century is not restricted just to a concoction of images, audio and texts however, it encompasses far more than that. Student's reference books are linked to websites that include videos, animations and evaluations. These offer a wider insight and understanding to the students in acquiring new knowledge with a much better understanding and interaction with their course mates and lecturers. Real-world and academic issues are facilitated in class by instructors and students are made to discover the responses for these issues outside the classrooms by themselves through interactive methods such as Flipped Learning.

Security at campuses

With the assistance of innovations like 3D positioning, students can be monitored twenty four hours a day and their locations can be detected at any point of time. Distress buttons can be supplied by these innovations for raising an alarm if in case the need arises in an emergency.

As there will be numerous students present in a class of any university, keeping track of the location and activities of each and every student is not a simple task for university administrations. Furthermore, the students in a university are more exposed to threats and need smart security compared to the population at any other communities. IoT can include tremendous value in regards to improving the security of schools, colleges, and institutions of higher learning.

For keeping track of student behaviour, smart electronic camera vision can be utilized in campuses. In the past decade, computer vision innovations have enhanced tremendously and can keep track of any motion or unwarranted movements. This activity can instantly stop any unforeseen occurrences from happening and this is vital for the safety of all students and staff of higher educational institutions.

Educational application at higher learning institutions

The educational applications leveraging IoT can be considered as effective imaginative tools and are changing the method which instructing, learning and facilitating is carried out. They make it possible for students and instructors to produce 3D graphics books which include videos and offer the ability to remember better.

These types of applications can be thought about as video game changers as they supply a great deal of instructional video games. These video games offer many functions that use fascinating possibilities in learning and teaching. This makes education more thrilling than ever to new generation of students who are digital natives who will only engage in exciting ways of gaining knowledge.

Efficiency in student management

In numerous colleges, a lot of time is invested on activities that do not include any worth to the core goal of their very presence. Presence of the students requires to be taken numerous times a day. With the aid of IoT end-devices, this information can be gathered and sent out to the main headquarters server, instantly removing the requirement for any human intervention. Due to this innovative shift towards the IoT, the tiresome job of students and instructors can be lessened. This permits them to focus more on learning and teaching which is the core function of any centre of knowledge.

Challenges of IoT Utilization

Although the benefits of the IoT are unlimited, it brings about increased security risks from all end-points and challenges to the network infrastructure along with it. Network administrators at educational institutions need to acclimatize conventional network designs to provide new platforms of automation, network intelligence and security. Simple and cost-effective network infrastructure that securely handles vast flows of data is needed by higher education institutions.

Malware.

Nevertheless, many higher education institutions do not realize to the need for IT security. (Wolff, 2015). Finding a balance between gaining academic freedom and internet security has been a never ending battle for many universities (Callahan, 2014). One of their most common security problems currently plaguing universities is malware and cyber-attacks are a growing problem which needs to be addressed immediately. It was estimated that security threats attributed to malware rockets to about thirty-six per cent of breaches in higher education (Smith, 2014). Educating users of the network on security best practices is one of the most powerful defensive steps a university can take. According to the 2018 Education Cyber Security Report, the education sector is the least secure

among 17 industries studied (Zimmerman, 2018). This problem is made more critical with university initiatives such as 'Bring Your Own Device' (BOYD).

One of the most serious security threats on the Internet is the malicious software or malware (Symantec Corporation, 2015; Kaspersky Labs, 2015; McAfee Labs, 2015).There are a few ways malware can be spread namely by social media, email, documents, removable media, programs, or by downloading sources from the Internet. Furthermore, viruses, worms, and Trojans are a few of the many forms of Malware that can be found. Cybercriminals are capable of hacking into campus' network to steal private and confidential information once malware has infected the network for example credit card information, social security numbers, student examination records or medical records.

In the past decade, many studies have linked malware infection to smartphones. A research conducted by the Chicago Better Business Bureau found that college students are the most at risk for malware infection because of their wide usage social media and smart phones (Jedra, 2013). Furthermore, a research carried out by Experian Simmons found that 98% of college students visited social media networking sites everyday (Griffin, 2015).Personal information such as birth date, place of birth, cell phone number, and home address are often requested on social networking profiles. The more personal information that students share over the internet, the more vulnerable the data is to be exploited and misused.

Security issues are becoming more complex as students, faculty, and staff are bringing their own devices and connecting to university networks. College and university campuses are being infiltrated by mobile devices such as notebooks, tablets, and smart phones. Moreover, colleges and universities have minimal control over the devices that users introduce to the network (Smith, 2014). Campus network can be easily infected by unprotected mobile devices which are susceptible to infection. According to a study by Verma (2011), top ten most common threats to smartphone security included malware, data loss, loss of the devices, insecure data transfer, and end user behaviour. BOYD technologies are great concerns with malware, intrusions, and data theft (Mahesh and Hooter, 2013). Many colleges and universities have to seriously rethink the structure of their computer networks due to the rising threat of hacking and malware.

Distributed Denial of Service.

'Distributed Denial of Service'(DDoS) is also one of the many challenges being faced by higher learning institutions which is rapidly increasing with the explosion of the internet usage especially by the younger generation (Akamai Technologies, 2016). A 'Denial-of-Service'(DoS) is a cyber-attack which occurs when an individual or a group of people disrupt a website which in turn denies access to clients; for instance services that rely on the affected computer or network like websites, email, and online accounts such as banking and online shopping (Goodin, 2018). A large-scale DoS attack where the perpetrator uses more than one unique IP address is known as a DdoS (Khalifeh, Soltanian & Reza, 2015). Besides enabling attackers to steal network data and metadata. the danger of DDoS is that makes university resources inaccessible to students and staff, thus making them handicapped in carrying out their daily work, research and development. A few universities who have fallen to the DDoS attacks are like the University of Virginia, Pennsylvania State University, University of Connecticut, Washington State University, Johns Hopkins University, University of Maryland, and the University of Southern California (Johnston, 2016). The Massachusetts Institute of Technology (MIT) was not spared of this internet catastrophe. In early 2016, 35 DDoS targeted attacks on the MIT. Later that year, many popular websites including Twitter, Amazon, PayPal, Comcast, Spotify and PlayStation Network were shut down due to a DDoS attack (Akamai Technologies, 2016).
Higher learning institutions will face a challenging and daunting task in securing the Internet of Things. With the threat of malware, network intrusions, BYOD technologies, and DDoS attack, the Internet is already under continuous attack caused by vulnerable systems. The IoT will inherit all the problems mentioned and also have its own concerns regarding security (Clarke et al., 2014). Since IoT is still at the infancy stage, it faces much vulnerability and cybercriminals are taking advantage of this situation. There are special search engines for IoT to look for devices which are connected. Shodan, which has been around for more than seven years was, the first IoT search engine and it links to IPv4 addresses (Snow, 2016). Censys is another IoT search engine created to make the internet more secure. Jimenez and Peris (2015) in Simmers and Anandarajan (2018) explained that both, Shodan and Censys have the ability to locate "things" based on physical location, hostname, operating system, IP address, and vulnerabilities. Although there are countless advantages with the internet being connected to a myriad of 'things', however, this exposes higher learning institutions to exploitations and attacks.

Data management.

Data storage, data retrieval, and data analysis are issues caused by the big data which is created by the IoT. As announced by Cisco Systems Global Cloud Index Report (2019), Big data will reach 403 EB by 2021, up almost 8-fold from 25 EB in 2016. Big data alone will represent 30 per cent of data stored in data centres by 2021, up from 18 per cent in 2016. The massive amount of data from sources around the world that will be generated by IoT will create issues concerning data storage. Universities would not have the capacity to back up zettabytes of raw data as it would be expensive and most campus networks will be overwhelmed with data processing loads.

Data Security and Privacy

The influx of large volumes of data produced by IoT may create privacy issues. Personal identifiable information can be generated by device sensors and RFID tags. Weber (2010) in Simmers and Anandarajan (2018) explained that students, faculty and staff would have no control over personal information embedded in object tags and without their knowledge; these information can be tracked by unauthorized personnel.

Decentralized Network Management.

Most higher learning institutions focus on ICT to augment student learning and not much emphasis is given to securing campus network environment. At colleges and universities, students, faculty and staff are given minimum security options and different schools have different degrees of needs and restrictions. Besides these, they also have different budgets, support staff and security requirements. This decentralized culture brings about silo mentality which is a 'reluctance to share information with employees of different departments in the same organization' (Gleeson & Rozo, 2013). This mentality can bring detrimental to organizations especially for educational departments for example the reduction of efficiency, morale and conducive learning environments. Furthermore, network securities across universities will face major challenges due to these silos as enforcing securities and procedures will cause difficulties to stakeholders.

Connectivity

.

One of the most significant challenges will be to connect as many devices as possible as it would counterattack existing structures and technologies associated with it. Currently, to authenticate, authorize and connect several terminals in a network, a centralized, server/client architecture is being utilized (Jindal, Jamar & Churi, 2018).

Suggestions to overcome challenges

Constructive measures must be taken to overcome obstacles and challenges if IoT is to become part of lives. As IoT applications generate extensive amounts of data, not everything is required to be stored on cloud as it might contain large amounts of unimportant data generated by devices. New methods of selecting storage of data on a cloud which will reduce the storage issue in the usage of devices where garbage data produced by IoT devices will be deleted selectively should be prioritized.

All the processes in IoT are managed by data in data centres. The reliability of the network which manages IoT applications should be enhanced. Reliable transmission of data, rapid delivery of sensor data, sending of details from sensors to a cloud all depend on high-speed Internet, thus it is utmost important to keep improving the speed and quality of the Internet (Marjani, Nasaruddin, Gani, Karim, Hashem, Siddiqa & Yaqoob, 2017).

Research and development on designing and developing IoT devices should place highest priority and utmost concern on security and privacy. Since technology has avenues to be abused, it is the responsibility of policy makers, manufacturers and all stake holders to foresee and address all future threats to IoT.

Conclusion

The digitization of education is a powerful vision as the IoT is making an impact by changing how Learning and Teaching is being implemented in Higher Education institutions. However utilization of the full potential of IoT applications with complete and effective security systems will require not only innovation in technologies but also huge investments by Education Ministries across the world.

The future of IoT is full of uncertainty. IoT is a revolution to change the lifestyles of humans with advancing technology. If the challenges are not addressed and reciprocated immediately, they could lead to unfavourable results which could affect every aspect of our lives and pose a threat to its own success. the responsibility of all

stakeholders of the Internet of Things to make the most out of the internet but at the same time be responsible for its safety and everything connected to it.

Recommendations

With the cooperation from all stakeholders and implementation of Education policies, Internet of Things can envisage to reach its fullest potential in this Digital Era. the responsibility of all stakeholders of the Internet of Things to make the most out of the internet but at the same time be responsible for its safety and everything connected to it.

References

Advanced MP Technology, *The Future of IoTs in Education.* Retrieved March 04, 2017 from http://www.advancedmp.com/the-future-of-iots-in-education/

Akamai Technologies Annual Report (2016). Retrieved 18, July, 2019, from http://www.ir.akamai.com/phoenix.zhtml?c=75943&p=irol-reportsannual

Aldowah, H., Rehman, S. U., Ghazal, S., & Umar, I. N. (2017). Internet of Things in higher education: a study on future learning. *Journal of Physics: Conference Series*, *892*(1), 012017, IOP Publishing. doi :10.1088/1742-6596/892/1/012017

Battons, C. (2018). How IoT Is Benefiting Education and Learning - DZoneIoT. Retrieved from https://dzone.com/articles/how-iot-is-changing-education-and-learning-positiv

Blewitt, J. (2010) Higher education for a sustainable world, *Education + Training*, Vol. 52 No. 6/7, pp. 477-488, Emerald Group Publishing Limited.

Botta, A.; De Donato, W.; Persico, V. & Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700.

Brandt, C. (2016) The Internet of Things and its impact on education, University Herald, Retrieved from http://www.universityherald.com/articles/41190/20160921/internet-of-things-and-education.htm

Callahan, M.E. (2014) "Cyber security and hospitals: What hospital trustees need to know about managing cyber security risk and response", American Hospital Association, USA.Retrievedfromhttps://www.researchgate.net/publication/283329102_the_information_confidentiality_and_cyber_security_in_medical_institutions

Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. (2018). Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

Clarke, J., Gritzalis, S., Zhou, J., & Roman, R. (2014). Security in a completely interconnected world. *Security and Communication Networks*, *7*(12), 2726-2727. Doi: 10.1002/sec.1175

Cyber Infrastructure Understanding Denial-of-Service Attacks. Retrieved 20 Julai 2019 from https://www.us-cert.gov/ncas/tips/ST04-015

Evans, D. (2011). The internet of things. How the next evolution of the internet is changing everything. Cisco IBSG, 2011.

Evans, D. (2011). The Internet of Things: How the next evolution of the internet is changing everything. *Cisco white paper*, *1*(2011), 1-11.

Gabai, A. (2015). Retrieved from https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/#pbYoum89VFRbtGlC.99

Gleeson, B., & Rozo, M. (2013). The silo mentality: How to break down the barriers. Retrieved 30 July 2019, from https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(1), 41-44.

Goodin, D (2018). US service provider survives the biggest recorded DDoS in history. *Ars Technica*. Retrieved 20 July 2019.

Griffin, R. (2015). Social Media Is Changing How College Students Deal With Mental Health, For Better Or Worse. *College Huffpost*, 1-4. Retrieved from https://www.huffpost.com/entry/social-media-college-mental-health_n_55ae6649e4b08f57d5d28845

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645-1660

IoT Analytics (2018). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating* .Retrieved from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Jedra, C. (2013). Study: Millennials indifferent to online risks. *USAToday*. Retrieved from https://www.usatoday.com/story/news/nation/2013/10/16/millennials-cyber-security/2995157/

Jin, D., (2012). Application of" Internet of Things" in electronic commerce. *International Journal of Digital Content Technology & its Applications,6*(8).

Jindal, F., Jamar, R., & Churi, P. (2018). Future And Challenges Of Internet of Things. *International Journal of Computer Science & Information Technology (IJCSIT) 10*(2), 13-25

Johnson, L., Adams Becker, S., Estrada, V. & Freeman, A. (2015). NMC Horizon Report: Library Edition. Austin, Texas: The New Media Consortium. Retrieved July 5, 2019 from https://www.learntechlib.org/p/151822/.

Kahlert, M., (2016). Understanding customer acceptance of Internet of Things services in retailing: an empirical study about the moderating effect of degree of technological autonomy and shopping motivations. University of Twente.

Kaspersky Lab. (2015). *The Volume of New Mobile Malware Tripled in 2015*. Retrieved from https://www.kaspersky.com/about/press-releases/2016_the-volume-of-new-mobile-malware-tripled-in-2015

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*,17(2), 243-259.

Lutz, R. (2014), The implications of the Internet of Things for education. Available at http://www.systech.com/systech-blog/384-theimplications-of-the-internet-of-things-for-education

Lyons, J. P., Hannon, J., & Macken, C. (2014). Sustainable practice in embedding learning technologies: Curriculum renewal through course design intensives. In *Curriculum Models for the 21st Century* (pp. 423-442). Springer, New York, NY.

Ma, L., Zhou, Y., Liu, S., Qiao, J., Han, Z., & Wang, J. (2014). Development and Research of Digital Campus System Based on Android. *International Journal of Smart Home*, *8*(4), 25-36.

Mahesh, S. & Hooter, A., 2013. Managing and Securing Business Networks in the Smartphone Era. In Fifth Annual General Business Conference, Sam Houston State University, Huntsville, Texas. Texas: Management Faculty Publications.

Maksimović, M. (2017) Green Internet of Things (G-IoT) at engineering education institution: the classroom of tomorrow, *INFOTEH-Jahorina*, *16*, 270-273.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I.(2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. IEEE Access, 5, 5247-5261

McAfee Labs. (2015). *McAfee Labs Threats Report: May 2015*. Retrieved from https://www.mcafee.com/br/security-awareness/articles/mcafee-labs-threats-report-aug-2015.aspx

Morphus, N. (2016) What you need to know about the internet of things for education, capterra school administration blog, Retrieved July 16, 2017 from http://blog.capterra.com/what-you-need-to-know-about-theinternet-of-things-for-education/

National Research Council (2000) How people learn: Brain, mind, experience, and school: Expanded Edition, Chapter: 9 Technology to Support Learning, Retrieved June 23, 2017 from https://www.nap.edu/read/ 9853/chapter/13

O'Connor, M. (2010). Northern Arizona University to Use Existing RFID Student Cards for Attendance Tracking. *RFID Journal*, 1. Retrieved 9 July 2019 from https://www.rfidjournal.com/articles/view?7628

Peña-López, I., (2005). Itu Internet Report 2005: The Internet of Things. *Geneva: ITU*.

Ralhan, B. D. (2017). How IoT is transforming the education sector, *Inc42*, Retrieved August 1, 2017 from https://inc42.com/resources/io-transforming-education/

Selinger, M., Sepulveda, A., & Buchan, J. (2013). Education and the Internet of Everything: How ubiquitous connectedness can help transform pedagogy. *White Paper, Cisco, San Jose, CA*.

Simmers, C., & Anandarajan, M. (2018). *The internet of people, things and services*. New York, NY: Routledge.

Smith, F. (2014). EDUCAUSE 2014: Cyberattacks Are a Growing Problem for Higher Education. Edtech,1.Retrievedfromhttps://edtechmagazine.com/higher/article/2014/10/educause-2014-cyberattacks-are-growing-problem-higher-education

Snow, J. (2016). Shodan and Censys: The ominous guides through the Internet of Things [Blog]. Retrieved from https://www.kaspersky.com/blog/shodan-censys/11430/

Stankovic, J.A., *Research directions for the internet of things.* IEEE Internet of Things Journal, 2014. **1**(1): p. 3-9.

Stošić, L. (2015). The importance of educational technology in teaching, *(IJCRSEE) International Journal of Cognitive Research in Science, Engineering and Education*. *3*(1).

Symantec Corporation World Headquarters. (2015). *Symantec Intelligence Report* (pp. 1-19). California.https://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015.en-us.pdf

Tan, P., Wu, H., Li, P., & Xu, H. (2018). Teaching management system with applications of RFID and IoT technology. *Education Sciences*, *8*(1), 26.

Thirty five percent of all security breaches take place in higher education. (2014). *SecurityMagazine*,1.Retrievedfromhttps://www.securitymagazine.com/articles/86000-percent-of-all-security-breaches-take-place-in-higher-education.

Verma, A., M. Rao, A. Gupta, W. Jeberson and V. Singh, 2013. A literature review on malware and its analysis. Int. J. Current Res. Rev., 5: 71-71.

Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: Converging technologies for smart environments and integrated ecosystems*. River publishers.

Vermesan, O., Friess, P. and Guillemin, P. (2011). Internet of things strategic research roadmap. *Internet of Things: Global Technological and Societal Trends*,1, 9–52.

Vujovic, V., & Maksimovic, M. (2015). The Impact of the Internet of Things on Engineering Education. The 2nd International Conference on Open and Flexible Education (ICOFE), Hong Kong, 135-144.

Wals, A.E.J. and Jickling, B. (2002). Sustainability in higher education: from double think and newspeak to critical thinking and meaningful learning, *International Journal of Sustainability in Higher Education*, 3(3), 221-32.

Wolff, J. (2015). *Cyber security as metaphor: Policy and defence implications of computer security metaphors.* (March 31, 2014). *In TPRC Conference Paper*. *Retrieved from http://dx.doi.org/10.2139/ssrn.2418638*

Zimmerman, E. (2018). 3 Cybersecurity Focus Areas for Education Institutions in 2019. *Edtech*, 1. Retrieved from https://edtechmagazine.com/higher/article/2018/12/3-cybersecurity-focus-areas-education-institutions-2019

Author Information

Arumugam Raman
Universiti Utara Malaysia
Sintok, Kedah, Malaysia
Contact e-mail: *arumugam@uum.edu.my*

Raamani Thannimalai
Ministry of Education
Malaysia
Contact e-mail :drraamani@gmail.com